

Révolution digitale responsable et développement durable au Maroc

Responsible digital revolution and sustainable development in Morocco

Imane TAIBI

Laboratoire Droit, Société et Systèmes Comparés, Faculté des sciences juridiques, économiques et sociales Ain Chok, Université Hassan II de Casablanca, Casablanca, Maroc.

Karim SEFFAR

Laboratoire Droit, Société et Systèmes Comparés, Faculté des sciences juridiques, économiques et sociales Ain Chok, Université Hassan II de Casablanca, Casablanca, Maroc

Résumé. La digitalisation responsable des services au Maroc émerge comme une priorité incontournable pour catalyser une innovation durable dans le pays. Cet article souligne l'urgence d'adopter des pratiques numériques juridiquement responsables afin de garantir un progrès soutenu et respectueux des droits de tous les acteurs impliqués. Dans cette optique, une digitalisation responsable met en lumière la nécessité pour le Maroc de positionner la durabilité au cœur de sa stratégie de transformation digitale, en veillant à ce que les bénéfices de cette révolution technologique soient équitablement distribués et préservent les valeurs fondamentales de la société.

Mots-clés: *Digitalisation responsable ; Encadrement juridique ; Inclusion numérique ; Développement durable ; Innovation révolutionnaire.*

Abstract— Responsible digitization of services in Morocco is emerging as an unavoidable priority to catalyze sustainable innovation in the country. This article highlights the urgency of adopting ethical and legally responsible digital practices to ensure sustained and respectful progress for all stakeholders involved. In this regard, responsible digitization underscores the need for Morocco to position sustainability at the core of its digital transformation strategy, ensuring that the benefits of this technological revolution are equitably distributed and preserve the fundamental values of society.

Keywords: *Responsible digitization; Legal framework; Digital inclusion; Sustainable development ; Revolutionary innovation.*

1. Introduction

La technologie est omniprésente dans notre quotidien, façonnant nos interactions sociales, nos modes de travail et même nos modes de consommation. Néanmoins, cette omniprésence soulève également des questions cruciales sur la responsabilité qui accompagne cette révolution numérique (Abou El Jaoud, 2023). Ainsi, l'innovation technologique ne peut plus être dissociée de la notion de responsabilité. Au contraire, elle doit être intrinsèquement liée à cette dernière afin de garantir une digitalisation plus compétitive, éthique et durable.

Alors que les avancées technologiques créent des opportunités inédites pour la croissance économique (Cassar, 2020) et sociale, leur mise en œuvre doit être guidée par des piliers résistants. En effet, il est temps de veiller à ce que la technologie soit réalisée de manière résiliente. Cela implique la capacité des systèmes technologiques à anticiper, à s'adapter et à se rétablir efficacement face aux perturbations et aux défis qui peuvent surgir.

Avant d'appréhender notre thématique, il convient tout d'abord de définir ce que l'on entend par ses concepts.

La « digitalisation » fait référence à l'intégration croissante des technologies numériques dans tous les aspects de la société et de l'économie. Elle englobe des domaines tels que l'internet

des objets, l'intelligence artificielle, la blockchain, le *cloud computing*, etc (Tazairt, 2022). Cette notion, bien que largement présente dans nos sociétés, reste une notion complexe à définir et à cerner. Les termes utilisés pour la décrire sont variés et peuvent englober des réalités différentes, comme la numérisation, l'informatisation, la dématérialisation ou encore l'automatisation. Parfois, ces termes sont même utilisés de manière interchangeable (Tazairt, 2022).

Étymologiquement, le mot "digitalisation" vient de l'adjectif "digital", qui renvoie aux doigts, ainsi que du terme latin "*digitus*" (Le Robert, s.d.). En anglais, "*digit*" signifie chiffre, et "digital" est associé à l'utilisation des nombres. En français, on utilise aussi parfois l'adjectif "numérique". Malgré ces nuances linguistiques, le concept de base reste le même : l'utilisation des technologies digitales pour améliorer les performances des entreprises et contribuer à une élévation du niveau de vie.

L'adjectif "responsable", quant à lui, désigne la qualité d'une personne ou d'une entité qui agit de manière consciente et réfléchie. Cela inclut également la capacité à assumer les conséquences de ses choix et à répondre de ses actions devant autrui ou devant la société dans son ensemble. En somme, être responsable revient à agir de manière transparente et en accord avec les normes et les attentes sociales et légales (Romain, 2017).

La digitalisation responsable au Maroc est marquée par une progression significative ces dernières années. Le pays a adopté diverses initiatives visant à promouvoir l'utilisation responsable des technologies numériques, notamment à travers des programmes de sensibilisation, des réglementations et des partenariats avec le secteur privé.

Au début des années 2000, le Maroc a amorcé sa transition vers une économie numérique en mettant en place des politiques et des programmes visant à encourager l'essor des TIC. En 2001, le gouvernement a lancé le Plan National de Développement des Télécommunications (PNDT), visant à libéraliser le secteur des télécommunications et à stimuler les investissements dans les infrastructures de télécommunication. Cette impulsion initiale a été renforcée par l'adoption en 2009 de la Stratégie Maroc Numeric 2013, un programme ambitieux visant à accélérer la transformation numérique du pays. Cette stratégie avait pour objectif de faire du Maroc un hub régional des TIC et de stimuler la croissance économique à travers le développement du secteur numérique.

Parallèlement, le gouvernement marocain a continué à investir massivement dans les infrastructures numériques, en déployant notamment des réseaux à haut débit à travers le pays et en favorisant l'essor des services numériques innovants. En 2016, le lancement du Plan Maroc Digital 2020 a marqué une nouvelle étape dans cette stratégie, avec un accent particulier mis sur la promotion de l'inclusion numérique et le développement de l'économie digitale.

Cette dynamique s'est ensuite renforcée avec le Plan National de la Réforme de l'Administration 2018-2021, qui a permis de moderniser les services publics. La note d'orientations générales pour le développement du digital au Maroc à horizon 2025 et la stratégie « Maroc digital 2030 » représentent une feuille de route ambitieuse pour la transformation numérique continue du pays dans tous les secteurs. Dans cette optique, le secteur des télécommunications et des TIC est devenu un moteur clé de l'économie marocaine (Janati-Idrissi, 2020), contribuant de manière significative au PIB national et créant des milliers d'emplois dans des domaines tels que les technologies de l'information, les services en ligne et le développement de logiciels.

