

L'adaptation des systèmes juridiques aux innovations technologiques : analyse comparée et étude du cas marocain

The Adaptation of Legal Systems to Technological Innovations : Comparative Perspectives
and the Moroccan Case

BOUCHRA KAMAR

Docteur en droit privé

bouchra.kamar006@gmail.com

DOI: <https://doi.org/10.65040/remeye.2026.11.v02n30.43>



This work is licensed under a Creative Commons Attribution 4.0 International License

<https://creativecommons.org/licenses/by/4.0/>

Résumé:

Les transformations numériques ont un impact considérable sur l'évolution des systèmes juridiques d'aujourd'hui, en modifiant en profondeur la manière dont le droit est produit, appliqué et régulé. La dématérialisation des procédures, l'essor de l'économie des données, le développement des plateformes numériques et l'automatisation croissante des décisions remettent en question les catégories juridiques traditionnelles ainsi que des principes fondamentaux comme la sécurité juridique, la responsabilité et la protection des droits et libertés. Face à ces changements, les systèmes juridiques doivent adapter leurs outils normatifs.

À l'échelle internationale, les réponses juridiques se distinguent par des approches progressives, souvent sectorielles, qui se basent sur la gestion des risques et cherchent à trouver un équilibre entre l'innovation technologique et les garanties juridiques. Ces évolutions montrent à quel point il est difficile de réguler des phénomènes techniques en constante évolution avec des cadres juridiques stables. Dans ce contexte, le droit marocain est un exemple intéressant d'adaptation progressive. Depuis le début des années 2000, le Maroc a mis en place plusieurs textes régissant les échanges électroniques, la protection des données personnelles, la cybersécurité et la digitalisation de l'action publique. Cependant, cette évolution est encore marquée par une fragmentation des normes et l'absence d'un cadre global capable d'anticiper les défis technologiques les plus récents, ce qui nécessite une refonte plus cohérente et évolutive de la régulation juridique du numérique.

Mots-clés : transformation numérique – adaptation du droit – droit comparé – gouvernance numérique – droit marocain.

Abstract:

Digital transformation has become a major driver in the evolution of contemporary legal systems, profoundly reshaping the ways in which law is produced, implemented, and regulated. The dematerialization of procedures, the expansion of the data economy, the rise of digital platforms, and the increasing automation of decision-making processes have

challenged traditional legal categories and tested core principles such as legal certainty, liability, and the protection of rights and freedoms.

In response to these developments, legal systems have been compelled to adapt their regulatory frameworks. At the international level, legal responses are characterized by progressive and often sector-specific approaches, grounded in risk management and aimed at balancing technological innovation with legal safeguards. These trends reflect the difficulty of regulating rapidly evolving technologies through rigid and static legal instruments.

Within this comparative perspective, Moroccan law offers a relevant case study of gradual legal adaptation. Since the early 2000s, Morocco has enacted several legislative measures governing electronic transactions, personal data protection, cybersecurity, and the digitalization of public action. However, this evolution remains marked by normative fragmentation and the absence of a comprehensive transversal framework capable of anticipating recent technological challenges. This situation highlights the need for a more coherent and adaptive legal approach to digital governance.

Keywords: digital transformation – legal adaptation – comparative law – digital governance – Moroccan law.

INTRODUCTION

Il est difficile d'ignorer aujourd'hui l'impact des innovations technologiques sur nos sociétés. Le développement rapide du numérique, l'essor de l'intelligence artificielle, la multiplication des échanges électroniques ou encore l'expansion des réseaux d'information ont profondément modifié notre manière de production, de communication et même de gouvernance⁽¹⁾.

Mais ces changements ne se limite pas à l'évolution des outils techniques. Ils reflètent une transformation beaucoup plus profonde qui se traduit par une évolution des structures économiques et sociales, marquée par la dématérialisation, l'accélération des échanges et une automatisation croissante des décisions.

Dans ce contexte, le droit, considéré comme un outil essentiel de régulation sociale, fait face à des défis sans précédent. Historiquement, les systèmes juridiques ont été élaborés pour gérer des situations relativement stables, enraciné dans un territoire et nécessitant une intervention humaine directe⁽²⁾.

La norme juridique s'inscrit dans une logique de prévisibilité et de hiérarchie, visant à assurer la sécurité juridique et la stabilité des relations sociales. Cependant, les technologies numériques apportent des dynamiques nouvelles, notamment la déterritorialisation des activités, l'immédiateté des échanges et l'autonomie croissante des systèmes techniques.

Ces changements créent un décalage structurel entre le rythme du droit et celui de l'innovation technologique. Alors que la création de normes juridiques repose sur des processus lents et réfléchis, les technologies évoluent à un rythme démesuré, avec une

⁽¹⁾ OCDE, Digital Transformation in the Age of Artificial Intelligence, Paris, 2019.

⁽²⁾ J. Carbonnier, Flexible droit. Pour une sociologie du droit sans rigueur, Paris, LGDJ, 10^e éd., 2001.

innovation constante⁽¹⁾. Ce décalage fragilise la capacité du droit à s'adapter efficacement aux nouvelles situations juridiques et soulève des questions cruciales sur la préservation de la sécurité juridique et la protection des droits fondamentaux.

Par ailleurs, le numérique ne modifie pas seulement le rythme du droit, il en remet aussi en cause les fondements. Par exemple, la dématérialisation change la manière dont se forment les actes juridiques (consentement, preuve, identification). De même, l'usage croissant des algorithmes remet en cause le rôle du juge et la place du raisonnement humain. Enfin, l'exploitation massive des données personnelles pose des enjeux majeurs en matière de vie privée⁽²⁾.

Ainsi, l'adaptation du droit aux innovations technologiques ne consiste pas simplement à moderniser des textes. Il s'agit d'une réflexion plus profonde sur la capacité du système juridique à évoluer sans perdre ses fonctions essentielles tel que la garantie de l'État de droit, la protection des droits fondamentaux et la sécurité des relations juridiques.

Dans le contexte marocain, cette question prend une dimension particulière. Face à l'essor du numérique, le Maroc a entrepris un processus d'adaptation de son cadre juridique, en adoptant des lois comme la loi n° 53-05 sur l'échange électronique de données juridiques, la loi n° 09-08 sur la protection des données personnelles, et la loi n° 05-20 sur la cybersécurité⁽³⁾.

Ces réformes montrent une volonté d'aligner le système juridique national sur les normes internationales de régulation du numérique, tout en tenant compte des spécificités économiques et institutionnelles du pays. Cependant, malgré ces progrès, le cadre juridique du numérique fait face à des défis importants, notamment la rapidité des évolutions technologiques, la complexité des enjeux qu'elles engendrent, et la nécessité d'assurer une cohérence entre les différents instruments normatifs. Ainsi, la question centrale se pose : dans quelle mesure les systèmes juridiques peuvent-ils s'adapter aux innovations technologiques sans compromettre la sécurité juridique et la protection des droits fondamentaux ? Dans cette optique, cette étude se propose d'analyser, dans un premier temps, les impacts de la transformation numérique sur les bases traditionnelles du droit, puis, dans un second temps, d'examiner les mécanismes d'adaptation mis en place par les systèmes juridiques, tant au niveau international que national, en mettant un accent particulier sur le droit marocain.

⁽¹⁾ M. Delmas-Marty, Les forces imaginantes du droit, Paris, Seuil, 2004, p. 58.

⁽²⁾ Conseil de l'Europe, Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires, 2018.

⁽³⁾ Loi n° 53-05 relative à l'échange électronique de données juridiques, promulguée par le Dahir n° 1-07-129 du 30 novembre 2007, Bulletin officiel n° 5584 du 6 décembre 2007 ;

- Loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, promulguée par le Dahir n° 1-09-15 du 18 février 2009, Bulletin officiel n° 5711 du 5 mars 2009 ;

- Loi n° 05-20 relative à la cybersécurité, Bulletin officiel du Royaume du Maroc, 2020.

PREMIÈRE PARTIE : La transformation numérique comme facteur de remise en cause des fondements traditionnels du droit.

La transformation numérique impacte profondément l'ensemble des disciplines juridiques. En effet elle ne se limite pas à l'intégration des outils techniques dans les pratiques juridiques déjà en place, mais cela s'inscrit dans un mouvement plus large qui redéfinit les catégories juridiques traditionnelles et les modes de régulation du droit. En changeant la manière dont les actes juridiques sont formés, les processus de décision et les relations entre les individus, les technologies numériques contribuent donc à redéfinir les fondements mêmes du droit contemporain.

Cette évolution se produit à deux niveaux. D'une part, elle modifie les relations juridiques en introduisant de nouvelles formes d'interaction, souvent marquées par la dématérialisation et l'automatisation. D'autre part, elle engendre des risques juridiques inédits qui pourraient affaiblir les protections traditionnelles que le droit offre, notamment en ce qui concerne la protection des droits fondamentaux et la sécurité juridique.

