

**Centre des Etudes Doctorales : Sciences Juridiques, Economiques, Sociales,
Chariaa et de Gestion**

Formation Doctorale : Droit privé

Discipline : Droit privé

Spécialité : Droit privé

Laboratoire de Recherche : Droit, Philosophie et Société

Thèse pour l'obtention du Doctorat

Sous le thème :

**La sécurité juridique à l'épreuve de la transformation
digitale des entreprises**

RESUME

La transformation digitale croît de façon exponentielle et tend à se généraliser. Le développement du digital envahit peu à peu tous les espaces de vie, marquant plus particulièrement celui des entreprises. L'approche technique de la transformation digitale des entreprises n'est pas sans failles, et l'aléa est omniprésent. D'où la nécessité aussi d'une approche juridique. De ce fait, accroître la sécurité juridique devient un enjeu majeur pour le développement de l'économie numérique. L'examen de la doctrine et de la jurisprudence témoigne largement de nouvelles problématiques liées à la sécurité juridique quant à l'utilisation du numérique sans limite de temps et d'espace. L'intégration du digital dans l'entreprise risque de déséquilibrer ses relations avec son environnement interne ainsi que son environnement externe. Dans ce cadre, cette thèse étudie la transformation conceptuelle du droit face à la transformation numérique des entreprises. En effet, cette dernière invite à remodeler la législation pour une garantie d'une sécurité juridique qui se veut efficace.

Mots-clés :

Entreprise ; Transformation digitale ; Sécurité juridique ; Données personnelles ; Responsabilité numérique ; Intelligence économique ; Contrats numériques ; Cybersécurité.

ABSTRACT

Digital transformation is growing exponentially and is becoming more widespread. The development of digital is gradually taking over all areas of life, with particular emphasis on companies. The technical approach to the digital transformation of companies is not without its flaws, and risk is ubiquitous. Hence the requirement for a legal strategy. Thus, increasing legal certainty becomes a major challenge for the development of the digital economy. The review of the doctrine and case law largely testifies to new issues related to legal security regarding the use of digital without any limit of time and space. The integration of digital in the company risks unbalancing its relations with its internal environment as well as its external environment. Within this framework, this thesis studies the conceptual transformation of the law in the face of the digital transformation of companies. Indeed, digital transformation calls for the legislation to be reshaped in order to guarantee an effective legal security.

Key words:

Company; Digital transformation; Legal security; Personal Data; Cybersecurity; Economic intelligence; Digital contracts; Digital responsibility.

ملخص

يشهد التحول الرقمي نموا كبيرا و يصبح أكثر انتشارًا مع مرور الوقت، فقد أصبح يغزو شيئًا فشيئًا معظم مجالات الحياة، خاصة تلك التي تخص الشركات. لا يخلو النهج التقني للتحول الرقمي للشركات من الرهانات. فالمخاطر موجودة في كل مكان. ومن هنا تأتي الحاجة أيضا إلى نهج قانوني. ونتيجة لذلك أصبح تطوير الأمن القانوني تحديا كبيرا لتطور الاقتصاد الرقمي، إذ يشهد تحليل آراء الاجتهاد القضائي و الفقه إلى حد كبير على قضايا جديدة تتعلق باستخدام الرقمنة دون التقيد بالزمان و المكان. إن ولوج الرقمنة للشركات يشكل خطرا في عدم توازن علاقاتها مع بيئتها الداخلية وكذلك الخارجية. في هذا السياق، تتطرق هذه الأطروحة لدراسة تحول المفاهيم القانونية في مواجهة التحول الرقمي للشركات، والواقع أن هذا الأخير يدعو إلى إعادة صياغة التشريعات لضمان أمن قانوني فعال.

الكلمات الدالة:

المقولة؛ التحول الرقمي؛ الأمن القانوني؛ البيانات الشخصية؛ الأمن السيبراني؛ الذكاء الاقتصادي؛ العقود الرقمية؛ المسؤولية الرقمية.

REMERCIEMENTS

DEDICACE

LISTE DES ABBREVIATIONS

ACCIS.	: Assiette Commune Consolidée pour l'Impôt sur les Sociétés.
ADD.	: Agence de Développement du Digital.
ADN.	: Anime Digital Network.
ADPIC.	: Accord sur les Aspects des Droits de Propriété Intellectuelle qui touchent au Commerce.
AFRIC.	: African Network Information Centre.
AMIE.	: Association Marocaines de l'Intelligence Economique.
ANPME.	: Agence Nationale pour la Promotion des Petites et Moyennes Entreprises.
ANRT.	: Agence Nationale de Réglementation des Télécommunications.
APNIC.	: Asia-Pacific Network Information Centre.
Arch.Phil.Droit.	: Archive de Philosophie du Droit.
ARIN.	: American Registry for Internet Numbers.
ATAF.	: African Tax Administration Forum.
BATX.	: Baidu, Alibaba, Tencent et Xiaomi.
BEPS.	: Base Erosion and Profit Shifting.
BIT.	: Bureau International de Travail.
B.O.	: Bulletin Officiel.
BYOD.	: Bring Your Own Device.
B2B.	: Business to Business.
B2C.	: Business to Consumer.
CCI.	: Chambre de Commerce Internationale.
ccTLD.	: Country Code Top Level Domain.
CD.	: Compact Disc.
CE.	: Commission Européenne.
CEI.	: Commission Electronique Internationale.
CEPEJ.	: Commission Européenne pour l'Efficacité de la Justice.
CISPA.	: Cyber Intelligence Sharing and Protection Act.
CJCE.	: Cour de Justice de la Communauté Européenne.
CJUE.	: Cour de Justice de l'Union Européenne.
CMI.	: Centre Monétique Interbancaire.
CMMB.	: Centre Marocain de Médiation Bancaire.
CNDP.	: Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel.
CNIL.	: Commission Nationale de l'Informatique et de Libertés.
CNN.	: Conseil National du Numérique.
CNP.	: Card No Present.
CNRST.	: Centre Nationale de la Recherche Scientifique et Technique.
CNUCED.	: Conférence des Nations Unies sur le Commerce et le Développement.
CNUDCI.	: Commission des Nations Unies pour le Droit Commercial International.
COMPAS.	: Corectional Offender Management Profiling for Alternative Sanctions.
CVV.	: Card Verification Code.
DGSSI.	: Direction Générale de la Sécurité des Systèmes d'Information.
DMA.	: Digital Market Act.
DNS.	: Domain Name System.
DNSSI.	: Direction Nationale de la Sécurité des Systèmes d'Information.
DSA.	: Digital Services Act.
DSP.	: Demand Side Platform.

DSSI.	: Directeur de la Sécurité des Systèmes d'Information.
ECODIR.	: Electronic Consumer Dispute Resolution.
EDI.	: Echange de Données Informatisé.
EIAT.	: Escale Institute of Advanced Technology.
EMN.	: Entreprises Multinationales.
ESV.	: Etablissement Stable Virtuel.
ETSI.	: European Telecommunications Standards Institute.
ETUC.	: European Trade Union Confederation.
ETUI.	: European Trade Union Institute
FAI.	: Fournisseur d'Accès à Internet.
FIBEN.	: Fichier Bancaire des Entreprises.
FIRST.	: Forum of Incident Response and Security Teams.
FMI.	: Fonds Monétaire International.
FRAND.	: Fair, Reasonable and Non-Discriminatory.
GAFAMI.	: Google Apple Facebook Amazon Microsoft IBM.
GE.	: Grande Entreprise.
GEG.	: Groupe d'Expert Gouvernementaux.
GFCE.	: Global Forum on Cyber Expertise.
GSM.	: Global System for Mobile Communications.
gtld.	: Generis Top Level Domain.
GT9.	: Groupe de Travail n°9.
HCP.	: Haut Commissariat au Plan.
HIPSSA.	: Harmonization of the ICT Policies in Sub-Sahara Africa.
Http.	: Hyper Text Transfer Protocol.
Https.	: Hyper Text Transfer Protocol Secure.
IA.	: Intelligence Artificielle.
IaaS.	: Infrastructure as a Service.
IBA.	: International Bar Association.
IBM.	: International Business Machines Corporation.
ICANN.	: Internet Corporation for Assigned Names and Numbers.
ICCA.	: International Council for Commercial Arbitration.
ICO.	: Initial Coin Offering.
IEC.	: Indice de Création des Entreprises.
IFRI.	: Institut Français des Relations Internationales.
ILO.	: International Labor Organization.
Incoterms.	: International Commercial Terms.
IP.	: Internet Protocol.
IPC.	: International Post Corporation.
IP/IT.	: Droit de la Propriété Intellectuelle et du Numérique.
ISO.	: Organisation Internationale de Normalisation.
ISP.	: Internet Service Provider.
KOICA.	: Korea International Cooperation Agency.
LACNIC.	: Latin America and Caribbean Network Information Centre.
LPA.	: Layered Process Audits.
maCERT.	: Moroccan Computer Emergency Response Team.
MEAC.	: Mid-Eastern Athletic Conference.
MENA.	: Middle East and North Africa.
NCSC.	: National Cyber Security Center.
NTIC.	: Nouvelles Technologies de l'Information et de la Communication.

OCDE.	: Organisation de Coopération et de Développement Economiques.
OIPC.	: Organisation Internationale de Police Criminelle.
OIT.	: Organisation Internationale du Travail.
OMPI.	: Organisation Mondiale de la Propriété Intellectuelle.
OMPIC.	: Office Marocain de la Propriété Industrielle et Commerciale.
ONCLNT.	: Office Nationale Contre la Criminalité liée aux Nouvelles Technologies.
ONI.	: Organisation Internationale de Normalisation.
ONU.	: Organisation des Nations Unies.
PaaS.	: Platform-as-a-Service.
PARL.	: Procédure Alternative de Règlement des Litiges.
PDF.	: Portable Document Format.
PDG.	: Président Directeur Général.
PII	: Personal Identifying Information.
PME.	: Petites et Moyennes Entreprises.
PUF.	: Presses Universitaires de France.
REC.	: Registre Electronique du Commerce.
REMALD.	: Revue Marocaine d'Administration Local et de Développement.
RDT.	: Revue de Droit de Travail.
RGPD.	: Règlement Général sur la Protection des Données.
RIPE-NCC.	: Réseaux IP Européens - Network Coordination Centre.
RJDA.	: Revue de Jurisprudence de Droit des Affaires.
RTB.	: Real Time Bidding.
SaaS.	: Software as a Service.
SARL.	: Société à Responsabilité Limitée.
SCS.	: Société en Commandite Simple.
SIS.	: Système d'Information Sensible.
SLD.	: Second Level Domain.
SMS.	: Short Message Service.
SNC.	: Société en Nom Collectif.
SNE.	: Syndicat Nationale de L'Edition.
SSL.	: Secure Socket Layer.
SSP.	: Supply Side Platform.
STAD.	: Système de Traitement Automatisé de Données.
TGI.	: Tribunal de Grande Instance.
TIC.	: Technologie de l'Information et de la Communication.
TLD.	: Top Level Domain.
TMCH.	: TradeMark ClearingHouse.
TPE.	: Toute Petite Entreprise.
TPME.	: Toute Petite et Moyenne Entreprise.
TPS.	: Taxe sur les Produits et Services.
TSN.	: Taxe sur les Services Numériques.
TVA.	: Taxe sur la Valeur Ajoutée.
UDRP.	: Uniform Domain Name Dispute Resolution Policy.
UE.	: Union Européenne.
URL.	: Uniform Resource Locator.
URS.	: Uniform Rapid Suspension System.
USB.	: Universal Serial Bus.
VPN.	: Virtual Private Network.

SOMMAIRE

Introduction générale

Première Partie : La transformation digitale des entreprises et ses mesures de sécurité juridique internes.

Titre I : L'impact de la transformation digitale sur la vie de l'entreprise.

Chapitre I : L'intégration du digital en droit des sociétés.

Chapitre II : Le numérique et la transformation des relations de travail.

Titre II : Les instruments digitaux de l'entreprise.

Chapitre I : Les contrats numériques.

**Chapitre II : La propriété intellectuelle et la transformation digitale de
l'entreprise.**

Deuxième Partie : La transformation digitale des entreprises et ses mesures de sécurité juridique externes.

Titre I : L'impact de la transformation digitale sur l'environnement externe de l'entreprise.

Chapitre I : L'imposition des entreprises numériques.

Chapitre II : L'entreprise digitale entre concurrence et cybersécurité.

Titre II : L'engagement de la responsabilité de l'entreprise et la résolution des litiges au numérique.

Chapitre I : La responsabilité à l'ère du numérique.

Chapitre II : La compétence des litiges nés sur Internet.

Conclusion générale

*« At Microsoft there are lots of brilliant ideas but the image is that they all
come from the top – I'm afraid that's not quite right. »*

(Chez Microsoft, il y a beaucoup d'idées brillantes, mais l'apparence est qu'elles viennent
toutes d'en haut - j'ai bien peur que ce ne soit pas tout à fait exact.)

Bill Gates

Introduction générale

La transformation numérique dans les entreprises est devenue l'un des sujets les plus présents dans le monde des affaires¹ et de la recherche scientifique. La transformation digitale ressemble à un train qui passe très vite ; les entreprises qui sont à bord continuent et prospèrent tandis que celles qui traînent sur le quai restent loin derrière. L'expression transformation digitale fascine les entreprises qui deviendraient toutes subitement des éditrices de services tendances et innovants, 100% numériques. L'adoption stratégique du numérique par les entreprises est bel et bien en train de s'opérer. Elle revêt des formes, des ampleurs et des vitesses différentes selon le secteur, l'activité, l'organisation et les cibles de l'entreprise, celles de ses partenaires, fournisseurs ou distributeurs².

A l'échelle mondiale, le digital est un levier de compétitivité économique important et créateur de richesse économique, notamment grâce aux gains de productivité que permet la transformation digitale. A l'échelle nationale, la transformation digitale peut constituer un accélérateur de la croissance économique et de la compétitivité économique du Maroc notamment chez les PME et TPE. Par ailleurs, la transformation digitale offre au Maroc l'opportunité de se positionner en tant que Hub Digital Africain³, à même d'attirer des entreprises digitales innovantes et des talents de tout le continent, des investissements et ainsi fédérer les offres technologiques, et l'écosystème entrepreneurial national.

Le digital est aujourd'hui identifié au niveau mondial comme la 4^{ème} révolution industrielle. De tous les défis multiples auxquels nous sommes confrontés aujourd'hui, le plus important est de comprendre et orienter la nouvelle révolution technologique. Nous sommes à l'aube d'une révolution qui bouleverse déjà notre manière de vivre et de travailler⁴. La pandémie mondiale de la Covid-19 a de toute évidence rendue encore plus tributaires des outils digitaux pour travailler. L'expansion de l'univers numérique est si rapide que ses

¹N. AZOURY, « Une révolution enclenchée par le changement numérique », in Questions de management, N° 7, Septembre 2014, EMS Editions p. 158.

²E. MOTAIS, E. BLONS et L. PFEIFFER : « L'adoption stratégique du numérique », in Questions de management, N°7, Septembre 2014, EMS Editions p. 168.

³Hub Digital Africain est un projet à la fois fondateur et fédérateur. Fondateur, car l'enjeu est de réaliser un socle Numérique dont l'Afrique a besoin, tant au niveau connectivité que de capacité à domestiquer sur son propres données sur le continent. Fédérateur, car il est une solution primordiale pour orchestrer un véritable projet commun d'envergure à l'échelle de l'Afrique, qui doit faire face à une évolution démographique, et gagner en souveraineté stratégique, économique, et sociale.

⁴Klaus SCHWAB, La quatrième révolution industrielle, DUNOD, Malakoff, 2017, p. 23.

acteurs peinent quelquefois à suivre son infernale cadence¹. La vague digitale est une réalité aujourd'hui, poussée par les clients qui modifient leurs usages dans tous les secteurs de consommation. Elle constitue à la fois une impérieuse nécessité et une formidable opportunité de transformation des dimensions internes à l'entreprise, en termes d'organisation et de processus pouvant favoriser une organisation apprenante².

La numérisation des entreprises est devenue une condition de leur survie. Cette numérisation se caractérise par la dématérialisation croissante de tout ce qui, traditionnellement, permettait de les appréhender et d'en localiser les principaux éléments : le financement, l'activité, la gouvernance, les relations avec l'administration, le marketing et la distribution deviennent digitaux. Des industriels envisagent même de créer des entreprises sans intervention humaine³.

L'économie découvre de nouvelles sources de productivité en accélérant la robotisation et l'automatisation. Une nouvelle matière première s'invente, faite de *big data*⁴, de création de valeur contributive et coopérative (*crowdsourcing*, *crowdfunding*, etc...) mais aussi relationnelle avec des systèmes de notation susceptibles de changer radicalement la donne. Signe des temps, les grandes entreprises créent toutes leur direction de la transformation digitale, lancent les grandes manœuvres organisationnelles et managerielles et redessinent leurs espaces de travail⁵.

Le numérique oblige les organisations traditionnelles à se repenser. Il bouleverse leurs modèles économiques et remplace de nombreuses structures physiques. Le numérique permet aux nouvelles organisations d'être scalables, c'est-à-dire capables, grâce à des plateformes technologiques, de supporter des montées en charge très importantes. Loin d'être limité aux entreprises du secteur informatique, le numérique touche tous les acteurs économiques et tous les métiers.

¹Guillaume PITRON, L'enfer numérique : voyage au bout d'un like, Les liens qui libèrent, 2021, p. 11.

²C. FORASACCO, « Démystifier, piloter, accompagner, apprendre à faire confiance pour changer de paradigme », in Questions de management, N° 7, Septembre 2014, EMS Editions, p. 167.

³J-P. DOM, « Matérialité et localisation de l'entreprise numérique », in IP/IT, N° 12, Décembre 2019, Dalloz, pp.661-662.

⁴Littéralement, ces termes signifient mégadonnées, grosses données ou encore données massives. Le terme désigne de vastes ensembles de données collectées par les entreprises, pouvant être explorées et analysées afin d'en dégager des informations exploitables.

⁵Olivier CHARBONNIER et Sandra ENKART, Société digital : Comment rester humain?, DUNOD, Malakoff, 2018, p. 5.

Dans un monde numérique où l'innovation vient des comportements, les sciences humaines et sociales se replacent au cœur du jeu économique et industriel, au cœur de la société numérique. L'encadrement législatif dans le domaine du numérique se révèle délicat car il implique la maîtrise de problèmes techniques difficiles à appréhender, derrière lesquelles se dissimulent des enjeux importants. Le processus législatif devant guider l'adoption de la régulation du numérique se dévoile de manière tumultueuse en ce que les questions posées suscitent au mieux des débats assez ardues, au pire des polémiques assez stériles. Les évolutions créent à la fois des souplesses nouvelles et des risques de dérives accrus.

L'évolution des techniques suscitent toujours des interrogations quant à la capacité du droit de s'y adapter¹. Le développement très rapide du commerce électronique, justifie notamment l'adaptation des règles juridiques applicables à la preuve, à la formation et à l'exécution du contrat. Au-delà de la mise en place de règles relatives à la formation et à l'exécution des contrats, on relèvera que les pouvoirs publics doivent répondre à des problématiques complexes, d'un point de vue politique, économique (concurrence perturbée par les nouvelles pratiques contractuelles)² et fiscal, ou encore, en matière de sécurité et de responsabilité. Plus que jamais, il est nécessaire d'appréhender la matière juridique et de la rendre opérable dans ses différents champs.

Utilisé il y a quelques années, le mot digital s'employait autrefois comme anglicisme et pouvait donc renvoyer indistinctement au numérique. Aujourd'hui, ce n'est plus le cas. En effet, le mot digital a aujourd'hui un sens qui se rapproche davantage de son étymologie. Le mot digital, du latin *digitus* qui veut dire doigt, fait ainsi directement référence aux

¹A cet égard, Alain Supiot souligne que les nouvelles technologies de l'information et de la communication montrent que cette fonction anthropologique ne disparaît pas lorsqu'on bascule d'un type de technique à un autre. L'examen de ces problèmes permet de comprendre les relations que les techniques n'ont cessé d'entretenir avec le droit. Ces relations ne se laissent résumer ni à une simple adaptation d'un droit qui serait par définition en retard sur le progrès technique, ni à une soumission de ce progrès à des principes juridiques immuables. Le Droit, en tant que technique, a participé dès l'origine à l'émergence des technologies de l'information et de la communication, mais son contenu évolue aujourd'hui sous nos yeux pour soumettre l'utilisation de ces technologies à des valeurs proprement humaines. Le Droit du travail demeure ainsi un observatoire privilégié des rapports du droit et de la technique.

²Dans le domaine de la culture la révolution numérique fait naître de nouvelles menaces de comportements anticoncurrentiels, notamment sous la forme d'abus de position dominante de la part de mastodontes qui s'auto-distribuent. On les désigne d'un nouvel acronyme : « GAFA », pour Google, Amazon, Facebook, Apple.

appareils tactiles dont la manipulation se fait par le biais des doigts¹. En revanche, le mot numérique, qui a été officiellement retenu par la Commission d'Enrichissement de la Langue Française, vient du latin *numerus* qui signifie représentation par nombre. Il tire directement ses racines des nombres, ou plutôt des chiffres, qui sont la base de la programmation informatique, issu de système binaire².

Le terme digital remplacera progressivement, tout d'abord dans les milieux économiques, le terme numérique. Si les entreprises doivent absolument passer au digital, c'est parce qu'elles seraient trop lentes à évoluer. Elles croyaient s'être enfin adaptées au numérique, mais d'aucuns jugent cette adaptation non suffisante, et en viennent à utiliser le terme digital de façon à insister sur le caractère forcément nouveau de la situation. Bien que les mots « digital » et « numérique » possèdent une différence de signification, ils servent à désigner des procédés utilisés conjointement et fortement liés. En effet, la révolution digitale n'aurait jamais été possible sans la transition numérique. De ce fait, la transformation digitale qui a actuellement cours dans toutes les entreprises modernes utilise des procédés numériques.

Le terme digitalisation lui-même, qui au départ pourrait n'être qu'un anglicisme pour numérisation- mise sur support numérique- subit le même type de métonymie. On ne parle pas de digitalisation de documents et de livres, mais on exalte le fait que la digitalisation est une transformation totale de l'entreprise, le concept devient englobant, sans que l'on sache très bien sur quoi il porte³. A la vitesse d'internet et de la mondialisation qu'il induit, ce n'est plus la digitalisation des lignes de production ou des processus comptables de l'entreprise qui est visée, c'est la digitalisation de l'entreprise elle-même.

Par ailleurs, La numérisation de l'économie dépasse le simple emploi d'outils numériques⁴. L'essor du numérique facilite les interactions entre acteurs, et permet

¹« Quelle est la différence entre digital et numérique » consulté le 5-07-2022 à 10h sur <https://www.votre-it-facile.fr/quelle-est-la-difference-entre-digital-et-numerique/>

²Pour pouvoir être traitées par un ordinateur, les informations sont représentées de manière binaire, c'est-à-dire par un phénomène physique à deux états représentés symboliquement par les éléments binaires (*bits*, abréviation de *binary digits*) 0 et 1 (le courant passe ou ne passe pas, condensateur chargé ou déchargé, aimantation dans un sens ou dans un autre, etc.). Le mathématicien et philosophe allemand Gottfried Leibniz (1646-1716) est l'un des premiers à étudier la numération binaire et à envisager de coder des informations par ce système. Au XIX^e siècle le mathématicien anglais George Boole (1815-1864) développe une algèbre à base binaire (l'algèbre de Boole) qui fonde la logique moderne des propositions. Ces travaux sont à l'origine du traitement automatique des informations codées en binaire.

³A. MOATI, « Le numérique rattrapé par le digital ? », in *Le Débat*, N° 188, Janvier 2016, Gallimard, p.70.

⁴B. METTLING, *Rapport sur Transformation numérique et vie au travail*, 2015, p. 5.

d'optimiser la prise de décision et les processus de production¹. Peut-être voit-on apparaître ici une distinction entre numérique et digital. Le premier viserait ceux qui n'auraient pas fait d'efforts ou n'auraient pas compris l'enjeu : on leur enjoint de s'emparer du numérique. Le second viserait, de manière plus pernicieuse, ceux qui notamment dans le monde des entreprises, ont perçu l'enjeu et ont agi en conséquence, il ne suffit pas de s'installer dans le numérique, il faut passer à l'étape suivante, celle du digital. A la lumière de ces définitions, dans la présente étude, nous évoqueront la transformation digitale et la transformation numérique afin d'embrasser le concept dans sa totalité loin des définitions techniques.

Il est également important de bien souligner la différence entre l'ère des NTIC et celle du digital. Les TIC ou encore les NTIC² désignent en général, un ensemble de techniques innovantes dans le domaine de l'audiovisuel, de l'informatique et des télécommunications permettant le stockage, le traitement et l'obtention de l'information. Une fois combinées, les NTIC peuvent permettre non seulement le traitement de l'information, mais aussi la transmission de celle-ci. En effet, si les NTIC avaient permis de supporter avec efficacité les processus existants, la transformation digitale, elle, bouleverse ces mêmes processus pour supporter les nouvelles opportunités d'usage. Autrement dit, et en logique de transformation digitale, ce sont les nouvelles opportunités d'usage qui guident la mise en place des nouveaux processus, alors que les NTIC supportent ce qui existe déjà. C'est la logique de rupture qui se trouve au cœur de la transformation digitale.

La transformation digitale possède un sens très large. Elle consiste à permettre aux entreprises de s'adapter et de se développer en mettant en place de nouveaux processus qui reposent sur des techniques de pointe. Toutefois, cette transformation digitale est davantage liée à l'usage de l'électronique qu'au matériel en soi³. Les transformations sont des changements qui bouleversent une organisation sans pour autant que l'état à atteindre soit connu. Usuellement, les changements au sein des organisations sont classés en fonction de la cible qui est l'objectif visé, l'étendue qui est le périmètre concerné, la profondeur qui est le niveau d'impact, le rythme qui est la vitesse demandée pour le déploiement, le mode de gestion qui est la manière dont les différentes parties prenantes vont être impliquées, la

¹Modifiant de façon irréversible la manière dont les consommateurs et les entreprises s'informent, communiquent, produisent et commercent.

²Avec le temps et vu la fréquence fulgurante d'évolution des TIC, l'acronyme à évoluer pour devenir NTIC, le « N » pour attribuer le facteur de nouveauté presque constante.

³« Quelle est la différence entre digital et numérique » consulté le 30-07-2022 à 16h sur <https://www.votre-it-facile.fr/quelle-est-la-difference-entre-digital-et-numerique/>.

planification qui est la démarche d'implémentation¹. Sur la base de cette typologie, il est clair que la transformation digitale est bien une transformation.

La transformation digitale est maintenant reconnue comme un concept parapluie qui synthétise l'approche d'utilisation par les organisations des technologies numériques existantes et à venir pour ouvrir des voies à des manières nouvelles de travailler. L'aspect digital de cette transformation est bien identifié au travers de l'utilisation du *Web*, du *big data*, des réseaux sociaux d'entreprise, des terminaux mobiles, etc. Ainsi, si la transformation numérique agit sur le contenu de la transmission, elle agit aussi sur le droit qui est contraint de la prendre en compte et de s'y adapter tout en tentant de sauvegarder des principes antérieurs qui le fondent et le légitime. Le numérique n'est pas une zone de non droit. C'est au contraire un lieu de bouillonnement juridique, un champ délocalisé qui crée des règles juridiques ou adapte les règles traditionnelles à la technologie nouvelle².

En effet, au sein des sociétés développées, l'abondance s'est substituée aux carences. Dès lors qu'un certain niveau de culture et de richesse est atteint, une préoccupation élémentaire resurgit : la sécurité³. Celle-ci est la pierre angulaire de toute activité puisqu'elle consiste à minimiser les risques et garantir qu'aucun préjudice n'affecte la pérennité de l'activité.⁴ Or, l'approche technique du digital n'est pas sans failles, et l'aléa est omniprésent. D'où la nécessité aussi d'une approche juridique. De ce fait, accroître la sécurité juridique devient un enjeu majeur pour le développement de l'économie numérique⁵.

La sécurité juridique forme un concept à la fois universel et immuable. Elle constitue une exigence latente qui s'applique à l'ensemble des sociétés. De plus la société la plus élémentaire ne semble pouvoir s'en dispenser comme l'exprimait Carbonnier, « *c'est le besoin juridique élémentaire, et si l'on ose dire, animal* »⁶. La sécurité juridique se présente

¹D. MEINGAN, « Pourquoi parle-t-on de transformation dans la transformation digitale ? », in Questions de management, N° 7, Septembre 2014, EMS Editions, p. 164.

²Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, Le droit de l'internet dans l'entreprise, LGDJ, Paris, 2003, p. 5.

³Emma BEN MERZOUK-GLON, La sécurité juridique en droit positif, une valeur irréductible à la norme, Edition universitaires européennes, Saarbrücken, 2010, p. 11.

⁴C. EL OUFIR et A.DIK, « La complémentarité du droit et de la sécurité en matière informatique », in Revue Marocaine de Droit Commercial et des Affaires, N° 3, 2015, p. 33.

⁵Ibid., p. 38.

⁶Laurence BOY, Jean Baptiste RACINE et Fabrice SIRIAINEN, Sécurité juridique et droit économique, Larcier, Bruxelles, 2008, p. 6.

comme une notion récente, alors que certains de ses éléments constitutifs étaient déjà présents dans les premières sociétés organisées autour d'un droit essentiellement divin.

Ainsi, la recherche de sécurité juridique est aussi ancienne que le droit lui-même. Les premières codifications de Hammourabi¹ y sont inspirées, au moins en parties, par un sentiment d'accessibilité, de clarté et d'intelligibilité. De plus en droit romain, l'attachement de la supériorité de la loi écrite sur le droit coutumier et la lutte du peuple romain a abouti à la rédaction de la fameuse loi des douze tables, traduit à nouveau l'importance de la sécurité juridique à travers l'exigence de règles de droit claires, connues de tous, immuables et égales pour tous. Enfin, La dernière décennie a connu un regain en force. Le succès actuel de la sécurité juridique se manifeste par la fréquence à laquelle revient l'expression même dans le vocabulaire des juristes et des autorités publiques. Parmi les raisons de l'engouement actuel pour la sécurité juridique. Il y a, le développement de l'insécurité juridique et il y a aussi, les exigences contemporaines relatives au respect des droits de l'homme².

En réalité, appréhender la sécurité juridique est une tâche complexe, tant la notion est fuyante. Tournons-nous alors vers ce que renferme la notion de sécurité juridique pour mieux saisir l'enjeu du débat. La sécurité juridique est utilisée dans le vocabulaire de la doctrine au Maroc et même par le législateur. L'étude de sécurité juridique peut s'avérer fort utile. Toutefois, son explication en est plus complexe. Fréquemment indiqué dans le discours des juristes. Plus éprouvé par le sentiment d'insécurité juridique. Ce terme désigne, parfois, un danger réel, ou un simple sentiment de danger imminent³. La sécurité juridique est inhérente au droit lui-même, de ses modes d'expression et d'application, sans pour autant négliger les droits subjectifs des personnes.

D'un point de vue théorique, à l'instar de la justice et de l'égalité, la sécurité juridique constitue une finalité, un idéal. Ainsi l'impératif de sécurité semble se confondre avec la notion de droit elle-même. Ces finalités de droit peuvent parfois se joindre, parfois s'opposer. Du point de vue de la technique juridique, la sécurité renvoie à un contenu précis. Il s'agit dans ce cas des modes d'expression et de réalisation du droit qui forme la sécurité juridique proprement dite. Généralement, la doctrine s'accorde sur le fait que la sécurité juridique peut être scindée en trois subdivisions : l'accessibilité, la stabilité et la prévisibilité de droit.

¹Le code de Hammourabi daté d'environ 1750 avant .J-C et à ce jour le plus complet des codes de lois connus de la Mésopotamien antique.

²Emma BEN MERZOUK-GLON, *Op.cit.* , p. 19.

³Thomas PIAZZON, *La sécurité juridique*, Lextenso, 2^{ème} éd., Coll. de thèse, Paris, 2006, p. 3.

Tout d'abord l'accessibilité du droit. Cette dernière intéresse donc principalement les sources du droit, à savoir la loi et la jurisprudence. Il s'agit de l'accessibilité matérielle, mais aussi intellectuelle, c'est-à-dire l'intelligibilité des lois. L'accessibilité intellectuelle a pour but de faciliter au destinataire la compréhension du sens de la règle juridique. Si la première norme ne pose pas de problème¹, la seconde est beaucoup plus complexe². Ensuite, la sécurité juridique est entendue comme l'exigence de garantir la stabilité des situations juridiques dans le temps. Lorsqu'on se réfère à l'adage « Nul n'est censé ignorer la loi », c'est pour justifier le fait que chaque personne doit connaître la loi de manière à agir conformément au bien de la société. Pour cela, la règle de droit doit être permanente et demeure stable pour que l'on puisse facilement s'y référer.

En contrepartie, dans la logique des choses, la société évolue et le droit suit cette évolution. Les règles de droit posées par l'Homme pour le présent et l'avenir, en fonction d'une situation passée, changent, se transforment, sont abolies et tombent en désuétude. Il y a un temps pour le droit. A cet égard, l'exigence de stabilité paraît logique. Entre changement et rigidité, il faut donc trouver un juste milieu. La norme juridique nouvelle est censée constituer un progrès, un pas en avant dans la réalisation d'une plus grande justice. C'est justement pour cette raison que l'instabilité du droit ne concerne pas le changement en tant que tel de la règle de droit, mais concerne le changement récurrent qui devient source d'insécurité juridique.

On a évoqué auparavant que l'insécurité juridique peut renvoyer à un danger réel ou bien un sentiment d'insécurité. Pour Jean Carbonnier, on parle ici d'angoisse contemporaine qui se transforme en une sorte d'inquiétude et d'anxiété juridique. La sécurité juridique suppose dans ce cas l'exigence d'un développement continu et maîtrisé des normes juridiques, conciliant leur nécessaire mutabilité avec un impératif de stabilité. Ainsi, le changement répétitif du droit peut créer un malaise pour les chefs d'entreprises. Les besoins de stabilité pour l'entreprise se sont intensifiés essentiellement pour des raisons proprement économiques et financières. La doctrine est unanime pour conclure que les attentes des entreprises se sont amplifiées sous l'effet des imperfections de notre système de production et d'application du droit. Enfin, si la stabilité du droit renvoie vers le passé, la prévisibilité renvoie vers le futur.

¹L'accessibilité matérielle de la loi peut être traitée sous l'angle de savoir comment l'Etat diffuse au mieux les textes juridiques. En d'autres termes elle se rapporte à la possibilité de trouver physiquement le droit applicable.

²L'accessibilité de la norme suppose sa compréhension, et cela ne veut pas forcément dire la simplicité. Nonobstant le fait que cette dernière en droit doit être considérée comme une vertu, elle n'est pas une valeur en soi. L'usage de la langue courante en matière juridique présente bien des dangers. En effet, c'est la simplicité qui s'oppose à la complexité. En d'autres termes, la loi peut très bien être complexe, mais demeure intelligible.

Elle permet de bâtir les prévisions. A cette fin, le droit doit écarter toute incohérence et bannir toute solution floue.

Les différents composants de la sécurité juridique que nous avons étudiés de manière sommaire sont alors : l'accessibilité, la stabilité et enfin la prévisibilité¹. En se basant sur ces éléments, on pourrait d'ores et déjà essayer de donner une définition mais qui peut prendre deux sens. Ainsi, la sécurité juridique peut être objective ou subjective. Dans le premier sens, la sécurité concerne la qualité du système juridique et des sources de droit. En effet, le respect des principes tels la séparation des pouvoirs ou de la hiérarchie des normes montrent la cohésion du système juridique. Dans le même ordre d'idées, la qualité du système de production des normes, ou plus particulièrement des sources du droit, est un élément déterminant de sécurité juridique². Dans le deuxième sens, la sécurité juridique subjective concerne la situation concrète des individus. La sécurité dans cette hypothèse concerne l'étude au cas par cas des situations juridiques individuelles.

De plus, d'autres avancent sans trop de risques que la sécurité juridique génère une confiance légitime des destinataires de la norme. Le concept de confiance légitime est le corollaire du principe de sécurité juridique. Elle implique le respect de la confiance que les citoyens peuvent légitimement placer dans la stabilité de leur environnement juridique tel que déterminé et caractérisé par la puissance publique. Ainsi, La confiance légitime protège la personne qui est directement concernée et subit effectivement les conséquences désavantageuses de la sécurité juridique.

Au final pour éviter toute sorte d'ambiguïté entre la sécurité juridique objective et subjective, entre la sécurité juridique et la confiance légitime, nous proposons de donner une définition³ qui regroupe en même temps les généralités et les particularités des définitions évoquées plus haut. La sécurité juridique serait, donc, l'idéal d'un droit stable, accessible et intelligible permettant aux sujets de droit de savoir et prévoir, convenablement, leurs situations juridiques dans le temps, et à défaut de pouvoir faire valoir leurs droits devant un juge. Une entreprise doit être en mesure de connaître et de comprendre le droit applicable pour pouvoir agir en toute certitude et faire le pas vers la transformation digitale. En effet, un

¹M. NEGGAOUI, « La sécurité juridique en droit fiscal lecture comparative », in Revue scientifique arbitral semestrielle des études juridiques juridictionnelles et jurisprudentielles N°4, 2018, p. 30.