Aujourd'hui, le Maroc se positionne comme l'un des leaders de la digitalisation (Gorlier, 2021) en Afrique du Nord, avec des réalisations remarquables dans des domaines tels que le commerce électronique, les services bancaires en ligne et l'e-gouvernement. Alors que le pays

poursuit sa marche vers une économie numérique plus avancée, il reste déterminé à exploiter le potentiel des technologies de l'information pour stimuler la croissance économique, renforcer l'inclusion sociale et améliorer la qualité de vie de ses citoyens.

Ce sujet revêt un intérêt théorique et pratique significatif : sur le plan théorique, il suscite l'intérêt pour décortiquer les mécanismes de transition vers une économie numérique tout en préservant les valeurs de responsabilité. L'exploration des modèles théoriques de la digitalisation responsable permet de mieux appréhender les principes sous-jacents à cette transformation et d'anticiper les implications sur les structures sociales et économiques. D'un point de vue pratique, la digitalisation responsable offre des solutions concrètes pour mettre à niveau l'efficacité et l'accessibilité des services au Maroc. En adoptant des technologies numériques tout en veillant à intégrer des principes de durabilité, de transparence et de respect des droits de l'Homme (Quemener, Wierre et Dalle, 2020), les organismes gouvernementaux peuvent mieux répondre aux besoins des citoyens et renforcer la confiance dans les institutions publiques.

Ainsi, l'originalité de cet article repose sur une approche visant à combler les lacunes identifiées dans la digitalisation, dominant la littérature scientifique contemporaine. Alors que la majorité des recherches académiques se concentrent sur les aspects techniques ou les retombées économiques de la transformation numérique, la présente étude ajoute un enrichissement au phénomène. Elle se distingue particulièrement par son intégration des dimensions juridiques et sociales, offrant ainsi un cadre d'analyse exhaustif et équilibré. Cette démarche novatrice permet d'examiner en profondeur l'articulation entre la protection des infrastructures numériques et son impact sur l'arrimage d'une digitalisation responsable, tout en mettant en lumière le décalage entre l'accélération du progrès technologique et les réalités sociales - une problématique souvent négligée dans la littérature académique.

Par conséquent, l'apport de cette thématique réside dans son approche multidisciplinaire de la digitalisation. Il apporte une contribution marquante en élucidant les menaces numériques tout en présentant les protections juridiques existantes, qui constituent par ailleurs une veille juridique essentielle, et propose des solutions concrètes pour minimiser la fracture numérique. De surplus, ce sujet se démarque particulièrement par l'élaboration de recommandations stratégiques destinées aux décideurs, offrant ainsi une cartographie opérationnelle pour une transformation numérique inédite. En outre, sa vision humaniste, qui place l'individu au cœur de l'innovation technologique, constitue un apport précieux au débat actuel sur la digitalisation.

De toutes ces constatations, bien des questions invitent à la recherche, mais en ce qui concerne le présent article, une problématique a retenu notre attention, et qui va nous servir de fil rouge tout au long de cette étude : « *Dans un contexte où la digitalisation des services émerge comme un impératif pour favoriser l'innovation durable au Maroc, comment peut-on concrètement mettre en œuvre une digitalisation responsable ?* »

Cette problématique nous pousse à s'interroger sur deux questions subsidiaires, à savoir:

- Quels sont les moyens disponibles pour garantir que cette transition numérique se fasse dans le respect des impératifs juridiques et sociaux tout en favorisant le progrès économique et social ?
- Quelles sont les lacunes actuelles dans la mise en œuvre de cette digitalisation responsable ?

La réponse à cette problématique nous amène à mettre l'accent sur l'importance de la digitalisation responsable dans le contexte marocain. D'où l'intérêt de notre thème, qui découle de la nécessité de comprendre comment la digitalisation peut être encadrée de manière à garantir à la fois la croissance économique et le bien-être social. Il s'agira, en fait,

d'examiner deux aspects essentiels de cette digitalisation responsable : premièrement, l'importance d'un cadre juridique solide pour encadrer les initiatives numériques, et deuxièmement, la nécessité de garantir un accès équitable aux technologies numériques pour tous les citoyens.

2. Une digitalisation encadrée

Si le numérique offre un potentiel immense en termes d'innovation et de progrès, il comporte également des risques et des défis considérables. Face à ces enjeux, le législateur marocain a entrepris des démarches significatives pour réguler deux aspects cruciaux de la transformation numérique : la cybersécurité et la protection des données personnelles.

À travers la mise en place d'un arsenal juridique progressiste, le Maroc s'engage dans la voie d'une digitalisation sans précédent. Dans cette optique, cette analyse se propose d'examiner de près le cadre juridique de la digitalisation au Maroc, en mettant en lumière les dispositions légales et les avancées réalisées dans ce domaine. Pour ce faire, nous nous attarderons d'abord sur les enjeux juridiques de la cybersécurité. Ensuite, nous nous pencherons sur les mécanismes juridiques de protection des données à caractère personnel.

a. Les enjeux juridiques de la cybersécurité

Pour appréhender de manière exhaustive le cadre juridique de la cybersécurité au Maroc, notre analyse sera articulée autour de deux axes principaux. Dans un premier temps, nous nous pencherons sur la protection des infrastructures numériques et des données sensibles. Par la suite, notre attention se portera sur la protection des systèmes de traitement automatisé des données.

i. La protection des infrastructures numériques et des données sensibles

La loi n° 05-20, adoptée en 25 Juillet 2020, vise à établir un cadre robuste pour la protection des infrastructures numériques et des données sensibles du pays. En adoptant cette législation, le Maroc reconnaît l'importance cruciale des acteurs du secteur numérique dans la sécurisation des réseaux, des systèmes d'information et des services en ligne. L'instauration de mesures de conservation des données techniques et de notification d'incidents permet une réactivité accrue face aux menaces cybernétiques, tout en assurant la protection des données sensibles (Maknoun, 2023).

Cette initiative s'intègre dans un cadre stratégique plus vaste ayant pour objectif de renforcer la résilience du pays face aux cyberattaques et à promouvoir un environnement numérique sécurisé et fiable (Russkevich, 2023). En érigeant l'Autorité Nationale de la Cybersécurité (ANC) et la Commission Stratégique de Cybersécurité, le Maroc démontre son engagement à coordonner efficacement la gestion des incidents de sécurité à l'échelle nationale, en alignant sa législation sur les normes internationales et en répondant aux défis posés par la transformation digitale.