Dans cette optique, il est essentiel d'examiner d'abord comment la transformation numérique modifie les relations juridiques, avant de se pencher sur les risques juridiques qui en résulte.

Section I – Le mutation des rapports juridiques sous l'effet de la transformation numérique

1. La dématérialisation des échanges et la réorganisation des relations juridiques

La dématérialisation des échanges est sans doute l'une des évolutions les plus marquantes de la transformation numérique du droit. Cela se traduit par un changement radical dans la façon de communiquer sur le plan juridique, marqué par un passage progressif des supports physiques vers des outils électroniques qui permettent des interactions à distance, instantanées et déterritorialisées⁽¹⁾. Les relations juridiques, qui reposaient autrefois sur la présence physique des parties et l'utilisation de documents papier, sont désormais largement médiatisées par des technologies numériques et des plateformes en ligne. Cependant, il est important de ne pas voir cette évolution simplement comme une mise à jour technique. Elle représente une transformation plus profonde du lien juridique lui-même. Comme l'a relevé la doctrine, les technologies numériques contribuent à modifier la « physionomie du rapport juridique », remplaçant les interactions directes par des échanges dématérialisés, souvent standardisés et médiatisés par des systèmes techniques⁽²⁾. Cette évolution impacte directement la manière dont la volonté juridique s'exprime, car le consentement se manifeste désormais à travers des interfaces numériques, comme des plateformes ou des applications, ce qui peut parfois restreindre la capacité réelle de négociation des parties⁽³⁾.

⁽¹⁾ L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, 2006.

⁽²⁾ S. Gueldi, *La réglementation des avancées technologiques au Maroc*, Rabat, 2024.

⁽³⁾ P. Malaurie, L. Aynès, P. Stoffel-Munck, *Les obligations*, LGDJ, 2020.

Cette recomposition se manifeste de manière plus évidente en matière contractuelle, le développement massif des contrats électroniques fréquemment conclus sous forme d'adhésion ; tend à accentuer le déséquilibre entre les contractants. En effet La liberté contractuelle qui représente le principe fondamental, du droit des obligations demeure intacte en théorie, mais son exercice en pratique encadré par des conditions générale préétablie et imposées souvent difficilement modifiables par l'utilisateur⁽¹⁾. Cette situation pose des questions sur la vraie liberté du consentement, en particulier dans un environnement où l'asymétrie d'information est accentuée.

Par ailleurs, la dématérialisation entraîne une transformation majeure du régime de la preuve. Le rôle traditionnel du document papier est peu à peu remplacé par des mécanismes qui s'appuient sur la fiabilité technique et la traçabilité numérique, comme la signature électronique, l'horodatage et les systèmes d'archivage électronique. Le droit doit donc s'adapter en reconnaissant ces nouvelles formes de preuve, tout en définissant leur admissibilité et leur force probante pour assurer la sécurité juridique⁽²⁾.

Dans le contexte marocain, cette transformation a été officialisée par la loi n° 53-05. Promulguée par le Dahir n° 1-07-129 le 30 novembre 2007, cette loi concerne l'échange électronique de données juridiques et reconnaît clairement la validité des écrits et signatures électroniques. Elle représente un pilier fondamental pour sécuriser les transactions numériques et marque une avancée significative dans l'adaptation du droit national aux exigences de la digitalisation⁽³⁾.

Cependant, la dématérialisation des échanges soulève également des questions cruciales concernant la protection des droits fondamentaux. Elle implique la collecte, le traitement et la conservation d'un volume plus important de données personnelles, ce qui expose les individus à des risques accrus pour leur vie privée. La Cour européenne des droits de l'homme a constamment affirmé que la protection des données personnelles est un aspect essentiel du droit au respect de la vie privée, tel que garanti par l'article 8 de la Convention européenne des droits de l'homme⁽⁴⁾. Par conséquent, le cadre juridique entourant la dématérialisation doit respecter les principes de légalité, de finalité et de proportionnalité, afin de garantir un équilibre entre l'efficacité technologique et la protection des libertés.

2. L'automatisation des processus décisionnels et la remise en cause du modèle juridique classique

⁽¹⁾ S. Martin, « La justice numérique : opportunités et limites », Revue française d'administration publique, n° 177, 2021.

⁽²⁾ R. Susskind, Online Courts and the Future of Justice, Oxford University Press, 2019.

⁽³⁾ Loi n° 53-05 relative à l'échange électronique de données juridiques, promulguée par le Dahir n° 1-07-129 du 30 novembre 2007, Bulletin officiel n° 5584 du 6 décembre 2007.

⁽⁴⁾ CEDH, Rotaru c. Roumanie, 4 mai 2000, § 43 ; CEDH, S. et Marper c. Royaume-Uni, 4 décembre 2008.

Au-delà de la simple dématérialisation des échanges, la transformation numérique se distingue par une automatisation de plus en plus marquée des processus décisionnels. Le développement des systèmes algorithmiques et des technologies d'intelligence artificielle permet désormais de traiter des volumes considérables de données et d'intervenir, directement ou indirectement, dans des décisions ayant des effets juridiques significatifs, notamment dans les domaines administratif, financier ou judiciaire. Cette évolution représente une véritable rupture avec le modèle traditionnel du droit, qui reposait historiquement sur l'intervention humaine et un raisonnement juridique explicite.

L'automatisation introduit une forme de décision technique, fondée sur des logiques statistiques et probabilistes, dont le fonctionnement est souvent difficile à saisir pour les personnes concernées. Ainsi, la décision juridique se transforme en un processus algorithmique, où la norme est appliquée à travers des calculs et des corrélations, plutôt que par une interprétation raisonnée.

L'un des enjeux majeurs de cette évolution réside dans la transparence des décisions automatisées. Les systèmes algorithmiques sont souvent caractérisés par une opacité structurelle, due à la complexité de leurs modèles internes ou à la nature propriétaire des technologies utilisées. Cette situation rend difficile l'identification des critères ayant conduit à une décision donnée, ce qui nuit à la possibilité d'un contrôle juridictionnel efficace. Pourtant, la jurisprudence européenne souligne que le droit à un recours effectif est un principe fondamental de l'État de droit, impliquant la capacité de comprendre et de contester les décisions qui impactent les individus⁽¹⁾.

D'autre part, l'automatisation soulève des risques majeurs en matière d'égalité et de non-discrimination. Les systèmes algorithmiques, qui s'appuient sur des données historiques, peuvent non seulement reproduire voire amplifier des biais déjà existants, conduisant à des traitements différenciés injustifiés entre les individus. Ces formes de discrimination, souvent invisibles, sont d'autant plus inquiétantes qu'elles sont difficiles à contester.

Dans ce contexte, certains chercheurs ont mis en évidence les risques d'une évolution vers une « gouvernance par les nombres », où les décisions seraient principalement basées sur des données statistiques et des corrélations, au détriment des normes juridiques générales et abstraites⁽²⁾.

Une telle évolution pourrait conduire à un affaiblissement de la fonction du droit et à une marginalisation du rôle du juge, pourtant garant de l'individualisation des décisions et du respect des droits fondamentaux.

Ainsi, l'automatisation des processus décisionnels soulève des questions cruciales sur la capacité du droit à réguler des systèmes techniques complexes tout en préservant les principes fondamentaux de l'État de droit. Cela nécessite la création de mécanismes juridiques adaptés pour assurer la transparence, la responsabilité et le contrôle des décisions automatisées.

⁽¹⁾ CEDH, Sunday Times c. Royaume-Uni (n°1), 26 avril 1979.

⁽²⁾ A. Supiot, La gouvernance par les nombres, Fayard, 2015.

Section II : Les nouveaux risques juridiques et la fragilisation des garanties fondamentales

La transformation numérique ne se limite pas simplement à changer la manière dont le droit s'exprime ou à modifier les interactions entre les acteurs juridiques. Elle apporte aussi des nouveaux risques qui pourraient menacer les garanties fondamentales sur lesquelles repose l'État de droit. En effet, avec l'essor des technologies numériques, qui reposent sur l'utilisation massive de données et l'automatisation des décisions, de nouvelles atteintes aux droits fondamentaux émergent, tout en affaiblissant les mécanismes traditionnels de responsabilité et de sécurité juridique. Cette évolution nous pousse donc à réfléchir en profondeur sur la capacité du droit à maintenir ses fonctions protectrices dans un environnement technologique en perpétuelle évolution.

1. Les atteintes potentielles aux droits fondamentaux à l'ère numérique

La transformation numérique engendre des risques juridiques d'une nature et d'une intensité importante, surtout en ce qui concerne la protection des droits fondamentaux. Le développement des technologies de traitement des données, associé à la généralisation des dispositifs de surveillance et à l'utilisation croissante du profilage algorithmique, conduit à une redéfinition significative des conditions d'exercice des libertés individuelles. En effet la protection de la vie privée se révèle particulièrement vulnérable. L'exploitation massive des données personnelles permet aujourd'hui de reconstituer de manière précise et détaillée les comportements individuels, souvent à l'insu des personnes concernées. Les traces numériques que chacun laisse dans ses activités quotidiennes alimentent des bases de données qui peuvent être utilisées à des fins commerciales, sécuritaires ou administratives. Comme l'a souligné Stefano Rodotà, la vie privée ne peut plus être considérée simplement comme un droit à l'isolement ; elle est désormais un élément fondamental de l'autonomie et de la liberté individuelle dans nos sociétés numériques⁽¹⁾.