²On ne parle pas ici que de la qualité du droit, mais aussi de la qualité de sa diffusion. Sur ce point, on regrette la difficulté d'accéder aux décisions judiciaires au Maroc même pour les juristes, pour les contribuables, c'est une autre histoire.

³Nonobstant l'impossibilité de constituer une définition parfaite de la sécurité juridique.

droit inadapté à la réalité économique est aussi un frein à l'activité économique. Dans le même temps qu'elles dénoncent l'insécurité juridique, les entreprises ne cessent, au frê de l'évolution de leur activité, de demander des évolutions du système juridique¹.

La régulation des techniques par le droit est par définition instable puisqu'elle doit suivre l'évolution des techniques et s'adapter aux contingences sociales modernes, celles de l'individualisme et de la mondialisation en sorte qu'il en résulte « *l'impossibilité de réduire le droit de l'Internet à un corps de règles spécifiques préconstituées et prêtes à être appliquées à tel ou tel problème* »². Les évolutions juridiques sont le reflet des évolutions sociétales induites par la révolution numérique, « *Il s'agit pour le législateur d'accompagner l'évolution des pratiques en offrant un cadre régulateur apte à favoriser les pratiques considérées comme vertueuses et à décourager les pratiques considérées comme nuisibles* »³.

Dans ce contexte, d'un point de vu théorique, le digital induit des changements dans le droit. A l'instar des autres mutations dans les technologies, les phénomènes associés au numérique appellent à relire ou à comprendre le droit de façon différente. Cela ne devrait pas surprendre. Il serait en effet étonnant que tout ait vocation à changer dans la société sauf le droit. Aussi, plutôt que de se complaire dans le discours selon lequel le droit serait exempté des changements résultant des évolutions numériques, le juriste doit se donner les moyens de comprendre les dynamiques associées au digital.

L'intervention du droit trouve plusieurs de ses justifications dans la détermination des niveaux de risques acceptables dans les différentes interactions que requiert la vie économique. Le droit agit également afin d'assurer, voire de renforcer la sécurité nécessaire au déroulement des transactions. Il peut intervenir pour délimiter les risques des transactions. Le droit peut aussi intervenir afin de répartir les risques ou encore afin de renforcer ou d'assurer la sécurité juridique.

Le thème de la sécurité juridique apparaît en effet comme central dans le cadre du mouvement de la digitalisation de l'économie. Ce processus introduit nécessairement un nouveau besoin de sécurité juridique. La transformation digitale accroît la complexité et

¹Laurence BOY, Jean Baptiste RACINE et Fabrice SIRIAINEN, *Op. cit.* , p. 20.

²Jean-Michel BRUGUIERE, « Les conditions générales d'utilisation sur l'internet. Nouvelles réglementations de droit privé ? » in *L'entreprise à l'épreuve du droit de l'internet*, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014, p. 10.

³F. PELLEGRINI et S. CANEVET, « Le droit du numérique : une histoire à préserver », 2012, p. 74, consulté le 05-08-2022 à 10h sur <https://hal.inria.fr/hal-00768912/document>.

le désordre, conduit à un enchevêtrement des normes, suscite de nombreuses contradictions et génère des incertitudes. Le besoin est alors ressenti d'une sécurité juridique du numérique¹. La croissance formidable de l'activité économique sur l'internet justifie pleinement le thème de cette thèse axé sur l'entreprise, acteur économique essentiel. Un acteur confronté à des bouleversements importants de son théâtre d'opérations ; un écosystème nouveau apparaît avec des déplacements formidables de valeur qui s'opèrent au profit de nouveaux protagonistes².

Bâtir la sécurité de l'environnement en ligne constitue un défi mondial que le phénomène d'internationalisation du droit essaie d'encadrer, et ce malgré le problème de la souveraineté des Etats qui se pose avec les transactions électroniques en environnement ouvert³. Mais avant tout l'apparition de cette nouvelle technologie, qui génère des applications nombreuses et variées, ne va pas sans problème juridique qui provoque, du seul fait de la mondialisation, l'éclatement des référents juridiques nationaux.

D'un point de vue pratique, selon un rapport⁴ publié par la Banque mondiale qui relate les avantages du numérique pour les pays du Moyen-Orient et de l'Afrique du Nord. La région devrait être sur la bonne voie pour une véritable transformation numérique en utilisant l'internet et les applications de télécommunications qui permettent le commerce en ligne via les plateformes numériques accessibles sur internet ou en communiquant avec les clients par courrier électronique ou au moyen de *sites web*.

La région MENA compte plusieurs entreprises numériques prospères notamment *Careem*⁵ et *Souq*⁶ et de jeunes écosystèmes numériques pleins d'avenir notamment en Arabie saoudite, en Jordanie, et au Maroc. Mais la transformation numérique n'est pas pour demain. Le fait est que les pays de la région, notamment ceux à revenus faibles ou intermédiaires, progressent lentement sur la voie de l'économie numérique. La question fondamentale selon

¹Jean-Philippe Dom, *Op. cit.*, pp. 661-662.

²Jean-Michel Bruguière, *Op. cit.*, p. 2.

³C. EL OUFIR et A.DIK, *Op. cit.*, p. 36.

⁴A-P. CUSOLITO, C. GEVAUDAN, D.LEDERMAN et C-A. WOOD, "Les avantages du numérique pour les pays du Moyen-Orient et d'Afrique du Nord », Rapport de la Banque mondiale, 2021, p. 2.

⁵Careem est la plate-forme Internet pour la grande région du Moyen-Orient. Pionnier de l'économie de covoiturage de la région, Careem étend les services sur sa plate-forme pour inclure le transport en commun, la livraison et les paiements pour devenir la SuperApp quotidienne de la région. La mission de Careem est de simplifier et d'améliorer la vie des gens et de bâtir une organisation durable qui inspire. Careem a été créée en juillet 2012 et a été acquise par Uber en 2020. Careem opère dans plus de 100 villes de 14 pays et a créé plus d'un million d'opportunités d'emploi dans la région.

⁶Application d'achat et de vente en ligne mise en place dans la région MENA.

le rapport est de savoir la raison de cette longue progression. Le rapport explique alors que de nouvelles données indiquent que la région a un vaste programme de réformes à mettre en œuvre en ce qui concerne le cadre réglementaire du commerce en ligne, tout particulièrement la protection des consommateurs, la protection des données et la cybersécurité.

Le rapport examine trois piliers essentiels à la transformation digitale des entreprises. Il s'agit de l'infrastructure numérique, le système de paiements électroniques et le cadre de réglementation du commerce électronique. Sur ce dernier point les éléments de preuve dont on dispose jusqu'à présent suggèrent que les pays du Moyen-Orient et d'Afrique du Nord ont encore du pain sur la planche. Les pays à revenu intermédiaire de la région sont comparables à ceux d'autres régions, sauf dans les domaines de la signature électronique, de la protection de la confidentialité des données, de la protection des consommateurs en ligne et de la cybersécurité. En revanche, les pays à revenu élevé du Moyen-Orient et d'Afrique du Nord se comparent bien à ceux d'autres régions en ce qui concerne les documents électroniques et les signatures électroniques, mais sont en retard dans tous les autres domaines de la réglementation¹.

Au niveau national, le HCP a mené deux enquêtes² relatives à l'intégration des TIC au niveau des entreprises. Les résultats des enquêtes étaient comme suit. En dépit que les entreprises ont une bonne connectivité à Internet avec un taux de 81% en moyenne pour les TPE, 97,9% pour les PME et 99,5% pour les GE en 2019³, l'intégration des nouvelles technologies de l'information n'est pas encore complète au niveau des entreprises. Elle a été jugée élevée dans la gestion des activités pour 36% des entreprises en 2019, mais encore modeste dans leurs échanges. Plus de la moitié des entreprises ont jugé faible l'intégration des

¹A-P. CUSOLITO, C. GEVAUDAN, D.LEDERMAN et C-A. WOOD, *Op. cit.*, p. 55.

²La Première enquête, menée en 2019 auprès de 2101 entreprises qui exercent dans l'industrie, la construction, le commerce et les services marchands non financiers, visait à appréhender les activités des entreprises, dans leur diversité, et le contexte économique et social dans lequel elles opèrent et à accueillir leurs perceptions sur l'utilisation des nouvelles technologies. La deuxième enquête a été réalisée en décembre 2020 auprès de 3600 entreprises, afin d'évaluer les effets de la crise sanitaire Covid-19 sur leurs activités et d'accueillir leurs appréciations sur les perspectives d'évolution de l'activité, de l'emploi et de l'investissement en 2021.

³L'usage principal de connexion internet reste les échanges des e-mails opérés par 92% des entreprises. Les autres usages sont encore moins généralisés, notamment l'accès et la modification des documents qui ne sont pas exploités par 38% des entreprises et l'utilisation des logiciels professionnels spécialisés qui se limite à 59% d'entre elles.

TIC dans la gestion des ressources humaines, dans leurs échanges avec les administrations publiques, avec les fournisseurs et avec les clients¹.

Le recours des entreprises aux services externes d'informatique a été également moins fréquent. Seule 20% des entreprises ont utilisé ce genre de services pour le stockage de leurs informations en 2019, alors que l'hébergement de leurs bases de données n'a été opéré qu'au niveau de 18%. La part des entreprises qui ont effectué des achats de services informatiques à partir d'un logiciel de gestion financière au comptable s'est limitée à 26% et n'a pas dépassé 16% pour les logiciels de gestion de la relation-clientèle.

Aussi, en comparant, les entreprises marocaines avec d'autres entreprises étrangères quant à la disposition d'un site web, les entreprises qui disposaient de leur propre site web n'ont pas dépassé 31% en 2019, contre 49% en Turquie, 70% en France et 89% en Allemagne. Ce retard de numérisation était encore plus important au niveau des entreprises de taille moyenne ou petite qui constituent 93% de l'ensemble des entreprises au Maroc. Plus 3 TPME sur 5 ne disposaient ni d'un site web ni d'une page sur les réseaux sociaux². C'est vrai que l'usage des TIC s'est intensifié depuis l'enclenchement de la crise Covid-19 en 2020. Cependant, pour les entreprises privées, les motivations d'investissement en TIC en période de post-crise et les stratégies de transformation numérique sont encore très différenciées suivant les branches d'activités³.

En revanche, une dernière enquête⁴ intitulée « *Digital Trends Morocco 2023* » a été menée sur 52 annonceurs et s'est intéressée à différents axes parmi lesquels la fonction digitale au sein de l'entreprise, les objectifs escomptés de celle-ci, les outils et plateformes utilisés, le budget et ressources alloués à cette fonction, ainsi que les facteurs clés de succès du digital. Cette enquête a révélé que 100% des répondants disposent d'une activité digitale au sein de leur entreprise contre 81% en 2017 et 96% d'entre-deux orientent leur stratégie digitale vers les clients et les consommateurs. Pour ce qui est des canaux digitaux utilisés, ils ont tous

¹Ces entreprises étaient principalement jeunes âgé de création ne dépassant pas 10 ans. En revanche, les entreprises âgées de plus 20 ans ont déclaré une intégration plus élevée des TIC dans la gestion de leurs échanges avec les fournisseurs, les clients et les administrations publiques

²L'usage du site web pour le développement commercial des entreprises a été également limité : 4 entreprises sur 7 parmi les entreprises qui disposaient d'une page web n'ont pas effectué des commandes ou des paiements en ligne à partir de leur page web. 78% des entreprises l'utilisaient un site web pour décrire leurs biens et services commercialisés ou pour lister les prix.

³« Intégration des TIC au niveau des entreprises au Maroc », Rapport du Haut-Commissariat au plan, 2021.

⁴Enquête menée par l'entreprise de sondage IPSOS sur les tendances du digital au Maroc pour l'année 2022 et qui a été présenté à l'occasion de la 5^{ème} édition de « l'African Digital Summit 2023 ».

connu une augmentation de l'usage par rapport à 2017, notamment les sites web marchands utilisés par 60% des entreprises, les réseaux sociaux (98%), le marketing direct (92%), les sites web non marchands (88%) et les applications mobiles (65%).

Au volet financier, le budget du digital représente en moyenne 17% du budget marketing 2023, et 56% des panélistes envisagent d'augmenter ce budget de 19%, contre 26% qui compte maintenir inchangé le budget et 2% qui souhaitent le diminuer à l'avenir. La moitié des sondés cumulent, par ailleurs, la fonction digitale avec d'autres fonctions. A ce titre, 27% des interrogés prévoient de recruter des personnes affectées à l'activité digitale et 69% des entreprises ont recours à des formations dans le digital. L'enquête conclut, par ailleurs, que les principaux leviers de développement du digital s'articulent autour de l'expertise (75%), le budget (63%) et aussi le soutien du Top management des entreprises (60%)¹.

Le Maroc conscient de ces résultats, a mis en place plusieurs programmes nationaux pour soutenir le développement du digital. Le pays souhaite donner un nouvel élan à la transformation digitale et promouvoir un développement volontariste et ambitieux des secteurs technologiques. Ce développement du digital engendre une multiplication d'échanges et de transactions électroniques, requérant l'élaboration d'un cadre réglementaire approprié, portant d'une part sur les aspects juridico-techniques intrinsèques au développement de ces échanges, et d'autre part, sur la protection des libertés individuelles et la lutte contre la cybercriminalité, autrement dit assurer une sécurité juridique. C'est tout l'intérêt de notre sujet, celui de déceler la portée et l'impact des interactions entre sécurité juridique et transformation numérique au sein des organisations. En effet, le contenu du cadre réglementaire du numérique est tiré d'au moins deux sources, la technique elle-même et les besoins des acteurs notamment les entreprises, tels que manifestés par eux ou supposés par les décideurs.

A titre de droit comparé, le numérique avant était considéré comme une sorte de « Far West Juridique », un secteur où tout était encore possible. Pourtant, les problématiques juridiques existaient déjà bel et bien. Tous les domaines du droit étaient touchés : la propriété intellectuelle, avec le développement de la contrefaçon dans l'univers numérique, la responsabilité civile, avec la question des obligations à la charge des prestataires techniques, les données personnelles, etc. Les seules règles étaient celles que se

¹IPSOS, « Digital Trends Morocco 2023 », 13 February 2023.

fixaient eux-mêmes les internautes de l'époque, précurseurs du réseau. En effet, face à un monde d'internet toujours plus mouvant, il est délicat pour le législateur de prendre des initiatives. Le temps législatif s'adapte mal à l'extrême évolutivité des technologies et des modèles économiques de l'internet. De plus, le risque est grand que les lois édictées soient volatiles¹.

Pendant un temps relativement bref, on considéra que l'internet n'était en lui-même soumis à aucune autorité : il devait être un espace virtuel de liberté. Or, la réalité juridique est bien différente. Le temps n'est plus ou certains ont cru pouvoir accorder quelque crédit à la Déclaration d'Indépendance du Cyberspace², aux termes de laquelle : « *Vos concepts juridiques ne s'appliquent pas à nous. Ils sont basés sur la matière. Il n'y a pas de matière ici* »³. Aujourd'hui, comme hier d'ailleurs, le droit s'applique à cet espace. Il n'y a pas de vide juridique⁴. La question était de savoir comment appréhender l'entreprise numérique pour la rattacher à un ordre juridique ? Différents pays ont doté leur arsenal juridique de dispositions spécifiques pour assurer la sécurité juridique dans l'économie numérique. Ces dispositions ont trait à plusieurs aspects et reflètent le même principe philosophique d'instauration de sécurité⁵.

De nombreux Etats ont au cours des deux dernières décennies, mis à profit la vague du digital pour mettre en place un cadre et des leviers incitatifs, accélérant ainsi l'accès à la digitalisation au niveau des entreprises. Ces programmes nationaux menés par les Etats leur ont permis d'avoir un impact significatif en matière de développement économique et social. Le législateur communautaire, bien conscient de l'enjeu des problématiques numériques, abordait déjà la question de la sécurisation des transactions dans l'univers des réseaux informatiques et adoptait, le 13 décembre 1999, la directive sur la signature électronique⁶.

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Le droit de l'internet : Lois, contrats et usages*, Lexis Nexis, 2^{ème} éd, Paris, 2013, p. 2.

²La Déclaration d'indépendance du cyberspace est un texte célèbre rédigé le 8 février 1996 à Davos en Suisse par John Perry Barlow, écrivain, militant et co-fondateur de l'Electronic Frontier Foundation. Il soutient l'idée qu'aucun gouvernement (ou qu'aucune autre forme de pouvoir) ne peut s'imposer et s'approprier Internet, alors en pleine extension. Il a été écrit en partie en réponse à l'adoption de la Loi sur les télécommunications de 1996 (*Telecommunications Act*) aux États-Unis.

³John Perry BARLOW, « Déclaration d'indépendance du cyberspace » in *Libre enfant du savoir numérique*, Ouvrage collectif sous la direction d'Olivier BLONDEAU, L'Eclat, Paris, 2000, p. 47.

⁴Eric CAPRIOL, *Droit International de l'économie numérique*, Lexis Nexis, Litec, 2^{ème} éd., Paris, 2007, p. 6.

⁵C. EL OUFIR et A.DIK, *Op. cit.*, p.38.

⁶Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.

Aussi, la directive relative à la protection des données personnelles¹ a également joué un grand rôle dans la construction du droit de l'internet, essentiellement, grâce au travail d'adaptation de la Commission nationale de l'informatique et des libertés (CNIL). Toutefois cette directive a atteint ses limites, notamment au regard du développement de l'internet, puisqu'un projet de règlement européen révisant la directive a vu le jour, il s'agit du Règlement général sur la protection des données (RGPD)². L'objectif du RGPD est de moderniser le cadre juridique de la protection des données personnelles. Le choix de l'institution législative n'est pas anodin : le règlement européen, d'application directe dans l'ensemble des Etats membres de l'Union européenne, permettra de renforcer l'harmonisation nationale mais aussi l'effectivité des dispositions. Par ailleurs, en France, plusieurs lois ont vu le jour tel que la loi informatique et Libertés du 6 Janvier 1978³, ou encore la loi pour la confiance dans l'économie numérique du 21 Juin 2004⁴ qui règle de nombreuses questions relatives au droit du commerce électronique ainsi que la loi du 1^{er} août 2006⁵ relative au droit d'auteur et aux droits voisins dans la société de l'information⁶.

Au niveau du continent Américain, et plus spécialement aux États-Unis, de nombreuses lois encadrent internet, la sécurité des données et la confidentialité. La loi *Privacy Act*⁷ de 1974 étant sans doute à la base de toutes. Cette loi a été adoptée pour contrôler la collecte, la maintenance, l'utilisation et la diffusion des informations personnelles par des agences du pouvoir exécutif du gouvernement américain. Aussi, La loi *Electronic Communications Privacy Act* (loi sur la protection des communications électroniques) a été adoptée en 1986. Cette loi autorise le gouvernement américain, grâce à un mandat, à accéder à des communications numériques telles que des messages électroniques, des messages sur les réseaux sociaux, des informations contenues dans des bases de données de *Cloud* public et bien plus. En 2015, une législation a été adoptée relative

¹Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

²Règlement (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).

³Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

⁴La loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, transpose la directive européenne sur le commerce électronique.

⁵Loi n° 2006-961 du 1 août 2006 relative au droit d'auteur et aux droits voisins dans la société de l'information.

⁶Eric CAPRIOL, *Op. cit.*, p. 2.

⁷Loi sur la protection de la vie privée.

au *Cyber Intelligence Sharing And Protection Act* (CISPA). Elle permet d'expliquer comment partager des informations sur des cybermenaces potentielles avec le gouvernement fédéral. Il existe également des lois relatives au partage des informations à l'échelle internationale, telles que l'accord de partenariat transpacifique. Cet accord concerne neuf pays du Pacific Rim, notamment le Pérou, le Chili et les États-Unis. L'accord avec l'United States Trade Office offre des avantages, particulièrement en ce qui concerne les accords commerciaux.

Malgré la lente mais sûre progression de la législation en Europe et aux États-Unis dans ce domaine, ces textes n'ont pas réglé toutes les questions à eux seuls, ne serait-ce que parce que l'internet ne s'arrête pas aux frontières d'un pays¹. Les échanges électroniques générés sur les réseaux numériques possèdent intrinsèquement en germe l'internationalité, même si la plupart des transactions commerciales s'effectuent encore sur le plan local. Ils tendent à renouveler les problématiques juridiques internationales. En effet, les relations qui se nouent via les réseaux numériques font fil des notions d'espace et de temps, des territoires et des frontières étatiques. Les échanges sont quasi instantanés et peuvent être initiés de n'importe quel point du globe. Les États, conscients du phénomène, tendent à agir sur ces paramètres en localisant responsabilité des personnes qui fournissent des services électroniques dans l'économie numérique et en régulant la circulation transfrontière des données qui s'opèrent en un trait de temps relativement bref et qui ne permet donc plus un contrôle physique, il faut agir en amont, poser un cadre normatif².

Au Maroc, le processus historique de la sécurité juridique du numérique n'est pas différent de celui de la plupart des pays. Au milieu des années 1990, aucun texte de droit ni aucune décision de justice n'évoquaient encore l'Internet ou le numérique. Mais le besoin s'est fait sentir de faire le pas vers une réglementation de l'économie numérique. Tout d'abord, il y a eu l'adoption de la loi n°24-96³ relative à la poste et aux télécommunications qui a consacré la libéralisation du secteur, suivie par la création de l'Agence Nationale de Réglementation des Télécommunication (ANRT) le 26 Février 1998.

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 4.

²Eric CAPRIOL, *Op. cit.*, pp. 4-5.

³Dahir n° 1-07-43 du 28 rabii I 1428 (17 avril 2007) portant promulgation de la loi n° 29-06 modifiant et complétant la loi n° 24-96 relative à la poste et aux télécommunications.

La loi n°24-96 a connu plusieurs modifications, la dernière date de 2019 par l'adoption de la loi n°121-12¹.

Le cadre juridique du numérique au Maroc ne s'est pas limité aux télécommunications. En effet plusieurs lois ont vu le jour pour combler le vide juridique causé par l'introduction du digital. Les premières lois qui ont suivi la libéralisation du secteur des télécommunications sont la loi n°34-05² modifiant et complétant la loi n°2-00 relative aux droits d'auteur et droits voisins³ et la loi n°53-05⁴ relative à l'échange électronique des données juridiques. Ainsi que la loi n°31-08⁵ relative à la protection du consommateur, qui inclut des dispositions relatives à la vente en ligne. Conscient de l'usage du numérique et soucieux d'instaurer un climat de sécurité juridique, le législateur a complété le Code pénal en adoptant la loi n° 07-03⁶ qui réglemente les infractions relatives aux systèmes de traitement automatisé des données.

S'ensuit une panoplie de lois comme la loi n°09-08⁷ relative à la protection des personnes physiques à l'égard des traitements de données personnelles, et dans l'objectif de contrôler les données du cybercommerçant, le décret d'application⁸ de la loi n°09-08 est venu mettre en place la Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel. Aussi le projet de loi n°67-13 formant Code du numérique qui ambitionne de s'inscrire efficacement dans le paysage des technologies de l'information et de la confiance numérique au Maroc⁹.

¹Dahir n° 1-19-08 du 18 joumada I 1440 (25 janvier 2019) portant promulgation de la loi n°121-12 modifiant et complétant la loi n°24-96 relative à la poste et télécommunication.

²Dahir n°1-05-192 du 15 moharrem 1427 (14 Février 2006) portant promulgation de la loi n° 34-05 modifiant et complétant la loi n°2-00 relative aux droits d'auteur et droits voisins.

³Dahir n° 1-22-35 du 23 chaouel 1443 (24 mai 2022) portant loi n° 66-19 modifiant et complétant la loi n° 2-00 relative aux droits d'auteur et droits voisins.

⁴Dahir n° 1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la loi n° 53-05 relative à l'échange électronique de données juridiques.

⁵Dahir n° 1-11-03 du 14 rabii I 1432 (18 février 2011) portant promulgation de la loi n° 31-08 édictant des mesures de protection du consommateur.

⁶Dahir n° 1-03-197 du 16 ramadan 1424 (11 novembre 2003) portant promulgation de la loi n° 07-03 modifiant et complétant le Code pénal.

⁷Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

⁸Décret n° 2-09-165 du 25 joumada I 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel.

⁹Le code du numérique est retiré de la liste des avant-projets publiés par le secrétariat général du gouvernement : Le débat est déclenché depuis le dévoilement du texte de l'avant projet de loi formant code du numérique et s'est attiré beaucoup de critique sur la toile marocaine.

Le Maroc a adopté durant la dernière décennie plusieurs programmes nationaux pour le développement du digital. Cependant, la mise en œuvre de ce programme a présenté des défis et des difficultés majeurs, parmi lesquels les barrières réglementaires ne permettant pas la mise en œuvre effective et l'usage à grande échelle des plateformes digitales. Le Maroc veut promouvoir un développement volontariste et ambitieux des secteurs technologiques. Le pays est aujourd'hui déterminé à s'inscrire dans la révolution digitale mondiale, principal moteur du développement humain et économique des pays en forte émergence. De ce fait, et en vue d'ancrer son ambition dans le domaine du digital, le législateur marocain a adopté trois nouvelles lois pour accroître la sécurité juridique du monde numérique. Il s'agit de la loi n°43-20¹ relative aux services de confiance pour les transactions électroniques, la loi n°05-20² relative à la cybersécurité ainsi que la loi n° 95-17³ relative à l'arbitrage et la médiation conventionnelle qui prend en compte les avancées technologiques en matière d'arbitrage.

Par ailleurs, le Maroc s'est doté d'un établissement stratégique dédié au digital, l'Agence de Développement du Digital (ADD), créée en vertu de la loi n° 61-16⁴ en 2017. L'ADD est en charge de mettre en œuvre, pour le compte de l'Etat, la stratégie digitale du Maroc et de proposer au gouvernement les orientations générales à suivre en matière de développement du digital pour définir une vision claire, objective et intégrée, en cohérence avec les stratégies sectorielles et territoriales en cours⁵. Ainsi, une note d'orientations générales pour le développement du digital au Maroc à l'horizon de 2026 a été publiée en 2020 par l'ADD. Cette note a pour objectif de clarifier les orientations stratégiques du gouvernement marocain pour le développement du digital au cours de cinq années, dans un contexte national et international en profonde mutation sur les sujets de transformation technologiques et digitale.

¹Dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020) portant promulgation de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques.

²Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité.

³Dahir n° 1-22-34 du 23 chaoual 1443 (24 mai 2022) portant promulgation de la loi n° 95-17 relative à l'arbitrage et à la médiation conventionnelle.

⁴Dahir n° 1-17-27 du 8 hija 1438 (30 août 2017) portant promulgation de la loi 61-16 portant création de l'Agence de développement du Digital.

⁵Une note d'orientations générales pour le développement du digital au Maroc à l'horizon de 2026 a été publiée en 2020 par l'ADD. Cette note a pour objectif de clarifier les orientations stratégiques du gouvernement marocain pour le développement du digital au cours de cinq années, dans un contexte national et international en profonde mutation sur les sujets de transformation technologiques et digitale.

Le Nouveau Modèle de Développement du Maroc place le pari audacieux pour le pays de devenir une nation numérique, où le potentiel transformationnel des technologies numériques est pleinement mobilisé. Au premier rang des principaux paris d'avenir à relever pour en faire un pôle économique et de savoirs parmi les plus dynamiques et les plus attractifs de la région et du continent.¹ Toutefois, la digitalisation est avant tout une transformation dont le principal facteur clé de réussite est le développement d'une culture du changement au niveau de l'administration. Afin d'accompagner les entreprises marocaines dans la réussite de leur transformation digitale, l'Etat marocain doit, avant tout, s'impliquer dans la digitalisation de ses services administratifs publics. Parmi les leviers de cette transformation citons à titre d'exemple : le développement de l'e-administration, le renforcement de l'infrastructure numérique par la stimulation de très haut débit et la sécurisation des échanges et paiements, l'amélioration de l'e-commerce via l'instauration de marchés de produits et services numériques, etc.

La transformation digitale gouvernementale et de gouvernance est primordiale. L'acquisition d'une telle maturité digitale par les pouvoirs publics s'accompagnera assurément d'une transformation digitale des entreprises marocaines privées, moteur de compétitivité, de rentabilité, d'agilité et d'inclusion. Pour mettre en œuvre cette vision, il faut mettre en place un environnement favorable au développement du digital, qui repose sur une meilleure adaptation du cadre réglementaire et garantir une sécurité juridique.

C'est presque une évidence de dire et d'écrire que la transformation numérique a confronté le droit à de nouveaux défis qui ont provoqué en retour une modification de ces règles. Le bouleversement serait aussi profond qu'il ne susciterait pas une adaptation simplement technique de la règle de droit au numérique, mais atteindrait son cœur même. Les principes juridiques seraient contraints d'évoluer sous la pression de nécessités nouvelles. Il faudrait forger des concepts nouveaux à même de saisir un phénomène nouveau².

Il serait alors intéressant de voir la réaction du droit face à la transformation numérique des entreprises, mais aussi la manière dont le numérique converge vers le droit. D'ailleurs, l'enjeu ultime du droit devient de plus en plus la construction d'une sécurité

¹Direction de l'économie numérique, « Missions et axes phare de l'économie numérique », consulté le 15-07-2022 à 10h sur <https://www.mmmp.gov.ma/fr/economie-num%C3%A9rique>

²W. DROSS, « L'encadrement des technologies par le droit : nécessité et source de changements », in Revue du Notariat, N° 3, 2004, p. 343.

juridique au service des entreprises souhaitant franchir le pas vers la digitalisation. De nombreuses propositions de lois qui ont émergé ces dernières années interrogent systématiquement sur leur pertinence dans un contexte d'inflation législative.

Ceci étant dit, la présente thèse retiendra la transformation numérique comme l'introduction d'éléments numériques dans l'entreprise. Ces éléments numériques produisent un impact sur la fonction du juriste au sein de l'entreprise et l'invite à collaborer avec le législateur ainsi que l'utilisateur pour assurer une sécurité juridique. Dans ce contexte, durant notre analyse une question revenait assez souvent à savoir, est ce que les lois adoptées par le législateur qui sont les outils de travail du juriste procurent une sécurité juridique aux entreprises en phase de transformation digitale ?

En effet, d'importants efforts ont été entrepris par le législateur au niveau national comme au niveau international dans la légifération en matière numérique et qui sont au service de l'entreprise en phase de digitalisation. Dans ce cadre, nos hypothèses de recherche portent sur l'impact de la transformation digitale sur la vie de l'entreprise ainsi que sur son environnement externe, les différents instruments digitaux qui sont au service de l'entreprise et enfin, la responsabilité et la résolution des litiges nés du numérique. La sécurité juridique de la transformation numérique des entreprises, dans ses effets, ses risques mais aussi ses opportunités, s'analyse de manière binaire.

Dans un premier temps, sous l'angle des mesures internes de sécurité juridique qui sont en intersection avec le droit de travail, le droit des sociétés, le droit de la propriété intellectuelle, et le droit des contrats. Cette thèse sera l'occasion d'aborder la transformation digitale des entreprises et ses mesures de sécurité juridique internes. (Première partie).

Dans un second temps, la transformation digitale touche la relation de l'entreprise avec son environnement externe que ce soit les autres concurrents ou l'administration ce qui peut engager sa responsabilité et donner lieu à des litiges. Il sera donc opportun de traiter la transformation digitale des entreprises et ses mesures de sécurité juridique externes (Deuxième partie).

Partie I

La transformation digitale des entreprises et ses mesures de sécurité juridique internes

Le monde n'a jamais été autant connecté. L'économie numérique est aujourd'hui un phénomène planétaire. Depuis les produits personnels jusqu'aux systèmes industriels complexes. Le digital est partout. L'entreprise ne fait pas exception¹, parler de transformation digitale en entreprise c'est parler de conduite de changements liés à la mise en œuvre des technologies digitales dans toutes les strates de l'entreprise. La digitalisation croissante a nécessairement un effet profond sur la manière dont les entreprises vivent et travaillent et transforme de plus en plus la manière dont les entreprises doivent opérer et proposer leurs services aux clients.

Personne ne doute aujourd'hui du bienfait de la transformation digitale dans la vie des entreprises au monde, engagées dans la compétitivité sur le plan national et international. En effet, le digital permet à l'entreprise de se construire une identité numérique, de se bâtir une e-réputation qui participe à son image et revêt de plus en plus une valeur patrimoniale². Mais si la technologie offre un avantage, le professionnel doit souvent intervenir en appui de cette technologie pour qu'elle soit efficace³.

Ainsi, la transformation numérique nécessite des compétences et une formation chez le juriste. Il est évident que les juristes doivent avoir la possibilité d'apprendre à utiliser les nouveaux outils du numérique pour comprendre leurs implications et leurs potentialités. Il faut permettre au juriste de se former à l'utilisation des algorithmes, d'une *blockchain* ou de *smart contract*. Cette formation des professionnels du droit est seule à même de permettre une bonne compréhension des outils, mais également d'appréhender ceux-ci pour garantir une sécurité juridique. En effet, les différents travaux de recherche consacrés au digital ont bien montré que la question essentielle aujourd'hui est avant tout liée à la sécurité juridique du digital. L'outil, la technique ou la technologie, c'est une chose, mais surtout la question de sécurité qui est primordial.

On constate que de sa rencontre avec le numérique, la sécurité juridique de l'entreprise ne ressort jamais intact. Le digital constitue aujourd'hui un facteur nouveau puissant de changement ou d'évolution de la sécurité juridique interne à l'entreprise⁴. Sans doute

¹S. FRIMOUSSE et J-M. PERETTI, « Comment accompagner la transformation digitale des entreprises en Afrique ? », in Questions de management, N° 8, Mars 2017, EMS Editions, p. 199.

²Jean-Michel Bruguière, *Op. cit.*, p. 155.

³B. DEFFAINS, « Le monde du droit face à la transformation numérique », in Pouvoirs, N° 170, Mars 2019, Seuil, p. 54.

⁴Y. PECH, « Vers une intelligence cyber ? », in Prospective et stratégie, N° 10, Janvier 2019, APORS Editions, p. 74.

la sécurité juridique réclamée sera différente suivant que son besoin est affirmé par les créateurs de l'entreprise ou les collaborateurs, ou encore les consommateurs concernés par leurs données circulant sur internet. Cela est important pour notre propos, la sécurité obtenue par le numérique ne sera pas de la même nature que celle projetée par les législations et cela risque de fausser les équilibres consacrés par le droit. L'impression générale qui se dégage est celle de la réforme permanente du droit confronté au numérique. Ainsi de nouvelles lois sont dans les tuyaux, d'autres sont sur la sellette¹.

Ainsi, la mise en œuvre d'une transformation digitale nécessite des mesures de sécurité juridique internes à l'entreprise. Cette sécurité doit être présente au moment de la création numérique de l'entreprise, dans sa relation avec ses salariés, ainsi que les différents instruments digitaux qu'elle utilise : contrats numériques, site web, créations numériques, etc.

En admettant que le digital va tout changer dans l'entreprise², il nous reste à déterminer à quel degré et de quelle manière ? D'où la nécessité de s'intéresser à l'impact de la transformation digitale sur la vie de l'entreprise (Titre I). Ce qui fait vraiment la spécificité de la transformation digitale de l'entreprise, ce sont les instruments digitaux auxquels elle fait appel pour contractualiser en ligne et protéger ses créations numériques (Titre II).

¹J-B. THOMAS-SERTILLANGES, « Droit et Technologies : Concilier l'Inconciliable ? », in Les Cahiers du numérique, vol. 10, Février 2014, Lavoisier, p. 21.

²F. GEUZE, « Trois points clefs pour accompagner la révolution digitale » in Questions de management, N° 7, Septembre 2014, EMS Editions, p. 164.

Titre I

L'impact de la transformation digitale sur la vie de l'entreprise

La transformation digitale agit sur la vie de l'entreprise et représente une chance inouïe pour la transformation et la mise à niveau des entreprises, l'automatisation des outils constitue un levier à forte valeur ajoutée pour les entreprises. En effet, parler de transformation digitale en entreprise c'est parler de conduite de changements liés à la mise en œuvre des technologies digitales dans toutes les strates de l'entreprise¹. Cette mise en œuvre porte non seulement sur les conditions de travail des salariés mais également sur la gouvernance de l'entreprise.

D'une part, la transformation digitale influence non seulement les fonctions fondamentales de l'organisation, mais également tous les niveaux hiérarchiques, y compris les directions générales et les conseils d'administration². Elle accompagne en plus l'entreprise depuis sa création jusqu'à sa disparition en passant par sa gouvernance ainsi que sa e-réputation. D'autre part, la digitalisation offre l'opportunité de transformer les pratiques en matière d'analyse de la contribution de chaque salarié en entreprise. Autrement dit, c'est une occasion appropriée pour façonner massivement les salariés au numérique et leur attribuer des compétences nécessaires permettant de les aider à affronter aisément le monde très dynamique du travail et surtout à devenir des employés adaptés aux mutations de l'entreprise digitale.

Compte tenu de l'impact de la transformation sur la vie de l'entreprise. Le développement des nouvelles technologies favorise donc des transformations remettant en cause les catégories par lesquelles on avait l'habitude de définir les cadres juridiques de plusieurs activités. Cette mutation ne peut manquer d'avoir des effets sur le droit et notamment le droit des sociétés et le droit du travail. Les conditions engendrées par les nouvelles technologies appellent une révision des paradigmes à partir desquels le droit est généralement envisagé.

¹S. FRIMOUSSE et J-M. PERETTI, *Op. cit.*, p. 202.