Dans cette perspective, les dispositions de la loi n° 05-20 sont structurées autour de trois axes principaux : la détection et la gestion des risques, la notification des incidents de sécurité (Russkevich, 2023), ainsi que la mise en place de mesures de sécurité et d'audits.

Inspirée de la législation française tout en préservant une approche nationale, cette loi exige la désignation d'un responsable de la sécurité des systèmes d'information au sein de chaque entité, agissant en tant que principal point de contact de l'Autorité Nationale de la Cybersécurité (ANC). Des mesures spécifiques sont également prévues pour les infrastructures d'importance vitale (Article 15, Dahir n° 1-20-69 du 4 hija 1441, loi n° 05-20 relative à la cybersécurité, 2020), incluant la fixation réglementaire de la liste des secteurs

concernés, tenue secrète et révisée au moins tous les deux ans (Article 16, Dahir n° 1-20-69 du 4 hija 1441, loi n° 05-20 relative à la cybersécurité, 2020). Par ailleurs, l'ANC est chargée de définir un guide d'homologation de la sécurité des systèmes d'information sensibles, avec une obligation juridique pour tous les opérateurs de se conformer à ses directives (Article 19, Dahir n° 1-20-69 du 4 hija 1441, loi n° 05-20 relative à la cybersécurité, 2020). En termes de gouvernance de la cybersécurité, un comité stratégique est mandaté pour élaborer les orientations stratégiques de l'État dans ce domaine et évaluer annuellement le bilan d'activité de l'ANC (Article 35, Dahir n° 1-20-69 du 4 hija 1441, loi n° 05-20 relative à la cybersécurité, 2020).

L'ensemble de ces mesures vise à améliorer la gestion de la cybercriminalité au Maroc en renforçant la sécurité des systèmes d'information au sein des institutions et dans l'espace numérique. Cependant, la mise en œuvre efficace de ces dispositions nécessitera des ressources humaines et financières adéquates (Missaoui et Elhila, 2021).

En cas de non-respect des mesures édictées, l'Autorité Nationale de la Cybersécurité (ANC) est habilitée à dresser des procès-verbaux de constatation, transmis ensuite au ministère public pour engager des poursuites judiciaires à l'encontre des contrevenants. Les amendes prévues peuvent être significatives, allant de 100 000 à 400 000 dirhams, en fonction de la gravité des violations constatées, servant à la fois de sanction financière et de moyen de dissuasion contre les pratiques non conformes en matière de cybersécurité (Article 49, Dahir n° 1-20-69 du 4 hija 1441, loi n° 05-20 relative à la cybersécurité, 2020).

En outre, la loi impose des obligations spécifiques concernant la confidentialité et la localisation des données sensibles, exigeant notamment que ces dernières soient hébergées exclusivement sur le territoire national (Article 11, Dahir n° 1-20-69 du 4 hija 1441, loi n° 05-20 relative à la cybersécurité, 2020). Tout manquement à ces dispositions est passible de sanctions de 200.000 à 400.000 DH, conformément aux dispositions légales énoncées dans l'article 49 de la loi relative à la cybersécurité. Ainsi, les sanctions prévues contribuent à renforcer l'efficacité du cadre réglementaire en matière de cybersécurité, incitant les acteurs à respecter scrupuleusement les obligations établies pour promouvoir un environnement numérique plus sécurisé.

ii. La protection des systèmes de traitement automatisé des données

Avant l'adoption de la loi n° 07-03, complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, le Maroc était confronté à un vide juridique en matière de cybercriminalité, ce qui rendait difficile la poursuite des criminels opérant dans le cyberespace. Les infractions informatiques, telles que les intrusions frauduleuses dans les systèmes informatiques et les atteintes aux données, étaient largement répandues, mais il n'existait pas de cadre juridique adéquat pour les réprimer (Karamé, 2020).

Inspirée de la loi française du 5 janvier 1988, la loi n° 07-03 a été adoptée en 2003 pour lutter contre la cybercriminalité au Maroc. Ce texte fondateur a pour objectif de mettre à jour le cadre juridique marocain en tenant compte des infractions liées à la cybercriminalité. Elle traite notamment des intrusions frauduleuses dans les STAD, des atteintes au fonctionnement de ces systèmes et des atteintes aux données qu'ils contiennent.

A cet effet, la loi n° 07-03 établit un cadre juridique complet pour réprimer les infractions liées aux systèmes de traitement automatisé des données. Elle définit clairement les types d'infractions, les sanctions applicables et les modalités de preuve nécessaires pour engager des

poursuites judiciaires contre les cybercriminels. Elle prévoit également des mesures de prévention et de protection des données pour renforcer la sécurité des systèmes informatiques. Ce cadre robuste fait une distinction entre l'accès frauduleux à un système automatisé de traitement de données (STAD) et le maintien frauduleux dans ce système. L'accès frauduleux se produit lorsqu'une personne pénètre ou s'introduit dans un système informatique sans autorisation, comme lorsque des données personnelles stockées sur un ordinateur personnel sont consultées par un tiers sans permission, également appelé « délinquant informatique ». Dans ce cas, si la culpabilité de la personne est prouvée, elle peut être condamnée par la justice pour cet acte délictueux (Séjean, 2023).

Plus précisément, l'accès frauduleux à un système se produit lorsqu'une personne entre illicitement dans celui-ci, que ce soit physiquement ou logiquement, par des moyens tels que le "hacking" ou le "sniffing" (Raveleau, 2022). En s'appuyant sur l'article 607-3 du code pénal marocain, ce type d'accès est punissable par la loi. Pour qu'une personne soit reconnue coupable, elle doit agir de manière frauduleuse, sans droit apparent.

En revanche, le maintien frauduleux concerne le fait de rester illégalement dans un système après y avoir initialement accédé. Il s'agit d'une prolongation de l'accès initial. A titre d'illustration, un informaticien licencié conservant l'accès au système de son ancien employeur et y causant des dommages graves peut être condamné pour maintien frauduleux dans un STAD (Lestari et Rasji, 2024). Néanmoins, un accès licite et répété, conforme aux conditions de connexion établies, comme dans le cas d'un annuaire, ne constitue pas un maintien frauduleux.