Dans ce cadre, la Cour européenne des droits de l'homme a affirmé que les États doivent établir des mécanismes juridiques efficaces pour protéger les individus contre les atteintes liées à l'utilisation des technologies numériques. Cette obligation exige non seulement l'adoption de normes juridiques appropriées, mais aussi la mise en place de dispositifs de contrôle et de recours efficaces permettant aux individus de contester les atteintes subies⁽²⁾. La protection des droits fondamentaux nécessite donc une approche globale, combinant prévention, encadrement et contrôle juridictionnel.

Au-delà de la vie privée, le numérique soulève également des enjeux majeurs en matière d'égalité et de non-discrimination. Les systèmes de profilage algorithmique, qui reposent sur l'analyse de données massives, peuvent entraîner des traitements différenciés basés sur des critères implicites ou indirects. Ces mécanismes ont le potentiel de reproduire, voire d'amplifier, des biais sociaux déjà présents, menant à des discriminations difficilement détectable et encore plus difficilement contestable. Cette situation met à l'épreuve les

⁽¹⁾ S. Rodotà, La vie et les règles. Entre le droit et le non-droit, Fayard, 2010, p. 116-118.

⁽²⁾ CEDH, S. et Marper c. Royaume-Uni, 4 décembre 2008, §§ 67-69.

principes fondamentaux d'égalité devant la loi et de non-discrimination, qui sont des piliers essentiels de notre système juridique.

Par ailleurs, le développement des technologies de surveillance numérique, qu'elles soient publiques ou privées, remet en question l'équilibre entre sécurité et liberté. La généralisation des dispositifs de contrôle, notamment à travers l'analyse de données ou la reconnaissance biométrique, peut conduire à une normalisation des atteintes aux libertés individuelles. Cette évolution nécessite une vigilance particulière pour éviter un glissement vers des formes de surveillance généralisée qui seraient incompatibles avec les exigences d'un État de droit.

Ainsi, les technologies numériques imposent une redéfinition des mécanismes traditionnels de protection des droits fondamentaux, afin de garantir un équilibre durable entre l'efficacité technologique et le respect des libertés individuelles.

2. La crise de la responsabilité juridique et la sécurité juridique

La transformation numérique met en lumière une remise en question profonde des modèles traditionnels de responsabilité juridique. Les systèmes technologiques d'aujourd'hui reposent sur des architectures complexes, impliquant de nombreux acteurs, comme les concepteurs d'algorithmes, les fournisseurs de données, les exploitants de plateformes et les utilisateurs finaux. Cette diversité d'intervenants rend particulièrement difficile l'identification de la personne responsable en cas de dommage.

Dans ce contexte, les mécanismes classiques de responsabilité civile, qui se basent sur l'imputation individuelle de la faute, semblent partiellement inadaptés car la chaîne causale est fragmentée, et établir le lien entre un comportement fautif et le dommage devient incertain ; ce qui engendre un risque d'irresponsabilité, dans lequel aucun acteur ne peut être clairement tenu pour responsable, au détriment des victimes.

Cette évolution engendre une insécurité juridique croissante ; en fragilisant la prévisibilité et la stabilité des règles de droit, principes essentiels de l'État de droit. La complexité de ces innovations et leur évolution accélérée rendent difficile l'anticipation des situations juridiques ainsi que la détermination des responsabilités. Cette incertitude, en compromettant la garantie des droits fondamentaux contribue à affaiblir la confiance des individus dans le système juridique et souligne la nécessité d'une adaptation constante du droit afin de préserver l'efficacité de la protection juridique.

Comme l'a souligné Mireille Delmas-Marty, le droit doit « inventer de nouvelles formes de responsabilité » qui puissent intégrer l'incertitude et la complexité des sociétés technologiques ⁽¹⁾.

Cette perspective nous pousse à repenser les catégories juridiques traditionnelles et à envisager des mécanismes de responsabilité plus adaptés, tels que la responsabilité objective, la responsabilité partagée ou encore des régimes spécifiques pour les systèmes d'intelligence artificielle.

⁽¹⁾ M. Delmas-Marty, Les forces imaginantes du droit, Paris, Seuil, 2004, p. 58.

En plus de la question de la responsabilité, la transformation numérique a également un impact sur la qualité même de la norme juridique. L'adaptation continue du droit aux avancées technologiques peut entraîner une multiplication de textes et une certaine instabilité normative, ce qui nuit à la clarté et à la cohérence du droit.

Ainsi, cette transformation numérique met à l'épreuve les principes fondamentaux du droit, en remettant en question les mécanismes traditionnels de responsabilité et les garanties de sécurité juridique. Cette situation appelle à une analyse, dans la seconde partie, des mécanismes d'adaptation que les systèmes juridiques ont développés pour faire face à ces défis.

Deuxième partie: L'adaptation des systèmes juridiques aux transformations numériques : approches comparées et cas du Maroc

Après avoir mis en lumière dans la première partie les profondes mutations causés par la transformation numérique et les tensions qu'ils créent par rapport aux fondements traditionnels du droit. Il convient d'examiner les réponses apportées par les systèmes juridiques afin de faire face à ces évolutions technologiques qui se distinguent par leur complexité, leur rapidité d'innovation et leur portée transnationale, le droit ne peut se contenter d'une simple adaptation ponctuelle ou fragmentaire. Il doit repenser ses méthodes d'intervention, ses sources normatives et ses mécanismes d'application. Cette adaptation se déroule dans un contexte où les acteurs normatifs se multiplient, les instruments juridiques se diversifient et de nouvelles formes de régulation émergent, notamment à travers des autorités administratives indépendantes et des instruments de soft law⁽¹⁾.

Dans cette perspective, les systèmes juridiques modernes oscillent entre deux exigences essentielles. D'une part, ils doivent garantir la stabilité et la prévisibilité du droit, qui sont des conditions indispensables pour assurer la sécurité juridique et la confiance des acteurs. D'autre part, ils doivent faire preuve de flexibilité pour s'adapter à des innovations technologiques en perpétuelle évolution⁽²⁾. Cette tension entre stabilité et adaptation est l'un des défis majeurs de la régulation du numérique.

À l'échelle internationale, cette problématique a conduit à l'émergence de divers modèles de régulation, reflétant des choix politiques, économiques et juridiques différenciés. L'Union européenne privilège une approche axée sur la protection des droits fondamentaux et la prévention des risques ; les États-Unis, quant à eux, adoptent une logique libérale qui privilégie le marché et l'innovation ; tandis que la Chine opte pour un modèle de régulation centralisée, fondé sur le contrôle étatique et la souveraineté numérique. En parallèle, des pays émergents comme le Maroc doivent développer leur propre modèle d'adaptation, en prenant en compte à la fois les normes internationales et leurs spécificités nationales. Cette dynamique

⁽¹⁾ « Le droit souple est constitué d'instruments qui visent à orienter les comportements sans créer par eux-mêmes de droits ou d'obligations juridiquement contraignants. »

– Conseil d'État, Rapport public 2013, Le droit souple.

⁽²⁾ Charte des droits fondamentaux de l'Union européenne, JOUE C 326, 26 octobre 2012.

soulève des questions sur la cohérence, l'efficacité et la durabilité des solutions juridiques mises en place. C'est pourquoi il convient d'analyser dans une première section les principaux modèles internationaux d'adaptation du droit aux technologies numériques, avant de se pencher dans une seconde section sur la manière dont le système juridique marocain s'adapte à ces transformations.

Section I : Les modèles internationaux d'adaptation juridique au numérique

À l'ère numérique La mondialisation des technologies numériques a considérablement remis en cause les cadres juridiques traditionnels, fondés sur la territorialité et la souveraineté de l'État. Le flux transfrontalier de données, l'influence croissante des grandes plateformes numériques et le développement rapide de l'intelligence artificielle soulignent tous l'urgence de réponses juridiques adaptées à ces nouvelles réalités. Dans ce contexte, trois principaux modèles réglementaires se démarquent, chacun reflétant des points de vue différents sur le rôle du droit : le modèle européen, fondé sur les droits fondamentaux ; le modèle américain, qui se concentre sur le marché ; et le modèle chinois qui met l'accent sur la primauté de l'État.