²Christophe COUPEZ, *Le digital interne en entreprise*, Mardaga, coll. Gestion, Entreprise, Finance, Paris, 2019, p. 29.

C'est dans cette optique qu'il serait opportun de mettre la lumière sur l'intégration du digital au droit des sociétés (Chapitre 1), ce qui permettrait par la suite de dégager la relation du numérique avec la transformation des conditions de travail au sein de l'entreprise (Chapitre 2).

Chapitre I

L'intégration du digital au droit des sociétés

L'une des préoccupations majeures du législateur marocain ayant été, ces dernières années, d'adapter le droit en vigueur au numérique, notamment le droit des sociétés. Le digital procure plusieurs avantages au droit des sociétés notamment en matière de création, et de gouvernance et même de disparition. Cependant, l'opportunité que peut offrir le recours à la technologie digitale ne doit pas devenir un facteur de risque supplémentaire pour l'entreprise¹.

Notre droit des sociétés a commencé à intégrer des dispositions nouvelles qui tendent à faciliter le recours par les sociétés aux moyens offerts par les technologies digitales. Et les outils numériques sollicités sont de plus en plus diversifiés, courrier électronique, vote électronique, numérisation des documents, visioconférence, etc. Le recensement des dispositions actuelles du droit des sociétés intéressant le domaine du numérique permet non seulement de relever les ambitions nourries par le législateur dans cette matière, mais aussi de saisir les lacunes et enjeux de cette démarche.

En effet, le recours au numérique en droit des sociétés, permet d'une part, de faciliter les relations que les sociétés entretiennent avec l'administration en générale. D'autre part, l'ambition présidant au développement du numérique dans le droit des sociétés réside dans le souhait du législateur de saisir les opportunités offertes par les nouvelles technologies de communication pour, à la fois, simplifier la vie interne des entreprise et, en même temps, renforcer l'effectivité des droits attribués par la loi aux acteurs sociétaires.

Il reste que, au-delà de cette double ambition, l'opération de recensement des dispositions légales et réglementaires relevant du droit des sociétés et participant à l'adaptation des sociétés au numérique, fait naître un sentiment mitigé entre les services et enjeux procurés par le numérique au droit des sociétés². Dans ce mouvement global, comment le droit des sociétés appréhende-il, cette révolution numérique ? Commencer par l'étude de l'entreprise face aux services numériques (Section 1) nous permettra par la suite de soulever la question des enjeux du numérique au sein de l'entreprise (Section 2).

¹Jean-Marc MOULIN, « Numérique et droit des sociétés » in *L'entreprise face aux défis du numérique*, Ouvrage collectif sous la direction d'Jean-Marc MOULIN, Sylvain CHARTRY et Alexandre RIERA, Mare&Martin, Paris, 2018, p. 18.

²Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, *Op. cit.*, p. 108.

Section 1 : L'entreprise face aux services du numérique.

La révolution numérique n'est pas cottonnée à quelques *startups* ou quelques mastodontes transnationaux de l'économie numérique ; elle attire dans son lit de jeunes sociétés innovantes comme des entreprises matures relevant de domaines d'activités traditionnels¹. Qu'il s'agisse de la création de l'entreprise, de la tenue du registre de commerce numérique, du fond de commerce électronique, de la gouvernance de l'entreprise ou autres, le numérique est partout et entre toujours plus en contact avec l'entreprise dans toutes ses fonctions, cela quelle que soit la taille ou le secteur de l'activité de l'entreprise.

Ainsi, les technologies numériques ne se sont pas contentées de transformer la manière dont les entreprises travaillent, elles affectent tout le mode de vie depuis la création. Pour comprendre les différents services procurés par le numérique aux sociétés, il convient d'étudier la création de l'entreprise par voie électronique (Sous-section 1) avant de s'étaler sur le rôle du numérique dans la gouvernance de l'entreprise (Sous-section 2).

Sous-section 1 : Création et accompagnement de l'entreprise par voie électronique.

Dans le cadre de l'amélioration du climat des affaires et l'accompagnement des entreprises dans leurs processus de digitalisation , le Maroc a procédé à une nouvelle réforme du cadre juridique régissant la création d'entreprise, portant particulièrement sur l'instauration de la voie électronique pour toutes les démarches liées à la création d'entreprises et aux opérations postérieures tel que l'inscription au registre de commerce. Trois lois ont ainsi été promulguées : la loi n° 88.17 relative à la création et à l'accompagnement d'entreprises par voie électronique², la loi n° 87.17 modifiant et complétant la loi n°13.99 portant création de l'Office Marocain de la Propriété Industrielle et Commerciale (OMPIC) ³; et la loi n° 89.17 modifiant et complétant la loi n°15.95 formant Code de Commerce⁴.

Nous allons traiter successivement, les modalités de création de l'entreprise par voie électronique (Paragraphe 1). Ensuite, la tenue d'un registre de commerce dématérialisé

¹François LEVEQUE, Les entreprises hyperpuissantes, Odile Jacob, Paris, 2021, p. 181.

²Dahir n° 1-18-110 du 2 jourmada I 1440 (9 janvier 2019) portant promulgation de la loi n° 88-17 relative à la création d'entreprises par voie électronique et leur accompagnement.

³Dahir n° 1-18-79 du 23 kaada 1439 (6 Aout 2018) portant promulgation de la loi n° 87-17 modifiant et complétant la loi n° 13-99 portant création de l'Office marocain de la Propriété Industrielle et Commerciale.

⁴Dahir n° 1-18-110 du 2 jourmada I 1440 (9 janvier 2019) portant promulgation de la loi n°89-17 modifiant et complétant la loi n° 15-95 formant code de commerce.

(Paragraphe 2). Enfin, la consécration et la reconnaissance du fonds de commerce électronique (Paragraphe 3).

Paragraphe 1 : La création d'entreprises par voie électronique.

Le Maroc a adopté en Janvier 2019 la loi n°88-17 relative à la création et l'accompagnement d'entreprises par voie électronique. Ce texte de loi vise à simplifier les démarches et réduire les délais des différentes étapes de constitution et de création d'entreprises afin de promouvoir les investissements aussi bien à l'échelle nationale qu'à l'échelle internationale, l'amélioration du climat des affaires ainsi que le développement du classement du Maroc dans les organismes internationaux , plus particulièrement ceux relatifs à l'Indice de Création des Entreprises (IEC) adopté par la Banque mondiale¹.

Cette loi concerne le développement d'une plateforme en ligne dédiée à la création d'entreprise. Son objectif est opté pour la voie électronique en tant que seul moyen pour effectuer les procédures liées à la création d'entreprises en ligne, et ce en déposant tous les contrats, décisions, états de synthèse, procès-verbaux des délibérations, documents et décisions judiciaires sur la plateforme électronique².

Selon l'article premier de la loi n° 88-17, il est prévu la création d'une plateforme électronique dénommée : « Plateforme électronique de création et de l'accompagnement d'entreprises par voie électronique ». La gestion, l'exploitation et la tenue de la base de données de cette plateforme sont assurées par l'Office Marocain de la Propriété Industrielle et Commerciale (OMPIC). Cette plateforme permettra à l'OMPIC, aux particuliers et professionnels d'obtenir en toute sécurité les données concernant les entreprises et de les suivre³.

En effet à travers la plateforme, le déclarant de la création d'entreprise doit obligatoirement effectuer toutes les démarches légales requises pour la création de

¹ADD, Note d'Orientations Générales pour le Développement du Digital au Maroc à horizon 2025, Mars 2020.

²« Création en ligne de l'entreprise : Le cadre légal peaufiné petit à petit », 28 Janvier 2019, consulté le 05-02-2022 à 10h sur <https://www.ecoactu.ma/creation-en-ligne-de-lentreprise-le-cadre-legal-peaufine-petit-a-petit/>

³Centre Régional d'Investissement Souss Massa, « Dahirs du 9 janvier 2019 portant promulgation des lois n° 88-17 et 89-17 relatives à la création d'entreprises par voie électronique et leur accompagnement » consulté le 05-02-2022 à 10h sur <https://agadirinvest.com/investir-a-agadir/dahirs-du-9-janvier-2019-portant-promulgation-des-lois-n-88-17-et-89-17-relatives-a-la-creation-dentreprises-par-voie-electronique-et-leur-accompagnement.html>

l'entreprise, les inscriptions postérieures au registre de commerce ainsi que toutes les formalités de publication des données et autres documents la concernant. Ce dernier est dispensé de la production, sur support papier, des copies et extraits des contrats, décisions, rapports, états de synthèses, procès-verbaux de délibération, auprès des administrations et organismes concernés¹. Ces formalités doivent être effectuées à travers la plateforme électronique soit par l'intéressé en personne ou son mandataire disposant d'une procuration spéciale, soit par un notaire, avocat un expert-comptable ou un comptable agréé.

Par ailleurs, l'OMPIC a publiée une note d'information² qui a pour objectif d'informer les usagers de changement concernant la procédure de demande et de délivrance du certificat négatif et qui s'inscrivent dans le cadre de l'amélioration et la simplification des procédures concernant la création d'entreprise. Ce changement apparaît à travers la mise en place d'une plateforme de dépôt en ligne des demandes de certificats négatifs qui permet de dématérialiser la procédure de dépôt et de délivrance de certificat négatif³. Selon l'article 3 de la loi n°87.17 modifiant et complétant la loi n°13.99 portant création de l'OMPIC, ce dernier a pour objet la tenue du registre central électronique du commerce, la gestion, au profit de l'Etat, de la plateforme électronique de création et d'accompagnement d'entreprises par voie électronique, ainsi que la tenue et l'exploitation de la base de données y afférente et la garantie de son utilisation sécurisée par tous les intervenants⁴.

Aussi, l'OMPIC a pour rôle la perception, pour son compte et pour le compte des autres administrations et organismes concernées, de tous les taxes, rémunérations pour services rendus et droits relatifs à la création d'entreprises par voie électronique, ainsi que ceux relatifs aux inscriptions au registre électronique du commerce prévu par la loi n° 15-95 formant Code de commerce. De plus, l'office permet la conservation des exemplaires des actes afférents au registre électronique du commerce. Enfin, il permet aux administrations et organismes concernés l'accès à ladite plateforme électronique en vue d'accomplir, directement ou à travers leurs systèmes d'information, les tâches relevant de leur domaine de compétence concernant la création et l'accompagnement d'entreprises et de procéder aux inscriptions postérieures au registre électronique du commerce.

¹V. Article 2 de la loi 88-17.

²OMPIC, « Note d'information sur le changement concernant le certificat négatif », 2019.

³Cette plateforme est nommée « directompic.ma ».

⁴OMPIC, « Directive d'examen d'une demande de certificat négatif », Octobre 2019.

Paragraphe 2 : Inscription au registre de commerce dématérialisé.

Selon l'article 27 du Code de commerce modifié et complété en vertu de l'article premier de la loi n° 89-17, Il est créé un registre électronique de commerce à travers lequel sont tenus les registres locaux du commerce et le registre central du commerce et ce par le biais de la plateforme électronique créée par la loi n° 88-17 relative à la création et à l'accompagnement d'entreprises par voie électronique. L'objectif de cette loi est l'adaptation des nouvelles dispositions du Code de commerce avec les dispositions préalables, en créant un registre électronique constitué d'un registre du commerce central géré par l'OMPIC et des registres commerciaux locaux gérés par les greffes des tribunaux.

Les inscriptions au registre électronique du commerce à savoir les immatriculations, les inscriptions modificatives et les radiations, sont effectuées à travers la plateforme électronique de création et d'accompagnement d'entreprises par voie électronique. Le registre central du commerce est public. Il est consulté à travers la plateforme électronique de création et d'accompagnement d'entreprises par voie électronique. L'immatriculation d'une société au registre électronique ne peut être requise que par les gérants ou par les membres des organes d'administration, de direction ou de gestion et, par le directeur, s'il s'agit d'un établissement public, d'une succursale, d'une agence ou d'une représentation commerciale.

Par ailleurs, un décret d'application, consacrant la digitalisation de la publicité au registre du commerce et du dépôt des états de synthèse des sociétés, a été publié en Juin 2021¹. Il permet de simplifier les procédures administratives, à travers les services électroniques tout en apportant des nouveautés importantes. Le décret fixe également les modalités de déclaration des inscriptions au registre électronique du commerce, ainsi que les modalités de dépôt électronique des états de synthèse et documents des sociétés².

Lorsque l'inscription demandée a été effectuée, le déclarant est informé via la plateforme électronique, conformément à l'article 6 du décret. C'est également par voie électronique que les taxes, redevances et rémunérations relatives à ces services sont payées³.

¹Décret n° 2-20-956 du 22 Chaaban 1442 (5 avril 2021), consacrant la digitalisation de la publicité au registre du commerce et du dépôt des états de synthèse des sociétés.

²Selon l'article 2 du Décret, la déclaration des inscriptions au registre du commerce se fera par voie électronique et ne peut être effectuée que via des modèles préétablis et annexés au décret, par l'intéressé lui-même, ou son mandataire

³Décret n° 2-20-956 du 22 Chaaban 1442 (5 avril 2021), consacrant la digitalisation de la publicité au registre du commerce et du dépôt des états de synthèse des sociétés.

Enfin, Le décret prévoit la création, auprès du ministère de la Justice, d'une commission de coordination relative au registre électronique du commerce, cette commission est chargée de veiller à la bonne exécution des textes législatifs et réglementaires relatifs au registre électronique du commerce¹.

Paragraphe 3 : Le fonds de commerce électronique.

Malgré l'ancienneté de la notion, le fonds de commerce connaît en droit une seconde jeunesse, la notion connaît aujourd'hui une expansion considérable. Le fonds de commerce se diversifie suite à plusieurs mutations qui l'affectent. On parle de plus en plus de fonds de commerce industriel, de fonds de commerce commercial, de fonds de commerce financier. Mieux encore on commence à parler de fonds de commerce électronique. En effet, plusieurs sociétés n'ont pas de point de vente réel et se limitent à commercialiser leurs marchandises sur internet. Un grand nombre d'entreprises n'ont plus de local commercial et exercent leurs activités commerciales par le biais de site internet.

La notion de fonds de commerce électronique a suscité de nombreuses interrogations doctrinales et pratiques avec le développement du commerce électronique. Ainsi, tous les auteurs ou presque², militent en faveur de la reconnaissance du fonds de commerce électronique (I), mais leurs études s'achèvent bien souvent par un point d'interrogation qui remet en cause le fonds de commerce électronique (II) dû à une adaptation délicate du fonds de commerce électronique au régime juridique (III).

I- La reconnaissance du fonds de commerce électronique.

Le fonds de commerce électronique est bel et bien une réalité qui ne peut être ignorée. L'appropriation d'un fonds de commerce a été depuis longtemps une question juridique épineuse qui a fait couler beaucoup d'encre et qui a toujours suscité chez les juristes des controverses à la fois passionnées et passionnantes³.

Le fonds de commerce peut être défini comme l'ensemble des éléments permettant d'attirer la clientèle. A l'aune de cette définition, il n'y a d'obstacle à ce qu'une activité

¹V. art 19 du décret n° 2-20-956 du 22 Chaaban 1442.

²T. VERBIEST, « le fonds de commerce électroniques : vers une reconnaissance juridique ? », in Communication commerce électronique, N° 4, 2008, p. 14.

³J. GUEZMIL, « L'hébergement du fonds de commerce électronique », in Revue de la Jurisprudence et de la Législation, N° 4, Avril 2015, p. 17.

commerciale en ligne fasse apparaître un fonds de commerce dès lors que le commerçant dispose d'une clientèle et cela en dépit de son absence implantation géographique¹. Force est donc de constater que l'activité commerciale sur internet réunit toutes les caractéristiques du fonds de commerce classique : une clientèle et un ensemble d'éléments corporels et incorporels. La condition de la reconnaissance du fonds de commerce électronique tient à l'admission d'une clientèle en ligne, une clientèle certaine², personnelle³ et licite⁴. La clientèle constitue la finalité du fonds de commerce. Pour le juriste⁵, la clientèle n'est autre que l'ensemble des relations d'affaires habituelles ou occasionnelles du commerçant.

Qu'elle soit attiré ou occasionnelle sa réalité ne soulève pas de difficulté en raison de l'accessibilité du site internet de commerce électronique. Ainsi, la preuve de l'existence d'une clientèle peut être facilement rapportée en matière de commerce électronique. En effet, tout site internet dispose d'un site de statistique et de gestion comptabilisant le nombre des cyber-clients visitant le site chaque jour et effectuant des opérations d'achats. Une simple consultation dudit site permet d'en apporter la preuve inéluctable.

La clientèle apparaît donc comme une notion variable et mouvante dans la mesure où le cybercommerçant peut invoquer l'existence d'une clientèle virtuelle, certaine personnelle et licite, créée par le développement d'une activité commerciale en ligne et ce, à l'image de l'activité commerciale exploitée dans un local fermé⁶. En effet, la plasticité de la notion classique de fonds de commerce permet l'extension de son champ d'application au commerce électronique du moment que l'élément principal pour l'existence de l'identification du fonds de commerce est la clientèle. Rien n'empêche dès lors que cette dernière soit numérique ou virtuelle.

Reste la question de l'influence du mode d'exercice de l'activité commerciale sur la clientèle : le commerçant disposant d'une boutique en ligne peut être bien exploité une boutique physique. Il n'y a alors pas nécessairement une clientèle unique et donc un fonds de

¹T. DOUVILLE, « Le fonds de commerce électronique : de sa reconnaissance à sa marginalisation », in IP/IT, N°12, Décembre 2019, Dalloz, p. 28.

²La clientèle doit exister de manière actuelle, une simple virtualité ne suffit pas. La clientèle future n'est pas prise en considération.

³La clientèle doit être réellement attirée par le fonds de commerce et propre au commerçant concerné.

⁴Il faut que l'activité exercée dans le commerce soit autorisée par la loi.

⁵L'économiste y voit une valeur, des besoins à satisfaire.

⁶S. KHALED, « Le fonds de commerce électronique », in Infos juridiques, N° 190-191, Déc.2014, p.15 cité dans Mohamed MANOUBI, « Réflexions sur la notion de fonds de commerce électronique », in Mélanges offerts en l'honneur du professeur Hafed BEN SALAH, Centre de publication universitaire, Carthage, 2018, p. 362.

commerce unique, c'est le cas si l'activité exercée en ligne est différente. Inversement, si la boutique en ligne n'est que le prolongement de la boutique physique, il y a tout lieu de considérer que la clientèle unique. Un exemple est donné par les pharmaciens qui vendent en ligne des médicaments sur le site internet qui est considéré comme le prolongement de leur office. Les critères utilisés pour l'évaluation de la clientèle pourront toutefois varier selon ses caractères. Evidemment, ces questions ne se posent pas lorsque le commerçant exerce seulement son activité en ligne au moyen d'un site dédiée, bref, il s'agit d'un *pure player*¹ qui dispose d'un véritable fonds de commerce électronique².

En plus de la clientèle, d'autres éléments incorporels existent au sein du fonds de commerce électronique. Ainsi, le cybercommerçant dispose aussi bien du nom commercial que de l'enseigne³. Toutefois, l'élément de ralliement de la clientèle est ici signe particulier à savoir le nom de domaine. Ce nom se décompose en deux parties : un vocable, qui peut correspondre au nom commercial, et une extension en « .com » ou « .ma »⁴. C'est grâce à ce nom que l'internaute pourra trouver le site internet recherché. Au titre des éléments corporels, se trouvent classiquement le matériel et les marchandises. Le matériel, car on ne peut imaginer un site internet sans informatique, sans téléphone ou bureautique. Quant aux marchandises, le fait qu'elles soient vendues sur internet ne leur imprime aucune spécificité⁵.

II- La remise en cause du fonds de commerce électronique.

Le commerce électronique s'opère de plus en plus à partir de plateformes ou de place de marchés. Les opérateurs sont nombreux entre autres *Alibaba*⁶, *Amazon*⁷ et leurs activités sont diverses. Certaines d'entre elles consistent à mettre en relation les commerçants proposant des biens et des services et des internautes consommateurs ou professionnels.

¹Un *pure player* est un commerçant proposant et vendant ses produits / services exclusivement en ligne. Il ne détient donc aucun point de vente physique, et l'ensemble de son offre est entièrement digitalisée.

²T. DOUVILLE, *Op. cit.*, p. 29.

³L'expression nom commercial désigne de façon générale toute appellation sous laquelle un commerçant personne physique ou morale, exerce son commerce.

⁴Voir infra p. 190.

⁵Il existe des cas où l'entreprise ne dispose pas de marchandises dans son fonds de commerce, c'est notamment le cas des entreprises de services, vu l'intangibilité de ses produits (ex : agences de voyage, assurance...).

⁶Alibaba est une société chinoise cotée en bourse qui tire principalement ses revenus de ses activités sur Internet, dont un marché public destiné à faciliter les échanges entre entreprises (qu'ils soient internationaux ou chinois), des plateformes de paiements et de ventes au détail, un moteur de recherche pour le magasinage et des services de cloud computing. Son activité est proche de celle d'Amazon, mais Amazon génère des revenus plus élevés.

⁷Amazon est une entreprise de commerce en ligne américaine basée à Seattle. Elle est l'un des géants du Web, créée par Jeff Bezos en juillet 1994.

Elles jouent le rôle d'intermédiaire entre les commerçants et leurs clients et constituent un marché biface où chaque face est dépendante, le renforcement de l'une allant de pair avec celle de l'autre. Ainsi plus l'offre de bien ou de service est importante, plus les clients seront nombreux.

Les plateformes d'intermédiation peuvent être définies comme des services de la société de l'information, permettant aux entreprises utilisatrices de proposer des biens ou de services aux consommateurs en vue de faciliter l'engagement de transactions directes entre eux, les services étant fournis aux entreprises utilisatrices sur la base de relations contractuelles entre elles et le fournisseur de ces services. S'il ne fait aucun doute que les plateformes disposent d'une clientèle et d'un fonds de commerce, nous voulons savoir la situation de ces commerçants utilisateurs de ces plateformes qui sont placés dans leur dépendance pour entrer en contact avec les consommateurs¹.

En effet, nous constatons, une absence de clientèle autonome. Sur la plupart des plateformes d'intermédiation, les clients ont accès à une liste de résultats par catégorie de produits recherchés dont certains peuvent être proposés par la plateforme tandis que le sont par les commerçants annonceurs². L'identité des commerçants apparaît à côté du résultat ainsi que les avis laissés par les clients ; la qualité de ces avis étant ou sautant un guide pour les clients que l'une des obligations imposées au commerçant dont le respect détermine son maintien sur la plateforme. L'accès direct à l'offre du commerçant est impossible. Plus généralement, le commerçant exerce son activité dans les conditions commerciales et techniques fixées par la plateforme.

Or, le problème est la vérification de l'existence d'une clientèle personnelle ou autonome de certains commerces dont l'activité était placée dans la dépendance d'un autre sachant que le commerçant en ligne n'a aucune clientèle autonome lorsqu'il commercialise ses produits sur une plateforme. En l'absence d'une clientèle personnelle, le commerçant ne dispose pas d'un fonds de commerce. Le développement des plateformes d'intermédiation a donc pour effet de marginaliser la notion de fonds de commerce et de placer les commerçants

¹T. DOUVILLE, *Op. cit.*, p. 28.

²Gilles JEAN MARTIN, « Quelle régulation pour l'économie collaborative ? Un défi pour le droit économique. Réflexions à mi parcours » in *Quelles régulations pour l'économie collaborative ? Un défi pour le droit économique*, Ouvrage collectif sous la direction d'Irina PARACHKEVIVA et Marina TELLER, Dalloz, Paris, 2017, p. 59.

en situation de dépendance. Un récent règlement européen¹ cherche justement à mieux protéger les entreprises utilisatrices contre les pratiques de ces plateformes notamment par des exigences de transparence.

III- Une adaptation délicate du fonds de commerce électronique au régime juridique.

Malgré une consécration juridique qui se fait encore attendre, le fonds de commerce électronique existe aujourd'hui dans le cadre du commerce sur internet. Ce fonds constitue actuellement une véritable réalité économique qui se développe au fil des jours et nécessite l'édification d'un régime juridique qui s'adapterait à ses éléments constitutifs. La composition du fonds de commerce électronique présente des spécificités par rapport à un fonds de commerce physique. C'est le cas du bail commercial, du moins si l'activité est exercée exclusivement en ligne. Chacun sait que la protection du fonds de commerce classique s'exprime à travers le régime du bail commercial ou encore la propriété commerciale. Or, si l'activité commerciale est exercée exclusivement électronique il n'existe pas de local dans lequel s'exerce l'activité commerciale.

De ce fait, et par analogie au local d'exploitation permettant d'identifier le fonds de commerce, le nom de domaine constitue l'adresse électronique permettant aux internautes d'identifier le site internet recherché. Son existence conditionne celle du fonds. Son rôle est comparable à celui du bail pour le fonds de commerce classique dans la mesure où toute cession du nom de domaine d'un site marchand est susceptible d'être qualifiée de cession de fonds électronique. Le contrat d'hébergement² importe peu dans ce domaine, car il est possible au cybercommerçant de changer d'hébergeur, sans que l'accessibilité au site internet n'en pâtisse.

Par conséquent, la stabilité et la pérennité du fonds de commerce électronique sont exclusivement tributaires du renouvellement du contrat d'enregistrement du nom de domaine. Il est donc possible d'assimiler le nom de domaine au local d'exploitation et le faire bénéficier d'une réglementation similaire. Dans ce cas, le site marchand, éléments constitutifs d'un

¹Règlement du parlement européen du 20 Juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices des services d'intermédiation en ligne. Il est applicable à partir du 12 Juillet 2020.

²Voir infra p. 157.

fonds de commerce électronique peut être considéré comme la vitrine dématérialisée de l'entreprise en vue de réaliser de façon répétée et renouvelées actes de commerces¹.

Une telle assimilation permettra une protection efficace et durable du cybercommerçant. Mais encore faut-il favoriser les opérations juridiques sur le fonds. En effet, toute entreprise disposant d'un fonds de commerce électronique désirerait comme tout commerçant à la tête d'un fonds de commerce traditionnel, bénéficier du droit de la propriété commerciale, vendre son fonds, le nantir, le louer ou même l'apporter en société. Il s'agit dès lors de relancer et favoriser toutes ces opérations juridiques ayant pour objet le fonds de commerce électronique. Ce qui pourrait lui assurer un régime juridique adapté et spécifique².

Il est question de favoriser non seulement la cession du fonds de commerce électronique, sa location-gérance mais surtout le nantissement du fonds. En effet, a priori, le site web peut être nanti en garantie d'un prêt, mais en pratique la question qui se pose est de savoir si un nantissement constitué sur un fonds de commerce peut grever par extension le site web qui a été créé postérieurement. Traditionnellement, un nantissement initialement constitué sur un fonds de commerce peut s'étendre aux fonds de commerce constitués postérieurement si le fonds concerné n'a pas une clientèle propre et individualisée.

Par conséquent, si le site web dispose d'une clientèle propre et individualisée, ce qui est généralement le cas, il doit alors faire l'objet d'un nantissement autonome et indépendant³. En réalité, le nantissement d'un fonds de commerce est une opération assez délicate surtout en matière électronique. Plusieurs questions se posent auxquelles la législation ne peut répondre vu dans l'état actuelle cette dernière ne traite pas ni du nom de domaine ni du contrat d'hébergement. Une actualisation des textes s'impose même si le nom de domaine peut faire partie de la rubrique des droits de propriété industrielle, littéraire et artistique⁴.

Par ailleurs, l'enregistrement du nantissement, de la cession ou la location-gérance du fonds de commerce électronique au registre du commerce auprès du tribunal pose problème du fait que le fonds exploité à l'échelle nationale voire internationale, on ne saurait le

¹Mohamed MANOUBI, « Réflexions sur la notion de fonds de commerce électronique » in Mélanges offerts en l'honneur du professeur Hafed BEN SALAH, Centre de publication universitaire, Carthage, 2018, p 367.

²Tamara BOOTHERSTONE, « Sécuriser les transactions par la notion de e-fonds de commerce » in La propriété intellectuelle et la transformation numérique de l'économie, Ouvrage collectif sous la direction de Fatima GHILASSENE et Laurence JOLY, INPI, 1^{ère} éd., France, 2015, p. 176.

³Mohamed MANOUBI, *Op. cit.*, p. 367.

⁴Voir infra p. 186.

rattacher à aucun tribunal, à moins d'imposer un enregistrement auprès du tribunal du Maroc pour toute opération relative à un fonds de commerce électronique hébergé sur le territoire marocain.

Quoiqu'il en soit ce ne sont pas des obstacles à la prise en compte du fonds de commerce électronique, une modification législative pour adapter la réglementation en vigueur s'impose à cette nouvelle notion juridique¹. Ainsi, même si l'idée de fonds de commerce demeure jeune malgré son âge, bien des éléments de son régime juridique méritent d'être réformés et modernisés si on veut l'adapter au temps nouveau. Le régime juridique du fonds de commerce électronique pose de multiples problèmes juridiques auxquels la législation en vigueur n'apporte aucune réponse. Une adaptation du contexte juridique au contexte technologique, en mutation continue, mérite d'être réalisée en vue de transformer le fonds de commerce en un véritable facteur d'évolution socio-économique.

Sous-section 2 : La gouvernance des entreprises numériques.

La gouvernance d'entreprise regroupe l'ensemble des relations entre les dirigeants de l'entreprise et son organe de gouvernance avec les actionnaires d'une part et les autres parties prenantes d'autre part ; et ce, dans l'objectif de création de valeur pour l'entreprise. La gouvernance d'entreprise s'intéresse donc à la manière dont les entreprises sont dirigées et contrôlées et s'assure de la capacité des organes de gestion à poursuivre des objectifs conformes aux intérêts des actionnaires et des autres parties prenantes, et à mettre en œuvre des systèmes de contrôle efficaces pour gérer les conflits d'intérêt potentiels et les risques éventuels et prévenir les abus de pouvoir de nature à faire prévaloir des intérêts particuliers sur l'intérêt social².

L'accueil accordé au numérique par la partie du droit s'intéressant à l'organisation interne des sociétés est plus mitigé. Devant essentiellement servir à communiquer, soit des documents, soit du son et de l'image, le recours aux nouvelles technologies de communication trouvera un terrain propice à son développement en droit des sociétés chaque fois qu'il s'agira de permettre à ceux qui participent à la société de communiquer entre eux plus aisément tout en demeurant à distance. Précisément, les divers moyens utilisés sollicités (communication par message, l'exploitation d'un site internet, la numérisation des divers documents sociaux,

¹T. DOUVILLE, *Op. cit.*, p. 31.

²Le Code Marocain de Bonnes Pratiques de Gouvernance d'Entreprise, Commission national de gouvernance d'entreprise, CGEM, Mars 2008.

la signature électronique et l'usage de la visioconférence) doivent permettre de favoriser la vie interne des sociétés et de ses membres¹.

C'est ainsi qu'il sera utile de se focaliser d'abord sur les modes d'accueil du numérique dans l'organisation des organes sociaux de l'entreprise (Paragraphe 1) avant de s'attarder sur les cas de recours à la technologie de la *blockchain* dans la gouvernance des entreprises (Paragraphe 2).

Paragraphe 1 : L'accueil du numérique dans l'organisation des organes sociaux.

L'examen de l'état du droit dans le domaine du droit des sociétés laisse clairement apparaître une intégration certaine du numérique dans l'organisation des organes sociaux (I). Cependant, il n'en demeure pas moins qu'une certaine défiance perdure vis-à-vis du numérique (II). Cette défaillance est due au souci de protection des données personnelles (III).

I- L'intégration certaine du numérique dans l'organisation des organes sociaux.

Les nouvelles technologies sont en effet apparues comme nécessaires et pratiques, permettant une tenue plus aisée des séances des organes de directions collectifs lorsque les dirigeants sont situés en divers points d'un pays ou du monde offrant d'abolir les distances géographiques et temporelles tout en permettant de réaliser des économies voire de limiter l'impact écologique de l'activité sociétaire. Elles permettent aussi d'accroître la réactivité des organes de direction lorsque l'urgence commande de tenir des réunions très rapidement. Enfin, le numérique permet de renforcer l'effectivité des droits des organes sociaux en évitant que des contingences matérielles ne conduisent trop fréquemment à la tenue de conseils de papier².

L'organisation des assemblées des associées a aussi constitué un champ d'investissement des nouvelles technologies du numérique dans le droit des sociétés. Ce recours est, depuis l'origine, justifié par un souhait de simplifier la tenue de ces assemblées (notamment dans les très grandes sociétés comptant des milliers d'actionnaires,

¹Véronique MAGNIER, « La Blockchain, un choix de gouvernance pertinent ? » in Blockchain et droit des sociétés, Ouvrage collectif sous la direction de Véronique MAGNIER et Patrick BARBAN, Dalloz, Paris, 2019, p.170.

²Jean-Marc MOULIN, *Op. cit.*, p. 28.

parfois étrangers) et celui de garantir et renforcer l'effectivité des droits que notre législation reconnaît aux associés.

L'image d'assemblées générales qui font davantage le vide que le plein lorsqu'elles ne se tiennent pas uniquement sur le papier ne relève pas de l'imagier d'Epinal. Sous cet angle, le recours aux moyens de communication électroniques peut offrir de restaurer une vie sociétaire quelque peu perdue puisque le numérique offre de communiquer facilement à distance ; notamment dans les sociétés cotées où la part des investisseurs étrangers s'établit à près de la moitié de l'actionnariat total.

Néanmoins, le recours au numérique n'a cependant été dans un premier temps conçu que comme un mode complémentaire de participation des associés aux assemblées générales ; le mode principal de tenue de l'assemblée générale demeurerait cependant une tenue physique mais à laquelle certains actionnaires pouvaient demander à participer à distance par des moyens de communication électronique. Il reste que si l'intégration du numérique dans la vie interne des sociétés est donc un fait attesté et certain, il n'en demeure pas moins qu'un sentiment de défiance peut cependant être relevé à l'examen de certaines dispositions.

II- La permanence d'une défiance vis-à-vis du numérique dans l'organisation des organes sociaux.

L'introduction du numérique dans le droit des sociétés se réalise, de manière quelque peu anarchique. En effet, à ce jour, seules les sociétés anonymes connaissent des dispositions qui permettent d'organiser le fonctionnement de leurs organes collégiaux de direction et la tenue de assemblées générales en ayant recours à des moyens électroniques de communication alors même que les SNC, et les sociétés en commandite simple, les SARL ou encore les sociétés civiles peuvent être dirigées de manière collégiale. Or les dispositions propres à ces sociétés sont muettes quant à la possibilité de recourir au numérique pour l'organisation des travaux de ces organes.

Reste donc, le cas des sociétés anonymes dans lesquelles le recours au numérique est admis mais sous certaines conditions. En effet, Le régime prévu par la loi 17.95¹ est en quelque sorte discriminatoire. En premier lieu, le recours à la visioconférence est encadré par l'article 50 bis de la loi en question, l'article oblige à ce que ce recours soit impérativement

¹Dahir n° 1-96-124 du 14 rabii II 1417 (30 août 1996) portant promulgation de la loi n° 17-95 relative aux sociétés anonymes

prévu par les statuts de la société. Donc, les sociétés où il n'a pas été fait preuve d'anticipation ou encore les sociétés qui n'ont pas opéré, au préalable, une modification des statuts de manière à ce que le recours à la vidéoconférence soit prévu, ne pourront ni bénéficier de cette option ni bénéficier de l'option offerte par l'article 131 bis de la loi 17.95, à savoir la possibilité dévolue aux actionnaires de voter par correspondance.

Le recours à la visioconférence par les membres du conseil de surveillance ou actionnaires en vue de participer, à distance, aux réunions des organes de direction ou des organes sociaux n'est pas systématique et suppose la réunion de trois conditions *sine qua non*, notamment : il faut que le moyen employé présente des caractéristiques techniques garantissant une participation effective aux réunions des organes de direction ou des organes sociaux. Aussi l'identification préalable des personnes participantes. Et enfin l'enregistrement fiable des discussions et délibérations, tout en sachant que les procès-verbaux de réunions doivent faire état de tout incident technique¹.

En ce qui concerne la question du vote par correspondance prévu par l'article 131 de la loi 17.95, cette méthode est prévue comme mesure accompagnatrice de la visioconférence, en dehors d'une quelconque prédisposition quant à la rédaction anticipatrice des statuts de la société. Les formulaires de vote par correspondance doivent être remis ou adressés à tout actionnaire qui en fait la demande par tous moyens prévue par les statuts ou l'avis de convocation, et ce à compter de la convocation jusqu'à un délai de 10 jours avant la tenue de l'assemblée². Cependant, il est impératif, dans ce cadre, que l'avis de réunion de l'assemblée générale, en plus d'y faire figurer les mentions légales, doit faire référence aux mesures pratiques destinées à l'identification des actionnaires, mais également les modalités de consultation des documents qui seront présentés.

Il faut noter que lors de l'état d'urgence sanitaire causé par la Covid-19, les travaux des organes de direction des sociétés anonymes et ceux de leurs assemblées générales ont été entravé. D'où la naissance de la loi 27.20³ mettant en place des mesures particulières

¹V. Article 50 bis de la loi 17-95 (Ajouté par l'article 3 de la loi n° 20-05 promulguée par le dahir n° 1-08-18 du 23 mai 2008 - 17 jourmada I 1429 ; B.O. n° 5640 du 19 juin 2008).