Dans ce contexte, il est essentiel de prendre en compte diverses menaces et infractions susceptibles de compromettre l'intégrité des systèmes automatisés de traitement de données (STAD). Parmi celles-ci, figurent les atteintes au fonctionnement des STAD et les atteintes aux données des STAD (Lestari et Rasji, 2024).

L'atteinte au fonctionnement des STAD consiste à entraver intentionnellement le fonctionnement normal d'un système informatique, le rendant temporairement ou définitivement inutilisable (El Azzouzi, 2010). La loi prévoit des sanctions sévères pour ce type d'infraction, notamment des peines d'emprisonnement et des amendes. L'article 607-5 du code pénal marocain dispose à cet effet que : *« le fait d'entraver ou de fausser intentionnellement le fonctionnement d'un système de traitement automatisé des données est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une des deux peines seulement »*.

Les atteintes aux données des STAD comprennent l'introduction frauduleuse de données, la détérioration, la suppression ou la modification frauduleuse des données qu'ils contiennent. Ces infractions sont également réprimées par la loi n° 07-03, avec des peines proportionnées à la gravité de l'atteinte (El Azzouzi, 2010). En effet, l'article 607-6 du code pénal dispose que : *« le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de détériorer ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni d'un an à trois ans d'emprisonnement et de 10.000 à 200.000 dirhams d'amende ou de l'une de ces deux peines seulement »*.

Outre la répression des infractions, la loi n° 07-03 prévoit des mesures de prévention et de lutte contre la cybercriminalité. Elle encourage la sensibilisation et l'éducation à la sécurité informatique, renforce la coopération internationale et met en place des stratégies d'anticipation des risques pour prémunir les systèmes informatiques contre les cyberattaques (Brigitte, 2016). Cependant, des défis persistent en matière d'application effective de la loi et de protection des systèmes informatiques contre les menaces cybernétiques. Malgré les avancées législatives, la complexité croissante des technologies numériques et l'évolution

rapide des tactiques des cybercriminels rendent nécessaire une adaptation constante des mesures de sécurité.

En somme, la loi n° 07-03 constitue un instrument essentiel pour lutter contre la cybercriminalité au Maroc. En complétant le cadre juridique existant, elle permet de réprimer efficacement les infractions liées aux systèmes de traitement automatisé des données (Benslimane, 2020) et de renforcer la sécurité des systèmes informatiques contre les cyberattaques. Toutefois, son efficacité dépendra de sa mise en œuvre rigoureuse et de la coopération entre les autorités nationales et internationales pour lutter contre ce fléau mondial (Chabaud, 2023).

b. La protection des données à caractère personnel

Les données à caractère personnel sont des informations cruciales permettant d'identifier directement ou indirectement une personne, jouant ainsi un rôle phare dans la vie quotidienne, que ce soit pour accéder à des services, effectuer des transactions ou interagir en ligne. Afin de préserver la confidentialité et la sécurité de ces informations, il est indispensable de mettre en place un cadre légal et institutionnel solide. Dans cette optique, nous examinerons d'abord le cadre légal régissant la protection des données au Maroc, puis nous nous pencherons sur le rôle et les responsabilités de la Commission Nationale de Contrôle de la Protection des Données à caractère Personnel (CNDP), en tant qu'organe de supervision et de régulation dans ce domaine.

i. Le cadre légal

La loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (Jarraya, 2013), promulguée le 21 mai 2009, constitue un jalon significatif dans le paysage juridique marocain. Inspirée de la loi française dite « la loi informatique et libertés » n° 78-17 du 6 janvier 1978, cette législation vise à garantir la protection des individus face aux traitements de leurs données à caractère personnel. Par une approche novatrice, cette loi introduit pour la première fois des dispositions légales harmonisées avec le droit européen, marquant ainsi une convergence avec les standards internationaux en matière de protection des données.

Dès son entrée en vigueur, la loi 09-08 établit un cadre juridique rigoureux, définissant le champ d'application de ses dispositions et spécifiant la qualité des données ainsi que les conditions requises pour obtenir le consentement préalable de la personne concernée. En outre, elle consacre les droits fondamentaux de cette dernière, régulant notamment l'accès aux informations la concernant, le droit de rectification et de suppression des données inexacts ou obsolètes, et le droit d'opposition à leur traitement dans certains cas spécifiques (Sadik, 2023).

Quant au transfert de données vers des pays étrangers, la loi prévoit des mécanismes spécifiques visant à garantir la sécurité et la confidentialité des informations personnelles (Sadik, 2023). Cette disposition témoigne de la volonté du législateur de concilier impératifs de coopération internationale et protection des droits individuels, dans un contexte de mondialisation croissante des échanges de données.

Dans le cadre des droits de la personne concernée, chaque traitement de données à caractère personnel exige, en principe, un consentement clair et indubitable de la part de l'individu concerné (Article 4, Dahir n° 1-09-15 du 22 safar 1430, loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, 2009). Toutefois, des exceptions sont prévues dans certaines circonstances, notamment lorsque le traitement est nécessaire pour respecter une obligation légale, sauvegarder des intérêts vitaux ou remplir une mission d'intérêt public (Article 5, Dahir n° 1-09-15 du 22 safar 1430, loi n°

09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, 2009).

En ce qui concerne les obligations du responsable du traitement, ces derniers sont tenus de garantir que les données à caractère personnel sont collectées et traitées de manière équitable, légale et transparente. Cette exigence renforce la confiance des individus dans la gestion de leurs informations personnelles, tout en assurant une protection adéquate contre les abus ou les utilisations frauduleuses de leurs données.

ii. Le cadre institutionnel : La CNDP

La Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), créée par la loi 09-08, joue un rôle central en assurant une mission d'information et de sensibilisation à l'égard des acteurs concernés. En premier lieu, elle s'attelle à informer les individus, qu'ils soient des personnes physiques ou morales, sur les droits qui leur sont conférés par le nouveau cadre juridique régissant l'utilisation de leurs données personnelles au Maroc. Cette action vise à renforcer la conscience des citoyens quant à la protection de leur vie privée et à leur capacité à exercer leurs droits en matière de données.

Parallèlement, la CNDP se charge de sensibiliser les organismes publics et privés sur leurs obligations en matière de traitement des données à caractère personnel. En fournissant des conseils et des directives sur les meilleures pratiques, elle contribue à promouvoir une culture de la protection des données au sein des organisations marocaines, favorisant ainsi une approche proactive de la conformité réglementaire.