1. Le modèle européen : une réglementation fondée sur les droits fondamentaux

Le modèle européen de régulation numérique repose sur une conception particulièrement exigeante du rôle du droit, dans laquelle la protection des droits fondamentaux constitue le principe directeur à l'intervention normative. Contrairement aux approches purement économiques ou techniques, l'Union européenne considère les technologies numériques comme des phénomènes pouvant impacter l'équilibre des sociétés démocratiques et, en tant que telles, doivent être régies par des mécanismes juridiques garantissant le respect de la dignité humaine et des libertés individuelles. Cette approche trouve son fondement dans la Charte des droits fondamentaux de l'Union européenne, qui consacre le droit au respect de la vie privée suivant l'article 7⁽¹⁾, le droit à la protection des données personnelles (article 8)⁽²⁾ et le droit à un recours effectif (article 47)⁽¹⁾.

⁽¹⁾Article 7–Respect de la vie privée et familiale

Charte des droits fondamentaux de l'Union européenne, article 7, Journal officiel de l'Union européenne (JOUE), C 326, 26 octobre 2012, p.391.

L'article 7 de la Charte consacre le droit de toute personne au respect de sa vie privée et familiale, de son domicile ainsi que de ses communications. Publié au Journal officiel de l'Union européenne le 26 octobre 2012, il s'inscrit dans le prolongement de l'article 8 de la Convention européenne des droits de l'homme et constitue un socle fondamental de la protection de la sphère personnelle dans l'ordre juridique de l'Union.

⁽²⁾ Article 8 – Protection des données à caractère personnel

Charte des droits fondamentaux de l'Union européenne, article 8, JOUE, C 326, 26 octobre 2012, p. 391.

La reconnaissance de la protection des données comme un droit autonome souligne l'importance accordée au contrôle de l'information dans les sociétés numériques d'aujourd'hui. Le droit du numérique s'inscrit dès lors dans une logique axiologique, dans laquelle les innovations technologiques doivent être subordonnées au respect des valeurs fondamentales de l'ordre juridique européen.

Le Règlement (UE) 2016/679 du 27 avril 2016 connu sous le nom de Règlement général sur la protection des données (RGPD)⁽²⁾, constitue un cadre juridique bien défini, imposant aux responsables de traitement des obligations claires en matière de licéité, de transparence, de sécurité et de limitation des finalités. En plus, le RGPD renforce les droits des personnes concernées, comme le droit d'accès, de rectification, d'effacement et d'opposition, ce qui aide à rétablir un équilibre entre les individus et les acteurs économiques.

L'un des grands apports du RGPD est l'introduction du principe d'« accountability », qui oblige les acteurs à prendre une responsabilité proactive pour se conformer à leurs pratiques. Cela marque un tournant vers un modèle de régulation préventif, où les opérateurs doivent intégrer les exigences juridiques dès la conception de leurs systèmes de traitement, avec les concepts de « privacy by design » et « privacy by default ». Le droit ne se contente plus de punir les infractions, il cherche à prévenir les risques dès le départ. Cette approche préventive a été renforcée par l'adoption du Règlement (UE) 2024/1689 relatif à l'intelligence artificielle (AI Act), qui représente la première tentative de régulation globale des systèmes d'IA à l'échelle mondiale. Ce texte repose sur une classification des systèmes d'intelligence artificielle selon leur niveau de risque, distinguant les pratiques interdites, les

L'article 8, tel que publié le 26 octobre 2012, érige la protection des données à caractère personnel en droit fondamental autonome. Il impose un traitement loyal des données, fondé sur des finalités déterminées et encadré par le consentement ou une base légale. Il prévoit également le contrôle par une autorité indépendante, consacrant ainsi un niveau élevé de protection dans les sociétés numériques contemporaines.

⁽¹⁾ Article 47 – Droit à un recours effectif et à un procès équitable

Charte des droits fondamentaux de l'Union européenne, article 47, JOUE, C 326, 26 octobre 2012, p. 396.

L'article 47, publié au Journal officiel le 26 octobre 2012, garantit le droit à un recours effectif devant un tribunal ainsi que le droit à un procès équitable. Il assure l'effectivité des droits reconnus par le droit de l'Union en consacrant les exigences d'un jugement impartial, rendu dans un délai raisonnable, et en garantissant l'accès à l'assistance juridictionnelle.

⁽²⁾ Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données – RGPD), Journal officiel de l'Union européenne, JO L 119 du 4 mai 2016, p. 1-88.

systèmes à haut risque soumis à des obligations strictes, et les systèmes à faible risque bénéficiant d'un encadrement allégé⁽¹⁾.

Ce mécanisme montre une volonté d'anticiper les effets des technologies émergentes, en privilégiant une régulation ex ante.

Dès lors, le modèle européen se distingue par une régulation qui est à la fois normative, structurée et anticipatrice, axée sur la prévention des risques et la protection des droits fondamentaux. Il se présente ainsi comme l'un des systèmes les plus protecteurs à l'échelle internationale, surtout en ce qui concerne la protection des données et la régulation de l'intelligence artificielle. Cependant, cette richesse normative n'est pas sans critiques. Certains experts soulignent que la complexité des obligations imposées par le droit européen peut entraîner des coûts de conformité élevés, ce qui pourrait freiner l'innovation, notamment pour les petites et moyennes entreprises⁽²⁾.

Le modèle européen se trouve confronté à une tension entre la protection des droits et la compétitivité économique. Malgré ces défis, il est clair que l'approche européenne est devenue une référence incontournable en matière de régulation du numérique, comme le montre son influence qui dépasse ses propres frontières. Le phénomène du « Brussels Effect » illustre la capacité de l'Union européenne à exporter ses normes, incitant ainsi les acteurs économiques internationaux à s'y conformer pour accéder au marché européen⁽³⁾. Cette influence joue un rôle clé dans la diffusion d'un modèle juridique qui place les droits fondamentaux au cœur de la gouvernance numérique.

2. Le modèle américain : une régulation fondée sur le marché et la flexibilité normative

Le modèle américain de régulation numérique se caractérise par son approche libérale, dans laquelle l'innovation, la concurrence et la liberté économique constituent les principes directeurs de l'intervention juridique. Héritier d'une tradition qui se méfie d'une intervention étatique trop intrusive, ce modèle favorise une régulation minimale et flexible,

⁽¹⁾ Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle – « Artificial Intelligence Act » ou « AI Act ») et modifiant le règlement (CE) n° 300/2008, les règlements (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 ainsi que les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828, Journal officiel de l'Union européenne, JO L 1689 du 12 juillet 2024, p. 1 et s.

⁽²⁾ N. Petit, *Big Tech and the Digital Economy*, Oxford University Press, 2020.

⁽³⁾ A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

Le « Brussels Effect » peut être défini comme un mécanisme de projection externe du droit de l'Union européenne, par lequel les normes européennes acquièrent une portée globale en raison de l'attractivité économique et réglementaire du marché européen (Bradford, 2020).

considérant que le marché est le principal moteur d'ajustement des pratiques technologiques. Dès lors, le rôle du droit consiste moins à encadrer a priori les innovations qu'à corriger, a posteriori, les déséquilibres ou les abus susceptibles d'en résulter.

Cette philosophie se manifeste notamment par l'absence d'un cadre juridique fédéral unifié pour la protection des données personnelles. Contrairement à l'Union européenne, qui a mis en place une régulation globale avec le Règlement général sur la protection des données (RGPD), les États-Unis adoptent une approche sectorielle et fragmentée. Cela se traduit par l'adoption de lois spécifiques pour des domaines sensibles, comme le Health Insurance Portability and Accountability Act (HIPAA) pour les données de santé⁽¹⁾ ou le Gramm-Leach-Bliley Act (GLBA)⁽²⁾ pour les données financières⁽³⁾.

Cette structure normative permet une adaptation pragmatique aux particularités de chaque secteur, mais elle crée aussi une protection inégale des individus selon le domaine concerné. Dans ce cadre, la Federal Trade Commission (FTC)⁽⁴⁾ joue un rôle clé dans la régulation numérique. Établie par le Federal Trade Commission Act de 1914, cette autorité agit principalement de manière ex post, en sanctionnant les pratiques commerciales déloyales ou trompeuses en matière de protection des données et de concurrence. Cette régulation corrective a pour rôle de protéger les consommateurs et de maintenir l'équilibre et la dynamique du marché tout en limitant ses excès.

En outre, le modèle américain accorde une place particulière aux les instruments de soft law. Dans le domaine de l'intelligence artificielle, cette tendance se manifeste à travers le Blueprint for an AI Bill of Rights, publié en octobre 2022 par la Maison Blanche. Ce document établit les principes directeurs concernant la protection contre les biais algorithmiques, la transparence des systèmes automatisés et le respect de la vie privée, tout en évitant de créer des obligations juridiquement contraignantes⁽⁵⁾. Cette approche montre une

⁽¹⁾ Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), complété notamment par la Privacy Rule (45 C.F.R. Part 160 et Subparts A et E de Part 164) et la Security Rule (45 C.F.R. Part 160 et Subparts A et C de Part 164), régissant la protection et la sécurité des données de santé aux États-Unis.