²V. Article 131 bis de la loi 17-95 (Ajouté par l'article 3 de la loi n° 20-05 promulguée par le dahir n° 1-08-18 du 23 mai 2008 - 17 jourmada I 1429 ; B.O. n° 5640 du 19 juin 2008).

³Projet de loi n°27-20 portant application des dispositions spéciales relatives au déroulement des travaux des organes d'administration des sociétés anonymes et les modalités de tenue de leurs assemblées générales durant la période de l'état d'urgence sanitaire.

afférentes au déroulement des travaux des organes de direction des sociétés anonymes ainsi qu'à la tenue des assemblées générales durant l'état d'urgence sanitaire¹.

Avant de se pencher sur les mesures décidées par le législateur dans le cadre de la loi 27.20. Il convient d'affirmer comme on l'a cité précédemment que la loi 17.95 relative aux sociétés anonymes contient déjà des dispositions susceptibles de régir, en partie, les travaux des organes de direction des sociétés anonymes ainsi que les travaux de leurs assemblées générales en cette période de crise, mais cela n'aurait concerné que celles ayant fait preuve d'anticipation. Il est fait référence dans ce cadre à l'article 50 bis de ladite loi, auquel renvoient les articles 91, 110 et 111 concernant, respectivement, la réunion du conseil de surveillance, la tenue des assemblées générales extraordinaires et celle des assemblées générales ordinaires.

Nous constatons que la naissance de la loi 27.20 en cette période de crise sanitaire n'est pas anodine. Ainsi l'article premier du projet de loi 27.20 offre aux sociétés dont les conseils d'administration n'auront pas été réunis à la date de sa publication au bulletin officiel et pendant toute la durée de l'état d'urgence sanitaire, la possibilité de recourir à la visioconférence ou à tout moyen équivalent pour la tenue des réunions des conseils d'administration dans le dessein d'arrêter les comptes, d'établir le rapport de gestion, d'établir les états de synthèse et de convoquer l'assemblée générale des actionnaires qui doit statuer sur les comptes tout en fixant son ordre du jour.

Par ailleurs, dans le cadre du troisième article, le texte autorise les sociétés anonymes, sans distinction faite entre celles dont les statuts prévoient le recours à la visioconférence et celles dont les statuts ne le prévoient guère, et donc en dérogeant au régime contenu dans les articles 110 et 111 tel que mentionné en sus, d'user ce moyen en vue de la réunion de leurs assemblées générales ordinaires ou extraordinaires. Néanmoins, l'article 3 de la loi 27.20 précise des modalités à respecter pour utiliser ces modes de participation à distance. Ainsi, les moyens de visioconférence ou équivalent doit remplir certaines conditions. D'abord, ces moyens doivent satisfaire à des caractéristiques techniques garantissant une participation effective à la réunion, dont les délibérations sont retransmises de façon continue. Ensuite, pouvoir identifier au préalable les personnes participantes par ce moyen de réunion.

¹H. MOUMEN, « Le Fonctionnement des Sociétés Anonymes et l'Etat D'Urgence Sanitaire au Maroc », 25 Mai 2020, consulté le 17-02-2022 à 10h sur <https://www.village-justice.com/articles/les-travaux-des-organes-direction-des-societes-anonymes-leurs-assemblees,35435.html>.

Enfin, permettre un enregistrement fiable des discussions et délibérations pour les moyens de preuve.

Pour ce qui est de la question du vote de l'actionnaire par correspondance prévu par l'article 131 bis de la loi 17.95, elle a été érigée par le troisième article de la loi 27.20 en tant que mesure accompagnatrice de la visioconférence dans le cadre de la tenue de l'assemblée générale des actionnaires. Dans ce cadre, aucune indication quant au régime encadrant le recours au vote par correspondance, à savoir le régime contenu dans l'article 131 bis de la loi 17.95 impliquant des délais de rigueur pour l'envoi du formulaire de vote à l'actionnaire par la société et qui ne tient compte que des formulaires reçus par la société avant la réunion de l'assemblée, ou un régime dérogatoire à celui-ci. C'est là un point très important qui a été négligé, d'autant plus que l'esprit de la loi 27-20 tend à mettre de côté les délais de rigueur qui se révèlent particulièrement contraignants en cette période¹.

III- La protection des données à caractère personnel en matière d'organisation des organes sociaux.

Il faut noter que le recours à la visioconférence lors des assemblées générales précis implique de s'intéresser à une question particulière celle des données personnelles. Ainsi, la visioconférence est caractérisée par la capacité de transmettre des images et du son, et ses moyens mis en œuvre doivent permettre un enregistrement fiable des discussions et délibérations. Ce qui pose la question de l'application de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

La loi n° 09-08 définit les données à caractère personnel comme : « toute information, de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne physique identifiée ou identifiable ». Les images et le son étant définis comme des données personnelles, leur enregistrement doit faire l'objet d'une déclaration préalable auprès de la CNDP. Donc par application de l'article 4 de la loi 09-08, il faut un accord préalable des personnes concernées pour que leurs données personnelles soient collectées et traitées dans les conditions prévues par ladite loi. Nous pouvons supposer que la

¹Ilham MOUNTAJ, « Visioconférence : les règles en matière d'organisation des assemblées générales », in Média 24, 2 Juin 2020, consulté le 19-02-2022 sur <https://medias24.com/2020/06/02/visioconference-les-regles-en-matiere-dorganisation-des-assemblees-generales>.

présence en visioconférence manifeste l'acceptation. Aussi, il faut l'interdiction d'utiliser les enregistrements à d'autres fins que la participation aux délibérations¹.

Quant à la durée de conservation des données, la loi précise que les données collectées doivent être traitées conformément à ces finalités et conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées². Par application de cet article, une fois le procès-verbal validé et signé par les personnes compétentes, les enregistrements doivent être effacés. A défaut, le responsable du traitement se verra infligé les sanctions pénales prévues par l'article 55 de la loi 09-08.

Par ailleurs, en matière de protection et de confidentialité des données le responsable du traitement doit prendre les mesures techniques et organisationnelles de nature à préserver les images et la voix contre toute atteinte notamment l'accès non autorisé³, à défaut il sera sanctionné conformément à l'article 58 de la loi 09-08. Enfin se pose le problème des moyens de visioconférence mis à disposition par un tiers, il risque de porter atteinte à la confidentialité. C'est pourquoi l'entreprise doit s'assurer que le tiers respecte ses obligations à savoir, mettre en œuvre des mesures techniques et organisationnelles de nature à les préserver contre toute atteinte les images et sons et déclaré la collecte et les traitements à la CNDP, sinon l'entreprise est pénalement responsable⁴.

Paragraphe 2 : Le recours à la *blockchain* dans la gouvernance des entreprises.

La *blockchain* est envisagée comme un dispositif d'enregistrement électronique partagé permettant l'authentification de certaines opérations, elle est définie comme un registre sur lequel sont inscrits chronologiquement des faits et des actes de manière immuable. Elle est présentée comme offrant de nombreux atouts. Cette technologie promet plus de transparence et de confiance pour les utilisateurs qui, mieux informés, feront un meilleur usage de leurs droits sociaux. Elle permet également une grande sécurité du fait de

¹Raphael PEUCHOT, « Gestion des données personnelles : quels changements le règlement européen apportera-t-il ? » Ouvrage collectif sous la direction d'Jean-Michel BRUGUIERE, Dalloz, Paris 2014, p. 57.

²V. article 5 de la loi 09-08.

³Sylvain CHATRY, « Les données collectées par l'entreprise : documenter sa conformité au RGPD », in L'entreprise face aux défis du numérique, Ouvrage collectif sous la direction de Alexandre RIERA et Sylvain CHATRY, MARE & MARTIN, Paris, 2018, p. 116.

⁴A. BENSETTI, S. ALASSAIRE, « Usage des moyens de visioconférence dans les sociétés anonymes », Chambre française de commerce et d'industrie du Maroc, 1 Avril 2015 consulté le 17-02-2022 à 11h sur http://www.cfcim.org/wp-content/uploads/2015/04/CFCIM_01042015_%C2%AB-Usage-des-moyens-de-visioconfe%CC%81rence-dans-les-socie%CC%81te%CC%81s-anonymes-%C2%BB.pdf.

l'immutabilité des informations qui y sont inscrites. Se doter d'une technologie *blockchain* au sein d'une entreprise relève d'un choix stratégique qui suppose de bien mesurer les avantages, le potentiel, les limites et les risques induits par cette technologie innovante, non seulement en termes de coûts et de temps mais aussi en termes qualitatifs et de sécurité.

Les principales fonctions communément reconnues à la *blockchain* sont triples : répertorier, organiser, réaliser des transactions. De tels usages s'avèrent d'une grande utilité pour les entreprises dont les besoins vont du stockage et de l'organisation des données, comptables ou personnelles, à la réalisation de transactions, le tout de manière sécurisée et immuable. C'est pourquoi, elles n'ont pas attendu l'intervention du législateur pour faire appel à des services fondés sur la technologie de la *blockchain* qui automatisent certaines tâches¹ comme le transfert de fonds², gèrent leurs ressources humaines et préconstituent des preuves sécurisées. L'objectif est d'augmenter leur compétitivité en réduisant coûts et insécurité.

En dehors de tout cadre légal la technologie *blockchain* améliorera donc le fonctionnement quotidien des entreprises qui réalisent ainsi des opérations sécurisées dans un laps de temps réduit. La *blockchain*, fondée sur la règle « *Le code est la loi* »³, semble adaptée pour des transactions simples comme l'application de la *bitcoin* par exemple. En matière de société, les choses peuvent à priori sembler aisées surtout dans le fonctionnement d'une société anonyme ou d'une société en commandite par action, du moins si on envisage le fonctionnement idéal.

A ce jour, la *blockchain* semble offrir essentiellement deux usages : une fonction de registre et une fonction transactionnelle. Ces deux fonctions peuvent passer par une *blockchain* publique ou privée. Dans la première, tout participant se cache derrière un pseudonyme, le fonctionnement ne fait intervenir aucun régulateur et le contrôle se fait de

¹C. IBACH : « La blockchain en entreprise : des applications concrètes », consulté le 17-02-2022 à 10h sur <https://www.cadre-dirigeant-magazine.com/manager/la-blockchain-en-entreprise/> consulté.

²La compagnie d'assurance AXA automatise certaines opérations simples comme le dédommagement en ligne pour compagnie s'aviation. Aussi, le Crédit Agricole utilise une nouvelle technologie fondée sur la blockchain pour transférer des salaires d'un pays à un autre.

³Le code est la loi fait référence à l'idée selon laquelle, avec l'avènement de la technologie numérique, le code s'est progressivement imposé comme le moyen prédominant de réguler le comportement des internautes.

façon horizontale et décentralisée. Dans la seconde, les acteurs doivent être identifiés et les règles de fonctionnement sont contrôlées par l'initiateur de la *blockchain*¹.

Une bonne gouvernance a pour objet de permettre une gestion harmonieuse de la société dans son intérêt propre. A cet effet, le droit marocain offre plusieurs formules fondamentales de structuration des sociétés commerciales. Le code marocain de bonnes pratiques de gouvernance d'entreprise recommande d'avoir un certain nombre d'administrateurs indépendants au conseil d'administration. L'exigence d'indépendance tend à écarter de cette qualification des administrateurs risquant de se trouver en conflit d'intérêt au sein de la société. Plusieurs cas de figure en atteste ; occupations présentes ou passées de fonctions de dirigeant mandataire social ou de salarié dans la société ou le groupe, relations d'affaire.

L'examen de la gestion des conflits d'intérêt dans les sociétés par la technologie de la *blockchain* conduit à s'intéresser au mécanisme des conventions réglementées, instrument juridique par excellence visant à protéger les sociétés commerciales contre les conflits d'intérêts. Nous pouvons donc envisager de consigner dans un registre de *blockchain* toutes les opérations réalisées entre la société, les administrateurs et les actionnaires intéressés. Tout projet de convention entre la société et un intéressé serait placé dans un registre spécifique, le conseil de l'administration systématiquement alerté pouvant alors s'autosaisir de la convention pour entamer la procédure d'autorisation. Une telle automatisation permettrait d'échapper à une initiative aujourd'hui réservée à l'intéressé lui-même, ce qui conduit à des comportements d'évitement de la loi.

La procédure des conventions réglementées s'étend également aux rémunérations dont le versement est soumis à des critères de performance sous contrôle des organes sociaux. Leur tâche sera facilitée grâce à la technologie de la *blockchain* venant renforcer la discipline des dirigeants sociaux. C'est l'exemple de l'automatisation du versement de certaines rémunérations. Toutefois, une limite serait qu'un contrôle sera toujours nécessaire pour vérifier que toutes les conditions sont réunies pour ce versement. D'autres conditions peuvent en effet être ajoutées, telle une condition de présence dans la société, voire de bon comportement du dirigeant, ce qui pose la question de ces critères sous formes d'algorithmes. Le caractère mécanique de la *blockchain* se prête mal à la souplesse d'appréciation requise

¹M. MEKKI, « Le contrat, objet des smart contracts (Parti I) », in IP/IT, N° 7 et 8, Juillet- Aout 2018, Dalloz, p. 409.

pour le bon fonctionnement des organes, laissant penser qu'un recours à une telle technologie sera rarement pertinent.

Le vote en ligne réalisé par la *blockchain* correspond parfaitement à sa philosophie initiale. Il s'agit de favoriser la transparence et de développer une démocratie directe. Dans tout domaine, le vote en ligne est une aspiration en raison de sa rapidité et de sa simplicité. La sécurité est en effet le plus grand défi de la cote en ligne. La *blockchain* permet d'enregistrer le vote dans un registre infalsifiable en toute transparence. La cote en ligne est exploitée dans les sociétés privées. Ainsi, il est concevable, grâce à une *blockchain* privée, de garantir le vote sécurisé des actionnaires. Il est aussi concevable d'imaginer que la *blockchain*, en favorisant la communication entre actionnaires, puisse favoriser l'exercice collectif des droits des actionnaires¹. D'ores et déjà des *start-ups* se positionnent sur ce marché.²

Section 2 : L'entreprise face aux enjeux du numérique.

Infini, illimité, éternel, ubiquiste, tels sont les qualificatifs les plus souvent employés pour traduire l'immensité de la technologie internet, décontençant le juriste dans son rapport au temps et à l'espace. Le développement du numérique est un phénomène récent et comme toute nouveauté il suscite des craintes en même temps que des espoirs. En effet, la révolution numérique au point qu'elle procure des avantages et des services à l'entreprise, elle est source d'insécurité et peut conduire à l'extinction de l'entreprise.

Ainsi, la présence de l'entreprise sur internet est souvent considérée par ses dirigeants comme un mal nécessaire. Cette présence qu'il convient de gérer pour garder une bonne e-réputation de l'entreprise (Sous-section 1). De plus les retombées que le développement du numérique peut avoir sur le droit des entreprises en difficulté n'échappent pas à cette ambivalence (Sous-section 2).

Sous-section 1 : L'e-réputation de l'entreprise.

L'e-réputation est définie comme étant les informations que l'on peut trouver sur une personne grâce aux moteurs de recherche, sur les blogs, les réseaux sociaux, etc. Or, cette

¹Xavier VAMPARYS, La Blockchain au service de la finance : Cadre juridique et applications pratiques, Revue Banque, Paris, 2018, p. 145.

²On peut citer Belem en France et Voats aux Etats-Unis.

définition n'est pas satisfaisante car l'e-réputation n'est pas le constat neutre de l'amalgame d'informations numériques sur une personne physique ou morale. Elle possède une dimension subjective, car la réputation relève avant tout de l'opinion et de l'évaluation sociale. En d'autres termes, elle n'est pas seulement la connaissance de la personne, mais elle en est la reconnaissance. En effet, c'est un jugement, qui implique le classement basique entre une bonne et une mauvaise réputation¹.

Par ailleurs, la réputation numérique se construit, se défend, en somme elle se gère. Parce qu'elle représente tant une chance qu'un risque, elle implique donc une stratégie d'entreprise au sein de laquelle juriste, économistes et gestionnaires se retrouvent. A partir de ce double constat, nous pouvons retenir la définition suivante de l'e-réputation à savoir l'action d'une personne physique ou morale pour maîtriser l'évaluation sociale portée sur son image numérique.

L'entreprise expose et s'expose sur internet. La maîtrise des informations concernant son image, ses produits ou services représente un enjeu commercial stratégique. D'une part, l'entreprise double son identité réelle d'une identité virtuelle, en opérant un contrôle de l'ensemble des informations qui lui sont relatives sur internet et plus précisément sur les moteurs de recherche et les réseaux sociaux. D'autre part, l'entreprise peut s'employer à augmenter le trafic et la visibilité de son site internet et des espaces sociaux qu'elle occupe. Elle crée ainsi du lien avec les internautes afin de pérenniser la relation client. Sans oublier que l'entreprise participe à l'intelligence économique, c'est-à-dire qu'elle conduit des stratégies industrielles qui reposent sur sa capacité à accéder aux informations².

L'e-réputation, parce qu'aléatoire, appelle à la mise en place d'un dispositif de gestion adapté, elle interpelle donc les juristes principalement en termes de risques, d'atteinte et de défense (Paragraphe 1). Et pourtant, l'e-réputation est un outil de promotion indispensable pour les entreprises. Ainsi, elles sollicitent des agences de communication pour promouvoir et valoriser l'image d'une marque, elles protègent leur patrimoine informationnel et leur e-business par des assurances adaptées ou encore elles utilisent l'outil informatique pour organiser l'accès à l'information. Il est à noter que toutes les entreprises, selon leur dimension et leur conscience numérique ne gèrent pas leur e-réputation avec le même degré de contrôle

¹B. GRUSELLE, « Le défi des nouveaux usages numériques : La sécurité des entreprises à la peine », in Sécurité et stratégie, N°11, Avril 2012, Club des Directeurs de Sécurité des Entreprises, p. 63.

²Amélie FAVREAU, « Protéger la e-réputation de l'entreprise » in L'entreprise à l'épreuve du droit de l'Internet, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris 2014, p.144.

ou de réactivité. De ce fait en cas d'atteinte l'e-réputation d'une entreprise, cette dernière dispose d'un certain nombre d'actions judiciaires pour protéger son e-réputation (Paragraphe 2).

Paragraphe 1 : La gestion préventive de l'e-réputation de l'entreprise.

L'entreprise est la première actrice dans la construction de sa réputation numérique. Seule la personne morale de droit privé nous intéresse dans cette thèse. Du fait de sa personnalité juridique, à savoir son aptitude à être titulaire de droits et assujetties à des obligations, les personnes morales bénéficient d'une réputation pour la défense de laquelle elles peuvent agir en justice. La personnalité d'une personne morale doit être distinguée de celle de ses membres, y compris de celle de ses dirigeants, et ce, quand bien même la structure serait unipersonnelle. Pour autant, la frontière est parfois difficile à tracer entre les atteintes causées aux personnes physiques comme les dirigeants sociaux et celles subies par les personnes morales par ricochet¹.

Dans la communauté des internautes, il existe différents acteurs de l'e-réputation de l'entreprise. Le risque ou la chance de réputation peut être d'un côté une conséquence directe ou indirecte interne à l'entreprise ; émanant des salariés, des concurrents ou encore des influenceurs, ou professionnels. Dans certains cas, il est la conséquence d'un événement externe tel qu'une attaque médiatique provenant de journalistes, de consommateurs, de clients. Ces bâtisseurs de réputation peuvent aussi bien participer avec l'entreprise à la construction d'une réputation numérique positive que la détruire. Pour cela, différentes pratiques sont employées, sur lesquelles nous reviendrons dans la suite de cette thèse, à savoir le *phishing*, le *cybersquatting*, l'utilisation de documents secrets appartenant à l'entreprise, les atteintes à la marque, etc.

Les personnes morales poursuivent un impératif : construire leur image numérique, afin de créer l'influence recherchée. Ainsi, lorsqu'une entreprise décide d'investir dans le développement de son image, elle doit veiller à ce que l'information qu'elle véhicule ne puisse pas altérée. Pour cela, elle peut notamment utiliser des logiciels comme collecteurs

¹R. EDDE, « Le droit : Un outil de régulation du cyberspace ? Le cas du droit à l'oubli numérique », in *L'Homme & la Société*, N° 206, Janvier 2018, L'Harmattan, p. 80.

d'informations directes ou indirectes¹. D'un côté, la veille s'effectue sur les acteurs de l'entreprise, employés clients ou partenaires. Les dirigeants doivent s'assurer que les accès aux divers comptes de l'entreprise (site institutionnel, pages *Facebook* ou *Twitter*...) soient sécurisés au risque de voir de fausses informations diffusées. D'un autre côté, la surveillance porte sur les acteurs d'internet, qu'ils soient consommateurs ou experts-professionnels. Décrivant le pouvoir des consommateurs, un auteur illustre l'impact de l'information diffusé par de simples clics « j'aime » sur un réseau social ou par l'influence générée des influenceurs.

Par ailleurs, dans l'objectif d'une maîtrise de son e-réputation, l'entreprise entre en conversation avec ses publics, ses salariés et ses clients, notamment par l'intermédiaire des réseaux sociaux. Les risques sont évidemment ceux d'une parole donnée et donc déliée. La conversation présente toutefois, l'opportunité pour l'entreprise de conserver un pouvoir de modération du débat, voire de l'orienter. Ces pratiques préventives pour la maîtrise de son e-réputation tendent aujourd'hui à être efficacement doublées d'un cadre juridique².

Paragraphe 2 : Les actions préventives de l'e-réputation de l'entreprise.

Parmi les actions de la gestion préventive figure la présence volontaire qui se manifeste par les techniques de référencement naturel³. L'entreprise qui décide d'optimiser la visibilité de son site internet dispose de plusieurs moyens dont notamment le référencement sur des moteurs de recherche. Elle peut alors améliorer son positionnement, même si l'indexation des sites internet dans les moteurs de recherche est réalisée de façon automatique. Elle emploie des techniques dites de « référencement naturel », qui par des algorithmes confidentiels et évolutifs évaluent automatiquement la pertinence d'un site internet en fonction des mots-clés saisis par un internaute dans le moteur de recherche. Il est donc nécessaire de connaître ces algorithmes pour agir sur le positionnement d'un site. L'entreprise qui souhaite ainsi enfouir certaines informations la concernant, afin que ces informations ne soient plus accessibles au public, pourra agir en vue du référencement. Il s'agit en pratique de définir le nombre de pages que l'entreprise souhaite interposer devant le lien négatif.

¹Le moteur de recherche offre également cette possible surveillance : soit avec le célèbre goggling qui consiste à rechercher des informations sur Google à partir d'un nom ou d'une marque : soit en automatisant ce travail par le service « Google Alerte », qui permet de définir des alertes par mots-clés.

²B. GRUSELLE, *Op.cit.*, p. 62.

³Voir infra p. 172.

L'entreprise peut également faire appel au droit à l'oubli ou droit à l'effacement. L'engouement doctrinal et médiatique pour le droit à l'oubli fait sonner l'expression comme un slogan aux revendications aisées, alors qu'il est aujourd'hui complexe d'en dessiner les contours et de lui assigner un fondement¹. Le droit à l'oubli ne fait pas encore l'objet d'une consécration législative marocaine. Parmi les composants du droit à l'oubli numérique figure le droit au déréférencement. Le déréférencement total de l'entreprise sur internet conduit à sa mort numérique. Ce déréférencement a une portée pratique équivalente à la mise en œuvre d'un droit à l'effacement.

Sous-section 2 : Le numérique et le droit des entreprises en difficulté.

Evoquer les entreprises en difficulté dans le cadre de ce chapitre est indispensable. Le droit des entreprises en difficulté est souvent oublié alors que c'est généralement lorsque l'entreprise est en difficulté et en particulier lorsqu'elle est soumise à une procédure collective que les problèmes apparaissent dans toute leur ampleur surtout avec le développement du numérique. De surcroît, c'est souvent dans ce cadre que l'on peut identifier les causes de la défaillance, même si c'est souvent trop tard². Ainsi, par certains aspects, on peut légitimement se demander si le développement du numérique ne se traduira pas par une déstabilisation du droit des entreprises en difficulté (Paragraphe 1). En revanche, par d'autres aspects, on peut espérer que le développement du numérique permettra un renforcement du droit des entreprises en difficulté (Paragraphe 2).

Paragraphe 1 : Le rôle du numérique dans la déstabilisation du droit des entreprises en difficulté.

Le numérique peut déstabiliser le droit des entreprises en difficulté que ce soit en favorisant la révélation des difficultés des entreprises c'est-à-dire la circulation de l'information (II) ou en favorisant l'apparition de nombreuses et nouvelles entreprises en difficulté autrement dit, il favorise les entreprises vulnérables (II).

¹R. EDDE. *Op. cit.*, p.76.

²P-R. GALLE : « Ubérisation et difficultés de l'entreprise », in IP/IT, N° 7-8, Juillet-Aout 2017, Dalloz, p. 30.

I- Le numérique favorise la circulation de l'information.

L'efficacité de la lutte contre les difficultés des entreprises peut ainsi supposer que les informations sur leur situation plus ou moins précaire ne fassent pas l'objet d'une grande publicité dans le but de protéger leur réputation et éviter un effet de panique de la part de ses collaborateurs, clients, fournisseurs et distributeurs. C'est ainsi que dans le cadre des procédures de prévention des difficultés des entreprises, le législateur met un point d'honneur à prévoir expressément des dispositions visant à assurer la confidentialité du processus.

Or le numérique favorise la circulation de l'information et offre une possibilité de la diffuser rapidement et aisément sous des formes multiples. Le risque est donc que le numérique ne fragilise la confidentialité des procédures de prévention des difficultés des entreprises en favorisant la révélation de ces difficultés. En effet, le droit des entreprises en difficulté pose la règle de la confidentialité des procédures préventives de manière générale dans le monde physique ainsi que dans l'univers numérique. Cependant, la fluidité et la rapidité de circulation propres au numérique rendront nécessairement plus difficile la préservation d'une certaine discrétion dans le cadre des procédures préventives.

Dans les relations entre le droit des entreprises en difficulté et le numérique, ce n'est pas seulement la révélation des difficultés actuelles de l'entreprise qui peut poser problème, mais aussi celle de ses difficultés passées. Le droit des entreprises en difficulté doit donc donner une seconde chance à celui qui, sans faire preuve de mauvaise foi, a connu une première expérience entrepreneuriale malheureuse mais entend revenir sur le marché pour y tenter sa chance. Mais ce nouveau départ sera nécessairement compromis ou extrêmement ardu si le passé économique peu glorieux de l'entrepreneur est sans cesse remonté à la surface. Or si les hommes peuvent oublier, le numérique, lui, n'oublie pas¹. Ainsi, même longtemps après la défaillance, des informations sur une faillite peuvent continuer à circuler sur Internet.

Il est vrai que l'entrepreneur individuel ayant connu un échec et le dirigeant d'une société ayant connu une défaillance pourront invoquer le droit à l'oubli numérique mais malheureusement, au Maroc Il n'existe pas de législation spéciale relative au droit à l'oubli. Ce dernier permet à un individu de demander le retrait de certaines informations qui

¹David. DECHENAUD, Le droit à l'oubli, Mission de recherche Droit et justice, 2014 cité dans L'entreprise face aux défis du numérique, Ouvrage collectif sous la direction d'Alexandre RIERA et Sylvain CHATRY, Mare & MARTIN Paris, 2018. p. 78.

pourraient lui nuire sur des actions qu'il a faites dans le passé. Par contre, en Europe, un entrepreneur ou un dirigeant pourra demander le déréférencement d'une page web associant leur nom à une défaillance passée ou encore l'effacement d'information les reliant à une ancienne faillite et ceci en invoquant le droit à l'oubli numérique tel que renforcé par le règlement sur la protection des données.

Mais au-delà des informations circulant sur Internet, les outils numériques permettent de constituer des fichiers automatisés relatifs aux difficultés passées des entrepreneurs et en favoriser leur diffusion à un public plus ou moins large. C'est le cas du fichier bancaire des entreprises FIBEN¹ de la Banque de France. Le fichier FIBEN permet de recenser des informations sur les entreprises, leurs dirigeants et les entrepreneurs individuels provenant des greffes de tribunaux de commerce, des journaux d'annonces légales ou de tous autres établissements. La consultation du fichier est ouverte notamment aux établissements de crédit, aux établissements de paiement pour leur activité de fourniture de crédit aux entreprises, ainsi qu'à certains services et organismes publics à vocation économique. Il faut noter que l'existence du fichier FIBEN ne devrait pas entrer en conflit avec le règlement général sur la protection des données.

II- Le numérique favorise l'apparition d'entreprises vulnérables.

Le développement du numérique peut également déstabiliser le droit des entreprises en difficulté en fragilisant les entreprises existantes et en favorisant l'apparition de nouvelles entreprises plus vulnérables que celles existantes jusqu'à présent. Pour ce qui est de l'impact du numérique sur les entreprises existantes, on peut noter que la crainte que l'introduction de nouvelles technologies ne se traduise par des destructions d'activités et d'emplois. Ainsi *« avant l'Eden de la création il y a donc l'enfer de la destruction »*².

Le développement du numérique pourrait donc se traduire par des faillites massives d'entreprises traditionnelles. Il est porteur d'innovations radicales qui sont susceptibles d'entraîner dans un premier temps une destruction de valeurs. Les entreprises traditionnelles se retrouvent concurrencées, à travers un phénomène d'ubérisation qui permet, grâce au développement de plateformes facilitant la rencontre entre l'offre et la demande, à une

¹Le Fichier bancaire des entreprises.

²Cheik GALOKHO « Droit des entreprises en difficulté et numérique » in L'entreprise face aux défis du numérique, Ouvrage collectif sous la direction d'Alexandre RIERA et Sylvain CHATRY, Mare & MARTIN Paris, 2018. p.81.

multitude de nouveaux acteurs économiques de les concurrencer ; elles sont également concurrencées par le haut, à travers un phénomène de « *GAFAlisation* », les très grandes entreprises du numérique : *Google, Apple, Facebook, Amazon* attirent vers elles des masses de clients et de consommateurs se détournant des entreprises traditionnelles¹.

La question que l'on peut se poser est celle de savoir si le droit des entreprises en difficulté sera en mesure d'offrir des solutions de sauvetage à l'ensemble de ces entreprises traditionnelles mises en difficulté à cause du développement du numérique. Une réponse négative s'impose. Certes, le droit des entreprises en difficulté pourra permettre à certaines entreprises de se restructurer au sein de procédures collectives notamment pour se doter d'une ossature plus en phase avec les défis économiques posés par la montée en puissance du numérique². Ainsi, délestée du poids d'une grande partie de son passif, l'entreprise pourra, au moins le temps de la procédure collective, mobiliser ses moyens économiques et financiers pour se moderniser et s'adapter à la transformation numérique³. Selon certaines études, une entreprise qui réussit sa mutation numérique bénéficierait d'une augmentation de son résultat opérationnel pouvant aller jusqu'à 40%⁴.

En effet, lors de la réalisation de la mutation numérique, il ne faut pas attendre du droit des entreprises en difficulté des solutions miraculeuses, et ce pour deux raisons. La première c'est qu'il faut concéder que le droit des entreprises en difficulté est loin de constituer un simple outil de gestion. En effet, c'est un droit contraignant, en grande partie judiciaire, rigide et risqué tant pour l'entreprise elle-même que pour ses partenaires. Il est opportun de tenter de procéder à sa mutation numérique avant d'être dans une situation dégradée au point de faire appel aux outils du droit des entreprises en difficulté. La deuxième raison est celle relative aux entreprises dont le modèle économique même sera remis en cause par le développement du numérique, le droit des entreprises en difficulté ne pourra pas leur offrir les débouchés que le marché ne leur offre plus à moins de trouver un nouveau modèle économique, ces entreprises termineront alors en liquidation judiciaire.

¹Ibid. p. 82.

²D. Cuny, « Folie des cryptomonnaies : même Kodak lance Kodakcoin », in La Tribune, N°11, Janv.2018, p.13.

³A cet égard, on peut remarquer, qu'aux Etats-Unis, l'entreprise Kodak, qui a raté le virage des appareils photo numérique et a connu de graves difficultés, semble, après avoir fait l'objet d'une procédure collective en 2012, renaître de ses cendres. En effet, début 2018, Kodak a vu son cours s'envoler en bourse après avoir annoncé son intention de lancer sa cryptomonnaie.

⁴McKinsey Global Institute, « Accélérer la mutation numérique des entreprises : un gisement de croissance et de compétitivité pour la France », Rapport, 2014.

Cela étant, si le développement du numérique devait se traduire par une nouvelle grande phase d'extinction des espèces constituées par les entreprises traditionnelles cela aurait pour conséquence d'accroître le déséquilibre déjà constaté actuellement entre la fonction de sauvetage du droit des entreprises en difficulté et sa fonction d'élimination des entreprises vaincues par le marché. En plus de la fragilisation des entreprises traditionnelles, la révolution numérique entraîne aussi l'apparition de nouvelles entreprises plus nombreuses mais plus fragiles que celles qui existaient jusqu'à présent.

En effet, de multiples acteurs économiques tentent leur chance sur le marché en s'appuyant sur le développement du numérique. C'est le phénomène d'ubérisation. La montée en puissance des plateformes numériques stimule donc la liberté d'entreprendre, mais les entreprises qui naissent ainsi sont le plus souvent de taille extrêmement réduite et présentent des fragilités. Aussi, lorsque la relation entre ces entreprises avec les plateformes ne sont pas requalifiées en contrat de travail, les nouveaux opérateurs économiques issus de l'ubérisation relèveront des procédures préventives et collectives en cas de difficulté¹.

L'interrogation qui peut émerger est celle de savoir si le droit des entreprises en difficulté dispose des outils appropriés pour traiter les difficultés de ces petits débiteurs. En instaurant, un cadre souple et accéléré favorable au rebond, ces procédures sont adaptées aux nouvelles entreprises de l'âge numérique : la fluidité de leur création répond ainsi une certaine fluidité de leur disparition. Il faut sans doute constater, que le phénomène d'ubérisation étant nouveau, on ne dispose pas pour l'heure d'un recul suffisant pour connaître les formes particulières des difficultés que rencontre les entreprises de ce nouvel univers numérique et, par voie en conséquence, les adaptations éventuelles dont le droit des entreprises en difficulté devra faire l'objet. Mais le développement du numérique ne se traduit pas seulement par un risque de déstabilisation du droit des entreprises en difficulté, par certains traits, il peut aussi se traduire par un renforcement de ce droit.

Paragraphe 2 : Le rôle du numérique dans le renforcement du droit des entreprises en difficulté.

Le développement du numérique peut d'abord renforcer le droit des entreprises en difficulté en favorisant la transparence et l'efficacité des procédures collectives (I). La montée

¹CE, « Puissance publique et plateformes numériques : accompagner l'ubérisation », Etude annuelle, Juill. 2017.

en puissance du numérique peut ensuite renforcer le droit des entreprises en difficulté en favorisant la prévention des défaillances (II).

I- Le numérique au service des procédures collectives.

On peut relever que le développement du numérique favorise la transparence et l'efficacité des procédures collectives dans les relations avec les candidats repreneurs, avec les créanciers et avec le débiteur. Pour ce qui est des relations avec les candidats à la reprise d'une entreprise en difficulté, il convient de rappeler au préalable que la transparence est une nécessité dans le cadre de la cession des entreprises en difficulté. Le législateur a pris conscience du rôle positif que pouvait jouer la transparence dans le cadre des procédures de cession des entreprises en difficulté. En effet, une certaine dose de transparence est indispensable dans les procédures de cession pour susciter un nombre suffisamment important de candidatures concurrentes et offrir ainsi au tribunal une diversité de choix qu'il pourra mettre à profit pour opter pour l'offre qui permettra de préserver le plus d'activités et d'emplois, et qui permettra de désintéresser le plus de créanciers.

De plus, pour que la concurrence puisse jouer entre les candidats à la reprise il faut que les offreurs potentiels soient informés de l'existence et des caractéristiques de l'entreprise ainsi que des actifs cédés. Raison pour laquelle une publicité de l'appel d'offre doit être générale d'où le rôle important du numérique. Néanmoins, le législateur marocain n'a pas prévue une publicité sur internet. En effet, le non appel à la publicité électronique limite la portée de la publicité et donc de sa concurrence. La publicité servirait en effet à la concurrence en permettant aux personnes susceptibles de faire une offre concurrente de consulter les offres existantes. Aussi, cette concurrence se fera au profit des salariés, des créanciers, et, en définitive, de l'ensemble de la collectivité.

Pour ce qui est des relations entre les créanciers, le développement du numérique favorise les échanges entre ces derniers et les professionnels du traitement des difficultés des entreprises. En atteste les initiatives prises au niveau européen qui facilitent les démarches des créanciers dans le cadre de procédures collectives étrangères en s'appuyant sur le numérique. Ainsi, il y'a possibilité pour les créanciers d'obtenir des informations et documents sur les procédures d'insolvabilité via le portail européen e-justice et le système d'interconnexion des registres de commerce européens qui a été mise en place en 2019¹. Ce système

¹Cheik GALOKHO, *Op.cit.*, p. 88.

d'interconnexion permet aux créanciers d'accéder gratuitement à un ensemble d'informations relatives aux procédures d'insolvabilité ouvertes dans tout Etat membre de l'UE. La recherche de ces informations peut se faire dans toutes les langues officielles de l'UE, même si ces informations elles-mêmes ne seront pas forcément traduites. Le numérique pourra ainsi permettre d'atténuer les barrières constituées par la distance et la langue pour les créanciers dont les intérêts sont en cause dans une procédure d'insolvabilité ouverte dans un Etat membre de l'UE autre que celui dont ils sont ressortissants.