En outre, la commission assume la responsabilité d'expliquer aux opérateurs économiques les règles et les mécanismes régissant le transfert des données à caractère personnel à l'étranger (Khuan, 2024). Cette démarche vise à clarifier les exigences légales et les procédures à suivre pour assurer la conformité lors de tout échange transfrontalier de données, renforçant ainsi la confiance des parties prenantes (Jarraya, 2013) dans les transactions internationales impliquant des informations personnelles.

3. Une digitalisation inclusive

L'inclusion sociale émerge comme un impératif majeur pour garantir que personne ne soit exclu des bénéfices de cette transformation. Une digitalisation responsable doit donc être inclusive, c'est-à-dire qu'elle doit viser à réduire les inégalités et à offrir des opportunités équitables à tous les individus, quelles que soient leur origine sociale, leur situation géographique ou leurs capacités. En effet, une approche inclusive de la digitalisation permet non seulement de renforcer la cohésion sociale, mais également de stimuler l'innovation et la croissance économique en exploitant pleinement le potentiel de tous les membres de la société.

Cette partie explorera deux dimensions cruciales de la digitalisation responsable. Tout d'abord, elle examine l'importance de l'adaptation au changement et de l'inclusion numérique, en mettant en évidence la résilience et l'accès équitable aux technologies comme piliers de cette approche. Ensuite, elle aborde la nécessité d'un cadre juridique performant pour encadrer l'innovation et l'intelligence artificielle, en soulignant les défis et les opportunités liés à l'évolution technologique dans un contexte de respect des droits fondamentaux et de promotion de la compétitivité économique.

a. Une digitalisation équitable

Il est essentiel d'aborder en premier lieu la nécessité d'adapter les stratégies pour répondre au changement et de promouvoir l'inclusion numérique (Mission société numérique, 2018). Cette approche se matérialise par la promotion de la résilience numérique, qui renforce la capacité des individus et des organisations à relever les défis technologiques et à saisir les opportunités qui en découlent. Ensuite, cette démarche incite à examiner l'importance de l'inclusion

numérique, qui aspire à garantir un accès équitable aux technologies et à réduire la fracture numérique.

i. La résilience numérique

La résilience numérique, dans le contexte contemporain, émerge comme un pilier fondamental pour surmonter les défis inhérents à l'adoption des technologies émergentes. L'une des embûches majeures à cette résilience est la peur de l'inconnu, qui se manifeste par une appréhension à l'égard de nouvelles technologies inexplorées (Blondi, 2018). Cela peut découler d'une méconnaissance des avantages potentiels de ces technologies ou d'une crainte de l'impact sur les emplois traditionnels. Par conséquent, cette peur peut freiner l'exploration et l'adoption de solutions numériques innovantes, limitant ainsi le progrès et l'innovation dans divers domaines.

Une autre barrière significative à la résilience numérique réside dans la méfiance à l'égard des nouvelles technologies. Cette méfiance peut découler d'expériences passées négatives, de préoccupations concernant la fiabilité des technologies émergentes, ou encore de récits médiatiques alarmistes sur les conséquences potentielles de ces innovations (Erragragui et Aoufir, 2023). En conséquence, les individus et les organisations peuvent être réticents à adopter de nouvelles technologies par crainte de subir des pertes financières, une dégradation de la qualité de vie ou des atteintes à leur vie privée. Cette méfiance constitue ainsi un obstacle majeur à la résilience numérique, bornant l'exploration et l'exploitation des solutions technologiques novatrices (Erragragui et Aoufir, 2023).

Reste à signaler, les préoccupations concernant la sécurité et la confidentialité des données représentent un défi non négligeable à la résilience numérique. Avec la prolifération des cyberattaques et des violations de données à l'échelle mondiale, les individus et les organisations sont de plus en plus conscients des risques potentiels liés à la numérisation de leurs activités (Bouquet et Jaeger, 2015). Cette conscientisation accrue se traduit souvent par une méfiance à l'égard des plateformes numériques et des services en ligne, entravant ainsi l'adoption et l'utilisation généralisée de ces technologies.

Pour surmonter ces obstacles, une approche proactive de sensibilisation et d'éducation s'avère essentielle. Ces efforts doivent viser à informer et à rassurer les citoyens sur les avantages de la numérisation. À cet égard, des campagnes de sensibilisation ciblées peuvent être mises en place pour démystifier les idées fausses et clarifier les bénéfices tangibles des technologies numériques. De plus, des programmes de formation adaptés aux besoins spécifiques des différents segments de la population peuvent contribuer à renforcer les compétences numériques et à accroître la confiance dans l'utilisation des outils technologiques (Annarelli et Palombi, 2021).

Par ailleurs, la résilience numérique nécessite une collaboration étroite entre les acteurs du secteur public, privé et de la société civile. En favorisant le dialogue et la coopération entre ces différentes parties prenantes, il est possible de créer un écosystème favorable à l'innovation et à l'adoption des technologies numériques. De plus, la collaboration peut permettre de développer des solutions intégrées qui répondent aux besoins et aux défis spécifiques de la société marocaine (Annarelli et Palombi, 2021).

En outre, il est important d'investir dans des infrastructures numériques robustes et sécurisées pour renforcer la résilience numérique du Maroc. Cela comprend non seulement le développement de réseaux et de systèmes technologiques fiables, mais aussi la mise en place de mesures de sécurité et de protection des données efficaces. En garantissant la sécurité et la fiabilité des infrastructures numériques, le Maroc peut promouvoir la confiance des citoyens et des entreprises dans l'utilisation des services en ligne et des technologies numériques.

ii. L'inclusion numérique

L'inclusion numérique s'inscrit au cœur des enjeux sociaux modernes, comme le souligne le groupe d'experts de l'Europe (Cauchard et N'Goala, 2021 ; Mocquet, Péliissier et Cotreaux, 2021), qui affirme que « l'inclusion n'est rien d'autre que l'inclusion sociale ». Celle-ci est définie par ce même groupe comme « l'intégration sociale dans une société et une économie où le numérique joue un rôle essentiel ». Le Conseil National du Numérique (CNNUM) renforce cette idée en identifiant deux objectifs majeurs : « réduire les inégalités et les exclusions sociales grâce au numérique, et en faire un levier de transformation individuelle et collective » (Bouquet et Jaeger, 2015). Dans ce cadre, la promotion de l'inclusion numérique ne se borne pas à l'accès aux technologies, mais vise également à minimiser les disparités sociales et économiques, un défi particulièrement pertinent au Maroc, où ces écarts restent prononcés en raison de facteurs géographiques et socio-économiques.