⁽²⁾ Gramm-Leach-Bliley Act (GLBA) ou Financial Services Modernization Act of 1999, Public Law 106-102, adopté le 12 novembre 1999, 113 Stat. 1338, codified at 15 U.S.C. § 6801 et seq., encadrant la protection, la confidentialité et la sécurité des données financières des consommateurs aux États-Unis.

⁽³⁾ D. J. Solove, P. M. Schwartz, Information Privacy Law, Wolters Kluwer, 6^e éd., 2018.

⁽⁴⁾ Federal Trade Commission, créée par le Federal Trade Commission Act de 1914 (15 U.S.C. 41-58), autorité administrative indépendante chargée de la protection des consommateurs et de la régulation des pratiques commerciales, notamment en matière de protection des données personnelles et de concurrence aux États-Unis.

⁽⁵⁾ The White House, Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People, octobre 2022.

volonté d'encadrer les pratiques tout en permettant l'épanouissement de l'innovation technologique car l'utilisation de mécanismes non contraignants et la régulation ex post permet au modèle américain de créer un environnement particulièrement favorable au développement des entreprises technologiques, ce qui explique en partie la position dominante des États-Unis dans l'économie numérique mondiale. Cependant, cette flexibilité réglementaire n'est pas sans critiques. En effet, de nombreux experts soulignent les limites de ce modèle en matière de protection des droits fondamentaux. L'absence d'un cadre juridique global et contraignant peut entraîner une fragmentation des protections et un déséquilibre entre les individus et les grandes entreprises technologiques. Comme l'a souligné Frank Pasquale ; les systèmes numériques modernes fonctionnent souvent comme des « boîtes noires », dont les mécanismes échappent largement au contrôle des utilisateurs et des autorités publiques⁽¹⁾. Cette opacité augmente le risque d'atteintes aux droits individuels, notamment en ce qui concerne la vie privée et la non-discrimination.

Il semble que le modèle américain adopte une approche pratique et axée sur l'innovation, même si cela signifie parfois une protection juridique limitée pour les individus. Ce modèle met en avant une vision du droit comme un outil qui soutient l'activité économique, plutôt que comme un cadre normatif structurant et protecteur.

3- Le modèle chinois : une régulation centralisée fondée sur la souveraineté numérique et le contrôle étatique

Le modèle chinois de régulation du numérique se distingue par une approche très centralisée et souverainiste, dans laquelle l'État joue un rôle clé dans la gouvernance des technologies.

À la différence des modèles européen et américain, qui cherchent à encadrer ou à soutenir l'innovation, le modèle chinois intègre la régulation numérique dans une stratégie globale, axée sur des impératifs tels que la sécurité nationale, la stabilité sociale et la souveraineté informationnelle.

Dans ce contexte, les technologies numériques ne sont pas seulement considérées comme des outils de développement économique, mais aussi comme des moyens de gouvernance et de contrôle. Le droit est considéré comme un levier pour encadrer strictement les activités numériques, afin d'assurer le contrôle étatique sur les flux d'information et les infrastructures critiques.

Cette orientation s'est concrétisée par l'adoption d'un cadre juridique bien défini, reposant sur plusieurs textes fondamentaux. La Cybersecurity Law, adoptée le 7 novembre 2016 et entrée en vigueur le 1er juin 2017. Elle impose aux opérateurs de réseaux et aux fournisseurs de services numériques des obligations strictes concernant la sécurité des systèmes d'information, la localisation des données et la coopération avec les autorités

⁽¹⁾ F. Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.

publiques⁽¹⁾. Cette loi témoigne d'une volonté claire de contrôler les infrastructures numériques et de réduire les risques liés à la circulation des données.

Ce dispositif a été renforcé par la Data Security Law et la Personal Information Protection Law (PIPL) adoptées en 2021⁽²⁾. La première régule la gestion des données en fonction de leur importance stratégique, en instaurant des catégories de données soumises à des régimes juridiques variés. La seconde encadre la collecte et le traitement des données personnelles, tout en intégrant des exceptions notables liées à la sécurité nationale et à l'intérêt public⁽³⁾. Bien que cette loi présente des similitudes avec le RGPD européen, elle s'inscrit dans une logique différente, où la protection des droits individuels est souvent subordonnée aux besoins de l'État.

En ce qui concerne l'intelligence artificielle et les systèmes algorithmiques, la Chine adopte une approche particulièrement interventionniste proactive. En effet Les autorités ont mis en place des réglementations spécifiques, notamment à travers les Provisions on the Management of Algorithmic Recommendation Services⁽⁴⁾, qui sont entrées en vigueur en 2022. Ces règles obligent les entreprises à surveiller leurs algorithmes et à s'assurer qu'ils respectent les orientations politiques et sociales établies par l'État⁽⁵⁾. Ces mécanismes visent non seulement à gérer les risques liés à l'intelligence artificielle, mais aussi à orienter son développement en cohérence avec les objectifs stratégiques nationaux.

Le modèle chinois présente ainsi certains avantages, notamment en termes d'efficacité et de réactivité. La centralisation du pouvoir normatif permet une adaptation rapide aux évolutions technologiques et garantit une mise en œuvre cohérente des politiques publiques. Cependant, cette efficacité s'accompagne de limites significatives.

C'est vrai que ce modèle soulève de nombreuses interrogations sur la protection des libertés individuelles. Le renforcement du contrôle par l'État, associé à la surveillance numérique, peut conduire à une restriction significative des droits fondamentaux en matière de la vie privée, de liberté d'expression et d'accès à l'information. Comme le souligne la

⁽¹⁾ Cybersecurity Law of the People's Republic of China, 7 novembre 2016 (entrée en vigueur le 1er juin 2017).

⁽²⁾ Personal Information Protection Law of the People's Republic of China (PIPL), adoptée le 20 août 2021 et entrée en vigueur le 1er novembre 2021, établissant un cadre juridique relatif à la collecte, au traitement et à la protection des données personnelles en Chine.

⁽³⁾ Data Security Law (2021) ; Personal Information Protection Law (PIPL), 20 août 2021.

⁽⁴⁾ Provisions on the Management of Algorithmic Recommendation Services in Internet Information Services, adoptées le 31 décembre 2021 par la Cyberspace Administration of China (CAC) et entrées en vigueur le 1er mars 2022, établissant un cadre juridique encadrant l'utilisation des systèmes de recommandation algorithmique par les plateformes numériques en Chine.

⁽⁵⁾ Cyberspace Administration of China (CAC), Provisions on the Management of Algorithmic Recommendation Services, 2022.

doctrine, la concentration du pouvoir réglementaire entre les mains de l'État limite les contre-pouvoirs et affaiblit les mécanismes de contrôle juridictionnel⁽¹⁾.

On peut donc dire que le modèle chinois représente une vision du droit centré sur la souveraineté et le contrôle, ou la régulation du numérique est étroitement intégrée à une stratégie politique globale. Bien que cette approche soit jugée efficace, elle diverge des modèles occidentaux, en privilégiant les impératifs de sécurité et de stabilité au détriment de la protection des droits individuels.

L'analyse comparative des modèles de régulation numérique en Europe, aux États-Unis et en Chine révèle trois logiques fondamentales qui façonnent les approches juridiques contemporaines face aux évolutions technologiques. Ces logiques vont bien au-delà de simples choix techniques ou réglementaires ; elles reflètent des visions distinctes du rôle du droit dans la société, ainsi que des relations variées entre l'État, le marché et individus⁽²⁾.

Tout d'abord, le modèle européen s'appuie sur une logique de protection des droits fondamentaux. Il s'inscrit dans une tradition juridique normative et axée sur des valeurs, où le droit joue un rôle préventif pour encadrer les risques associés aux technologies numériques. La priorité est donnée à la préservation des libertés individuelles, notamment à travers la protection des données personnelles et le respect de la vie privée. Cette approche attribue au droit une fonction structurante, visant à orienter l'innovation tout en respectant les valeurs fondamentales⁽³⁾.

En second lieu, le modèle américain se distingue par une approche axée sur la libéralisation et l'innovation, où le marché occupe une place centrale dans la régulation des activités numériques. Le droit intervient de manière concrète, et principalement a posteriori, pour rectifier les problèmes qui se présentent, tout en laissant le développement technologique se poursuivre librement. Cette méthode favorise la flexibilité et la compétitivité économique, mais elle tend à limiter la protection juridique des individus, surtout en l'absence d'un cadre global et unifié⁽⁴⁾.

En fin, le modèle chinois repose sur une logique de contrôle étatique et de souveraineté numérique. Dans le quel, les technologies sont intégrées dans une stratégie globale de gouvernance, axée sur la sécurité nationale, la stabilité sociale et la gestion des flux d'information. Le droit est utilisé comme un outil de contrôle et d'organisation, au service des

⁽¹⁾ R. Creemers, « China's Data Governance », Stanford Cyber Policy Center, 2021 ; R. Clarke, « China's Surveillance State », Surveillance & Society, 2019.

⁽²⁾ J. Carbonnier, Flexible droit, LGDJ.