Pour ce qui est des relations avec les débiteurs, le numérique peut être utilisé pour réunir et faire circuler plus facilement les informations permettant de favoriser le traitement de leurs difficultés et éventuellement les poursuites dans les cas où ils auraient eu des comportements abusifs au détriment de l'entreprise et de ses créanciers.

II- Le numérique : un outil de prévention des difficultés des entreprises.

Le droit des entreprises en difficulté peut être bouleversé par ce qu'on appelle la justice prédictive¹. La question qui se pose ici est celle de savoir si l'on peut, grâce au numérique, prédire les défaillances et ainsi les prévenir bien avant qu'elles ne surviennent. A cet égard, on peut remarquer que, pour améliorer la prévention des difficultés des entreprises, on peut utiliser les données collectées afin de développer un algorithme qui servirait de modèle prédictif de défaillance des entreprises. Une fois la prédiction de difficulté établie, une alerte serait envoyée dans le but d'enclencher une mise en relation avec le médiateur des entreprises ou le tribunal de commerce compétent².

Avec le développement des algorithmes, le droit des entreprises en difficulté entend lui aussi prédire les défaillances bien avant leur apparition et ainsi les empêcher. Une telle approche numérique de la prévention des difficultés des entreprises, si elle devait se développer et d'imposer, poserait d'immenses problèmes juridiques³. La principale question

¹Appelé aussi par le traitement informatisé de la jurisprudence c'est un logiciel d'anticipation des décisions de justice sur la base de l'analyse d'une grande quantité de jurisprudence.

²Une expérience de ce type est menée depuis 2015 dans la région Bourgogne-Franche-Comté. Semble ainsi appelée à se développer une sorte de droit des entreprises en difficulté « minority report ». Dans la fameuse nouvelle de Philip K. Dick, adaptée au cinéma par Steven Spielberg, est décrit un monde dans lequel des êtres humains mutants dotés du don de préséance peuvent prédire un crime et permettre l'arrestation de son auteur en puissance avant même que l'infraction n'ait germé dans son esprit. La première édition de la nouvelle date de 1956.

³J. DUPRE et J. LEVY VEHEL, « L'intelligence artificielle au service de la valorisation du patrimoine jurisprudentiel », in IP/IT, N°10, Octobre 2017, Dalloz, p. 500.

donc qui se pose est : jusqu'ou iront ces nouvelles technologiques ? dans un futur plus ou moins proche, on peut ainsi imaginer des machines mettant en œuvre des algorithmes permettant de déterminer à partir des expériences d'un individu, de son passé, de sa formation, de sa psychologie, de sa manière d'être, de sa manière de penser, si l'entreprise qu'il envisage de créer n'est pas prédestinée à une faillite certaine¹.

Les algorithmes permettraient de n'autoriser la création que des entreprises qui ne rencontreraient pas de difficulté. Ainsi apparaîtrait une société sans entreprise en difficulté, sans faillites, sans défaillances et sans droit des entreprises en difficulté, celui-ci disparaissent faute d'objet. Et l'homme vivrait heureux dans un univers aseptisé, sans risque, sans erreur, sans faille. Tout serait ainsi bien dans le meilleur des mondes numériques possibles. Tout se passerait comme dans un rêve, mais il faudra être vigilant car on sait que la limite entre le bon et le mauvais rêve est parfois ténu.

¹Hubert KRIVIN, L'IA peut-elle penser ? Miracle ou Mirage de l'intelligence artificielle, De Boeck, Paris, 2021, p. 25.

Chapitre II

Le numérique et la transformation des relations de travail

Digitalisation, robotisation, intermédiation, uberisation etc. Les débats ont pris, en droit du travail, une coloration nouvelle : celle du numérique. « *La révolution numérique frappe à la porte du droit du travail* »¹. Bien qu'elle ne s'ouvre pas suffisamment vite, elle produit tout même ses effets, et cela de très nombreuses manières. Aujourd'hui, les nouvelles technologies de l'information et des communications (NTIC), la capacité de générer et d'exploiter des quantités magistrales de données² couplées avec les nombreuses et surprenantes avancées de la robotique, façonne le monde du travail.

L'utilisation des nouvelles technologies de l'information et des communications dans la production de biens et services influence de façon substantielle le modèle organisationnel des entreprises. Les rapports consacrés à la question de la digitalisation du monde de travail se sont multipliés, les premières décisions de justice commencent à tomber. La doctrine s'est également emparée du sujet. Cette dernière s'est donnée pour programme de travail l'analyse des rapports entre le droit du travail et les nouvelles technologies.

Au cœur de cette problématique : le courriel, le secret des correspondances et la frontière entre la vie professionnelle et la vie privée. Depuis lors, la problématique s'est mue vers les conditions de contrôle des salariés, les modes de preuves admissibles et la protection des données personnelles des salariés. L'ensemble de ces évolutions impose un constat : celui de la malléabilité de la technique juridique aux évolutions technologiques. Aujourd'hui encore la problématique a évolué. C'est un lieu commun d'affirmer que les frontières de la subordination se trouvent très largement réinterrogées depuis que certaines entreprises profitant du formidable potentiel offert par les technologies du numérique, ont investi des pans entiers de l'activité³.

¹Sébastien TOURNAUX, « Droit du travail et numérique : de quelques aspects relatifs aux relations individuelles de travail » in *L'entreprise face aux défis du numérique*, Ouvrage collectif sous la direction d'Alexandre RIERA et Sylvain CHATRY, MARE & MARTIN, Paris, 2018, p. 59.

²G. VALENDUC et P. VENDRAMIN, « Le travail dans l'économie digitale : continuités et ruptures », European Trade Union Institute, Working Paper, Mars 2016, Bruxelles, p. 20.

³B. PEREIRA, « Mutation du rapport de subordination : le salarié « autonome » ou l'indépendant « subordonné » en France », in *Management et Avenir*, N° 104, Octobre 2018, Management Prospective, p. 38.

La digitalisation pose au droit de travail un défi à deux niveaux : un défi dans les relations individuelles de travail (Section 1) et un défi dans les relations collectives de travail (Section 2).

Section 1 : Le numérique et les relations individuelles de travail.

Dans le monde du travail, la numérisation sous sa forme actuelle désigne le recours accru à l'informatique en nuage, aux outils de planification et aux applications facilitant le télétravail et le travail collaboratif sur plateforme. Depuis le début de la pandémie de la Covid-19, la progression de la numérisation s'est accélérée, et les entreprises ont recouru aux technologies numériques pour permettre aux travailleurs de poursuivre leur travail à domicile. Avant même la pandémie, le processus de numérisation avait déjà commencé à modifier profondément les modes d'organisation de l'emploi et des milieux de travail, avec plusieurs conséquences potentiellement importantes tant en ce qui concerne les qualifications et compétences exigées des travailleurs, que leur bien-être et les normes du travail.

La compréhension des formes de mobilisation du travail dans l'économie du numérique n'est pas une sinécure. Cette compréhension invite en effet à s'abstraire des catégories d'analyse traditionnelle. On parle désormais de télétravail (Sous-section 1) et de travail par intermédiation des plateformes numériques (Sous-sections 2). Par ailleurs, l'utilisation des nouvelles technologies dans le monde du travail implique un traitement corrélé des données à caractère personnel de manière intensive notamment ceux des salariés, se pose alors la question de la protection des données personnelles des employés dans le cadre de la relation du travail (Sous-section 3).

Sous-section 1 : La dématérialisation du travail : le télétravail.

Le numérique est l'un des moyens ayant permis l'apparition puis le développement de nouvelles conditions de réalisation du travail à distance, ce qui peut aussi bien convenir à l'entreprise qu'à ses salariés. Il s'agit essentiellement ici de la question du télétravail qui a connu un développement spectaculaire au cours des dernières années¹. L'essor des NTIC a permis l'avènement de l'une des premières manifestations de la dématérialisation, soit le télétravail au tournant des années 2000. Un certain nombre d'entreprises et de grands cabinets de conseil avaient institué des environnements et des règles de télétravail afin de mutualiser

¹Sébastien TOURNAUX. *Op.cit.*, p. 62.

les espaces et d'économiser sur les loyers.¹ Plus proches de nous, la pandémie de la Covid-19 a mis un gros coup de projecteur sur ce mode de travail à distance qui n'est pas si nouveau. Tous les pays pour lesquels on dispose de données comparables ont enregistré une hausse des taux de télétravail durant la pandémie de Covid-19².

Le télétravail progresse dans toutes les économies développées, ce qui confirme qu'il apporte de nombreux avantages, tant pour les salariés que pour les entreprises. Il s'agit d'une forme nouvelle d'organisation du travail, qui découle de l'évolution des technologies et des mentalités. Les hommes et les organisations doivent s'adapter à cette nouvelle réalité. Cette réalité qu'il convient d'analyser son cadre général (Paragraphe 1) avant de développer son cadre juridique (Paragraphe 2).

Paragraphe 1 : Le cadre général du télétravail.

Le télétravail se définit comme un travail à distance. Télé signifie à distance comme dans les mots téléphone ou télévision. Le télétravail salarié se définit comme, un travail fait hors des locaux de l'entreprise, de façon volontaire, en utilisant les technologies de l'information et de la communication. Cette définition juridique peut être complétée par la définition de L'Organisation International du Travail (OIT) dans son rapport de 2017³ qui distingue trois types de télétravailleurs : les télétravailleurs à domicile qui travaillent de la maison plusieurs fois par mois, les télétravailleurs nomades qui travaillent de la maison plusieurs fois par semaine dans différents lieux autres que les locaux de l'employeur et les télétravailleurs occasionnels qui travaillent hors des bureaux moins souvent que les nomades.

Ces deux définitions illustrent le fait que le télétravail prend de nombreuses formes, et porte des noms variés (télétravail, travail à domicile, *coworking*, *cyberworking*, e-travail,

¹J-M. MOREL, « Le télétravail, mode de travail en évolution ou en révolution ? », in Revue française de comptabilité, N° 551, Mars 2021, p. 37.

²En France, le taux de télétravail a plus que doublé, ce qui représente une hausse de 25 points de pourcentage, tandis qu'au Royaume-Uni, en avril 2020, le taux de télétravail était 1.8 fois supérieur à celui observé avant la pandémie, soit une hausse de 20 points de pourcentage. En Australie, en décembre 2020, le niveau de télétravail était 1.5 fois supérieur à celui d'« avant mars 2020 », soit une hausse de 15 points de pourcentage. Au Japon, qui n'a pas instauré de confinement généralisé en 2020, les taux de télétravail ont nettement augmenté, passant de 10 % en décembre 2019 à près de 28 % en mai 2020, même s'ils sont restés bien en deçà des niveaux observés dans les pays susmentionnés. En Italie, au deuxième trimestre 2020, les taux de télétravail étaient plus de quatre fois supérieures à ceux enregistrés avant la pandémie, progressant de 15 points de pourcentage en un an. Enfin, le télétravail a doublé au Brésil, passant de 5 % en 2019 à plus de 10 % en mai 2020. OCDE, Digital Economy Outlook 2020, éd. OCDE, 2021, Paris.

³OIT et Eurofound, « Travailler en tout temps, en tout lieu: les effets sur le monde du travail », Rapport, Genève, 2017.

travail à distance, *remote*, travail nomade, travail flexible, *home-office*, flex office...). Mais toutes ces formes de télétravail, comportent de nombreuses caractéristiques communes. On parle souvent de travail à domicile lorsqu'on parle de télétravail. Cela se comprend car cette situation est la plus courante. Mais les deux notions ne sont pas équivalentes d'un point de vue juridique¹.

Le travail à domicile est défini au niveau de l'article 8 du Code de travail marocain.² Avant les salariés travaillaient à leur domicile pour effectuer des tâches d'assemblage de petits objets (ciseaux, montres...). Ces salariés étaient payés à la tâche, souvent très peu. Pour pouvoir survivre, ils devaient travailler de nombreuses heures et également faire travailler leurs enfants. Des situations épouvantables ont amené le législateur à voter des lois sociales pour protéger les travailleurs à domicile.

Le télétravail, lui, suppose l'utilisation de l'informatique et des télécommunications. En d'autres termes, le télétravail est un travail effectué par un ou plusieurs salariés hors des locaux de l'entreprise au moyen des technologies de l'information et de la communication³. La caractéristique du télétravail c'est qu'il permet de travailler sans contrôle direct c'est-à-dire sans la pression sociale de l'employeur. La contrepartie c'est qu'il faut réaliser un travail suffisant pour que la situation puisse perdurer. C'est-à-dire être son propre employeur, être capable de se mettre au travail sans qu'autrui ne vous dicte cette action.

L'unité de temps et de lieu qui caractérisait la collectivité de travail, le fait que le personnel d'une entreprise travaille sur un même lieu de travail, aux mêmes horaires et dans une organisation hiérarchique pyramidale tend à s'effacer (I). Cet effacement procure des avantages et des inconvénients pour l'entreprise. (II). Raison pour laquelle les entreprises ont le choix de mettre en place la forme de télé travail qui leur convient (III).

¹OIT, « Le travail à domicile de l'invisibilité au travail décent », Résumé analytique, Genève, 2020, p. 1.

²Article 8 du Code de travail énonce que : « sont considérés comme salariés travaillant à domicile, ceux qui satisfont aux conditions suivantes et ce, sans qu'il y ait lieu de rechercher s'il existe ou s'il n'existe pas entre eux et leur employeur un lien de subordination juridique, s'ils travaillent ou ne travaillent pas sous la surveillance immédiate et habituelle de leur employeur, si le local où ils travaillent et l'outillage qu'ils emploient leur appartiennent ou non, s'ils fournissent, en même temps que le travail, tout ou partie des matières premières qu'ils emploient lorsque ces matières leur sont vendues par un donneur d'ouvrage qui acquiert ensuite l'objet fabriqué ou leur sont livrées par un fournisseur indiqué par le donneur d'ouvrage auprès duquel les salariés sont tenus de s'approvisionner ou s'ils se procurent eux-mêmes ou non les fournitures accessoires : 1° être chargés soit directement, soit par un intermédiaire d'exécuter un travail, moyennant une rémunération, pour le compte d'une ou plusieurs des entreprises visées à l'article premier ci-dessus ; 2° travailler soit seuls, soit avec un seul assistant ou avec leurs conjoints ou leurs enfants non salariés. »

³A.GHALI, « Le télétravail et le droit du travail », in Revue du droit marocain, N° 14, Avril 2009, p. 57.

I- Lieu et temps du télétravail.

Le télétravail en pratique, peut s'effectuer depuis n'importe quel lieu du moment que l'on a accès à internet et qu'on peut accéder au système d'information de l'entreprise. Dans les entreprises, des règles précisent les lieux autorisés, le plus souvent, le domicile. De nombreux accords d'entreprise autorisent également le télétravail depuis une maison secondaire ou depuis le domicile d'un proche. Des télétravailleurs travaillent depuis un hôtel, et dans tous les lieux de déplacement que sont les trains, les métros, les aéroports, après une mission d'inspection, une action commerciale, une mission de dépannage. Enfin il est possible de télétravailler depuis un télécentre, un tiers-lieu, un espace de *coworking*, ou un bureau délocalisé de l'entreprise.

Le télétravail peut se faire n'importe quand, 24 heures sur 24, 7 jours sur 7, contrairement au travail au bureau, qui se déroule durant les heures d'ouverture physique de l'entreprise. Cette limitation des horaires, induit par le bureau, a des vertus pour protéger la santé du salarié qui normalement, passé 8h, s'arrête de travailler. L'employé est incité à partir car il voit ses collègues faire de même, il subit les contraintes de transport, etc¹. Au contraire, à la maison, il est possible de travailler en dehors des horaires officiels. Cette liberté est intéressante car elle permet une organisation adaptée à sa vie privée et ses contraintes personnelles. Mais d'un autre côté c'est évidemment un risque important qui apparaît pour la santé et pour la vie familiale.

Cette possibilité de travailler à toute heure du jour et de la nuit est exclue par les chartes du télétravail dans les entreprises, pour les salariés, qui normalement, doivent suivre les règles officielles calquées sur les horaires de bureaux. Des situations sont pires lorsque par exemple les salariés d'une multinationale travaillent avec des interlocuteurs en Asie ou en Amérique. Dans ce cas, la journée peut débuter à 6 heures du matin et de terminer à 23 heures. Dans ces situations, la mise en place du télétravail permet d'améliorer la vie du salarié, qui n'a plus à se déplacer au bureau, et gagne ainsi de nombreuses heures de sommeil, à des horaires variables. En revanche, les risques de dérives sont accrus, et la vigilance et l'hygiène de vie doivent être préservées.

¹Matthieu BILLETTE DE VILLEMEUR, Le Télétravail en pratique, GERESO, coll. L'essentiel pour agir, Paris, 2019, p. 13.

II- Les avantages et les inconvénients du télétravail.

Le télétravail comporte de nombreux avantages pour l'entreprise. Il permet de renforcer la motivation des salariés. Cette satisfaction est naturellement favorable à l'entreprise. Par ailleurs le télétravail réduit l'absentéisme pour de nombreuses raisons. Par exemple un salarié qui, avec deux heures de trajet matin et soir, se retrouve ensuite dans un lieu ouvert dont l'ambiance est mauvaise. Il va souffrir. Une telle situation est grandement améliorée par la mise en place du télétravail qui réduit la fatigue du salarié. De plus le télétravail facilite le recrutement, lorsque par exemple on recrute un salarié avec des compétences rares, il est facile de le trouver si on accepte le télétravail, car il pourra habiter beaucoup plus loin, éventuellement dans un autre pays, et venir une fois par trimestre dans l'entreprise. Les économies permises par le télétravail constituent également un atout essentiel et permettent de réduire les mètres carrés de bureau nécessaire. Aussi les gains de productivité sont le premier argument en faveur du télétravail. On constate systématiquement des gains de productivité importants lorsqu'une personne travaille depuis son domicile.¹

En outre, le télétravail préserve l'activité en cas de problème extérieur à l'entreprise. Par exemple au moment de la menace de pandémie de la Covid-19, toutes les entreprises ont été invitées à mettre en place des plans de continuité d'activité intégrant le télétravail. On souhaitait éviter des contaminations². Au cas où l'on aurait du confiner les salariés à leur domicile, pour éviter qu'ils ne s'infectent dans les transports ou au bureau, il fallait que l'économie continue à fonctionner. Enfin le télétravail renforce la flexibilité de l'entreprise car il permet de réaffecter des ressources d'un simple mail sans avoir à déménager physiquement les bureaux ou les salariés.

¹La société Danone a mis en place le flex office : plus de bureau attiré, tous se partagent les tables au gré des absences des uns et des autres. Les salariés sont poussés hors les murs « plus on libère, meilleure sont la productivité et l'engagement. La preuve, c'est qu'avec le télétravail on obtient 30% de productivité plus » affirme le DRH.

²S. FRIMOUSSE et J-M. PERETTI, « Repenser la culture d'entreprise après la crise Covid-19 », in Questions de management, N° 3, Janvier 2021, EMS Editions, p. 151.

Néanmoins, le télétravail pose également des problèmes pour l'entreprise, notamment au démarrage car il faut modifier l'organisation et changer les mentalités. Le premier inconvénient du télétravail est d'augmenter les risques pesant sur les données de l'entreprise. Elles doivent être désormais accessibles via Internet. Il faut donc mettre une infrastructure informatique pour sécuriser ces accès Internet. Cette infrastructure est couteuse en matériels, logiciels et ressources humaines et n'est pas sans faille. Le télétravail ne fait qu'augmenter le nombre de personnes connectées à distance. Le service informatique doit redimensionner les serveurs en conséquence.

Encore, le plus sérieux inconvénient lié au télétravail est le risque de perdre l'attachement à l'entreprise et au service de la part des télétravailleurs. Lorsque tous les matins chacun retrouve ses collègues autour de la machine à café, un esprit d'équipe se crée spontanément. En revanche, si les employés sont à distance, isolés le risque de désintérêt, de détachement vis-à-vis de la structure grandit. Egalement, une objection que l'on fait parfois, lors de la mise en place du télétravail, est le risque qu'il fait courir à l'innovation. Cette crainte s'appuie notamment sur l'exemple d'IBM¹ qui a arrêté le télétravail en utilisant cet argument. La productivité n'est pas le plus important pour les entreprises, ce qui compte c'est la capacité à innover. Et selon certains le télétravail nuit à l'innovation car il réduit l'enthousiasme permis par les rencontres sur site, le télétravailleur isolé a moins d'idées nouvelles, celles-ci reçoivent moins d'attention.

III- Les formes du télétravail.

Le télétravail peut prendre de nombreuses formes. Il est utile de les passer en revue.

D'abord, le télétravail pendulaire c'est une forme très répandue de télétravail, qui consiste à travailler quelques jours par semaine à la maison et quelques jours au bureau. Cette forme de télétravail est très simple à mettre en place tant que le nombre de jours télétravaillés est limité à un ou deux. Les modifications générées par ce changement sont relativement limitées. L'isolement, souvent évoqué comme une menace pour le télétravailleur, est réduit. Les changements de fonctionnement du service restent également limités. Il suffit de quelques mois pour que la situation devienne routinière.

¹International Business Machines Corporation : une société multinationale américaine présente dans les domaines du matériel informatique, du logiciel et des services informatiques.

Ensuite, le télétravail alterné. C'est une forme moins courante du télétravail que l'on rencontre notamment lors de missions de contrôle comme l'audit ou l'inspection. Un déplacement sur site permet de contrôler que les règles sont bien respectées. Cette partie du travail ne peut se faire qu'en déplacement. Une deuxième partie de rédaction de rapport, se réalise très bien en télétravail car elle nécessite de la concentration et du silence¹.

Puis, le télétravail fixe qui est la méthode la plus simple. Le jour ou les jours de télétravail étant fixés, cela devient très vite une habitude de mettre de côté, en prévision du jour de télétravail, les dossiers à traiter au calme. Mais cette fixité doit comporter une certaine souplesse. Il est important de rappeler ici qu'il faut systématiquement tracer par mail cet accord entre l'employeur et son salarié sur la modification du jour de télétravail. Parce que si durant le trajet de retour sur le site, un accident se produit, il existe un risque que le caractère d'accident de trajet et donc d'accident de travail soit contesté par la sécurité sociale. Le salarié aurait du rester chez lui puisqu'il était en télétravail. En revanche si cette modification de l'organisation habituelle du travail a été notée, l'accident de trajet survenu un jour qui aurait du être en télétravail ne sera pas qualifié d'accident domestique².

De même, durant le jour de télétravail choisi en remplacement du jour initial, un accident peut survenir. Le risque serait que la qualification d'accident du travail soit refusée au motif que ce jour-là, le salarié aurait du être au bureau et donc, s'il se trouvait chez lui, cela signifie qu'il était en congé. L'accident survenu à son domicile n'est donc pas un accident du travail. Tous ces problèmes disparaissent si la modification du jour de télétravail a bien été notée au préalable³.

Par ailleurs, le télétravail variable (appelé aussi flottant, flexible) consiste en une modalité où, tous les mois, les salariés décident avec l'employeur des jours de télétravail du mois à venir. Ainsi les variations de l'organisation sont plus faciles à gérer. Le défaut de cette organisation est de rendre moins transparents les jours de télétravail pour les collègues. Cette solution est en revanche beaucoup plus souple, elle convient très bien une fois que de bonnes habitudes de gestion du temps pour les télétravailleurs et les non télétravailleurs ont été mises en place dans l'entreprise. Il faut noter enfin que de nombreuses entreprises combinent entre les deux possibilités, fixe et variable.

¹Matthieu BILLETTE DE VILLEMEUR, *Op.cit.*, p. 15.

²Ibid., pp. 16-17.

³OIT, « Le télétravail Durant la pandémie de Covid-19 et après », Guide Pratique, 1^{ère} éd. Genève, 2020, p. 12.

En outre, le télétravail complet correspond aux situations de travail à domicile à 100%. Des entreprises ferment des établissements entiers afin de faire des économies de mètres carrés ou en raison de crise comme par exemple au cours de la crise sanitaire de la Covid-19. Ils placent leurs salariés en télétravail à 100%.

Enfin, le télétravail nomade concerne l'immense cohorte des dépanneurs, techniciens qui se déplacent et se connectent à distance au système d'information de l'entreprise pour travailler. Et également les voyageurs qui travaillent depuis l'hôtel, la gare, l'aéroport, ou qui restent chez eux à leur retour de mission, pour traiter les mails accumulés, plutôt que de revenir au bureau après une nuit trop courte.

Paragraphe 2 : Le cadre juridique du télétravail.

A l'origine, le télétravail est généralement mise en place pour des périodes limitées. Aujourd'hui, suite aux développements du numérique de nombreux travailleurs sont actuellement contraints de télétravailler à temps plein. Ce changement du mode de travail à suscité des interrogations quant à son cadre juridique et beaucoup d'employé et employeur ont fait appel à sa réglementation (I). De plus, l'utilisation du numérique peut accroître la durée effective du travail se qui pose la question du droit à la déconnexion (I).

I- L'appel à une réglementation du télétravail.

La réglementation en matière de télétravail s'avère insuffisante et le respect de la réglementation en vigueur demeure un véritable défi, précise l'Organisation Internationale du Travail. De nombreux pays à travers le monde disposent d'une réglementation, parfois complétée par des conventions collectives, afin de s'attaquer aux différentes formes de lacunes en matière de travail décent liés au télétravail. Cependant, seuls dix Etats membres de l'OIT ont ratifié la convention n° 177 chargée de promouvoir l'égalité de traitement entre les travailleurs et travailleur à domicile et les autres salariés, et peu de pays disposent d'une politique globale sur le travail à domicile.

Dans son guide pratique intitulé : « le télétravail durant la pandémie de la Covid-19 et après » publié en 2020, l'OIT vise à offrir des recommandations pratiques et aider les décideurs à actualisé le cadre juridique existant et proposer un cadre plus flexible. En effet, le guide met l'accent sur l'importance d'axer les efforts sur les conséquences juridiques et contractuelles du télétravail. Ainsi, il est essentiel de prévoir dans les accords de télétravail

des dispositions sur les postes de travail, le remboursement des frais liés au télétravail, les modifications du contrat de travail et les procédures de signalement en cas d'empêchement de travailler, de maladie ou d'accident du travail. Les entreprises doivent sécuriser plusieurs aspects juridiques liés au télétravail et souscrire une police d'assurance couvrant les risques d'accidents du travail pendant la période de télétravail. Egalement, il convient de sensibiliser les télétravailleurs aux questions relatives à la responsabilité juridique en cas de perte, dommage ou vol des équipements dont ils se servent à domicile, qu'ils leur appartiennent ou qu'ils soient la propriété de l'entreprise.

L'OIT a ensuite publié un rapport¹ en 2021 qui contient un certain nombre de recommandations concrètes afin de donner de la visibilité au travail à domicile et, de cette manière, améliorer la protection dans ce domaine. En ce qui concerne les personnes en télétravail, le rapport demande aux législateurs de mettre en place des mesures spécifiques afin d'atténuer les risques psychosociaux et d'introduire un droit à la déconnexion pour assurer le respect des frontières entre vie professionnelle et vie privée. Le rapport estime enfin que le télétravail devrait prendre une importance encore plus grande dans les années à venir. Les gouvernements, en collaboration avec les organisations de travailleurs et d'employeurs, doivent œuvrer ensemble afin de s'assurer que l'ensemble des télétravailleurs puissent passer de l'invisibilité au travail décent.

En droit marocain force est de constater un vide juridique remarquable régissant le télétravail notamment. Le législateur marocain a modifié la loi n° 65-99 formant le Code de travail, qui est intervenu à la lumière des transformations internationales caractérisées par le changement économique et technologique. Or, bien que le législateur a avait essayé d'instaurer un arsenal juridique adéquat à ces mutations technologiques et économiques, mais il n'avait pas réglementé le cadre légal du télétravail². La seule intervention réglementaire a été durant la période de la crise sanitaire de la Covid-19 et notamment lors du confinement ou le ministre de l'Economie, des Finances et de la réforme de l'administration a mis en place un guide pratique pour la possibilité d'organiser le télétravail au sein de la fonction publique³.

¹International Labor Organization, « Working from home: From invisibility to decent work », Geneva, 2021, p.19.

²I. CHIBANI et H. KABIR, « Le télétravail comme mode alternatif : Quel statut juridique ? », in Revue du Chercheur dans les Etudes et les Recherches Juridiques et Judiciaires, N° 38, Janvier 2022, p. 527.

³Ministre de l'économie des finances et de la réforme de l'administration, « Guide pratique des mesures préventives dans les services publics », Mai 2020, p.24.

Au niveau de la doctrine, rare sont les auteurs certains auteurs ont dégagé d'innombrable problématique sur le télétravail tel que lien de subordination du télétravailleur, ou encore la qualification des télétravailleurs. Au niveau du contrat de travail conclu entre l'employeur et le télétravailleur, il est vrai que le contrat de travail fait partie des contrats consensuels pour lesquels aucune forme spécifique n'est requise¹, sauf dans certains cas où le législateur prévoit la nécessité d'un écrit², cependant le contrat de travail à distance connaît quelques particularités dues à son articulation avec des moyens de communication modernes. Dans ce cadre, le législateur a pris l'initiative de promulguer loi n° 53-05 relative à l'échange électroniques de données juridiques, permettant la possibilité de conclure des contrats numériques³, y compris le contrat de travail à distance, tout en respectant les dispositions juridiques en vigueur⁴. Néanmoins, cette loi reste insuffisante pour régir les lacunes juridiques qui se posent en matière de télétravail.

A titre de droit comparé, en France le droit du télétravail remonte à 2002, date du premier texte définissant les règles régissant ce nouveau mode de travail. L'article 46 de la loi du 22 Mars 2012 introduit le mot télétravail dans le Code de travail français, mais n'apporte pas de précisions complémentaires. Un décret du 11 février 2016⁵ a apporté quelques règles supplémentaires. Enfin les ordonnances Macron de Septembre 2017⁶ simplifient le cadre juridique national pour le secteur privé.

Lorsqu'on étudie ces textes, on constate qu'ils établissent des règles très générales, qui permettent de nombreuses variantes de télétravail. Chaque entreprise peut et doit apporter des précisions dans un accord d'entreprise qui fixe les règles relatives au télétravail ou une charte qui est une solution plus simple à mettre en œuvre, car elle est élaborée directement par l'employeur, de façon unilatérale⁷. Même un simple mail entre un salarié et son chef peut suffire. Cette situation se rencontre déjà dans de nombreuses entreprises, de nombreuses occasions. L'accord de l'employeur est évident, implicite, non contestable, s'il utilise les mails, SMS ou autres pour communiquer avec le salarié, car celui-ci n'est pas dans les locaux.

¹V. art. 723 du DOC et art. 15 du Code de travail.

²V. art. 80 et 501 du Code de travail.

³V. infra p. 115.

⁴Il faut que le contrat de travail à distance obéisse aux dispositions juridiques du code de travail marocain.

⁵Décret n° 2016-151 du 11 février 2016 relatif aux conditions et modalités de mise en œuvre du télétravail dans la fonction publique et la magistrature.

⁶Ordonnance n° 2017-1387 du 22 septembre 2017 relative à la prévisibilité et la sécurisation des relations de travail.

⁷Matthieu BILLETTE DE VILLEMEUR, *Op.cit.*, p. 24.

L'accord collectif ou à défaut la charte précise plusieurs règles dont les modalités de contrôle du temps de travail ou de régulation de la charge du travail. Dans les entreprises, cette clause se traduit souvent par un rappel sur les horaires légaux et sur l'égalité de la charge de travail pour les télétravailleurs. Cette clause est importante pour préserver la vie privée du salarié, elle préserve le droit à la déconnexion.

L'action syndicale est également modifiée par la présence du télétravail dans l'entreprise. Lorsque les salariés télétravaillent, on ne peut plus distribuer des tracts à l'entrée de l'entreprise. Mais l'action syndicale garde son utilité. Les modalités d'action doivent évoluer vers un recours accru aux moyens de communication modernes comme les messageries et réseaux sociaux. Enfin en cas de survenance d'un accident sur le lieu où est exercé le télétravail pendant l'exercice de l'activité professionnelle du télétravailleur. Il est présumé être un accident de travail. Ce point est une garantie pour le télétravailleur. Toutefois, les tâches télétravaillables, le plus souvent assis devant un ordinateur, ne sont pas risquées et n'entraînent que très peu d'accidents de travail. L'essentiel des accidents du travail dans les entreprises sont des accidents de trajet qui disparaissent avec le télétravail.

Quant à la jurisprudence, elle a précisé certains points, mais elle reste limitée, car pour que la Cour de cassation puisse statuer sur le télétravail, il faut conflit entre un employeur et son salarié en télétravail, et ces situations sont longtemps restées rares.

II- Le droit à la déconnexion.

Les outils numériques (Smartphones, portables) offrent de nouvelles possibilités de travail à distance. Ces nouveaux outils entraînent aussi des nuisances. Nous devons désormais collectivement définir et respecter de nouveaux usages, de nouvelles règles de savoir-vivre, de nouvelles façons de travailler, pour éviter des dérives. Les personnes salariées utilisent de plus en plus les NTIC à leur disposition pour mettre en place un régime de travail souple et à assurer un équilibre travail-vie personnelle plus satisfaisant. Les régimes de travail flexibles permettent aux personnes salariées de modifier de façon permanente ou temporaire leur horaire de travail, le nombre d'heures qu'elles travaillent ou l'endroit où elles exécutent leur travail. Le télétravail, qui consiste généralement à travailler à l'extérieur du lieu de travail habituel semble également contribuer à accroître la rétention du personnel et à améliorer le rendement des personnes salariées.

Néanmoins, les TIC sont susceptibles d'accentuer le brouillage entre les temps sociaux, et ce, de deux principales façons. D'une part, les TIC peuvent accroître la durée effective du travail, les personnes salariées se voyant dans l'obligation, implicite ou explicite, de travailler au-delà de leurs heures habituelles ou normales de travail. D'autre part, les TIC facilitent la mise en place de périodes de « disponibilité » pendant lesquelles les personnes salariées ont l'obligation d'être facilement joignables. Le fait d'être branché de façon quasi permanente aux terminaux de communication mobile définit le concept d'hyperconnectivité.

Reconnaissant la porosité¹ grandissante de la séparation entre le temps de travail et le temps de repos des travailleurs dans un contexte d'hyperconnectivité professionnelle, quelques États ont adopté des lois visant à fournir aux travailleurs et aux travailleuses un droit à la déconnexion. Ces dispositions ont pour objet général le respect des périodes de repos et de congé des travailleurs et travailleuses mis en péril par l'hyperconnectivité. En effet, les problématiques liées aux conséquences de l'utilisation des technologies numériques sur le temps de travail ne sont pas nouvelles. Depuis plusieurs années, déjà, sont évoqués les risques que génère la disponibilité permanente du salarié connecté à son téléphone ou à son ordinateur portable. L'idée même d'un droit à la déconnexion est déjà ancienne.²

Le droit à la déconnexion mérite le qualificatif du droit mou à double titre : d'une part en raison de ses incertitudes techniques, et d'autre part, en raison de son contenu incertain³. Ainsi le droit à la déconnexion est la traduction juridique d'une idée de bon sens : un salarié n'a pas à être connecté aux outils numériques professionnels en dehors des horaires de travail. Ce droit concerne tous les salariés, télétravailleurs ou non, qui peuvent rester connectés à leur entreprise grâce à leurs appareils technologiques. Mais cela concerne au premier lieu les télétravailleurs. Ces derniers doivent absolument réussir à se déconnecter, sans bénéficier des rituels que constitue le déplacement physique hors des locaux de l'entreprise. Ne doutons pas que les responsables des ressources humaines et les représentants syndicaux trouveront les moyens de faire de la notion de déconnexion un instrument d'accompagnement des entreprises à la transformation numérique.

¹E. GENIN, « Proposal for a Teoretical Framework for the Analysis of Time Porosity », in *International Journal of Comparative Labour Law and Industrial Relations*, N° 3, 2016, pp. 280-300 cité dans Jean BERNIER, *L'intelligence artificielle et les mondes de travail, Perspectives et socio juridiques et enjeux éthiques*, Presse de L'Université de Laval, Québec, 2021.

²J-E. RAY, « Naissance et avis de décès du droit à la déconnexion, le droit à la vie privée du XXI siècle », in *Revue de Droit Social*, N° 11, Novembre 2002, Dalloz, p. 939.

³C. WILLMANN, « La déconnexion des salariés : un droit « mou », aux forts enjeux », in *IP/IT*, N° 12, Décembre 2019, Dalloz, p. 684.

Le premier État à légiférer sur cette question fut la France. Depuis le 1er janvier 2017 la loi Travail française (*loi khomri*) introduit ce droit dans la législation du travail et pose une obligation de négociation d'un accord ou l'élaboration d'une charte sur le droit à la déconnexion.¹ Ainsi la négociation sur la déconnexion est prévue par la loi française selon deux cadres. les partenaires sociaux doivent négocier les modalités du plein exercice par la personne salariée de son droit à la déconnexion et la mise en place par l'entreprise de dispositifs de régulation de l'utilisation des outils numériques, en vue d'assurer le respect des temps de repos et de congé ainsi que de la vie personnelle et familiale. À défaut d'accord, l'employeur élabore une charte, après l'avis du comité d'entreprise ou, à défaut, des délégués du personnel. Cette charte définit les modalités de l'exercice du droit à la déconnexion et prévoit en outre la mise en œuvre, à destination des personnes salariées et du personnel cadre et de direction, d'actions de formation et de sensibilisation à un usage raisonnable des outils numériques².