Premièrement, les disparités de revenu représentent l'un des principaux obstacles à l'inclusion numérique. Les individus et les familles à faible revenu peuvent avoir des difficultés à se procurer des appareils informatiques et à payer des services Internet, ce qui limite leur accès aux ressources et aux opportunités en ligne. Pour remédier à cela, des solutions telles que la subvention des équipements informatiques et la tarification sociale des services Internet peuvent être mises en œuvre pour rendre les technologies numériques plus accessibles aux populations défavorisées (Copestake, Estefania-Flores et Furceri, 2022).

De plus, l'analphabétisme et le manque de compétences numériques constituent des obstacles majeurs à l'inclusion numérique. De nombreuses personnes, en particulier dans les zones rurales et défavorisées, n'ont pas les compétences nécessaires pour utiliser efficacement les technologies numériques, ce qui les empêche de bénéficier des services en ligne et des opportunités d'apprentissage disponibles sur Internet. Pour surmonter cette barrière, des programmes de formation et de sensibilisation aux compétences numériques peuvent être mis en place dans les communautés mal desservies pour renforcer les capacités des individus et faciliter leur intégration dans l'économie numérique.

En outre, la localisation géographique constitue un facteur critique influençant l'accès numérique, notamment dans les zones rurales et éloignées où l'infrastructure Internet est limitée ou inexistante. Pour combler cette lacune, des investissements dans l'extension des réseaux de télécommunications et le déploiement de technologies d'accès à large bande peuvent être réalisés pour étendre la connectivité numérique aux régions sous-desservies (Copestake, Estefania-Flores et Furceri, 2022).

L'accès au numérique est également influencé par des facteurs démographiques, notamment l'âge, qui joue un rôle déterminant. Les personnes âgées, en particulier, sont souvent moins familiarisées avec les technologies numériques et peuvent se montrer plus réticentes à les adopter. Cette fracture générationnelle constitue un obstacle important à l'inclusion numérique. Pour y remédier, il est essentiel de mettre en œuvre des initiatives spécifiques, telles que des programmes de sensibilisation et d'accompagnement personnalisés, afin de les aider à surmonter ces barrières et à tirer pleinement parti des opportunités offertes par le numérique (Hauret, Martin et Poussing, 2023).

De même, les disparités d'accès numérique entre les zones urbaines et rurales constituent un obstacle significatif à l'inclusion numérique. Alors que les zones urbaines bénéficient généralement d'infrastructures et de services numériques plus développés, les populations rurales, en revanche, sont souvent confrontées à un accès limité, ce qui accentue le fossé numérique. Cette fracture territoriale freine non seulement l'accès aux opportunités numériques, mais renforce également les inégalités socio-économiques. Pour réduire ces écarts, il est crucial de mettre en place des politiques de développement régional et des

initiatives spécifiques de connectivité rurale, afin d'élargir l'accès aux technologies numériques aux populations vivant dans les zones éloignées et mal desservies.

Par ailleurs, les barrières linguistiques peuvent également entraver l'inclusion numérique, avec de nombreuses ressources en ligne étant disponibles uniquement dans certaines langues, ce qui limite l'accès des populations francophones et arabophones à ces ressources. Pour occulter cette barrière, des efforts peuvent être déployés pour traduire et localiser les contenus numériques dans différentes langues pour garantir un accès équitable à l'information et aux services en ligne (Hauret, Martin et Poussing, 2023).

b. L'Homme et l'intelligence artificielle en harmonie

Dans un contexte d'innovations technologiques effrénées, telles que l'intelligence artificielle (IA), un cadre juridique solide et adapté est urgent pour concilier innovation et protection des droits fondamentaux. A cet égard, nous explorerons l'importance d'un tel cadre pour promouvoir une digitalisation au service de l'humanité (2.2.1.). Plus spécifiquement, nous nous pencherons sur un nouveau texte européen sur l'IA, visant à promouvoir une innovation contrôlée et éthique dans le développement et l'utilisation de cette technologie émergente (2.2.2.).

i. Une digitalisation au service de l'humanité

La présence croissante de la robotique remplace progressivement l'interaction humaine, tandis que l'Homme adopte de plus en plus des comportements robotiques. Les interactions avec des dispositifs toujours plus intelligents deviennent plus fréquentes. Nous nous dirigeons vers une société où l'individu s'intègre de manière croissante dans un vaste système technologique, devenant ainsi une partie intégrante de sa vie quotidienne (Ferry et Jousset-Couturier, 2016).

Dans l'ère actuelle, un dilemme persiste quant au rôle de la technologie dans la société : va-t-elle remplacer l'Homme ou va-t-elle travailler en tandem avec lui pour favoriser le progrès ? Cette question soulève des préoccupations quant à la place de l'Homme dans un monde de plus en plus automatisé. Toutefois, il est impératif de reconnaître que la technologie doit être au service de l'Homme et non l'inverse. Plutôt que de créer une division entre l'Homme et la machine, une approche centrée sur l'humain met l'accent sur la collaboration et la complémentarité entre les deux (Gelin et Guilhem, 2016).

Ainsi, l'objectif principal de la digitalisation devrait être de créer des opportunités pour les individus et de renforcer leurs capacités plutôt que de les remplacer. Cela implique que les innovations numériques devraient être conçues pour soutenir et améliorer les compétences humaines, en offrant de nouvelles avenues d'apprentissage et de développement. En privilégiant la formation et le développement des compétences numériques, la digitalisation peut aider à combler les écarts de compétences et à promouvoir l'inclusion numérique, permettant à un plus grand nombre de personnes de participer à l'économie numérique (El Yamani, Kasbaoui et Ait Larbi, 2023).

Par ailleurs, la digitalisation doit également créer des opportunités d'emploi dans le secteur des technologies de l'information et de la communication (TIC). En encourageant l'entrepreneuriat et en soutenant les startups technologiques, la digitalisation peut stimuler la création d'emplois et la croissance économique. En investissant dans des programmes de formation professionnelle et en fournissant un soutien aux petites entreprises, les gouvernements peuvent aider à créer un écosystème propice à l'innovation et à la création d'emplois dans le secteur numérique (El Yamani, Kasbaoui et Ait Larbi, 2023).