⁽³⁾ Charte des droits fondamentaux de l'Union européenne, JOUE C 326, 2012.

- Règlement (UE) 2016/679 (RGPD), JOUE L 119, 2016.

- Règlement (UE) 2024/1689 (AI Act).

⁽⁴⁾ D. Solove, Information Privacy Law, 2018.

- White House, AI Bill of Rights, 2022.

objectifs de l'État. Bien que cette approche se distingue par son efficacité et sa cohérence, elle soulève d'importantes questions sur la protection des libertés

Individuelles⁽¹⁾.

Ces trois modèles reflètent des visions profondément différentes du rôle du droit dans l'environnement numérique. Alors que l'Union européenne met l'accent sur l'individu et ses droits dans la régulation, les États-Unis favorisent l'innovation et la dynamique du marché, tandis que la Chine insiste sur la primauté de l'État dans la gouvernance numérique. Cependant, aucun de ces modèles ne s'impose comme une norme universelle. La complexité des enjeux liés aux technologies numériques et leur portée mondiale rendent difficile l'établissement d'un cadre de régulation unique. Ainsi, les États, en particulier ceux en développement, se voient contraints de créer des approches hybrides, intégrant divers éléments de ces modèles selon leurs priorités nationales et leurs contraintes institutionnelles. Dans ce contexte, le Maroc se distingue par son cas particulièrement révélateur. Il montre une dynamique d'adaptation progressive, influencée de manière significative par le modèle européen, tout en adoptant une approche pragmatique qui tient compte des réalités économiques et institutionnelles locales. Cette hybridation met en lumière la nécessité de trouver un équilibre entre la protection des droits, le développement économique et la souveraineté numérique, qui représente l'un des principaux défis du droit contemporain.

Section II: L'adaptation du système juridique marocain à l'innovation technologique : entre modernisation normative et contraintes structurelles

En examinant les modèles internationaux de régulation numérique, il est clair que les États doivent développer des réponses juridiques qui correspondent à leurs contextes institutionnels, économiques et sociaux. Dans ce cadre, le Maroc s'engage dans un processus d'adaptation progressive de son cadre juridique, visant à encadrer les changements apportés par les technologies numériques. Cette adaptation ne suit pas un modèle unique ou centralisé, mais plutôt une approche graduelle et sectorielle, qui combine interventions législatives, régulation administrative et intégration progressive des normes internationales. Cependant, cette évolution est encore limitée par certaines contraintes structurelles, notamment la fragmentation des normes, la capacité institutionnelle et les défis technologiques émergents. Il est donc essentiel d'explorer, d'une part, les bases de la modernisation juridique du numérique au Maroc et, d'autre part, les mécanismes de gouvernance ainsi que les défis qui en résultent.

1- Une modernisation juridique progressive et sectorielle du droit marocain du numérique

L'adaptation du système juridique marocain aux changements apportés par le numérique se déroule dans un cadre progressif et pragmatique. Ce processus se caractérise par une intervention graduelle du législateur et une évolution sectorielle des normes. Contrairement à certains modèles étrangers qui privilégient des approches globales et structurées pour réguler le numérique, le Maroc a opté pour une adaptation progressive, fondé

⁽¹⁾ Cybersecurity Law, Chine, 2017 ; Data Security Law, 2021.

- CAC, réglementation des algorithmes, 2022.

sur l'adoption des textes spécifiques qui répondent à des besoins juridiques clairement identifiés.

Cette approche montre à la fois une volonté d'intégrer les technologies numériques de manière réfléchie dans le droit positif et une certaine prudence face aux évolutions rapides et complexes du numérique. Elle s'inscrit dans une tradition juridique qui valorise la sécurité juridique et la stabilité normative., tout en cherchant à accompagner les changements économiques et technologiques.

A. L'intervention graduée du législateur : une adaptation fragmentée mais structurante

Au cours des vingt dernières années, les autorités marocaines ont progressivement mis en place un ensemble cohérent de mesures pour intégrer le numérique comme un levier de modernisation de l'action publique et de renforcement de la compétitivité nationale. Cette dynamique s'est traduite par l'adoption d'un cadre normatif structurant, articulé autour de plusieurs textes législatifs majeurs. Parmi ceux-ci, on trouve la loi n° 07-03 qui modifie le Code pénal, promulguée par le dahir n° 1-03-197 le 11 novembre 2003 ; la loi n° 53-05 sur l'échange électronique de données juridiques, promulguée par le dahir n° 1-07-129 le 30 novembre 2007 ; la loi n° 09-08 sur la protection des personnes physiques concernant le traitement des données personnelles, promulguée par le dahir n° 1-09-15 le 18 février 2009 ; ainsi que la loi n° 31-08 qui établit des mesures de protection des consommateurs, promulguée par le dahir n° 1-11-03 le 18 février 2011.

À ces textes s'ajoutent la loi n° 132-13 qui approuve le protocole additionnel à la Convention européenne pour la protection des données personnelles, promulguée par le dahir n° 1-14-136 le 31 juillet 2014 ; la loi n° 88-13 sur la presse et l'édition ; la loi n° 05-20 sur la cybersécurité, promulguée par le dahir n° 1-20-69 le 25 juillet 2020 ; ainsi que la loi n° 43-20 sur les services de confiance pour les transactions électroniques, promulguée par le dahir n° 1-20-100 le 31 décembre 2020.

Cet ensemble normatif témoigne d'une volonté claire d'encadrer juridiquement les transformations numériques, tout en veillant à maintenir un équilibre entre innovation technologique et protection des droits fondamentaux ⁽¹⁾

Dans ce cadre, la loi n° 09-08 joue un rôle clé en établissant les règles pour la protection des données personnelles. Pour cela, elle a créé la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), responsable de garantir le respect des droits des individus concernant le traitement de leurs données, qu'elles soient dans des fichiers publics ou privés. Reconnaisable à l'échelle internationale, notamment lors de la 33^e Conférence internationale des autorités de protection des données, la CNDP a un rôle crucial dans l'accompagnement des acteurs publics et privés pour se conformer aux normes, tout en sensibilisant les citoyens à la gestion de leurs données personnelles.

⁽¹⁾ Delmas Marty, 200).

En tant qu'institution administrative indépendante, la CNDP n'a pas de pouvoir coercitif absolu, mais elle remplit des fonctions consultatives, de contrôle et de sanction. Elle veille à ce que l'utilisation des technologies respecte la dignité humaine, les droits fondamentaux et la vie privée, conformément aux normes internationales de protection des données¹.

Dans une optique d'intégration internationale, le Maroc a entrepris des démarches pour obtenir une décision d'adéquation de la part de la Commission européenne, tout en travaillant à son adhésion à la Convention 108 du Conseil de l'Europe, qui concerne la protection des données personnelles.

Plus récemment, la loi n° 05-20 sur la cybersécurité montre une prise de conscience croissante des enjeux liés à la protection des infrastructures numériques et à la gestion des risques Cybernétiques⁽²⁾. Elle s'inscrit dans une démarche visant à sécuriser les systèmes d'information et à renforcer la résilience numérique de l'État.

Ainsi, bien que fragmentée, cette intervention législative progressive présente un caractère structurant. Elle permet au droit marocain de s'adapter progressivement aux évolutions technologiques tout en préservant une certaine cohérence globale dans le système juridique.

Toutefois, cette approche sectorielle peut également entraîner des difficultés d'articulation entre les différentes normes, limitant la lisibilité et l'efficacité du dispositif juridique.

D'autre part La Constitution marocaine de 2011 a joué un rôle clé dans le renforcement du cadre juridique lié au numérique, en établissant un ensemble de droits fondamentaux applicables aux environnements numériques. Par exemple, l'article 24⁽³⁾ protège clairement le droit à la vie privée, en affirmant le principe de l'inviolabilité du domicile et le secret des communications, peu importe leur forme. Cette disposition est particulièrement cruciale à l'ère numérique, où les échanges électroniques sont au cœur de notre vie sociale et économique. De plus, l'article 25⁽⁴⁾ assure les libertés de pensée, d'opinion et d'expression sous toutes leurs formes, y compris dans le domaine numérique. En outre, la

¹ Rodotà, 2009 ; RGPD, art. 5.

⁽²⁾ Loi n° 05-20 relative à la cybersécurité, Bulletin officiel du Royaume du Maroc, 2020.

⁽³⁾ L'article 24 de la Constitution du Royaume du Maroc de 2011 dispose que :

« Toute personne a droit à la protection de sa vie privée. Le domicile est inviolable. Les communications privées, sous quelque forme que ce soit, sont secrètes. Seule la justice peut autoriser, dans les conditions et selon les formes prévues par la loi, l'accès à leur contenu, leur divulgation totale ou partielle ou leur invocation à la charge de quiconque. ».

⁽⁴⁾ L'article 25 de la Constitution du Royaume du Maroc de 2011 dispose que « Sont garanties les libertés de pensée, d'opinion et d'expression sous toutes leurs formes. Sont également garanties les libertés de création, de publication et d'exposition dans les domaines littéraire, artistique et scientifique. ».