Néanmoins, aucune définition légale n'est prévue dans le Code de travail français. De plus, si ce droit à la déconnexion doit théoriquement être négocié, le défaut de parvenir à une entente sur cette question aura pour effet de transférer à l'employeur la prérogative de déterminer la nature et la portée de ce droit. Or, un accord collectif a un effet normatif et est opposable en justice, ce qui n'est pas le cas de cette charte de l'employeur. Ainsi, le droit à la déconnexion doit s'accompagner d'un mécanisme de mise en œuvre approprié afin qu'un tel droit ne constitue pas un simple énoncé de principe³.

De même, l'Espagne et l'Italie ont également adopté des lois demandant aux employeurs de prévoir explicitement les modalités de l'exercice du droit à la déconnexion des travailleurs et de travailleuses. La loi espagnole s'applique à toutes les entreprises, peu importe le nombre de travailleurs et de travailleuses, et la loi italienne ne s'applique qu'à certaines catégories de personnes salariées : dans les deux cas, à l'instar de la loi française, aucune sanction ni définition n'y sont prévues si l'employeur omet de mettre en place de

¹Matthieu BILLETTE DE VILLEMEUR, *Op.cit.*, p. 35.

²L. GRATTON, « Révolution numérique et négociation collective », in *Revue Droit social*, N° 12, Décembre 2016, p. 1054.

³C. MATHIEU, M.-M. PERETIE et A. PICAULT, « Le droit à la déconnexion : une chimère ? », in *Revue de droit du travail*, N° 10, 2016, p. 592.

telles politiques. Par ailleurs quelques autres États, comme l'Allemagne, l'Irlande, l'Inde et l'État de New York, étudient des projets de loi à ce sujet¹.

Au Canada, après avoir entendu différents représentants d'employeurs, de syndicats et de travailleurs et avoir étudié les normes en vigueur tant au Canada qu'ailleurs dans le monde, le comité a reconnu le flou législatif existant, mais a jugé, à l'été 2019, « *qu'il serait difficile à l'heure actuelle de mettre en œuvre et de faire appliquer un droit à la déconnexion* »². Avant d'envisager l'introduction dans le Code canadien du travail d'un droit à la déconnexion, le comité souligne notamment l'importance d'introduire une définition législative.

Plusieurs employeurs semblent réticents à l'idée de légiférer sur cette question, préférant que chaque entreprise déploie ses propres solutions. De fait, quelques entreprises, en l'absence de norme statutaire prévoyant un droit à la déconnexion, ont négocié des mesures précises à ce sujet, de concert avec les représentants des travailleurs et de travailleuses. Par exemple, en Allemagne, les serveurs des cellulaires fournis par Volkswagen à son personnel non cadre n'envoient aucun courriel hors des heures normales de travail, et ce, depuis 2012 : les courriels sont soit supprimés, soit envoyés lors de la plage horaire de travail suivante³. Toujours en Allemagne, les travailleurs et travailleuses du fabricant automobile Daimler peuvent⁴, depuis 2014, utiliser un programme informatique supprimant de leur boîte de réception tout courriel reçu pendant leurs vacances, après que l'expéditeur en eut été avisé et eut été dirigé vers d'autres personnes.

Comment donc encadrer les effets des NTIC sur la vie professionnelle et personnelle des travailleurs et des travailleuses ? Afin de favoriser un droit effectif à la déconnexion, il semble essentiel de revoir les normes portant sur la durée du travail. D'une part, il semble indispensable d'encadrer la mise en disponibilité des personnes salariées, laquelle est

¹Jean BERNIER, *L'intelligence artificielle et les mondes de travail, Perspectives sociojuridiques et enjeux éthiques*, Presse de L'Université de Laval, Québec, 2021, pp. 168-169.

²Emploi et Développement social Canada, *Rapport du Comité d'experts sur les normes du travail fédérales modernes*, Ottawa, 2019, pp. 103-122.

³Les appels téléphoniques sont toutefois toujours possibles : G. CORERA, « Volkswagen turns o Blackberry email after work hours », in BBC News, 8 mars 2012, consulté le 14 Décembre 2021 à 10h sur <https://www.bbc.com/news/technology-16314901>.

⁴Chacun des 100000 employés visés décide s'il veut ou non appliquer cette option : R. J. ROSEN, « Daimler Employees Can Set Emails to Auto-Delete During Vacation », in Atlantic, 14 août 2014 consulté le 14 Décembre 2021à 10h sur <https://www.theatlantic.com/business/archive/2014/08/daimlers-german-employees-can-set-emails-to-auto-delete-during-vacation/376068/>.

susceptible de se déployer à l'extérieur des lieux de travail. D'autre part, le temps de travail effectif doit être compensé, peu importe le mode de rémunération préconisé¹.

Finalement, l'introduction de normes fixant une durée maximale de la journée et de la semaine de travail permettrait aux normes d'ordre public portant sur la durée du travail d'assurer leur fonction originelle de protéger la santé et la sécurité des travailleurs et des travailleuses. De telles normes favoriseraient également un réexamen de l'organisation du travail.

Sous-section 2 : Le travail par intermédiation des plateformes numériques.

La notion de lieu qu'est l'établissement physique de l'entreprise se voit aujourd'hui bousculée, en raison même de la dématérialisation des milieux de travail, réalité qui se manifeste à différents degrés et sous différentes formes tant dans les milieux traditionnels que dans les nouvelles entreprises. Il en découlerait que la destruction du lieu physique comme contrainte de travail permettrait une plus grande automatisation des tâches et augmenterait le rôle des plateformes numériques. Ces propriétés technologiques caractériseraient ainsi cette nouvelle et quatrième révolution et les entreprises de cette ère.

L'accroissement des technologies, par les TIC, la géolocalisation ainsi que la capacité à générer et à exploiter une quantité massive de données amènent d'ailleurs avec elles l'émergence de nouvelles formes d'organisation du travail dont les plateformes numériques sont l'archétype. Le numérique ne révolutionne pas seulement le travail, il produit également des effets sur l'emploi. Sont ainsi apparues de nouvelles formes d'emploi désignant essentiellement le travail par intermédiation de plateformes numériques² et notamment le travail en réseau ou le *crowdworking* (Paragraphe 1). Ce travail par intermédiation de plateformes numérique a suscité de nombreux débats et nombreuses questions quant à la situation de ses travailleurs (Paragraphe 2).

Paragraphe 1 : Le travail en réseau ou le *crowdworking*.

Employé pour la première fois en 2005 par Jeff Howe, journaliste au magazine *Wired*, le terme *crowdsourcing* désigne le fait de confier l'exécution d'un travail autrefois effectué

¹L. MOREL, « Le droit à la déconnexion en droit français. La question de l'effectivité du droit au repos à l'ère du numérique », in *Labour and Law Issues*, N° 2, 2017, p. 5.

²Sébastien TOURNAUX. *Op.cit.*, p. 60.

par un agent précis (qu'il s'agisse d'un salarié, d'un travailleur indépendant ou d'une entreprise) à un ensemble vaste et indéfini de personnes en lançant un appel ouvert, généralement par l'intermédiaire d'internet¹. Le travail en réseau (traduction libre de la notion de *crowdwork*), est effectué sur ces plateformes numériques.

Si l'on admet que le *crowdsourcing* consiste à externaliser le travail, les plateformes de *crowdworking* peuvent être assimilées aux services numériques (site internet ou applications) qui le facilitent. Elles fournissent en effet l'infrastructure technique grâce à laquelle des donneurs d'ordre peuvent diffuser leurs offres à un grand nombre de travailleurs potentiels, couvrant un large spectre géographique et économique, récupérer et évaluer les résultats des tâches à exécuter et payer les travailleurs pour les services rendus. Elles offrent également des services et une infrastructure aux travailleurs, auxquels elles permettent d'accéder depuis un lieu unique à des tâches proposées par de multiples donneurs d'ordre, de soumettre le produit de leur travail et de disposer de l'infrastructure technique et financière nécessaire pour recevoir un paiement au titre du travail effectué. Les plateformes numériques regroupent alors une multitude d'activités et de services offerts, comme des services de transport, de livraison, de vente et de commerce, des services financiers, de logements, etc. Le travail effectué sur ces plateformes peut être schématisé en deux catégories².

La première catégorie conserve certaines caractéristiques plus classiques, en ce sens que la prestation de travail devra être effectuée dans un lieu précis, sans toutefois que ce soit celui de l'entreprise traditionnelle. La prestation aura donc lieu où le donneur d'ouvrage ou le client aura demandé qu'elle soit effectuée. Cette première catégorie de plateformes concerne notamment les applications de livraisons à domicile et de transport (*Uber, Take it Easy, Lyft*)³. La deuxième catégorie est, quant à elle, l'illustration extrême de l'éclatement des milieux de travail, puisque le travail se fait virtuellement avec l'aide d'un simple ordinateur et d'une connexion Internet, quel que ce soit l'endroit où le travailleur se trouve sur terre (*TaskRabbit* et *Amazon Mechanical Turk*). L'industrie des plateformes de deuxième catégorie serait donc exemptée de toute contrainte physique et géographique. Les travailleurs de cette industrie ne

¹Bureau International du Travail, « Les plateformes de travail numérique et l'avenir du travail: pour un travail décent dans le monde en ligne », 1^{ère} éd., Genève, 2019, p. 4.

²V. DE STEFANO, « the Rise of the Just-in-Time Workforce: On-Demand Work, Crowdwork, and Labor Protections in the Gig-Economy », in *Comparative Labour Law & Policy Journal*, Geneva, 2016, p. 481.

³J. PRASSEL et M. RISAK, « Uber, Taskrabbit, and Co: Platforms as Employers – Rethinking the Legal Analysis of Crowdwork », in *Comparative Labor Law & Policy Journal*, N° 8, 2016, p. 624.

font plus face à une compétition uniquement locale et circonscrite, mais dorénavant mondiale¹.

Le *crowdwork* est parfois analysé comme une nouvelle forme de travail, en d'autres termes une transformation du travail qui se serait opérée sous l'effet de l'essor d'Internet et des plateformes numériques permettant actuellement son exercice. La thèse qui consiste à présenter cette forme de travail comme «nouvelle» – autrement dit différente du travail au sens où on l'entend traditionnellement – fait partie des arguments utilisés par les plateformes pour tenter d'échapper aux réglementations du travail en vigueur².

Si le droit n'est pas concerné par le phénomène dans son ensemble,³ il l'est au moins lorsque l'activité de mise en relation exercée par les plateformes numériques porte sur une prestation impliquant la force de travail de celui qui l'exécute (effectuer une course de taxi, la livraison d'un repas...). Les difficultés que soulève le travail par intermédiation numérique sont essentiellement de deux ordres.

D'un côté, se pose la question de l'encadrement juridique de l'activité d'intermédiation elle-même. Lorsque la mise en relation opérée par la plateforme consiste en une mise à disposition de la force de travail d'autrui, un encadrement juridique pourrait être justifié dans la mesure où les clients des plateformes utilisent cette force de travail pour leur propre activité professionnelle. Dans certains cas la plateforme met en relation une entreprise clients avec de la main-d'œuvre c'est le cas des plateformes de livraison de repas à domicile ou certaines plateformes de *crowdworking*. Ainsi, l'entreprise cliente externalise, via la plateforme une partie de ses activités puisque les prestations effectuées par les travailleurs (la livraison d'un repas, le traitement d'une base de données...) auraient tout aussi bien pu être exécutées directement par les salariés de l'entreprise cliente. Or ces formes d'intermédiations numériques s'exercent et se développent en marge des cadres légaux relatifs aux activités de travail temporaire et assimilés. D'un autre côté, la question de la protection accordée aux travailleurs par intermédiation numérique qui est directement posée par le phénomène dit d'ubérisation⁴ de l'économie.

¹Ibid., p. 623.

²Bureau International du Travail, *Op.cit.*, p. 5.

³V.B. GOMES, « Le crowdworking : essai sur la qualification du travail par intermédiation numérique », in RDT, N° 7, 2016, Dalloz, p. 465.

⁴Ubérisation : « la remise en cause du modèle économique d'une entreprise ou d'un secteur d'activité par l'arrivée d'un nouvel acteur proposant les mêmes services à des prix moindres, effectués par des indépendants

Paragraphe 2 : La situation des travailleurs des plateformes numériques.

Si les plateformes de travail numérique sont le fruit d'avancées technologiques, le travail effectué sur ces plateformes présente des modalités semblables à celles qui existent depuis longtemps, pour seule différence, l'intervention d'outil numérique servant d'intermédiaire. Cependant, le numérique impact les conditions de travail des travailleurs des plateformes du numérique (I) et pose le souci de qualification juridique du statut de ces travailleurs (II). Cette qualification qui diffère selon la classification des plateformes de travail par intermédiation (III).

I- L'impact des nouvelles technologies sur les conditions de travail des travailleurs des plateformes numériques.

Les répercussions des nouvelles technologies sur le salariat et ses conditions de travail se répercutent actuellement tant dans les milieux de travail dit traditionnels que dans les nouveaux modèles d'entreprises que sont les plateformes numériques¹. En effet, les répercussions des machines intelligentes sur les conditions de travail des salariés sont multiples. Elles peuvent être bénéfiques spécialement du point de vue de la santé et de la sécurité du travail.

Sur ce plan, le progrès technologique est un progrès social : quand la machine de la révolution industrielle abîmait les corps, la robotique intelligente permet de les préserver en prenant en charge des tâches dangereuses, répétitives, réduisant en conséquence la pénibilité. Mais il ne faut pas sous-estimer les risques liés aux conditions de déploiement des outils faisant appel à l'intelligence artificielle, notamment la perte d'autonomie ou l'intensification du travail. Des risques nouveaux ont de surcroît été décelés pour la santé physique, comme l'obéissance exclusive aux instructions d'une machine ou l'impossibilité de discuter avec ses collègues sans passer par une interface machine.

La législation concernant les conditions de travail est encore très largement inspirée par les modes de travail de l'ère industrielle, il lui faudra donc à l'avenir être adapté à la nouvelle organisation des tâches et en particulier à la complémentarité entre le travail humain

plutôt que des salariés, le plus souvent via des plates-formes de réservation sur Internet. » Dictionnaire Larousse, 2017.

¹Massimiliano NICOLI, Luca PALTRINIERI et Muriel PREVOT-CARPENTIER, « Travail et plateformes numériques : entre exploitation et opportunités » in Travail e(s)t liberté ?, Ouvrage collectif sous la direction d'Enrico DONAGGIO, José ROSE et Mariagrazia CAIRO, Erès, coll. Clinique du travail, Paris, 2022, p. 152.

et la machine. Cette complémentarité peut être dans certain cas, un facteur de développement des capacités des salariés qui, déchargés de certaines actions fastidieuses comme le tri de milliers de courriels reçu de la clientèle, peuvent se concentrer sur des tâches à valeur ajoutée. Mais elle peut aussi, à l'inverse, diminuer la capacité d'initiative et de réflexion. Dans les deux cas l'évolution des tâches se fait volontiers sous couvert d'une amélioration des conditions de travail¹.

En matière de contrôle de salariés le nombre et la variété des outils et logiciels permettant de contrôler leur activité ne cessent de croître. Les logiciels qui permettent de suivre à distance les frappes au clavier et les mouvements de souris, ou de télélocaliser les travailleurs, sont de nature intrusive et donc déconseillés. Les accès distants doivent être sécurisés afin que seules les personnes autorisées puissent se connecter au système d'information de l'entreprise. Les outils *VPN (Virtual Private Network)* permettent ce contrôle.

Les travailleurs des plateformes numériques sont d'ailleurs soumis à une gestion par algorithme. Les cotes de rendement attribuées à chaque travailleur influencent la manière dont l'algorithme répartit les tâches. Les travailleurs ayant les meilleurs rendements obtiennent de meilleures conditions de travail ou tout simplement le maintien de leur droit de fournir une prestation de travail. Le contrôle de la prestation de travail est alors soustrait de toute intervention humaine.

Par cette désappropriation du travail au profit de la machine, l'humain serait désormais au service de celle-ci dans la réalisation de la production de biens ou de services. Cet assujettissement diminuerait considérablement sa capacité de contrôler son travail et le maintien de son emploi et, plus fondamentalement, de préserver la dimension sociale intimement rattachée au travail². Cependant, la fin du salariat, potentiellement causée par cette substitution de l'humain par la machine, serait aussi engendrée par une insoumission délibérée aux normes juridiques, en raison de ces statuts de travailleurs que proposent les plateformes numériques.

¹G. LOISEAU, « Intelligence artificielle et conditions de travail des salariés : un impact à prendre au sérieux », in IP/IT, N° 7-8, Juillet et Aout 2018, Dalloz, p. 55.

²V. DE STEFANO, « Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection », in Comparative Labor Law & Policy Journal, N° 1, 2019, p. 17.

II- La qualification juridique des travailleurs de plateformes numériques.

Les protections du droit du travail, l'idée de contrat de travail et la notion juridique de subordination qui lui sert de support conservent, hélas, toute leur pertinence, y compris dans un univers de nouvelles technologies, peut-être même surtout dans cet univers peuplé de yeux électroniques, de notation permanente et de sanctions automatisées. Les travailleurs de plateformes ne sont pas protégés de la subordination, ils y sont même peut-être particulièrement sujets.

Le contrat de travail se fonde, à l'instar de la majorité des systèmes juridiques en droit comparé, sur la dichotomie salarié et travailleur indépendant¹. Cette binarité avait l'avantage lors de l'avènement des régimes législatifs en droit du travail d'offrir une simplicité et une stabilité dans les relations de travail. Dans cette perspective, certains pays ou États ont instauré des catégories dites intermédiaires, permettant aux travailleurs qui ne pouvaient pas se qualifier de salarié d'obtenir les protections sociales qu'offrent les institutions du travail. C'est le cas notamment de l'Allemagne², de l'Espagne, de l'Angleterre et de certaines provinces du Canada. Ces initiatives législatives visaient à satisfaire à la problématique des travailleurs ayant un statut d'emploi atypique.

Plusieurs tribunaux spécialisés ou judiciaires, qu'ils soient canadiens, américains, britanniques ou européens, ont eu à trancher la question du statut juridique de ces travailleurs de plateformes³. Certaines de ces instances ont considéré ces travailleurs comme des salariés. En atteste, les arrêts *Take Eat Easy* du 28 novembre 2018⁴ et *Uber* du 4 mars 2020⁵. Ce sont de grands arrêts ; l'effet de l'arrêt *Take Eat Easy* a été immédiat, la Cour d'appel de Paris

¹J. BERNIE, G. VALLEE et C. JOBIN, « Les besoins de protection sociale des personnes en situation de travail non traditionnelle », Rapport final du Comité d'experts chargé de se pencher sur les besoins de protection sociale des personnes vivant une situation de travail non traditionnelle, 2003, p. 71.

²N. COUNTOURIS et V. DE STEFANO, « New Trade Union Strategies for New Forms of Employment », ETUC, Brussels, 2019, p. 27.

³En premier lieu, l'affaire Canadian Union of Postal Workers contre Foodora est le premier dossier de syndicalisation au Canada des travailleurs de l'industrie des plateformes. Dans cette décision, l'Ontario Labour Relations Board conclut que les livreurs à vélo sont des entrepreneurs dépendants.

Le deuxième cas de jurisprudence provient de la jurisprudence britannique Independent Workers Union of Great Britain contre Deliveroo, dans lequel la demande de reconnaissance de l'association à des droits de négociation collective fut rejetée. L'élément fatal à cette demande de reconnaissance était la preuve démontrant la capacité des livreurs, bien que celle-ci était peu exercée, de trouver un remplaçant afin d'effectuer le travail, sans préautorisation de la part de Deliveroo.

⁴C. Cass., civile, ch. Sociale, décision n° 17-20.079, 28 Novembre 2018, Société Take Eat Easy contre le Livreur X.

⁵C. Cass., civile, ch. Sociale, décision n°19-13.316, 4 Mars 2020, Société Uber contre un chauffeur X.

ayant rapidement emboîté le pas de la Cour de cassation en requalifiant un chauffeur de la compagnie *Uber* de salarié, arrêt confirmé avec fermeté par l'arrêt de la Cour de cassation du 4 mars 2020.

Si l'on en reste à la motivation officielle des arrêts, on notera que l'arrêt *Take Eat Easy* se contente de viser l'existence d'un système de géolocalisation, qui permet le contrôle et la présence d'un pouvoir de sanction, ce qui suffisait à ses yeux à prouver la subordination. Les livreurs et les chauffeurs de personnes étant nécessairement géolocalisés par l'intermédiaire de leurs téléphones portables, même si cette géolocalisation n'est pas toujours permanente. L'arrêt *Uber* se contente de reprendre la série d'indices de subordination retenus en l'espèce par la Cour d'appel de Paris du 10 janvier 2019 relatifs à la situation particulière des chauffeurs *Uber*, soumis à des obligations de trajet, à une rémunération fixée par l'algorithme, menacés de sanction de déconnexion...

Ces arrêts sont importants pour le droit français, mais ils le sont aussi pour le droit international et européen. La qualification des travailleurs des plateformes est un débat mondial, dans lequel les premières décisions de justice sont scrutées avec beaucoup d'attention. Au-delà de la jurisprudence française qu'ils inaugurent, ils participent ainsi à la construction d'un mouvement jurisprudentiel international en faveur d'une assez large qualification appliquée aux travailleurs des plateformes informatiques.

La Cour de justice de l'Union européenne a déjà ouvert la voie de possible requalification, par un arrêt du 20 décembre 2017¹, qui qualifie d'entreprise de transport et non d'entreprise de la société de l'information, pour la Cour, la plateforme informatique gérée par *Uber* n'est pas simple intermédiaire, ce que cette société prétendait, elle organise un service de transport, dans lequel des travailleurs sont intégrés. Et l'on se rappelle qu'en droit français l'intégration dans un service organisé est déjà un fort indice de subordination².

Les arrêts de la Cour de cassation interviennent aussi après d'autres arrêts ayant ordonné la requalification de travailleurs de plateformes, dont les très commentés arrêts de la Cour d'appel du travail de Londres et de la Cour suprême de Californie. En effet, dans un jugement rendu public le 17 Juin 2015, La Commission du travail de l'Etat de Californie a

¹Fernand MORIN, Jean-Yves BRIERE, Dominic ROUX et Jean-Pierre VILLAGGI, *Le droit de l'emploi au Québec*, Wilson & Lafleur, 4^{ème} éd., Montréal, 2010, p. 1032.

²I. DAUGAREILH, C. DEGRYS et P. POCHET, « Économie de plateforme et droit social : enjeux prospectifs et approche comparative », ETUI, Working Paper, Bruxelles, 2019, p. 25.

reconnu la qualité de salariée à une ancienne chauffeuse de la société *Uber*. Aussi, le 28 Octobre 2016 un tribunal du travail londonien a reconnu aux chauffeurs de VTC travaillant avec *Uber* la qualité de *worker* au sens des *Employment Rights Acts*, leur offrant ainsi le bénéfice d'une partie de la législation sociale en matière de salaire minimum, de congés payés et de durée maximale de travail. L'analyse du tribunal se fonde sur l'absence de latitude des chauffeurs dans le choix des courses, le fait qu'*Uber* détermine les trajets, les tarifs et les conditions de travail, telles que la performance des chauffeurs et que la société détient le pouvoir de modifier unilatéralement les termes du contrat.

Si l'on envisage que la qualification du contrat de travail est souvent mal comprise. On la croit, déterminée uniquement par la subordination, alors qu'elle procède également d'une analyse des conditions de l'indépendance. Il a ainsi pu être proposé une analyse renversée du critère du contrat de travail partant, non plus de la subordination, mais des conditions de l'indépendance : le lien de subordination est une qualification négative qui se construit par opposition à celle de l'indépendance.

Ainsi, lorsque la qualité juridique d'un prestataire est discutée et mélange des indices d'indépendance et de subordination, les juges excluent par principe du champ du salariat les vrais indépendants, c'est-à-dire ceux qui disposent à la fois de la maîtrise de leur capacité de profits et des risques inhérents à cette maîtrise. Mais, à l'inverse, lorsque les indépendants ne sont pas maîtres de leurs capacité de profit, ils doivent être considérés comme des subordonnés. Rapportés aux travailleurs de plateformes, l'absence de clientèle propre apparaît comme un indice essentiel de l'absence d'indépendance. Du coup, et par voie de conséquence, les juges mettent l'accent sur les indices de subordination et reconnaissent l'existence d'un contrat de travail¹.

Il ne faut pas déduire des arrêts *Take Eat Easy* et *Uber* que tous les travailleurs qui utilisent des plateformes informatiques pour trouver un travail seront automatiquement qualifiés de salariés. Pour que le contrat entre la plateforme et le travailleur devienne un contrat de travail, encore faut-il qu'il ait pour objet essentiel ou prépondérant le travail. Pour cette raison, il semble que la qualification de travailleur salarié de la plateforme n'aura pas lieu lorsque la prestation de travail n'est qu'un accessoire, de valeur relativement

¹T. PASQUIER, « Le droit social confronté aux défis de l'ubérisation », in IP/IT, N° 7-8, Juillet-Aout 2017, Dalloz, p. 21.

modeste, comparativement à celle des biens et valeurs transmis par l'intermédiaire de la plateforme.

Les vendeurs sur des sites comme *Le bon coin*¹, *eBay*² ou *Amazon* travaillent, ne serait-ce que parce qu'ils emballent et envoient leurs produits. Mais ce travail n'est que l'accessoire de leur activité commerciale et aucune requalification de contrat de travail ne sera possible dès lors que cette activité commerciale n'est pas dirigée, gérée par la plateforme et qu'ils demeurent libres de choisir les marchandises qu'ils proposent à la vente. La situation des chauffeurs est toute différente. Même si le prix du transport qu'ils assurent avec leur véhicule recouvre d'importants frais d'essence et d'entretien du véhicule, leur travail de chauffeur demeure le principal ou du moins une part suffisamment importante de la relation pour qu'elle ne puisse pas être considérée comme l'accessoire de cette relation. Quant aux plateformes de location de véhicule sans chauffeur, comme *Drivy*, Le travail qui demeure, travail d'entretien et de nettoyage du véhicule, n'est plus qu'un accessoire de la location du véhicule. On peut donc penser que la qualification de salarié n'aura pas lieu et que le loueur restera un loueur.

III- La classification des plateformes de travail par intermédiation.

Il nous semble que seules les plateformes qui coordonnent des contrats dont l'objet est pour une part essentielle ou principale du travail sont susceptibles d'être qualifiées d'employeurs. Ces plateformes de fourniture de travail ne sont pas pour autant toutes des employeurs. Il convient plus précisément de les classer en trois catégories. Les premières sont celles qui fournissent un type de travail bien précis, coordonné et organisé par la plateforme. Le service est alors un service organisé par la plateforme, sous son contrôle, et les clients sont ses clients. Dans ces hypothèses, la plateforme doit être qualifiée d'employeur et les travailleurs, de salariés. Une plateforme de nettoyage de linge par exemple, à l'instar des plateformes de livraison de repas ou de transport de personne.

Les deuxièmes sont celles qui ouvrent la possibilité à des travailleurs de proposer des services divers, sur lesquels la plateforme ne prétend avoir aucune expertise. Elles ne coordonnent ni le contenu ni la manière dont ils sont fournis. On pense ici notamment aux nombreux sites qui proposent de petits travaux dits de bricolage. L'expertise et la compétence

¹ Le boncoin est un site web français de petites annonces.

² eBay est une place de marché américaine, connue pour son site web de commerce en ligne

sont alors celles des seuls travailleurs. Ils ne sont pas dirigés par la plateforme ni par les bénéficiaires de leur travail. Dans ces cas et à ces conditions, les plateformes de *jobbing* pourraient échapper à la qualification d'employeurs et les travailleurs de ces plateformes être considérés comme des travailleurs indépendants.

Une dernière catégorie de plateforme, du point de vue du droit du travail, concerne les plateformes qui servent d'intermédiaires entre un travailleur et un bénéficiaire qui dirige dans les faits l'activité de ce travailleur. Ce peut être notamment le cas de sites comme *Amazon Mechanical Turk*, *Onespace* ou parfois de certaines des plateformes de petits boulots susvisées. Par l'intermédiaire de ces sites, certains entrepreneurs obtiennent un travail, souvent un petit travail d'exécution, qu'ils encadrent et dirigent. Le travail réalisé est alors bien un travail subordonné¹.

On constate que le salariat des plateformes ne regroupe pas tous les travailleurs des plateformes. Mais une part importante de ces travailleurs devraient être qualifié de salariés, parfois de la plateforme – comme cela a été le cas pour les livreurs de *Take Eat Easy* et les chauffeurs d'*Uber* –, parfois du client, comme cela devrait être le cas lorsque celui-ci n'est pas un simple consommateur, mais qu'il exerce sur le travailleur un véritable pouvoir de direction.

Sous-section 3 : La protection des données des employés dans le cadre de la relation du travail.

La Commission national de contrôle et de la protection des données à caractère personnel contrôle strictement les dispositifs de collecte des données personnelles dans l'entreprise. Elle veille à ce que l'employeur procure une sécurité à son entreprise tout en respectant la vie privé de ses employés. Dans un premier temps afin de prévenir les éventuelles utilisations indélicates des données numériques au sein de l'entreprise et de prévenir les infractions, les entreprises sont fortement invitées à encadrer l'utilisation de l'Internet au sein de l'entreprise (Paragraphe 1).

Dans un second temps, l'utilisation de l'internet sur le lieu de travail n'est pas anodine. Elle conduit à une grande perméabilité entre la sphère privée et la sphère professionnelle du salarié, que ce soit pendant le temps de travail ou en dehors, et partant, à une modification des

¹ Jean BERNIER, *Op.cit.*, p. 150.

liens de subordination entre salarié et employeur. Ainsi, divers procédés peuvent porter atteinte au respect de la vie privée des salariés, seront donc abordées ci-après les règles dégagées par le législateur et la CNDP en la matière (Paragraphe 2).

Paragraphe 1 : L'encadrement d'utilisation d'Internet au sein de l'entreprise.

L'employeur a tout intérêt, dans un souci de sécurité juridique et de clarté, à arrêter et à rendre publiques les règles qu'il entend voir appliquer dans son entreprise concernant l'accès à Internet et l'utilisation de ce dernier par ses salariés¹. Ce double objectif de sécurité et de transparence peut être atteint par l'adoption en interne de dispositions particulière applicables en la matière, lesquelles pourront être portées sur le règlement intérieur de l'entreprise, voire incluses dans les contrats de travail².

Toutefois, ce sont les chartes internet qui sont utilisées pour la définition au sein de l'entreprise des règles de sécurité, confidentialité, utilisation et accès en matière numérique. Bien entendu, ces règles devront se conformer de manière stricte à la législation applicable, ainsi que, idéalement aux principes dégagés par la Commission nationale de la protection des données à caractère personnel. Les chartes d'utilisation d'internet sont applicables à chacun des salariés de l'entreprise et à défaut de définition claire et précise de telles règles, le risque d'apparition de conflits autour de l'utilisation de l'internet dans l'entreprise se voit considérablement accru.

Les chartes d'utilisation des moyens de communication dans l'entreprise réglementent en général l'accès aux systèmes d'information par le salarié, ce qui comprend les outils de travail : poste de travail, e-mail, l'accès à internet, etc. ainsi que les identifiants : un nom d'utilisateur auquel chaque utilisateur attribuera ou se verra attribuer un mot de passe. Ainsi les chartes encadrent le respect des logiciels et la constitution de fichiers informatiques contenant des données à caractère personnel. Egalement l'installation et l'utilisation de périphériques externes qui peuvent être limitées, voire interdites. Il en est de même pour l'ajout de logiciels personnels par le salarié.

¹Eric A. CAPRIOLI et Aurélie GURFINKIEL, « Cybersurveillance des salariés et communications électroniques » in *L'entreprise à l'épreuve du droit de l'Internet*, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014, p. 179.

²Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, *Op.cit.*, p. 103.

Les chartes réglementent généralement, l'usage professionnel qui doit être fait de l'adresse électronique mise à la disposition des salariés. Elles énoncent alors les usages prohibés de cette adresse tels que l'envoi de messages dont le contenu est susceptible de porter atteinte à la dignité d'autrui, ou contraire aux bonnes mœurs ou à l'ordre public et, aussi, dans le but de fournir de fausses informations, des informations offensantes ou diffamatoires envers l'entreprise.

De la même manière que pour la messagerie électronique, les chartes peuvent mettre en place une réglementation interne relative à l'utilisation d'internet. Dans ce cas, elles précisent que la navigation sur internet doit être faite essentiellement à des fins professionnelles, ce qui exclut des quelques usages prohibés, tel que la consultation de sites dont le contenu est susceptible de porter atteinte à l'ordre public et aux bonnes mœurs. Il est également interdit de procéder à la diffusion, sur des sites Internet externes à l'entreprise, des informations internes, notes, articles, produits, documentaires ou autres de l'entreprise¹.

Les mesures de contrôle entamées par l'employeur porte sur les sites internet visités par les salariés, le format et la taille des pièces jointes auxdits messages électroniques, les durées de connexion des employeurs du réseau informatique de l'entreprise à travers leur identifiant réseau. Les modalités de recours à des contrôles extraordinaires peuvent également être prévues par les chartes. Cet aspect de la charte devra faire l'objet d'une déclaration à la CNDP des moyens mis en œuvre. Autrement dit, en matière de contrôle, c'est la faculté de contrôler qui doit être prise en compte et non l'effectivité de ces contrôles. La déclaration adressée à la CNDP devra décrire de façon suffisamment précise les outils et conditions d'un éventuel contrôle, notamment par un descriptif technique du matériel, des modalités de stockage, etc. L'adoption d'une charte d'internet régulièrement mise à jour et opposable aux salariés ainsi qu'aux stagiaires et collaborateurs occasionnels, constitue une protection indispensable pour toute entreprise soucieuse de la protection de ses données confidentielles².

Paragraphe 2 : Le respect de la vie privée de l'employé.

Les procédés de surveillance électronique utilisés pour assurer la sécurité numérique et pour maintenir le niveau de productivité au sein de l'entreprise sont susceptibles d'entrer en conflit avec les droits et les libertés individuelles du personnel. La CNDP contrôle strictement

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, pp. 118-119.

²Ibid., p. 121.

les dispositifs de collecte des données personnelles dans l'entreprise. Néanmoins, divers procédés tels la biométrie ou la reconnaissance faciale (I) et le contrôle de l'accès à l'entreprise peuvent porter atteinte au respect de la vie privée des salariés (II).

I- La biométrie et la reconnaissance faciale dans l'entreprise.

Par délibération du 1^{er} Novembre 2013, la CNDP définit la biométrie comme un système qui recouvre l'ensemble des techniques permettant d'identifier un individu à partir de ses caractéristiques physiques, biologiques et comportementales. Ces caractéristiques ont la particularité d'être uniques et quasi permanentes tout au long de la vie. Le caractère particulier des systèmes biométriques constitue un risque en matière de protection de la vie privée. Entre autres, certaines données biométriques peuvent révéler de manière fortuite des informations qui n'étaient pas prévues dans le traitement de base, et qui peuvent constituer une atteinte sérieuse à la vie privée des individus. Par exemple, l'image de l'iris utilisé par un dispositif de contrôle d'accès est susceptible de dévoiler des données sur la santé de la personne¹.

Consciente de l'impact des techniques biométriques sur la vie privée des personnes et les risques de violation des libertés et droits humains fondamentaux, la CNDP a défini certaines règles conformes aux standards internationaux en la matière, règles que doivent respecter les responsables de traitement exploitant de tels systèmes. L'installation d'un dispositif biométrique dans une entreprise doit faire l'objet d'une demande d'autorisation auprès de la CNDP. La demande d'autorisation précitée doit être accompagnée d'un descriptif du dispositif biométrique et d'un engagement qui atteste que le système à installer respecte les dispositions de la loi 09-08. Par ailleurs, la biométrie ne peut être utilisée que de manière proportionnée afin de respecter l'intégrité de la personne humaine². C'est la raison pour laquelle la CNDP n'autorise pas systématiquement tous les procédés biométriques qui lui sont présentés. Les systèmes mis en activité par les entreprises privées sont validés par la CNDP que s'ils remplissent un certains nombres de conditions³.

¹CNDP, Délibération n° 478-2013 du 1er novembre 2013 portant sur les conditions nécessaires à l'utilisation des dispositifs biométriques pour le contrôle d'accès.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p.127.

³La CNDP peut autoriser le recours aux données biométriques pour le contrôle d'accès aux locaux et aux installations sensibles faisant l'objet d'une restriction de circulation et représentant un enjeu majeur de sécurité dépassant l'intérêt strict de l'organisme sous les conditions suivantes : 1) Le responsable du traitement doit justifier que les méthodes alternatives de contrôle d'accès ne sont pas suffisamment fiables pour sécuriser le site

La finalité de la biométrie, d'une part elle doit avoir pour objectif la sécurité de l'entreprise et non le contraire la surveillance des salariés sur leur lieu de travail. D'autre part, la conservation de la biométrie c'est-à-dire les traces que laisse l'application biométrique et le risque de détourner l'utilisation des données à caractère personnel de son objectif premier. C'est pourquoi la décision de la CNDP a délimité la durée de conservation des données biométrique qui équivaut aux temps nécessaire pour la réalisation de l'opération d'extraction des éléments caractéristiques. Les données biométriques utilisées doivent être supprimées dès que la personne concernée n'est plus habilitée à être présente sur le site sécurisé.