Ajoutant à cela, il est essentiel de souligner que l'innovation numérique doit être humanisée, c'est-à-dire qu'elle doit être guidée par des valeurs telles que l'éthique, la responsabilité sociale et la durabilité. Plutôt que de poursuivre uniquement la rentabilité à court terme, les

entreprises et les innovateurs doivent adopter une approche plus holistique qui tienne compte de l'impact social et environnemental de leurs actions. En plaçant l'humain au centre de l'innovation, la digitalisation peut devenir un puissant moteur de progrès social et économique (Pandey et Nathai, 2024).

En somme, une approche collaborative est essentielle pour garantir que la digitalisation profite à l'ensemble de la société. En encourageant le dialogue et la coopération entre les différents acteurs - gouvernements, entreprises, organisations de la société civile et individus - il est possible de créer un avenir numérique qui soit inclusif, équitable et durable. En travaillant ensemble, nous pouvons façonner un monde numérique qui soit véritablement au service de l'humanité (Gorlier, 2021).

ii. Vers une innovation contrôlée

L'innovation, pour être maîtrisée et bénéfique à la société, nécessite un cadre réglementaire adéquat. C'est dans cette optique qu'un nouveau texte européen sur l'intelligence artificielle (IA), modifiant certains actes législatifs de l'Union (COM (2021) 0206 – C9-0146/2021 – 2021/0106 (COD)), a été élaboré. Cette législation répond à un double impératif. D'une part, elle vise à harmoniser le marché intérieur en établissant un cadre juridique uniforme pour le développement et l'utilisation des systèmes d'IA. D'autre part, elle place résolument l'humain au cœur de cette transformation numérique, en assurant une protection renforcée en matière de santé, de sécurité et des droits fondamentaux, tels qu'ils sont inscrits dans la Charte des droits fondamentaux de l'Union européenne.

La législation sur l'intelligence artificielle, adoptée par le Parlement européen le 13 mars 2024, ne se limite pas à des objectifs économiques : il met également l'accent sur le respect des valeurs impératives de l'Union (Marquis, 2017). En promouvant une IA centrée sur l'humain et digne de confiance, elle cherche à assurer que les technologies de l'intelligence artificielle soient développées et utilisées dans le respect de la dignité humaine. Les systèmes d'IA doivent être conçus de manière à garantir la transparence, la responsabilité et l'équité, évitant ainsi les biais discriminatoires ou les atteintes aux droits individuels (Aziz, 2024).

Ce texte réglementaire vise pareillement à encourager l'innovation en garantissant la libre circulation des biens et services basés sur l'intelligence artificielle à travers les frontières. Il interdit aux États membres d'instaurer des limitations au développement, à la mise sur le marché et à l'utilisation des systèmes d'IA, sauf dans les cas explicitement prévus par le cadre légal. L'objectif est de favoriser l'innovation et la création d'emplois, tout en positionnant l'Union européenne comme un leader dans l'adoption d'une IA fiable et éthique.

Cette approche européenne de l'IA illustre parfaitement la possibilité d'une innovation contrôlée, où progrès technologique et protection des droits fondamentaux se renforcent mutuellement plutôt que de s'opposer. Elle ouvre la voie à un nouveau paradigme de développement technologique, où l'innovation n'est plus considérée comme une fin en soi, mais comme un moyen au service du bien-être collectif.

4. Conclusion

« Le digital n'est pas le futur : il est là, il est à l'œuvre, sous nos yeux (Diaz, 2015). »

La réalité indéniable de la digitalisation nous confronte à des choix cruciaux quant à la manière dont nous l'exploitons. Ainsi, la digitalisation, lorsqu'elle est mise en œuvre de manière responsable, offre des opportunités inégalées pour progresser vers une innovation durable et inclusive. Cependant, si elle est mal exploitée ou négligée, elle risque de creuser les écarts et d'exacerber les inégalités. À cet effet, plusieurs entraves freinent l'avènement d'une digitalisation pleinement responsable (Diaz, 2015). Parmi elles, on retrouve :

- **Le manque d'infrastructures numériques adéquates**, particulièrement dans les zones rurales, qui limite l'accès aux outils numériques.

- **L'analphabétisme numérique**, qui empêche une partie significative de la population de bénéficier des avantages du numérique.
- **Les risques accrus pour la vie privée et la cybersécurité**, qui mettent en danger les données à caractère personnel et les systèmes critiques.
- **La fracture numérique**, qui, loin de se réduire, s'accroît parfois entre ceux qui maîtrisent ces technologies et ceux qui en sont exclus.
- **Le manque de réglementations et de politiques claires**, qui laisse des zones d'ombre sur les responsabilités des acteurs du digital.
- **La résistance au changement**, présente à tous les niveaux, qu'il s'agisse d'individus ou d'organisations, freinant l'adoption de nouvelles technologies

Les constats de la digitalisation au Maroc soulignent l'importance d'une approche réfléchie et responsable dans l'adoption des technologies numériques, mettant en avant la nécessité de promouvoir l'inclusion, le respect des droits et la préservation des valeurs sociétales. En effet, la digitalisation peut être un puissant levier pour stimuler la croissance économique, améliorer l'accès aux services et renforcer la compétitivité, à condition qu'elle soit guidée par des principes de responsabilité et de durabilité.

Le principal objectif ici serait de réaliser un équilibre entre le développement de cette nouvelle ère technologique et la prise en considération des paramètres de la responsabilité. Il faut néanmoins veiller à ce que cette interventionnisme du digital, souple aux multiples textures, apporte des bénéfices tangibles à la société tout en lui offrant des opportunités inédites.