Constitution souligne l'importance des conventions internationales ratifiées, comme le Pacte international sur les droits civils et politiques (PIDCP), adopté par la résolution 2200 A (XXI) de l'assemblée générale des Nations Unies le 16 décembre 1966 entré en vigueur le 23 mars 1979 dont les articles 17⁽¹⁾ et 19⁽²⁾ protègent respectivement la vie privée et la liberté d'expression. Cela renforce l'obligation pour le législateur national d'intégrer les normes internationales dans la régulation du numérique.

B. Une convergence progressive vers les standards internationaux

L'évolution du droit numérique au Maroc s'inscrit dans une dynamique progressive qui vise à se rapprocher des normes internationales, surtout celles de l'Europe. Cette démarche montre clairement la volonté du Royaume de s'intégrer dans l'économie numérique mondiale et de renforcer la confiance de ses partenaires internationaux, notamment en ce qui concerne la circulation des données personnelles⁽³⁾.

Dans cet optique, la loi n° 09 08 sur la protection des données personnelles illustre bien cette influence. Ce texte reprend plusieurs principes issus du droit européen, bien avant l'arrivée du Règlement général sur la protection des données (RGPD). On y retrouve entre autres, la reconnaissance des droits des personnes concernées, des règles sur le traitement des données, et la mise en place d'une autorité de contrôle indépendante.

Au fil des années, cette influence s'est accentuée, notamment grâce à la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), qui a mis en place des lignes directrices pour aligner le cadre marocain aux exigences modernes en matière de gouvernance des données et de responsabilité des acteurs⁽⁴⁾.

Tout fois, cette convergence des normes soulève quelques questions. L'importation de modèles juridiques étrangers peut parfois se heurter aux spécificités institutionnelles, économiques et sociales du pays. L'efficacité de ces normes dépend donc de la capacité des institutions à les mettre en œuvre et du niveau de sensibilisation des acteurs publics et privés concernés⁽⁵⁾.

Ainsi, le droit numérique marocain peut être vu comme un système hybride, combinant influences internationales et adaptations locales. Cette approche permet une intégration progressive dans les dynamiques globales tout en préservant une certaine autonomie normative.

⁽¹⁾ Article 17 de la PIDCP « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance... ».

⁽²⁾ Article 19 (liberté d'expression)

« Toute personne a droit à la liberté d'expression ; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce... ».

⁽³⁾ A. Bradford, *The Brussels Effect*, Oxford University Press, 2020.

⁽⁴⁾ CNDP, recommandations et lignes directrices (Maroc).

⁽⁵⁾ O. De Schutter, *International Human Rights Law*, Cambridge, 2019.

En fin de compte, l'évolution du droit numérique au Maroc repose sur une approche progressive et sectorielle, marquée par une adaptation graduelle des normes et un rapprochement continu avec les standards internationaux. Bien que cette stratégie offre une certaine flexibilité, elle souligne aussi l'importance d'adopter une vision plus globale et cohérente pour le cadre juridique du numérique⁽¹⁾.

2- Les mécanismes de gouvernance numérique et les défis contemporains

A. La montée en puissance des autorités de régulation

L'adaptation du droit marocain face aux transformations numériques ne se limite pas simplement à l'intervention du législateur. Elle s'accompagne d'une évolution significative des mécanismes de régulation, où le rôle des autorités administratives spécialisées prend de plus en plus d'importance. Cette transformation marque un passage progressif d'une régulation strictement normative vers une gouvernance plus flexible et dynamique, reposant sur des mécanismes de supervision, d'accompagnement et de gestion des risques⁽²⁾.

Dans ce cadre, la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) créée par la loi n° 09 08, a pour mission de garantir le respect des règles concernant le traitement des données personnelles. Son action se traduit notamment par l'autorisation préalable de certains traitements, le contrôle des pratiques des organismes publics et privés, ainsi que la sensibilisation des acteurs aux enjeux liés à la protection des données. Elle contribue ainsi à instaurer une véritable culture de conformité et de responsabilité au sein de l'écosystème numérique.

En parallèle, l'Agence nationale de réglementation des télécommunications (ANRT), instituée par la loi n° 24-96 relative aux télécommunications, joue un rôle clé dans la régulation des infrastructures numériques et la gestion des réseaux de communication électronique. Elle veille notamment à ce que les règles de concurrence soient respectées et garantit un accès équitable aux services de communication.

La gouvernance numérique au Maroc a également pris de l'ampleur avec la mise en place, en 2011, de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI), qui dépend de l'Administration de la Défense nationale. Cette institution a pour mission d'assurer la sécurité des systèmes d'information et de lutter contre les cybermenaces, notamment grâce au Moroccan Computer Emergency Response Team (MaCERT). Elle contribue aussi à l'élaboration de stratégies nationales de cybersécurité, en se basant sur l'évaluation des risques, la protection des infrastructures critiques et le renforcement des capacités nationales⁽³⁾.

Dans la continuité de cette dynamique, la création, en 2017, de l'Agence de développement digital (ADD) a constitué une avancée supplémentaire dans la structuration de la gouvernance numérique. Avec sa personnalité morale et son autonomie financière, cette institution est chargée de piloter la stratégie nationale de transformation numérique et de

⁽¹⁾ M. Delmas-Marty, *Les forces imaginantes du droit*, 2004.

⁽²⁾ A. Supiot, *La gouvernance par les nombres*, 2015.

⁽³⁾ Loi n° 05-20 relative à la cybersécurité ; DGSSI.

promouvoir l'utilisation des technologies digitales. Elle encourage également une approche participative en organisant des concertations avec les différents acteurs institutionnels, économiques et sociaux⁽¹⁾.

L'intervention de ces différentes autorités souligne l'émergence d'un modèle de gouvernance numérique qui s'adapte aux évolutions technologiques. Ce modèle s'appuie sur une régulation spécialisée, technique et réactive, capable de faire face à la complexité des enjeux numériques contemporain.

Cependant, cette évolution n'est pas sans critiques. Le renforcement du rôle des autorités administratives indépendantes soulève des questions sur leur légitimité démocratique, car elles exercent des fonctions normatives sans être directement élues. De plus, la transparence de leurs décisions et l'efficacité du contrôle juridictionnel sont des enjeux cruciaux pour garantir leur conformité aux principes de l'État de droit⁽²⁾.

Ainsi, la gouvernance numérique au Maroc nécessite de trouver un équilibre entre une régulation efficace et le respect des garanties procédurales, ce qui est essentiel pour assurer la légitimité et la durabilité du cadre juridique numérique.

C. Les défis émergents : intelligence artificielle, plateformes et souveraineté numérique

Malgré les progrès significatifs réalisés dans le domaine de la régulation juridique du numérique, le système juridique marocain se heurte encore à des défis majeurs, surtout à cause de l'évolution rapide et incessante des technologies. Ces défis mettent en évidence les limites des cadres normatifs actuels, qui sont souvent mal adaptés à des phénomènes récents, complexes et, pour la plupart, de nature transnationale. Dans ce contexte, plusieurs initiatives montrent une volonté d'anticipation et de modernisation. Par exemple, le projet de loi cadre intitulé « Digital X.O », qui est actuellement en cours d'examen, représente une avancée importante. Ce texte a pour but de réguler l'utilisation de l'intelligence artificielle dans les secteurs public et privé, en mettant l'accent sur la gouvernance des données, l'identité numérique, l'interopérabilité et la cybersécurité. De plus, du livre blanc de l'année 2025 qui s'inscrit dans cette dynamique en définissant les grandes orientations stratégiques pour établir un modèle marocain d'intelligence artificielle. Cependant, malgré ces initiatives, il est important de noter qu'il n'existe pas encore de cadre juridique global et cohérent spécifiquement dédié à l'intelligence artificielle. Cette situation limite la capacité du droit à gérer efficacement les risques liés à l'automatisation des décisions, en ce qui concerne la transparence algorithmique, la responsabilité juridique et la protection des droits fondamentaux. Elle reflète également une certaine prudence législative, visant à éviter l'adoption prématurée de normes qui pourraient ne pas être adaptées à un environnement technologique en constante évolution.

En deuxième lieu, la régulation des plateformes numériques représente un défi majeur. Ces acteurs mondiaux détiennent un pouvoir économique et informationnel considérable,

⁽¹⁾ Agence de développement digital (ADD), missions institutionnelles.

⁽²⁾ F. Pasquale, *The Black Box Society*, 2015.

capable d'influencer la concurrence, la protection des consommateurs et la circulation des données. Cependant, le cadre juridique marocain reste fragmenté en la matière, reposant sur des dispositions sectorielles dispersées ; ce qui limite la capacité du droit à encadrer efficacement les pratiques des plateformes et à assurer un équilibre entre l'innovation économique et la protection des utilisateurs⁽¹⁾.