La reconnaissance faciale est une technologie très présente dans le débat public national et mondiale et soulève des questionnements éthiques au niveau de l'acceptabilité sociale et des questions juridiques. La reconnaissance faciale soulève des enjeux importants pour les droits et libertés individuelles des citoyens. Ainsi l'exploitation accrue et potentiellement à grande échelle de données à caractère personnel, dont certaines sont sensibles, et la restriction de l'anonymat, sont autant de problématiques essentielles pour le bon fonctionnement de notre société. La reconnaissance faciale s'entend d'une technique automatisée qui permettrait, à partir des traits du visage, d'authentifier une personne ou de l'identifier. Elle peut être utilisée pour accéder à un lieu, à un ordinateur, à un mobile, rechercher des personnes disparues, etc. Elle peut être mise en place avec l'accord de la personne, comme être effectuée à son insu. Cette technologie pose en particuliers la question du consentement des personnes dont les données biométrique sont utilisées¹.

Pour ce faire, il est question de trouver un juste équilibre entre d'une part, les impératifs de sécurisation, notamment des espaces publics, d'efficacité économique, de services de proximité et d'autre part, la préservation des droits et libertés de chacun. Il s'agit

; 2) Seules peuvent être traitées les données biométriques d'un nombre limité de personnes, dont la mission nécessite une présence régulière ou temporaire dans le site ; 3) Une donnée biométrique ne peut être utilisée à l'état brut. Par conséquent, le responsable du traitement doit procéder à une extraction partielle de la donnée sous forme d'un nombre limité d'éléments caractéristiques (par exemple pour l'empreinte digitale, extraire un nombre limité de points caractéristiques) ; 4) Le responsable du traitement ne doit pas constituer une base de données pour stocker les données biométriques collectées. Par ailleurs, dans certains cas particuliers, et sous réserve de mesures de sécurité très strictes, la constitution d'une base de données pourrait être autorisée par la Commission ; En règle générale, les données doivent être enregistrées sur un support exclusivement détenu par la personne concernée, telle qu'une carte à puce ou une carte magnétique ; 5) Le dispositif biométrique doit être utilisé à des fins d'authentification et non pas d'identification.

¹Myriam QUEMENER, Frédérique DALLE et Clément WIERRE, Quels droits face aux innovations numériques : Législation, jurisprudences et bonnes pratiques du cyberspace. Défis et protections face aux dérives du numérique, Gualino, 1^{ère} éd, Paris, 2020, p. 98.

d'encadrer les finalités pour lesquelles la reconnaissance faciale peut être déployée et prévenir tout mésusage des données à caractère personnel traitées par son biais. La CNDP a rappelé que « *Compte tenu de ce qui précède, la Commission Nationale de contrôle de la protection des Données à caractère Personnel (CNDP), décide d'instaurer, à compter du 2 septembre 2019, un moratoire de 7 mois, relatif à l'utilisation de cette technique* »¹. Ce moratoire a été prolongé à plusieurs reprises.

Les exemples concrets d'application de la reconnaissance faciale sont divers. Cette dernière peut être mise en place sur les lieux de travail. En effet les employeurs privés ou publics peuvent mettre en œuvre des dispositifs de contrôle d'accès biométriques à condition d'être conformes aux décisions élaborées par la CNDP. Au Maroc en Avril 2020 la CNDP a délivré une autorisation de traitement de données à caractère personnel aux établissements du secteur bancaire qui l'ont sollicité pour les autoriser à mettre en œuvre des systèmes d'authentification biométrique, en général, et à base de technologies de reconnaissance faciale, en particulier, lors de l'ouverture de compte et l'amélioration de l'entrée en relation digitale du parcours client².

II- Accès à l'entreprise : géolocalisation et vidéosurveillance.

Suite aux délibérations du 10 Janvier 2014³, la CNDP définit le système de géolocalisation comme étant une technique qui permet de connaître la position géographique d'un objet en s'appuyant sur des technologies permettant de déterminer avec une grande précision ses coordonnées géographiques. Les technologies les plus connues se basent sur des bornes *WiFi*, des antennes *GSM* ou sur les positions d'une constellation de satellites.

L'employeur peut avoir recours à des procédés de géolocalisation dans les véhicules de salariés amenés à se déplacer régulièrement dans leur activité professionnelle. C'est l'une des utilisations la plus courante des systèmes de géolocalisation. En revanche, la mise en œuvre de ce traitement légitime peut constituer une atteinte à la vie privée des conducteurs dont les déplacements sont collectés et analysés. L'employeur peut également mettre en place

¹CNDP, Délibération n° D-194-2019 du 30/08/2019 relative à un moratoire sur la reconnaissance faciale.

²CNDP, Délibération n° D-108-EUS/2020 du 23/04/2020 relative à la définition de l'usage des technologies de reconnaissance faciale dans le cadre du dispositif du compte à distance par les banques et établissements de paiement.

³ CNDP, Délibération n°17-2014 du 10/01/2014 portant modification de la délibération n°402-2013 du 12 Juillet 2013 portant sur les conditions nécessaires à la mise en place d'un dispositif de géolocalisation dans des véhicules utilisés par des employés.

des badges électroniques pour sécuriser l'accès à l'entreprise et gérer les horaires et la durée de travail des salariés. Ces dispositifs peuvent en outre être utilisés pour le contrôle de leur activité s'ils répondent aux conditions mise en place par la CNDP¹.

La procédure d'information et de consultation des instances représentatives des employés doit être respectée avant l'introduction de telles mesures compte tenu notamment du caractère intrusif des dispositifs traitant la donnée de géolocalisation des véhicules et des informations qui peuvent y être associées. De plus, La mise en place d'un dispositif de géolocalisation dans des véhicules utilisés par des employés doit être notifiée à la CNDP au moyen d'une demande de déclaration type. Tout traitement relatif à la mise en place d'un dispositif de géolocalisation non conforme aux conditions² prévues devra faire l'objet d'une demande d'autorisation préalable auprès de la CNDP. Enfin, le responsable de traitement ne peut mettre en œuvre le traitement relatif au dispositif de géolocalisation sans le consentement préalable libre et éclairé de la personne concernée ou la justification de l'existence d'une dérogation à l'exigence du consentement, conformément aux dispositions de la loi 09-08.

L'accès aux informations collectées par un système de géolocalisation doit être limité au gestionnaire du parc automobile et au service des ressources humaines. De plus, la durée de conservation de ces données ne doit pas dépasser un an. En somme, toutes les précautions utiles doivent être prises pour préserver la sécurité et la confidentialité des données traitées et, notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance et ce, conformément à la section 3 du chapitre III de la loi 09-08 susmentionnée³.

Par ailleurs, un système de vidéosurveillance consiste à utiliser un ensemble de caméras permettant la collecte, la visualisation et éventuellement l'enregistrement d'images, susceptibles d'identifier des individus. Ces images sont, de ce fait, des données personnelles, dont le traitement est soumis aux dispositions de la loi 09-08. L'installation des caméras dans des lieux où les salariés exercent leur activité n'est possible que sous réserve de certaines

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 129.

²Les Responsables du Traitement peuvent mettre en place des dispositifs de géolocalisation dans les véhicules utilisés à titre professionnel pour : - Optimiser et rationaliser la gestion du parc automobile ; - Assurer les secours de l'employé en cas d'incident ou d'accident survenu au véhicule ; - Assurer la sécurité des marchandises et des véhicules et notamment, en cas de vol ; - Evaluer le rendement des conducteurs, lorsque cela ne peut être effectué par d'autres moyens. - Facturer une prestation de service directement liée à l'utilisation d'un véhicule.

³CNDP, Délibération n°17-2014 du 10/01/2014 portant modification de la délibération n°402-2013 du 12 Juillet 2013 portant sur les conditions nécessaires à la mise en place d'un dispositif de géolocalisation dans des véhicules utilisés par des employés.

dispositions et dans des limites qui visent à préserver les libertés individuelles et le respect de la vie privée. Les délibérations de la CNDP du 31 Mai 2013 définissent certaines règles conformes aux standards internationaux en la matière, règles que doivent respecter les responsables de traitement exploitant de tels systèmes.

L'employeur peut mettre en place des procédés de surveillance sans en informer au préalable le comité d'entreprise et les salariés dans les locaux où les salariés ne travaillent pas. En revanche, l'installation d'un système de vidéosurveillance dans les lieux de travail et dans les lieux privés communs doit être notifiée à la CNDP à travers une déclaration préalable. La déclaration précitée doit être accompagnée d'un engagement du responsable de traitement, qui atteste que le système installé respecte les conditions des dispositions de la loi 09-08.

Dans les locaux d'une entreprise ouverte au public, la mise en œuvre d'un système de vidéosurveillance des salariés doit nécessairement respecter le principe de proportionnalité. Elle doit donc s'effectuer de façon adéquate, pertinente, non excessive et strictement nécessaire à l'objectif poursuivi. Ainsi, les caméras peuvent être installées aux entrées et aux sorties des bâtiments ; sur les voies de circulation, dans les entrepôts de marchandises, dans les parkings, face à des coffres forts, à l'entrée et à l'intérieur des salles techniques, etc. C'est pourquoi, le responsable de traitement doit prendre toutes les précautions utiles pour préserver la sécurité et la confidentialité des images traitées et, notamment pour empêcher qu'elles soient détruites, déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance et ce, conformément à l'article 23 de la loi 09-08 susmentionnée. La durée de conservation des images ne doit pas dépasser trois mois¹.

Si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, il ne peut être autorisé comme un mode de preuve les enregistrements d'un système de vidéosurveillance installé sur le site d'une société cliente permettant le contrôle de leur activité dont les intéressés n'ont pas été préalablement informés de l'existence². Ainsi le Tribunal social de Casablanca a refusé de visionner un enregistrement vidéo, présenté par l'employeur d'un établissement hôtelier filmant le directeur de nuit entrain de recevoir dans une chambre de l'hôtel, à 3 h du matin, une jeune femme qui a quitté l'hôtel trois heures après. Le propriétaire de l'établissement voulait apporter au tribunal la preuve que

¹CNDP, Délibération n°350-2013 du 31/05/2013 portant sur les conditions nécessaires à la mise en place d'un système de vidéosurveillance dans les lieux de travail et dans les lieux privés communs.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 130.

son directeur de nuit avait commis une faute grave justifiant son licenciement. Le juge, qui a considéré le licenciement comme régulier, a préféré se baser sur une preuve classique, le témoignage d'un employé de l'hôtel qui a servi au couple cette nuit-là, du champagne au début et une bouteille de whisky au réveil.

Section 2 : Le numérique et les relations collectives de travail.

Phénomène émergent, l'usage du numérique et des outils informatiques mobiles croît de façon exponentielle et tend à se généraliser. Leur développement envahit peu à peu tous les espaces de vie, marquant plus particulièrement celui des entreprises notamment les relations collectives au sein de l'entreprise¹. En effet, l'essor des moyens de communications électroniques (internet, messagerie électronique, réseaux sociaux, etc.) influe quotidiennement sur les relations collectives de travail et modifie sur le long terme les comportements des salariés, les organisations syndicales ainsi que les organisations représentatives du personnel. Ces dernières sont nécessairement touchées et doivent adapter leur communication mais aussi leurs modes d'intervention à ces nouveaux moyens. C'est dans ce sens que nous allons nous focaliser sur l'étude du rôle du numérique en mettant toute la lumière à la fois sur le rôle pratique du numérique dans les relations collectives du travail (Sous-section 1) puis le rôle du numérique dans la modernisation du dialogue social (Sous-section 2).

Sous-section 1 : Le rôle pratique du numérique dans les relations collectives du travail.

Les évolutions technologiques bouleversent les relations entre les personnes, ce qui n'est pas sans conséquence d'un point de vue juridique. Lorsque l'on se place dans le cadre des relations de travail notamment les relations collectives Les outils numériques c'est-à-dire en substance les outils liés à l'utilisation de l'internet- ont profondément transformé les relations collectives de travail. Et parce que l'outil du numérique est l'outil de communication, il joue un rôle pratique dans le travail des syndicats. En effet, les nouvelles technologies ont été rapidement appréhendées par les syndicats comme un moyen de communication rapide et direct. Qu'il s'agisse de l'information collective (Paragraphe 1) ou du vote électronique et de la visioconférence (Paragraphe 2), le législateur a autorisé certains usages que nous aborderons ci-dessous.

¹Yann-Maël LARHER, Les relations numériques de travail, Thèse en droit privé, Université Panthéon-Assas Paris II, Paris, 2017, p. 70.

Paragraphe 1 : Le numérique : un outil d'informations des syndicats et des salariés.

Le numérique constitue, un formidable outil de communication et d'information pour les syndicats comme pour les salariés. A l'heure où l'agitation sociale envahit les réseaux sociaux publics, où la loi oblige les entreprises à mettre en place une base de données, on peut s'interroger sur la réticence des entreprises à proposer aux syndicats des supports de communication digitaux. Les entreprises considèrent encore trop rarement les syndicats comme de véritables « partenaires sociaux ». Le dialogue se réduit trop souvent à un jeu d'acteurs sclérosés qui laisse peu de place à l'innovation et à la modernisation¹.

La meilleure solution serait de prévoir une place de plus grande neutralité technologique afin de ne pas définir des règles en fonction des supports utilisés (papier, format numérique) mais en fonction des usages. On peut par exemple distinguer l'information mise à disposition du salarié à qui il appartient de venir la rechercher et celle portée à sa connaissance. On peut faire un parallèle entre les panneaux d'affichage qu'il faut aller consulter, et les sites syndicaux sur lesquels l'information syndicale peut être consultée ou téléchargée. De manière symétrique, on peut s'assimiler l'envoi de messages électroniques en masse vers les adresses professionnelles de groupes de salariés.

De la même façon, on peut distinguer la stricte information des salariés par le biais de tracts papiers ou électronique et la communication interactive en ligne qui peut s'assimiler à des réunions d'échanges. Le législateur pourrait aller plus loin en incluant un volet numérique dans les phases obligatoires du dialogue social. Ainsi, dès qu'un syndicat le souhaiterait il pourrait informer les salariés concernés par un dossier en discussion dans les instances représentatives du personnel (orientation stratégique de l'entreprise, changement impactant, etc.), par l'intermédiaire d'un courrier électronique ou via des outils spécifiques.

A titre de droit comparé, La possibilité pour les syndicats d'utiliser les outils numériques tels que la messagerie électronique de l'entreprise est inscrite dans le code de travail français. Toutefois la réforme de ledit code comporte sur ce point une innovation. Ainsi cette dernière permet aux syndicats non représentatifs mais satisfaisant aux critères d'ancienneté, d'indépendance et de respect des valeurs républicaines, de diffuser des publications et des tracts sur un site syndical de l'internet lorsqu'il existe. C'est en vérité un

¹Uta DIRKSEN et Mirko HERBERG, Syndicats et Transformation 4.0 : Histoires de syndicats qui confrontent le nouveau monde du travail, Friedrich-Ebert-Stiftung, Berlin, 2021, p. 17.

moyen absolument essentiel pour ces syndicats. Ils doivent pouvoir faire compagnie à égalité de moyens numérique avec les syndicats représentatifs pour, le cas échéant, disposer eux-mêmes d'une légitimité électorale.¹

L'utilisation de l'internet ne concerne que l'envoi par courrier électronique de publications en tracts de nature syndicale. Ainsi, les syndicats sont tenus de respecter deux principes lors de la mise à disposition de ces e-tracts. D'une part, ils doivent respecter le principe d'information et d'opposition préalable, c'est-à-dire qu'ils doivent permettre aux salariés de manifester leur accord ou leur opposition à l'envoi de tracts. D'autre part, ils doivent respecter le principe de confidentialité. Ainsi, toute mesure de sécurité devrait être prise afin d'assurer la confidentialité des échanges électroniques éventuels des salariés avec les organisations syndicales.

Paragraphe 2 : Le numérique : un outil de vote électronique et de visioconférence.

Les technologies numériques offrent, de nouveaux outils aux négociateurs dont les élections syndicales par voie électronique. Ainsi le vote aux élections professionnelles constitue une condition d'habilitation des négociateurs. Le vote dématérialisé appelé communément ; vote électronique, vote par internet, élections électronique ou élections en ligne, considéré comme expérimental il y a quelques années focalise aujourd'hui l'attention. Tout d'abord, le terme vote électronique est source d'ambiguïtés, il englobe à la fois les ordinateurs placés dans les bureaux de vote et le vote à distance qui s'effectue depuis n'importe quel ordinateur connecté à internet, par exemple depuis le domicile de l'électeur.

Le vote électronique à distance désigne exclusivement une forme de vote électronique dans laquelle le vote se fait au moyen de dispositif qui n'est pas surveillés par des membres des services électoraux. Le vote par correspondance électronique ne constitue en fait qu'une adaptation du vote par correspondance sous pli fermé à l'évolution des nouvelles technologies consistant pour l'électeur à voter de son domicile au moyen d'un ordinateur relié au réseau internet².

Le vote électronique constitue une modalité de vote particulièrement adaptée au travail à distance et permet, plus généralement de pallier les inconvénients liés à l'éclatement géographique de la collectivité de travail. Rappelons seulement que les modalités du vote

¹L. GRATTON, *Op.cit.*, p. 1055.

²Yann-Maël LARHER, *Op.cit.*, p. 88.

électronique doivent respecter les principes généraux du droit électoral, c'est-à-dire les deux exigences fondamentales de secret et de sincérité du scrutin. C'est la raison pour laquelle le recours au vote électronique fait l'objet d'un encadrement légal assez strict en France : il est subordonné à un accord d'entreprise, lequel doit être conforme à un cahier des charges très précis.¹

Ainsi, la faculté de recourir à un vote électronique est ouverte par un accord d'entreprise ou par un accord comportant un cahier des charges respectant quelques prescriptions minimales. Le système retenu assure la confidentialité des données transmises, notamment de celles des fichiers constitués pour établir les listes électorales des collègues prévus par le Code de travail Français, ainsi que la sécurité de l'adressage des moyens d'authentification, de l'émargement, de l'enregistrement et du dépouillement des votes. La loi française prévoit également la possibilité de confier la conception et la mise en place du vote électronique à un prestataire externe spécialisé choisi par l'employeur sur la base d'un cahier des charges respectant certaines prescriptions afin d'offrir un maximum de garanties en termes de sécurité et de confidentialité².

Au Maroc, lors de l'étape de l'entrée en négociation. S'agissant de la négociation obligatoire d'entreprise, la convocation à l'assemblée générale doit être établie selon la forme et les conditions de l'article 122 de la loi 78-12 qui complète la loi 17-95 relative aux sociétés anonymes. L'employeur peut recourir à la convocation électronique des parties à la négociation et ceci par un courriel électronique. Soulignons seulement que l'employeur, s'il utilise la messagerie électronique, devra prendre soin de ménager la preuve que toutes les organisations syndicales représentatives dans l'entreprise ont effectivement été touchées par le message.

Une fois convoquées les parties entre alors en négociation. En pratique, les actionnaires ou leurs mandataires peuvent assister à l'assemblée générale soit physiquement ou virtuellement (lorsque les statuts de la société anonyme le prévoient). Ainsi, les sociétés anonymes peuvent prévoir dans leurs statuts la possibilité de tenir des assemblées générales d'actionnaires, ordinaire et extraordinaires par des visioconférences ou par des moyens de télécommunication et ce, conformément avec les dispositions de la loi n°20-05 qui complète la loi n°17-95.

¹L. GRATTON, *Op.cit.*, p. 1056.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 115.

Selon l'article 50 bis de ladite loi n° 20-05 il est désigné par visioconférence ou moyens équivalents tous moyens permettant aux administrateurs, membre du conseil de surveillance ou actionnaires de participer à distance aux réunions. Les moyens de visioconférence utilisés doivent remplir certaines conditions à savoir, satisfaire à des caractéristiques techniques garantissant une participation effective aux réunions des organes de direction ou des organes sociaux dont les délibérations sont retransmises de façon continue, permettre d'identifier préalablement les personnes participant par ce moyen à la réunion et enfin, permettre un enregistrement fiable des discussions et délibérations, pour les moyens de preuve. Les procès-verbaux des réunions de ces organes font état de tout incident technique relatif à la visioconférence lorsqu'il a perturbé le déroulement de la réunion.

Sous-section 2 : Le rôle du numérique dans la modernisation du dialogue sociale.

Les technologies de l'information et de la communication sont particulièrement adaptées à la communication moderne des représentants du personnel, dans un contexte où le milieu de travail à distance offertes par l'outil internet (télétravail...) et l'éclatement des représentants et des salariés sur différents sites à l'échelle du village planétaire. Le passage à l'ère du numérique est un puissant moteur de transformation des organisations qui donne une nouvelle dimension au dialogue sociale, notamment en sollicitant plus les salariés¹.

Les travailleurs devraient avoir à leur disposition des moyens juridiquement contraignants leur permettant de faire connaître leurs besoins et leurs souhaits aux opérateurs de plateformes, à travers la syndicalisation, la négociation collective et, dans les pays où ces structures existent, les comités d'entreprise et le droit à la codétermination². De ce fait, une reconnaissance syndicale semble s'imposer à l'ère du numérique (Paragraphe 1), renforcée par un droit à la négociation collective (Paragraphe 2).

Paragraphe 1 : La reconnaissance syndicale à l'ère du numérique.

Les difficultés de syndiquer les travailleurs de l'ère numérique et la remise en question des systèmes normatifs se vivent dans différents Etats, malgré des systèmes de rapports

¹J-M SERVAIS, « Travailleurs des plateformes numériques de services : quelles garanties sociales ? », in Revue Interventions Economiques, N° 60, 2018, p. 10.

²Françoise PIERSON, « L'organisation syndicale : du communautaire vers le réticulaire » in Où va le travail à l'ère numérique ?, Ouvrage collectif sous la direction d'Anne-France SAINT LAURENT-KOGAN et Jean-Luc METZGER, Presses des Mines, coll. Sciences sociales, Paris, 2007, p. 72.

collectifs de travail bien différents. À l'égard de la forme primaire de dématérialisation des milieux de travail que représente l'automatisation des tâches ou la robotisation au sein d'un établissement physique notre droit du travail devrait subir quelques modifications afin que cette institution en droit du travail appréhende mieux les changements technologiques.

Tout système de rapports collectifs doit, posséder les qualités de souplesse et d'adaptabilité pouvant permettre l'implantation et l'assimilation optimale et équitable de ces changements. Puisque ce problème de l'inadéquation des régimes de rapports collectifs relative aux travailleurs de plateformes sévit dans de nombreux pays ou Etats, il sera alors intéressant de voir comment ces pays et leurs organisations syndicales ont réfléchi à ces nouvelles réalités pour mieux les appréhender. Ces pistes de solutions serviraient à rétablir l'équilibre relationnel entre l'association de salariés et l'employeur, rompu par l'avènement, souvent unilatéral, de nouvelles technologies au sein de l'entreprise et constitueraient aussi de belles sources d'inspiration afin d'amorcer le dialogue social nécessaire dans l'instauration d'un régime de rapports collectifs du travail pour les travailleurs des plateformes numériques.

Certains pays européens ont amorcé le dialogue social relativement aux enjeux de la numérisation sur l'emploi¹. La France a pour sa part adopté une loi qui s'adresse précisément aux travailleurs des plateformes numériques, par l'entremise de la réforme *El Khomri* en 2016. Cette réforme considère ces travailleurs comme étant des travailleurs indépendants bénéficiant des droits collectifs : de s'associer, de négocier et de procéder à des actions collectives². L'Hexagone est d'ailleurs un des premiers territoires à avoir instauré un régime de rapports collectifs du travail destiné spécifiquement aux travailleurs des plateformes. Cette réforme législative a le mérite d'avoir amorcé une reconnaissance syndicale en fournissant un cadre légal par lequel les travailleurs de plateformes, qui ne pourraient réussir à obtenir le statut de salarié par voie judiciaire, peuvent exercer leur droit d'association.

À l'opposé de ces démarches plus traditionnelles de reconnaissance syndicale, empruntant le chemin du cadre légal, d'autres initiatives se font tout simplement en dehors des institutions du travail. Par exemple, une des plus grandes centrales syndicales allemandes, *IG Metall*, a lancé un site Internet, le Faircrowdwork¹⁵⁶, par lequel les travailleurs des plateformes numériques peuvent échanger entre eux et évaluer les entreprises donneuses d'ouvrages sur ces plateformes, notamment quant aux enjeux de rémunération. Ce site permet

¹En Allemagne, l'initiative s'intitule « Arbeiten 4.0 » et en France le rapport Mettling.

²I. DAUGAREILH, C. DEGRYS et P. POCHET, *Op.cit.*, p. 44.

également d'obtenir des conseils juridiques fournis par *IG Metall*. Des portails internet similaires à celui-ci existent également aux États-Unis et en Espagne¹. En Belgique, la Société mutuelle des artistes, plus connue par son acronyme Smart, est initialement destinée à la collectivité artistique. Néanmoins, cette société représente dorénavant des travailleurs issus des plateformes numériques, surtout celles concernant la livraison à domicile (*Take it Easy*, *Deliverro*, *Uber Eats*). Une première entente a été négociée pour les coursiers à vélo que la Smart représente².

Ces manifestations du syndicalisme dans l'univers du travail virtuel démontrent la nécessité d'entamer les démarches sociales afin de reconnaître ces travailleurs du Web, qu'ils soient pigistes, journalistes, traducteurs, livreurs à vélo, comme partie intégrante de notre force de travail et de réfléchir au régime de rapports collectifs du travail le plus adéquat pour ces groupes. À l'heure actuelle où les changements technologiques transforment radicalement le marché de l'emploi, la solution demeure donc d'établir de nouvelles balises d'accès à la liberté d'association reflétant véritablement le contexte organisationnel dans lequel œuvre les travailleurs et de rétablir l'équilibre relationnel entre les salariés et les employeurs.

Paragraphe 2 : Le droit à la négociation collective à l'ère du numérique.

Le droit international exhorte que tout Etat membre de l'Organisation Internationale du Travail fasse la promotion de la liberté d'association et la réalise par une reconnaissance effective du droit à la négociation collective³. En effet, La Déclaration de l'OIT relative aux principes et droits fondamentaux au travail adoptée en 1998 fait obligation aux 187 Etats Membres, oblige les Etat du seul fait de leur appartenance à l'Organisation, de respecter, promouvoir et réaliser des principes et des droits relevant de quatre catégories, dont la liberté d'association et la reconnaissance effective du droit de négociation collective. La déclaration consacre expressément le caractère universel de ces droits et rappelle qu'ils s'appliquent à chacun dans tous les Etats, quel que soit leur niveau de développement économique. Elle précise en outre que le critère à retenir pour définir les personnes auxquelles ces droits doivent

¹Ibid., p..45.

²Jean BERNIER, Op.cit., p. 130.

³OIT, « Déclaration de l'OIT relative aux principes et droits fondamentaux au travail et son suivi », Conférence internationale du travail, Genève, 18 juin 1998.

être reconnus n'est donc pas la relation d'emploi avec un employeur ; cette relation est en effet souvent absente, par exemple dans le cas des travailleurs indépendants¹.

La négociation collective, essentielle pour pallier les inégalités inhérentes de la relation entre l'employeur et l'association de salariés², permettra de limiter les droits de gestion de l'employeur sur l'avènement de changements technologiques, période qui peut s'avérer l'une des plus révélatrices de la précarité du statut dans l'entreprise des salariés. Qu'ils soient considérés comme des salariés ou comme des travailleurs indépendants non salariés, les travailleurs des plateformes devraient jouir de la liberté d'association et du droit à la négociation collective. Le fait que, en vertu du droit de la concurrence actuel, certaines juridictions interdisent aux travailleurs des plateformes considérés comme non salariés de s'organiser et de négocier des conventions collectives avec les opérateurs n'est pas un argument qui prouve que ces travailleurs ne doivent pas être autorisés à s'organiser ; c'est un argument qui plaide en faveur d'une réforme du droit de la concurrence.

De leur côté, les organisations syndicales, qu'elles soient européennes ou nord-américaines, se heurtent également à ces changements en profondeur dans l'évolution de l'organisation du travail du au NTIC. Malgré ces difficultés certaines, plusieurs initiatives syndicales ont été lancées dans les cinq dernières années. Ainsi en matière de négociation de convention collective, un des exemples les plus cités provient du Danemark. Un syndicat danois a négocié et signé un accord collectif avec une plateforme numérique qui fournit des services de nettoyage à domicile (*Hilfr*). Cet accord prévoit, entre autres, la possibilité pour les travailleurs engagés comme indépendants de devenir des salariés après 100 heures de travail. Également, en Autriche, un premier comité de travail a été mis en place par les travailleurs de livraison à domicile pour la plateforme *Foodora*³. Par ailleurs, certaines lois canadiennes se sont dotées de mécanismes de réouverture de la convention collective lorsque des changements technologiques surviennent dans l'entreprise en période de paix industrielle.

Ces instruments législatifs, supplétifs aux conventions collectives prévoyant déjà de telles procédures, obligent tout d'abord un préavis de changement technologique dans lequel l'employeur doit détailler les éléments relatifs à ces changements. Par la suite, le syndicat peut saisir un arbitre ou le tribunal administratif du travail si l'employeur n'a pas respecté son

¹BIT, « Les plateformes de travail numérique et l'avenir du travail: pour un travail décent dans le monde en ligne », 1^{ère} éd., Genève, 2019.

²Abdellah BOUDAHRAIN, Droit social marocain, Sochepress-Université, Casablanca, 1984, p. 115.

³I. DAUGAREILH, C. DEGRYS et P. POCHET, *Op.cit.*, p. 44.

obligation de préavis de changement technologique. Suivant le préavis ou l'ordonnance de l'autorité décisionnelle, le syndicat a la possibilité d'envoyer un avis de négociation à l'employeur. Un moratoire sur les changements technologiques peut dès lors s'enclencher pour permettre une juste négociation. Cette dernière porte alors sur les conditions de travail et la sécurité d'emploi compromis par les transformations technologiques. Ces exemples demeurent peu nombreux et l'on ne peut affirmer, à ce stade qu'ils essaient dans l'économie de plateforme. Mais ils montrent sans doute la voie à suivre.

Malgré certains succès remarquables, il n'est pas sûr que le répertoire d'action traditionnel suffise à relever les défis, en particulier en ce qui concerne la question du micro-travail¹ digital. De nouvelles alliances gagneraient sans doute à être construites, ainsi que de nouvelles stratégies pour aller à la rencontre des travailleurs les plus vulnérables de plateformes, souvent cachés, afin de mettre en lumière leurs conditions de travail et construire avec eux un modèle social réinventé, reconfiguré, qui soit le produit de la progression du numérique dans l'économie².

¹C'est un ensemble de toutes petites tâches informatiques qui ne peuvent être totalement déléguées à des ordinateurs ou à des robots. Il faut donc la sous-traiter à des humains mais pour un coût extrêmement faible. Ces micro-tâches numériques comprennent donc un ensemble de manipulations informatiques très simples comme l'identification et le nommage d'objets sur une image, la vérification de mots clés sur un produit en ligne, la réponse à un sondage en ligne, la transcription de sons en texte, la traduction de petits textes d'une langue à l'autre, l'inscription à des sites internet, la participation à des forums de discussion, la visite de sites web, la notation de vidéos ou d'articles, l'inscription à des concours en ligne ou encore l'écriture de commentaires et de critiques sur des articles

²C. DEGRYSE, « Du flexible au liquide : le travail dans l'économie de plateforme » in *Revue Industrielle*, N° 4, 2020, p. 661.

Conclusion du Titre I

Le développement de l'économie numérique a modifié de façon importante les modes de production des produits et des services, à telle enseigne qu'il oblige les entreprises à revoir leurs pratiques de fonctionnement sur tous les plans. Qui plus est, l'accélération vers le numérique envahit peu à peu le quotidien de chacun et chacune qui voit se transformer parfois en profondeur son activité de travail jusqu'à entraîner une certaine forme de déqualification professionnelle¹. La transformation digitale souvent commence par la création et la direction des entreprises. Par la suite elle intègre le monde du travail et la relation de l'entreprise avec ses collaborateurs et leurs modes de travail.

Dans ce cadre, la meilleure façon d'appréhender la transformation digitale est de rester à l'écoute des besoins de chaque salarié mais aussi de son écosystème pour prendre le rythme de transformation en accord avec les évolutions. Les salariés mis face à des outils et usages obsolètes au sein de l'entreprise ressentent un décalage technologique entre leur vie privée et leur vie professionnelle². En effet, le numérique impacte donc les relations du travail individuel et collectif. D'où la nécessité d'assurer une sécurité juridique pour pouvoir limiter les risques et incertitudes développées par le numérique.

Conscient du rôle du numérique dans la vie de l'entreprise, le législateur marocain a mis en place plusieurs lois assurant la création et l'accompagnement de l'entreprise dans son processus de digitalisation. Cependant, nous avons relevé plusieurs insuffisances, liées essentiellement à l'absence d'une réglementation régissant les nouveaux modes de travail : télétravail, *crowdworking*, etc. contrairement à son homologue français. Par ailleurs, il est vrai que le législateur marocain a prévu un processus électronique pour la création des entreprises. Néanmoins, la réglementation relative à la gouvernance des entreprises manque de précision sur l'importance de l'outil digital dans la direction de l'entreprise.

¹Jean BERNIER, *Op.cit.*, p. 11.

²Jean-Noël CHAINTREUIL, *RH et digital*, Diateino, Paris, 2015, p. 8.

Titre II

Les instruments digitaux de l'entreprise

Plusieurs entreprises ont fait le choix stratégique, et ce depuis plusieurs années, de miser sur la transformation digitale comme levier de croissance économique et sociale. Parmi les objectifs de ses stratégies on trouve notamment le développement accéléré de l'économie digitale¹. Ce développement économique et social escompté par la transformation numérique ne sera possible que si celle-ci bénéficie d'un climat de confiance pour les principaux instruments digitaux de l'entreprise à savoir les contrats numériques qu'elle conclut et ses créations numériques qui doivent faire l'objet de protection par le droit de la propriété intellectuelle.

D'une part, l'entreprise lors de sa transformation digitale fait appel à des contrats numériques pour réaliser ses activités. Ainsi, le contrat numérique permet de faciliter l'audit du contrat et la gestion des données importantes au sein de l'entreprise. C'est un outil fiable et sécurisé, constitue un gain de productivité et permet l'accélération du processus de contractualisation. De plus cette contractualisation en ligne engendre moins de dépenses liées à la gestion des contrats et facilite le contrôle du cycle de vie du contrat². D'autre part, le droit de la propriété intellectuelle constitue une composante importante de l'entreprise. Il demeure un instrument de protection que la transformation numérique de l'entreprise met à l'épreuve et appelle à compléter afin que les investissements des entreprises en matière de création numérique puissent être sécurisés³.

En effet, si au vu de la progression de la transformation digitale des entreprises, la confiance numérique semble acquise, elle est le fruit de la volonté du législateur de bâtir des règles juridiques à cet effet. Il s'est ainsi attaché à permettre et à faciliter la conclusion des contrats numériques et à protéger les créations numériques de l'entreprise. Dans ce contexte, notre analyse s'attardera dans un premier temps sur les contrats numériques (Chapitre 1), pour

¹Maryvonne de SAINT PULGENT, « Les besoins d'interrégulation engendrés par Internet. Propos introductifs » in Internet, Espace d'Interrégulation, Ouvrage collectif sous la direction de Marie-Anne FRISON ROCHE, Dalloz, Paris, 2016, p. 4.

²Nicolas CURIEN, « La régulation réflexive à travers le miroir de la transition numérique » in Internet, Espace d'Interrégulation, Ouvrage collectif sous la direction de Marie-Anne FRISON ROCHE, Dalloz, Paris, 2016, p. 132.

³André LUCAS, Droit d'auteur et numérique, Litec, Paris, 1998, p. 200.

se focaliser dans un second temps sur la propriété intellectuelle et la transformation numérique de l'entreprise (Chapitre 2).

Chapitre I

Les contrats numériques

A travers la révolution numérique que connaît le monde, le contrat numérique s'impose de plus en plus et devient une réalité qui s'est affirmée par l'existence de règles permettant d'assurer le respect des engagements. Ainsi, afin de faciliter les échanges et garantir la transition digitale de l'entreprise, les contrats ont été aménagés pour tenir compte de leur conclusion via internet et des contrats spéciaux relevant de la vente à distance et des services financiers à distance ont été créés.

Les contrats numériques ne constituent pas une nouvelle catégorie de contrat. Ce sont des contrats classiques – vente, location, service, mandat – passés par la voie numérique. Ils peuvent être exécutés en ligne ou exécutés en dehors du réseau¹. Et, à la différence des contrats informatiques auxquels ils sont naturellement liés par une même technologie numérique, et lesquels tiennent une bonne part de leur spécificité de la technicité de la matière sur laquelle ils portent, les contrats numériques tirent leur originalité de l'immatérialité du vecteur par lequel ils sont conclus, et parfois exécutés, ce qui a commencé par soulever des problèmes². De ce fait, le principe fondamental est que les contrats peuvent, en général, être conclus par voie numérique, c'est-à-dire sur ce support dématérialisé. Principe que nous développerons en examinant le processus de contractualisation sur internet (Section 1).