Une question demeure pertinente : *comment concilier le rythme des innovations technologiques avec l'adoption d'une digitalisation plus responsable, dans un monde où les avancées se succèdent à une vitesse effrénée ?*

5. Références

- ABOU EL JAOUUD Anouar, « la preuve numérique à l'épreuve de la cybercriminalité en droit marocain », *Revue Droit et Société*, Numéro 11, 2023.
- ANNARELLI Alessandro, PALOMBI Giulia, « Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework », *Sustainability*, Volume 13, Numéro 23, 2021.
- AZIZ Mostafa, « Opportunités et Risques de l'Intelligence Artificielle », *Revue d'histoire du droit*, N° 3, 2024.
- BENSLIMANE Abdeslam, *La cybercriminalité dans la législation marocaine: étude critique et comparative à la lumière des opinions doctrinales et des décisions judiciaires*, Dar Al Aman, (en arabe), 2020.
- BLONDI Carl, « Pour l'inclusion numérique: L'omniprésence du numérique », *Bibliothèque, technologie(s) et numérique*, 2018.
- BOUQUET Brigitte, JAEGER Marcel, « *L'e-inclusion, un levier?* », *Vie sociale*, N° 11, 2015/3.
- BRIGITTE Pereira, « La lutte contre la cybercriminalité : de l'abondance de la norme à sa perfectibilité », *Revue internationale de droit économique*, N°3, 2016.
- CASSAR Bertrand, *La transformation numérique du monde du droit*, thèse pour l'obtention du doctorat en sciences juridiques, Université de Strasbourg, École Doctorale Droit, Science Politique et Histoire, 2020.
- CAUCHARD Léa, N'GOALA Gilles, « L'inclusion numérique : se rapprocher de l'utilisateur pour des stratégies plus efficaces », in MOCQUET Bertrand, PÉLISSIER Chrysta, COTREAUX Sabine (dir.), *Impacts sociétaux et développements du management des technologies organisationnelles*, vol. 13, no 1, Presses des Mines, 2021.

- CHABAUD Laurent, *L'arme numérique : essai sur la dématérialisation des infractions pénales*, thèse pour l'obtention du doctorat en Droit, Université de Montpellier, 2023.
- COPESTAKE Alexander, ESTEFANIA-FLORES Julia, FURCERI Davide, « Digitalization and Resilience », WP/22/210, *IMF Working Paper, International Monetary Fund*, 2022.
- DIAZ Manuel, *Tous digitalisés : Et si votre futur avait commencé sans vous ?*, Dunod, Malakoff, Hors collection, 2015.
- EL AZZOUZI Ali, *La cybercriminalité au Maroc*, 2010.
- EL YAMANI Kaoutar, KASBAOUI Tarik & AIT LARBI Fatima Ezzahra, « De la transformation digitale responsable et inclusive: enjeux, risques et perspectives », *Revue Internationale des Sciences de Gestion*, Vol. 6, N° 2, 2023.
- ERRAGRAGUI Safaa, AOUFIR Mbarek, « Comprendre l'approche de la transformation digitale : Les déterminants de la TD, opportunités et défis, proposition d'un modèle théorique », *International Journal of Accounting, Finance, Auditing, Management and Economics (IJAFAME)*, Vol. 4, 2023.
- FERRY Luc, JOUSSET-COUTURIER Béatrice, *Le transhumanisme: Faut-il avoir peur de l'avenir?*, Eyrolles, Édition 1, 2016.
- GELIN Rodolphe et GUILHEM Olivier, *Le robot est-il l'avenir de l'homme?*, La Documentation française, 2016.
- GORLIER Vicent, *la digitalisation de l'accès au droit*, Les Éditions du Panthéon, 2021.
- HAURET Laetitia, MARTIN Ludivine, POUSSING Nicolas, « Inclusion numérique. Une identification des facteurs à l'origine de la fracture numérique », rapport du LISER, 2023.
- JANATI-IDRISSI Farid., « La transformation digitale des PME au Maroc : enjeux et perspectives », *Repères et Perspectives Economiques*, Vol. 4, N° 2, 2020.
- JARRAYA Wissem, « La protection des données personnelles dans le commerce électronique », Rapport de recherche, Faculté de droit de Sfax, 2013.
- KARAMECH Laila, *La gouvernance sécuritaire au Maroc - approche juridique en interaction avec les autres déterminants de la bonne gouvernance*, Remald, Manuels et Travaux Universitaires, N° 133, 2020.
- KHUAN Hendri, « The Legal Protection of Personal Data in Fintech Peer-to-Peer (P2P) Lending Practices: Orientation and Formulation », *Inspirasi Futura: Media Kajian Keislaman*, Vol. 22, N° 3, 2024.
- La mission société numérique, « stratégie nationale pour un numérique inclusif », rapport et recommandations, 2018.
- LESTARI Endang, RASJI Rasji, « Legal study on personal data protection based on Indonesian legislation », *Awang Long Law Review*, Vol. 6, N° 2, 2024.
- MAKNOUN Zaynab, « confiance et sécurité numérique: nouveaux principes régissant les liens juridiques », *Revue des études juridiques et judiciaires (en arabe)*, n° 6, 2023.
- MARQUIS François-Xavier, « Pensée ou intelligence artificielle ? : De la stratégie à la formation, l'humain au coeur du numérique », L'Harmattan, 2017.
- MISSAOUI Mohamed Karim, ELHILA Abdelaziz, « Le droit pénal et l'éthique à l'épreuve de la cybercriminalité », *Revue Marocaine d'Administration Locale et de Développement (REMALD)*, n° 157, 2021.
- MARCHILDON Allison, DUHAME André, *Quels lendemains pour la responsabilité ? : Perspectives multidisciplinaires*, Groupe Nota Bene, 2018.
- PANDEY Vimmi, NATHAI Neeta, « Human Machine Interaction », *Machine Learning: An Art of Computer Thinking*, 2024.

- QUEMENER Myriam, WIERRE Clément, DALLE Frédérique, *Quels droits face aux innovations numériques?*, Gualino, 2020.
- RAVELEAU Benoît, *Manager en responsabilité à l'heure du digital: Regards croisés de chercheurs*, Presses de l'Université Laval, Québec, 2022, pp. 1-135.
- ROMAIN Arnoux, *Éthique de la responsabilité: Enquête philosophique au cœur des enjeux contemporains*, Hermann, 2017.
- RUSSKEVICH Evgeny, « Personal Data in the Mechanism of Criminal Law Protection », Proceedings of the Southwest State University. Series: History and Law, Volume 13, N° 5, 2023.
- SADIK Sarah, *La protection des données dans les contrats de cloud computing*, thèse pour l'obtention du doctorat en droit, Université de Perpignan, 2023.
- SÉJEAN Michel, « Cybersécurité contre cybercriminalité : toutes les couches de l'espace numérique sont concernées », N° 63, *Lexbase Pénal*, 2023.
- TAZAIRT Tinhinane, *Servicisation, digitalisation et performances des PME industrielles*, thèse pour l'obtention du doctorat en Gestion et management, Université Lumière - Lyon II, 2022.