En troisième lieu, la question de la souveraineté numérique s'impose comme un enjeu stratégique majeur. La dépendance aux technologies étrangères, la localisation des données et le contrôle des infrastructures numériques soulèvent des questions essentielles sur la capacité de l'État marocain à gérer son environnement numérique. Dans un monde où les technologies se mondialisent, la souveraineté numérique ne se résume plus à une simple question territoriale, mais englobe également la maîtrise des flux d'information des données et des outils technologiques. Cette problématique prend une dimension particulière dans un contexte où les tensions géopolitiques autour du numérique sont de plus en plus présentes. Elle pousse le Maroc à élaborer une stratégie cohérente, combinant le développement des compétences nationales, le renforcement des capacités institutionnelles et la coopération internationale.

En fin de compte, les défis contemporains liés au numérique soulignent l'urgence d'une évolution continue du droit marocain, afin de garantir un équilibre entre l'innovation technologique, la protection des droits fondamentaux et la préservation de la souveraineté nationale.

CONCLUSION GÉNÉRALE

Au terme de cette analyse, il est clair que la transformation numérique joue un rôle clé dans la réorganisation des systèmes juridiques contemporains. Ce n'est pas juste une évolution technique des outils juridiques, mais une véritable révolution qui touche aux fondements mêmes du droit, à ses modes de régulation et à ses fonctions traditionnelles. La dématérialisation des échanges, l'automatisation des décisions et l'utilisation massive des données redéfinissent le paysage juridique et nécessitent une réévaluation des concepts classiques du droit.

La première partie de cette étude a mis en lumière les tensions créées par ces changements. En remettant en question les mécanismes traditionnels de création des actes juridiques, le rôle du juge et les modèles classiques de responsabilité, le numérique fragilise certains piliers essentiels de l'État de droit, notamment la sécurité juridique, la prévisibilité des règles et la protection effective des droits fondamentaux. Ces évolutions demandent donc une adaptation constante du droit pour maintenir sa fonction de régulation sociale dans un environnement de plus en plus incertain et complexe.

La seconde partie a permis d'identifier les principales réponses des systèmes juridiques contemporains. L'analyse comparative a montré qu'il existe des modèles de régulation variés, reflétant des visions différentes de la relation entre droit, technologie et

⁽¹⁾ OCDE, The Role of Digital Platforms in the Economy, 2019 ; A. De Streel, « The Governance of Digital Platforms », Journal of Network Industries, 2020.

société. Le modèle européen privilégie une approche normative axée sur la protection des droits fondamentaux et la prévention des risques ; le modèle américain adopte une logique plus pragmatique, centrée sur l'innovation et la régulation par le marché ; tandis que le modèle chinois s'inscrit dans une dynamique de contrôle étatique et de souveraineté numérique, intégrant les technologies dans une stratégie globale de gouvernance.

Cette diversité d'approches souligne qu'il n'existe pas de modèle universel pour réguler le numérique. Chaque système juridique développe ses propres solutions, en tenant compte de ses valeurs, de ses priorités économiques et de ses structures institutionnelles. Cela met aussi en lumière la complexité croissante de la régulation numérique, surtout dans un monde où les technologies se globalisent et où les données circulent sans frontières.

Dans cette dynamique le cas de Maroc illustre une démarche d'adaptation progressive, axée sur une modernisation des normes sectorielles et une convergence partielle vers les standards internationaux. Les réformes mises en place concernant l'échange électronique, la protection des données et la cybersécurité montrent une volonté d'aligner le droit marocain sur les évolutions contemporaines. Cependant, ces avancées font face à des défis structurels, comme l'absence d'un cadre juridique global cohérent, des limites institutionnelles et des enjeux croissants liés à la souveraineté numérique. Il est donc clair que le principal défi pour les systèmes juridiques d'aujourd'hui est de trouver un équilibre entre deux exigences qui semblent être opposées : l'innovation et la protection. D'une part, le droit doit accompagner les évolutions technologiques pour stimuler le développement économique et social, et d'autre part, il doit veiller au respect des droits fondamentaux et à la préservation des équilibres essentiels de l'État de droit.

À mon avis, l'avenir du droit numérique ne peut pas se construire dans une opposition entre régulation et innovation. Mais plutôt dans la recherche d'un équilibre dynamique entre ces deux aspects. La technologie ne devrait pas être vue comme une fin en soi, mais plutôt comme un outil au service de la justice, du développement et de la protection des individus.

En fin de compte, la capacité du droit à s'adapter aux avancées technologiques est essentielle pour maintenir la confiance des citoyens et renforcer les institutions juridiques. Cette adaptation ne se limite pas à une simple évolution des normes ; elle implique également une transformation des pratiques, des compétences et des modes de gouvernance.

Ainsi, le droit se présente moins comme un simple cadre restrictif mais davantage comme un système en constante évolution, prêt à accompagner les changements de la société tout en préservant les valeurs fondamentales qui garantissent sa cohésion et sa légitimité

BIBLIOGRAPHIE (STRICTEMENT 100 % TEXTE)

I. Textes internationaux et régionaux

- Déclaration universelle des droits de l'homme, 10 décembre 1948.
- Pacte international relatif aux droits civils et politiques (PIDCP), adopté par la résolution 2200 A (XXI) du 16 décembre 1966.
- Charte africaine des droits de l'homme et des peuples, 27 juin 1981.
- Convention européenne des droits de l'homme, 4 novembre 1950.

II. Droit marocain

- Constitution du Royaume du Maroc, 1er juillet 2011.
- Loi n° 07-03 modifiant le Code pénal, Dahir n° 1-03-197 du 11 novembre 2003.
- Loi n° 53-05 relative à l'échange électronique de données juridiques, Dahir n° 1-07-129 du 30 novembre 2007.
- Loi n° 09-08 relative à la protection des données à caractère personnel, Dahir n° 1-09-15 du 18 février 2009.
- Loi n° 31-08 relative à la protection du consommateur, Dahir n° 1-11-03 du 18 février 2011.
- Loi n° 132-13 relative à la protection des données (Convention 108), Dahir n° 1-14-136 du 31 juillet 2014.
- Loi n° 88-13 relative à la presse et à l'édition.
- Loi n° 05-20 relative à la cybersécurité, Dahir n° 1-20-69 du 25 juillet 2020.
- Loi n° 43-20 relative aux services de confiance pour les transactions électroniques, Dahir n° 1-20-100 du 31 décembre 2020.

III. Droit européen

- Directive 95/46/CE du Parlement européen et du Conseil, 24 octobre 1995.
- Règlement (UE) 2016/679 du 27 avril 2016 (RGPD).
- Règlement (UE) 2024/1689 relatif à l'intelligence artificielle (AI Act).
- Charte des droits fondamentaux de l'Union européenne.

IV. Droit américain cité

- Health Insurance Portability and Accountability Act (HIPAA), 1996.
- Gramm-Leach-Bliley Act (GLBA), 1999.
- Federal Trade Commission Act, 1914.
- Blueprint for an AI Bill of Rights, Maison Blanche, 2022.

V. Droit chinois cité

- Cybersecurity Law of the People's Republic of China, 7 novembre 2016 (entrée en vigueur le 1er juin 2017).
- Data Security Law of the People's Republic of China, 2021.
- Personal Information Protection Law (PIPL), 2021.
- Provisions on the Management of Algorithmic Recommendation Services, 31 décembre 2021 (entrée en vigueur le 1er mars 2022).

VI. Doctrine (uniquement celle citée dans TON texte)

- Rodotà, S., *La vie privée à l'ère numérique*.
- Delmas-Marty, M., *Les forces imaginantes du droit*.
- Pasquale, F., *The Black Box Society*.

VII. Rapports et études cités

- Policy Center for the New South (PCNS), Najah R., *Les technologies de surveillance à l'ère de la Covid-19*, 2020.

- National Institute of Standards and Technology (NIST), étude sur les biais de reconnaissance faciale.
- Georgetown University, *Facial Recognition Database Report*, 2016.
- British Medical Journal (BMJ), étude sur les biais en intelligence artificielle, 2020.
- UNESCO, Rapport sur l'éthique de l'intelligence artificielle, 2021.

VIII. Articles et sources en ligne (présents dans TON texte)

- New York Times, « Many Facial Recognition Systems Are Biased », 2019.
- ProPublica, *Machine Bias*, 2016.
- Odhran James McCarthy, *AI & Global Governance: Turning the Tide on Crime with Predictive Policing*, 2019.
- Les Échos, « Quand le logiciel de recrutement d'Amazon discrimine les femmes », 2018.
- BBC, « Germany starts enforcing hate speech law ».
- Le Point, « Syrie : suppression de vidéos par YouTube », 2017.
- Le Monde, « Censure de la loi Avia », 2020.

IX. Jurisprudence

- Conseil constitutionnel français, décision du 18 juin 2020 (loi Avia).
- Tribunal de grande instance de Paris, 12 février 2019, *UFC-Que Choisir c/ Google Inc.*
-