Par ailleurs, au sein même du monde numérique, deux modalités de conclusion de contrats numérique peuvent être distinguées. Le professionnel peut d'une part proposer directement sur le réseau une prestation de services ou un produit destinés aux consommateurs, et il peut d'autre part conclure des contrats avec d'autres professionnels. Le régime juridique des contrats passés avec des consommateurs ou entre professionnels diffère d'une catégorie de contractants à un autre. Ainsi, de nombreux contrats peuvent intéresser l'entreprise dans le cadre de sa transition digitale, il faudra ainsi traiter les régimes

¹Achat de produit (cuisinière, frigidaire, aspirateur, ordinateur...), consommation de services (transport, hôtel...).

²J. HUET, « Contrat électronique -Présentation générale », 27 Juin 2021, consulté le 02-06-2022 à 10h sur https://beta-lexis360-fr.ressources.imist.ma/encyclopedies/JurisClasseur_Contrats_-_Distribution/CX8-TOCID/document/EN_KEJC-211526_0KRR?q=contrat%20%C3%A9lectronique#EN_4.

spéciaux applicables à ces derniers en fonction de leur objet tout en évoquant certains d'entre eux (Section 2).

Section 1 : Processus de contractualisation en ligne.

Le processus de contractualisation en ligne se scinde en deux clics. Le premier clic consiste en la vérification de l'offre du contrat. Ainsi, le destinataire de l'offre doit avoir eu la possibilité de vérifier la commande et de son prix total, et de corriger d'éventuelles erreurs, avant de confirmer celle-ci pour exprimer son acceptation. Le deuxième clic consiste en la confirmation de la commande autrement dit exprimer une acceptation définitive pour exécuter le contrat.

Par conséquent, plusieurs étapes ponctuent ce parcours de contractualisation en ligne, du moins généralement. La logique commande de commencer par envisager la préparation et la conclusion du contrat définitif (sous-section 1), avant d'étudier les modes de sécurisation des échanges numérique (Sous-section 3), afin de pouvoir analyser l'exécution du contrat numérique (Sous-section 3).

Sous-section 1 : Préparation et conclusion du contrat numérique.

Les contrats simples se concluent rapidement et directement. Mais s'ils sont complexes, ils nécessitent une période préalable d'études préliminaires, qui se déroulent pendant le temps des pourparlers c'est-à-dire le moment précédent sa réalisation. Il en est particulièrement ainsi lorsqu'une entreprise d'une certaine mesure importante désire se digitaliser¹. Ainsi, la période préalable commence par l'ouverture des pourparlers (Paragraphe 1) qui donne naissance à des contrats préparatoires (Paragraphe 2) en vue de conclure le contrat définitif (Paragraphe 3) qui définit les obligations des parties (Paragraphe 4).

Paragraphe 1 : Ouverture des pourparlers.

L'ouverture des pourparlers s'opère de façon diamétralement différente, selon qu'est envisagé un contrat de gré à gré ou que l'entreprise soucieuse de se digitaliser lance un appel d'offres². La méthode venant en premier à l'esprit pour engager des pourparlers dans ce

¹Christophe LACHIEZE, Droit des contrats, ellipses, 3^{ème} éd., Paris, 2012, p. 50.

²Philippe LE TOURNEAU, Droit de la responsabilité et des contrats, Dalloz, 11^{ème} éd., Paris, 2018-2019, p. 95.

contrat du numérique est celle-ci : l'entreprise soucieuse de se digitaliser s'adresse elle-même à une société du numérique (constructeur, distributeur, société spécialisée de service) qu'elle choisit, parce qu'elle lui paraît présenter les qualités requises pour cette affaire. Elle lui propose de contracter ou plus exactement d'entrer en pourparlers pour contracter ensemble. Juridiquement, il n'y a pas ici d'offre véritable de contracter, bien que celle-ci puisse exister. C'est le marché de gré à gré, le plus répandu pour les petits contrats mais qui existe aussi pour les contrats importants.

Le contrat de gré à gré présente un avantage certain par rapport à l'appel d'offres à savoir la rapidité. De plus, lorsque le projet comporte des engagements au-delà de la mise en route de l'installation (formation, maintenance, etc...), cette formule est préférable par sa souplesse et parce qu'elle permet une meilleure compréhension entre les parties. Mais d'une façon générale, le contrat de gré à gré est plus onéreux que le contrat sur appels d'offres, n'étant que rarement forfaitaire, et la concurrence ayant été moins contraignante¹.

La méthode venant en deuxième lieu à l'esprit est celle de l'appel d'offre. Après une étude préalable effectuée souvent par une entreprise de service du numérique, l'entreprise en mal de digitalisation lance un appel d'offre. Elle propose un contrat déterminé dont elle laisse le soin aux destinataires de préciser les modalités. Juridiquement, le véritable offrant est donc la société soumissionnaire qui répondant à l'appel, propose un contrat précis à des conditions déterminées. Les candidats sont soumis à la concurrence. L'appel doit être maintenu dans un délai raisonnable à l'expiration duquel il devient caduc².

En effet, la décision de retenir telle ou telle société parmi les divers soumissionnaires à l'appel d'offre ou de confier le projet de gré à gré à telle ou telle société, ne signifie pas que l'affaire est conclue. Les négociations vont maintenant reprendre leur envol, des tractations vont intervenir, qui seront d'autant plus longues et complexes que le contrat est important. De plus, le devoir de loyauté et de bonne foi est exigé dès la phase précontractuelle y compris à propos des avant-contrats que nous allons détailler ci-dessous.

¹Christiane LARROUMET et Sarah BROS, *Traité de droit civil Tome 3 : Les obligations, Le contrat*, Economica, 10^{ème} éd., 2021, Paris, p. 115.

²Philippe LE TOURNEAU, *Op.cit.*, p.98.

Paragraphe 2 : Les contrats préparatoires.

Au cours des négociations et pourparlers plusieurs contrats peuvent être conclus successivement portant sur la même opération. Les contrats préparatoires sont d'une grande diversité, aux noms eux-mêmes trop variés¹. Les parties sont amenées à rédiger toutes sortes d'actes, tels un engagement d'honneur, un pacte de préférence, une promesse unilatérale ou synallagmatique, un contrat cadre etc. En dehors de ceux-ci, nous isolerons ceux que nous appelons ; les contrats préparatoires de précaution, l'accord de principe et le protocole d'accord. Ces divers contrats préparatoires ne sont pas obligatoires et dans les affaires simples, plusieurs de ces étapes, voire toutes, seront brulées².

En effet, dès le début des pourparlers, il est prudent de faire signer à son partenaire un contrat préparatoire de précaution comportant un certain nombre de clauses. D'abord la clause de limitation à travers laquelle les parties conviennent qu'aucune disposition du présent accord ne peut être interprétée comme obligeant l'une des parties à se lier contractuellement avec l'autre dans l'avenir. Ensuite, la clause de confidentialité dite aussi de secret ; vu qu'il y a des informations confidentielles et de savoir-faire conférant un avantage concurrentiel qui risquent d'être dévoilé. Par ailleurs, la clause de paiement des études préliminaires que la société numérique sera amenée à effectuer. Cette clause est importante car celle-ci représente souvent un pourcentage non négligeable du montant du contrat. Enfin, les parties peuvent ajouter divers clauses telle que la clause d'exclusivité, ou encore une clause de délais pour l'achèvement des pourparlers. Souvent tous ou une partie de ces dispositions seront adoptées dans un accord de principe³.

L'accord de principe est un accord préliminaire soit constatant des éléments sur lesquels les parties s'entendent mais sans qu'il vaille engagement, soit un acte par lequel les parties s'engagent à négocier de bonne foi un deuxième contrat dont elles ne précisent ni les clauses essentielles ni, les clauses accessoires, tout en relevant certains éléments sur lesquels elles sont déjà d'accord. Ce n'est que l'affirmation d'un engagement de négocier.

¹Jacques GHESTIN, Grégoire LOISEAU et Yves-Marie SERINET, La formation du contrat : le contrat, le consentement, LGDG, 4^{ème} éd. coll. Traités, 2013, Paris, p. 115.

²Ph. FOURNIER, « Les apports de l'ordonnance en matière de pourparlers et d'avant-contrats », in IP/IT, N° 5, Mai 2016, Dalloz, p. 237.

³بشرى النية، العقد المبرم بطريقة الكترونية، رسالة لنيل الدكتوراه في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، اكدال الرباط، السنة الجامعية 2011-2012، ص. 100.

La seule obligation qui en résulte est la reprise des pourparlers, sans du reste d'engagement quant à leur aboutissement¹.

Le protocole d'accord (*Draft agreement*), lui, contrairement à l'accord de principe engage les éléments sur lesquels les parties s'entendent, il consigne les conditions et les obligations dont les parties sont convenues. C'est généralement un véritable contrat, mais un contrat partiel, un contrat d'étape intervenant avant le contrat total définitif. C'est un contrat cadre sur lequel viendront éventuellement se greffer des contrats ultérieurs, précisant notamment des points sur lesquels les parties ne sont pas encore parvenues à un accord, ou régulant certains aspects techniques particuliers. Son exécution pourra commencer dès la signature de ce protocole, ce qui la différencie grandement du simple accord de principe raison pour laquelle les anglais disent qu'il est *self-executing*².

Paragraphe 3 : La formation du contrat définitif.

Le dénouement intervient, soit par la rupture des négociations, soit au contraire par la conclusion du contrat définitif. Toutes les questions ayant été enfin réglées, arrive le moment de la rédaction, puis de la conclusion du contrat définitif, qui succède aux avant-contrats. Le contrat peut se conclure sous forme électronique c'est alors un acte juridique électronique, mais aussi par voie électronique le cas d'une commande en ligne. Dans ce cadre, l'Assemblée générale de la CNUCID a adopté la convention des Nations Unies sur l'utilisation des communications électroniques dans les contrats internationaux en Novembre 2005³. Ce texte a pour objectif de renforcer la sécurité juridique et la prévisibilité commerciale lorsque les communications en matière de contrats internationaux se font par le biais de messages de données. Pour ce faire, elle requiert des pays signataires la reconnaissance de la validité des

¹François COLLART DUTILLEUL et Philippe DELEBECQUE, Contrats civils et commerciaux, Dalloz, 11^{ème} éd., coll. Précis, Paris, 2019, p. 900.

²Philippe LE TOURNEAU, Contrats du numérique informatiques et électroniques, Dalloz, 10^{ème} éd., Paris, 2018-2019, p. 98.

³La Convention n'a pas vocation à régir le droit interne et ne s'intéresse qu'à « l'utilisation de communication électroniques en rapport avec la formation ou l'exécution d'un contrat entre les parties ayant leur établissement dans des Etats différents » (art. 1). Le champ d'application de cette Convention est très large, puisque contrairement aux lois types qui ne s'appliquaient qu'en matière commerciale, les rédacteurs de la Convention ont préféré une application générale. Autrement dit, la Convention est applicable dans les relations avec les consommateurs.

communications électroniques et contient des dispositions traitant des problèmes qui surgissent généralement dans les accords électroniques¹.

Selon l'article 8 de ladite convention, le contrat peut également se former par l'interaction d'un système de messagerie automatisé avec un autre système de messagerie automatisé ou une personne. En outre, il recevra le même traitement que les contrats dans lesquels une personne physique est intervenue. Cet article vise par exemple les sites internet offrant des produits ou des services à la vente qui sont totalement informatisés, tel que la vente de billets de train ou d'avion en ligne et plus généralement, les relations qui se nouent entre des agents électroniques avec des sites internet.

Par transposition de ces dispositions, le D.O.C a intégré les nouvelles dispositions de la loi 53-05 relative à l'échange électronique de données juridiques. Le titre premier du livre premier du Dahir formant Code des Obligations et des Contrats a été complété par un chapitre premier bis relatif au « contrat conclu sous forme électronique ou transmis par voie électronique ». Vu qu'il s'agit d'un contrat entre absent, des précautions en amont ont été instituées par le législateur afin d'éviter tout risque d'erreur pour que le consentement soit suffisamment éclairé et qu'il soit celui d'un contractant informé. Ainsi, la voie électronique peut être utilisée pour mettre à disposition du public des offres contractuelles ou des informations sur des biens ou services en vue de la conclusion d'un contrat. Des dispositions précises sont donc venues régir l'offre et la conclusion du contrat sous forme électronique².

Pour ce qui est de la conclusion d'un contrat sous forme électronique. L'article 65-5 de la loi 53-05 énonce que le destinataire de l'offre doit avoir eu la possibilité de vérifier le détail de son ordre et de son prix total et de corriger d'éventuelles erreurs et ce, avant de confirmer ledit ordre pour exprimer son acceptation. Ainsi, pour que le contrat électronique soit valable, l'auteur de l'offre doit accuser réception de l'acceptation de l'offre qui lui a été adressé conformément à l'article 65-5 de la loi 53-05. Cet accusé de réception n'emporte pas pour autant validation contractuelle des échanges³. En effet, il n'a qu'un rôle technique dépourvu de toute valeur contractuelle, il permet seulement d'avoir confirmation que la commande a bien été prise ne compte. La loi précise dans le même article que « l'acceptation de l'offre, sa confirmation et l'accusé de réception sont réputé reçus lorsque les parties auxquelles ils sont

¹Eric CAPRIOL, *Op.cit.*, pp. 93-04.

²L. BASSIME, « Le Dahir des obligations et contrats à l'ère des nouvelles technologies : la signature électronique. », in *Revue Marocaine de Droit d'Economie et de Gestion*, N° 55, 2016, p.113.

³ R. BOUHLAL et S. LAHLOU, « Contrat et Immatériel », Rapport marocain, 2014.

adressés peuvent y avoir accès.»¹. Force est de constater que nous nous éloignons de la théorie de l'émission² telle que prévue dans un contrat par correspondance classique.

Paragraphe 4 : Les obligations des parties.

Tout contrat écrit d'affaires commence par identifier les parties de façon précise, la plupart des contrats numérique de quelque importance comportent ensuite un préambule et des définitions des termes employés. Vient ensuite l'indication de l'objet du contrat. Mais ce sont les obligations des parties qui constituent le corps du contrat. En effet, il est dans l'intérêt des parties de prévoir minutieusement leurs obligations respectives, tant celle du client que celle de la société numérique. Le D.O.C indique aussi que les contrats doivent être conclus de bonne foi. Les développements sur les obligations des parties doivent toujours être sous-entendus par ce principe. Nous constatons trois obligations principales qui pèsent sur le client à savoir le devoir de coopération, de discrétion et de paiement.

Dans tous contrats pèse sur le créancier une obligation de coopération, particulièrement lorsque son objet est complexe, comme dans un contrat numérique. Cette obligation n'a pas à être expressément stipulée, sauf pour en préciser les modalités ce qui est sans doute utile. Elle doit régner durant toute la vie contractuelle, du début des pourparlers à l'exécution du contrat. Le devoir de coopération se concrétise, lors des négociations sous la forme d'une obligation d'information. Une fois les négociations achevées, le devoir de coopération se poursuit durant la phase de mise à point du projet. Il se traduit encore une fois par la transmission d'informations. Le client doit fournir toutes les données qu'il possède ou dont il s'est chargé de recueillir. L'obligation de coopération du client se prolonge de même durant la phase d'installation et de mise en route, il doit notamment prévenir immédiatement son partenaire de toute information qui lui parvient, faciliter la coordination des personnels appelés à œuvrer ensemble. Cette obligation de coopération du client est le corollaire de celle d'information ou de conseil pesant sur l'entreprise du service numérique. La première atténue l'intensité de la seconde, car tout bon professionnel a le devoir de se renseigner avant de contracter dans la mesure de ses capacités³.

¹V. art. 65-5 de la loi 53-05.

²Selon l'article 24 du D.O.C le contrat par correspondance est parfait au moment et dans le lieu où celui qui a reçu l'offre répond en l'acceptant.

³Philippe LE TOURNEAU, *Op.cit.*, p.163.

Le client est tenu de plus d'un devoir de discrétion c'est-à-dire conserver le secret sur tous les procédés, techniques, plans, études, mise de point par l'informaticien qui ne sont pas protégés au titre du droit de la propriété industrielle et relèvent du seul savoir-faire, dès lors qu'il procure un avantage concurrentiel. Cette obligation est réciproque car la société numérique s'engage de son côté à garder le silence sur les données de toutes natures, propres à son cocontractant, qu'elle aurait été amenée à connaître lors du projet.

Enfin, pèse sur le client le devoir de paiement. Le prix est pour la société numérique, le but du contrat et pour l'entreprise, l'objet de son obligation. Sa fixation implique que la première ait pu au préalable mesurer assez finement le coût économique du projet ; et que le second ait pris conscience de l'ampleur de l'investissement. Il est alors possible de déterminer le prix de façon juridique et mathématique, selon divers procédés. Mais dans un monde instable, il est bon de prévoir sa révision et son contrôle¹.

Quant aux obligations de la société numérique, rappelons que nous traitons ici du contrat global de digitalisation ou du numérique, excluant les contrats parcellaires, comme la maintenance du site internet, contrat de publicité sur internet ou encore le contrat de commerce électronique dont nous parlerons plus tard.

L'entreprise ou la société numérique pèse sur elle un devoir général d'information dans le cadre d'un contrat numérique. En effet, les praticiens du contrat numérique savent que le professionnel du numérique a une obligation particulière en période de pourparlers contractuels d'informer son client, à l'époque nécessairement profane, sur les caractéristiques du produit ou service. Nous savons aussi que les contours de cette obligation sont devenus plus précis au fil des années pour exiger du prestataire, du fournisseur ou la société numérique qu'il informe le client sur l'adéquation du produit ou service au besoin exprimé, voire qu'il mette en garde ou qu'il alerte son client sur les limites de la prestation, ou encore sur les inexactitudes ou les incomplétudes de son besoin exprimé. Mais ce qui fait la particularité de cette obligation dite de conseil dans les contrats numériques, c'est que l'intensité de son application a toujours été déterminée par la qualité des parties aux contrats. Ainsi, le niveau d'information à fournir était plus ou moins selon que le client est plus ou moins reconnu comme averti².

¹Ibid., p. 165.

²S. LEMARCHAND, « Le devoir général d'information : un impact majeur dans la formation des contrats informatiques », in IP/IT, N° 5, Mai 2016, Dalloz, p. 234.

Sous-section 2 : La sécurisation des échanges.

En définitive, l'ensemble des développements et implications pratiques de l'internet sont tributaires de l'existence d'une sécurité réelle sur la toile. Afin de prendre en considération l'ensemble de ces impératifs, des dispositions particulières ont et sont toujours en train d'être adoptées, tant au niveau national qu'international¹. En effet, l'essor des contrats conclus par le biais de l'internet passe nécessairement par la mise en place de moyens techniques et règles juridiques de nature à garantir la sécurité des échanges. Il s'agit notamment d'assurer des services de confiance efficaces (Paragraphe 1) et garantir un paiement en ligne sécurisé (Paragraphe 2).

En outre, assurer une sécurité des échanges dans l'environnement numérique passe par la protection des données personnelles au moment de l'offre ainsi que toute au long du processus contractuel (Paragraphe 3). Enfin, dans le cadre du contrat électronique, les parties sont éloignées, elles ne sont ni présentes ni représentées, ce qui laisse des incertitudes quant à leur identification qui peut être facilement usurpées et pose ainsi la question de la recevabilité de la preuve dématérialisées (Paragraphe 4).

Paragraphe 1 : Les services de confiance.

A l'ère des nouvelles technologies de l'information et de la communication, la question du remplacement de la signature manuscrite par la signature électronique est devenue crucial pour assurer la sécurité des changes en matière de contrat numérique (II). Ce remplacement est mis en œuvre grâce à un prestataire de service de confiance (II).

I- La signature électronique.

La signature répond fondamentalement à plusieurs fonctions. Elle apporte, d'une part, la perfection à un acte juridique électronique et, d'autre part, elle identifie celui qui l'appose. En outre, elle permet de manifester le consentement de son auteur à un acte, le contenu de l'acte étant ainsi accepté par le signataire.

Le 5 Juillet 2001, la Commission des Nations Unies pour le Droit Commercial International (CNUDCI) a adopté la loi type sur les signatures électroniques et le guide pour son incorporation. Les travaux pour sa première conception avaient commencé tout de suite

¹Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, Op.cit., p.85.

après l'adoption de la première loi type. Il aura donc fallu près de cinq ans pour parvenir à son adoption à l'issue de longs débats. Cela s'explique par le fait que la signature, aussi bien manuscrite qu'électronique, revêt une importance majeure dans les systèmes législatifs qu'il soit *Common Law* comme d'inspiration civiliste. C'est la conscience de la grande utilité de la nouvelle technologie communément appelée signature électronique que l'Assemblée générale recommande aux Etats cette nouvelle loi type destinée à compléter utilement la première et à assurer la sécurité juridique par l'harmonisation des règles pour les signatures électroniques¹.

Le législateur marocain s'est inspiré de cette loi afin d'adopter une loi relative à l'échange électronique des données juridiques ; il s'agit de la loi 53-05 adoptée en 2007. Néanmoins, la loi 53-05 n'apportait pas la clarté souhaitée sur la force probante des certificats électroniques utilisés pour la signature lorsqu'ils ne sont pas sécurisés et ne traite pas de l'ensemble des services de confiance. Compte tenu de l'évolution des besoins, de la nécessité de définir plusieurs niveaux de confiance adaptés aux différents usages, et de la nécessité de réglementer de nouveaux services de confiance comme le cachet électronique, le besoin de refonte de la loi 53.05 s'est fortement ressenti². Ainsi, un nouveau cadre juridique, moins contraignant, plus complet et adapté a vu le jour en Décembre 2020. Il s'agit de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques. Cette loi établit le régime juridique applicable à la signature électronique et pose également le cadre juridique applicable aux prestataires de service de certification électronique et aux titulaires des certificats électronique³.

La signature électronique est un procédé d'identification de l'auteur d'un document électronique, en signant, il exprime, son consentement aux obligations découlant de l'acte. L'apport donc de la loi 43-20 se résume dans la validité juridique de la signature électronique dès lors qu'elle remplira certaines conditions. Le recours aux mécanismes de signature électronique s'explique par le fait que l'authenticité d'une transaction ou d'un contrat signé doit pouvoir être vérifiée a posteriori par un tiers⁴. Il est donc nécessaire d'utiliser des

¹Eric CAPRIOL, *Op.cit.*, p. 87.

²«Adoption par le parlement du texte de loi 43.20 relatif aux services de confiance pour les transactions électroniques » consulté le 23-03-2022 à 10h sur <https://www.dgssi.gov.ma/fr/content/adoption-par-le-parlement-du-texte-de-loi-4320-relatif-aux-services-de-confiance-pour-les-transactions-electroniques.html>

³V. art. 3 de la loi 43-20.

⁴ أحمد الشرقاوي، التوقيع الإلكتروني وحجته في الإثبات بين التشريع الوطني والقوانين الدولية، مجلة منازعات الأعمال الدولية، ع. 58، أكتوبر 2020، ص. 10.

procédés reconnus par tous, et pour ce faire, il fallait encadrer et normaliser largement les processus de reconnaissance de signature¹.

Selon l'article 4 de la loi 43-20 la signature électronique est soit simple soit avancée soit qualifiée. Pour ce qui est de la signature électronique simple et avancée, elle doit répondre selon l'article 5 de la loi 43-20 aux conditions suivantes : « Etre propre au signataire ; Permet d'identifier le signataire ; Etre créé par des moyens que le signataire puisse garder sous son contrôle exclusif, avec un niveau de confiance élevé défini par l'autorité nationale ;Repose sur un certificat électronique ou tout procédé jugé équivalent ;Etre liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ». En ce qui concerne la signature qualifiée c'est une signature avancée qui doit être produite par dispositif qualifié de création de signature électronique et qui repose sur un certificat qualifié de signature électronique². La signature électronique sécurisée doit être produite par un dispositif de création de signature électronique, attesté par un certificat de conformité délivré par l'autorité national des services de confiance pour les transactions électroniques³.

Par ailleurs, au Maroc, la loi 43-20 envisage dans son article 9 le tiers de confiance en tant que prestataire de service de certificat qualifié de signature électronique. Le prestataire de services de confiance joue un rôle prépondérant pour établir la confiance numérique des usagers. Cette confiance repose principalement sur différents facteurs, ceux qui sont d'ordre physique, tels que la fiabilité des matériels technologiques et logiciels⁴, et ceux d'ordre humain, comme l'organisation des prestataires en charge d'un service de confiance.

II- Le prestataire de service de confiance.

Le prestataire de services de confiance joue un rôle prépondérant pour établir la confiance numérique des usagers. Afin d'assurer le développement durable du réseau, plusieurs techniques permettent de gagner confiance des utilisateurs des nouvelles technologies. Ces techniques impliquent parfois le recours à un tiers⁵, dont le métier est précisément d'intervenir afin de créer, d'une autre manière que dans l'environnement

¹Khalid ENNASHI, La criminalité numérique en droit marocain, Librairie Rachad, Settat, 2020, p. 73.

²V. art. 6 de la loi 43-20.

³A. SLASSI MOUTABIR, « L'acte authentique à l'ère de la signature électronique », in Revue de Droit Commercial, N° 4, 2017, p. 234.

⁴V. art.12 loi 43-20.

⁵Autorité de certification, horodateur, etc.

traditionnel, un environnement dans lequel les transactions peuvent s'opérer en toute confiance et de manière sécurisée.

En l'absence d'une définition en droit marocain du prestataire de services de confiance, nous emprunterons la définition donnée par le Règlement européen du 23 Juillet 2014¹. Selon l'article 3 de ledit règlement : « Le prestataire de services de confiance est une personne physique ou morale qui fournit un ou plusieurs services de confiance, en tant que prestataire de services de confiance qualifié ou non qualifié ». Afin de matérialiser cette confiance, certaines conditions doivent être respectées dans le but de vérifier la qualité du servi fourni. Nous parlons ici de la conformité, de la qualification, de certification, de référencement des prestataires par rapport à un état de l'art normatif particulier.

Par ailleurs, toute demande d'agrément doit satisfaire aux critères définis par l'article 33 de la loi 43-20, en application duquel, le dispositif de création de signature électronique sécurisée doit être attesté par un certificat de conformité délivré par la DGSSI. A noter qu'à ce jour, *Barid e-Sign* de Poste Maroc est le seul prestataire de services de certification électronique agréé au Maroc, ce monopole s'expliquant en partie la sollicitation quasi-rare des services de certification du fait du peu d'intérêt pour cette technologie. Les demandes d'agréments augmenteront une fois la signature électronique deviendra assez souvent sollicité.

Paragraphe 2 : Le paiement en ligne.

Un des freins du développement et de la digitalisation des entreprises tient à la sécurité des paiements. En effet, certains clients s'abstiennent en raison des risques encourus en tapant leur numéro de carte bancaire pour payer un achat par internet, 30% des internautes dans le monde ne recourant pas à l'achat via internet invoquent leur crainte de donner des informations bancaires². Une précaution élémentaire consiste à n'utiliser sa carte bancaire qu'au bénéfice d'entreprises connues, dont le site comporte une zone de paiement sécurisée dite SSL³, symbolisée par un petit cadenas affiché en position fermée en bas à gauche de l'écran ; dans ce cas, l'adresse dans la fenêtre commence par *https* et non *http*¹.

¹Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

² أحمد محمود المساعدة، الشيك الإلكتروني كأحد وسائل الدفع الإلكترونية الحديثة، مجلة القانون المغربي، ع. 18، مارس 2012، ص. 177.

³Le protocole SSL (Secure Sockets Layer) est le protocole cryptographique le plus largement utilisé pour assurer la sécurité des communications sur Internet. Le SSL crée un canal sécurisé entre deux machines ou appareils communiquant sur Internet ou un réseau interne. Son usage le plus courant est la sécurisation de la

Un des procédés de sécurité de paiement utilisé est celui du chiffrement dit cryptographie. Ce procédé assure la confidentialité et la sécurité de l'échange ou du stockage de données par voie électroniques de manière à assurer leur authentification et le contrôle de leur intégrité. Ce mécanisme est réglementé par l'article 12 de la loi 53-5 relative à l'échange électronique des données juridiques ainsi que l'article 45 et suivant de la loi 43-20 relative aux services de confiance des transactions électronique. On déduit de la lecture de ces articles que la cryptographie est tout matériel ou logiciel qui a pour rôle de modifier des données électroniques c'est-à-dire transformé un texte brut en texte chiffré. Autrement dit, elle consiste à chiffrer des données pour en éviter la connaissance par des tiers.

Au Maroc, le système de la carte de paiement est utilisé depuis longtemps dans les transactions électroniques, mais sans réelle sécurité puisque ne sont utilisés que le numéro et la durée de validité de la carte. Afin de pouvoir utiliser le code confidentiel de celle-ci, il faut soit bénéficier de moyens de confidentialité parfaitement sûrs, soit disposer d'un lecteur de cartes. Or, la sécurisation constitue un élément indispensable au développement du numérique. Plusieurs opérateurs ont développé des systèmes mettant en place des relations transactionnelles tripartites ou un intermédiaire intervient entre les contractants afin de les identifier et de les authentifier, et afin de sécuriser par des moyens technologiques l'échange d'information. Il s'agit des tiers certificateurs que peuvent également gérer les relations avec les organismes bancaires et devenir ainsi des centres de paiement sécurisé.

L'opérateur peut également proposer à son client de créditer un porte monnaie virtuel ou électronique, préalablement à ses achats supprimant ainsi les relations a posteriori avec la banque. Cette monnaie dématérialisée peut être détenue directement sur un logiciel présent dans l'ordinateur du client ou dans une carte à puce, supprimant ainsi la présence d'un tiers détenteur². Raison pour laquelle le Maroc a adopté la loi n°103.12 dite loi bancaire relative aux établissements de crédit et organismes assimilés en mars 2015 reconnaissant ainsi la monnaie électronique comme nouveau moyen de paiement à la disposition de toutes les catégories sociales.

communication entre un navigateur web et un serveur web. L'adresse URL passe alors de HTTP à HTTPS, le 'S' signifiant 'sécurisé'.

¹Philippe LE TOURNEAU, *Op.cit.*, p. 493.

²Christiane FERAL-SCHUHL, *Cyberdroit: le droit à l'épreuve de l'Internet*, Dalloz, 8^{ème} éd., Paris, 2020-2021, p. 601.

Bank Al Maghrib dont l'une des principales missions est de veiller au bon fonctionnement et à la sécurité des systèmes de paiement est chargée d'octroyer des agréments à des établissements pour la gestion de comptes de paiement de leurs clients sans formalités. Ces établissements sont des structures légères avec peu de frais de gestion et au service adapté aux besoins de la clientèle. Au début ces établissements n'étaient autorisés à opérer que des transferts de fonds. Depuis 2018, l'agrément a été étendu à l'ouverture et la gestion de comptes de paiement. A chaque compte de paiement correspond un numéro de téléphone mobile. Ces comptes permettent à leur titulaire de réaliser les opérations de dépôt, retrait, virement de salaire, prélèvement, ou paiement par carte bancaire ou à travers le mobile. Le mobile devient alors une sorte de porte-monnaie virtuel.

Par ailleurs, pour la sécurisation des transactions et gestion de la fraude le Centre Monétique International (CMI) a mis en place des outils afin de détecter et prévenir les opérations frauduleuses lors des transactions e-commerce, et de garantir un paiement sécurisé, en conseillant fortement aux e-commerçants affiliés d'adopter le système « *3D Secure* » ou authentification forte des porteurs. Le *3D Secure* est un protocole sécurisé de paiement sur internet, reconnu sur le plan international qui consiste à s'assurer, lors de chaque paiement en ligne, que la carte est utilisée par son véritable titulaire. Ce système a été inventé pour éviter les fraudes de type CNP (*Card No Present*), c'est-à-dire les paiements frauduleux par carte bancaire sans présence réelle de la carte.

Paragraphe 3 : La protection des données à caractère personnel en matière d'échange numérique.

La protection de la vie privée au Maroc est un principe constitutionnel inscrit dans l'article 24 de la Constitution¹ du Royaume du Maroc qui dispose que « toute personne a droit à la protection de sa vie privée », mais aussi par la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette dernière édicte les règles relatives à la protection des données personnelles et institue une Commission nationale de contrôle de la protection des données à caractère personnel.

Le rôle de la protection des données à caractère personnel dans le droit des contrats est de lutter contre les abus d'utilisation des données de nature à porter atteinte à la vie privée des personnes concerner et de veiller à la conformité des traitements effectués par les contractants

¹Dahir n°1-11-91 du 27 Chaabane 1432 (29 Juillet 2011) portant promulgation du texte de la constitution.

à la loi 09-08 régissant la protection des personnes physiques à l'égard du traitement des données à caractère personnel (I) ainsi que les obligations du responsable du traitement et des sous-traitants. Pour garantir l'application de ces textes, il est important de s'intéresser au rôle joué par la CNDP (III).

I- Les conditions de traitement des données à caractère personnel sur Internet.

Les systèmes de traitement de données à caractère personnel sont liés à tout ce qui se rapporte de près ou de loin à la loi 09-08 qui prévoit des dispositions portant sur les conditions du traitement de cette catégorie de données, les droits de la personne concernée ainsi que les obligations du responsable du traitement. Elle s'applique au traitement des données à caractère personnel, sous quelque forme que ce soit, relatif à une personne physique identifiable ou non identifiable¹.

Le traitement des données à caractère personnel est défini par l'article premier de la loi 09-08 comme étant : « Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » . On en déduit de la lecture de cet article que le simple fait de collecter les données sans même les communiquer ou les diffuser, suffit à caractériser un traitement. La collecte et le traitement des données à caractère personnel doivent être effectuées de façon licite et loyale. L'acceptant de l'offre contractuelle doit donner son consentement clair, libre et averti pour toute opération de traitement des données à caractère personnel².

¹Selon l'article 1 de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel : « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques de son identité physique, psychologique, génétique, psychique, économique, culturelle ou social ».

²La commission nationale de contrôle de la protection des données à caractère personnel (CNDP) a lancé le 28 Janvier 2014 au Maroc une campagne de contrôle qui a porté sur cinq catégories de sites : les deals, les annonces, les offres d'emploi, la vente en ligne, et la réservation de chambres d'hôtel. L'analyse des résultats du contrôle a relevé plusieurs situations de non-conformités par rapport aux exigences de la loi n° 09-08, indique la CNDP. Le problème réside dans le fait que la majorité des sites web n'ont pas notifié leur traitement à l'organisme. Certes, la plupart des sites fournissent des informations sur la politique de protection des données personnelles, mais souvent ces informations sont vagues, incomplète et dispersés ; il en est de même pour le droit à l'information des internautes. La CNDP a également relevé que certains éléments essentiels ne sont pas

Ainsi, chaque traitement de données à caractère personnel ou son transfert à des tiers nécessite le consentement exprès ou explicite de la personne concernée par ledit traitement ou ledit transfert, ce qui exclut le consentement tacite qui n'a aucune valeur juridique dans ce sens. En effet, l'article 4 de la loi 09-08 met en place le principe selon lequel le traitement des données à caractère personnel ne peut être que si la personne concernée a indubitablement donné son consentement à l'opération ou à l'ensemble des opérations envisagées. Et pour que ce consentement soit clair, la loi 09-08 dans son article 5 et suivant a mis à la disposition de la personne physique quelques droits, qui sont au nombre de quatre.

D'abord le droit à l'information, ce droit est au cœur de la protection des données car il constitue une garantie de collecte transparente et loyale des données à caractère personnel l'obligation d'information est prévue par les articles 5 et 6 de la loi 09-08. Le législateur marocain donne droit à la personne, objet de traitement de ses données personnelles, d'être informée, par le responsable du traitement ou représentant, de façon claire et précise. Ce droit de regard sur ses propres données personnelles vise aussi bien la collecte des informations que leur utilisation.

Ce droit est essentiel dans la mesure où il conditionne l'exercice des autres droits tels que le droit d'accès ou le droit d'opposition. Ainsi, toute personne sollicitée en vue d'une collecte de ses données personnelles, doit être préalablement informée par le responsable du traitement de celles-ci ou son représentant d'un certain nombre d'éléments qui sont comme suit : identité du responsable du traitement, finalités du traitement, destinataires des données, référence de la déclaration ou de l'autorisation de la CNDP et, enfin, les modalités d'exercice des droits.

Néanmoins, il existe une dérogation à cette règle qui est prévue par l'article 6 de la même loi. C'est le cas des données à caractère personnel dont la collecte et le traitement sont nécessaires à la défense nationale, la sûreté intérieure de l'Etat, la prévention ou la répression du crime, lorsque l'information de la personne concernée se révèle impossible, ou encore lorsque les informations sont traitées à des fins statistiques, historiques ou scientifiques. Dans ce cas le responsable de traitement doit informer la commission et lui présenter les motifs de l'impossibilité d'information.

indiqués comme les finalités poursuivies par la collecte des données, la communication éventuelle de ces données à des tiers ou encore de l'existence des droits d'accès, de rectification et d'opposition. Il ressort de cette enquête que peu de sites présentent un contenu relativement satisfaisant en matière de protection des données personnelles.

Ensuite le droit d'accès, ce droit est garanti par l'article 7 de la loi 09-08. Cette dernière donne le droit à la personne concernée d'être au courant de l'application de ces données et d'y avoir accès pour s'assurer de leur véracité et si elles font l'objet d'un usage sain. L'accès peut se faire à intervalles raisonnables sans qu'il y ait entrave à ce droit. Or, le responsable du traitement peut demander à la commission nationale des délais de réponses aux demandes d'accès légitimes et peut s'opposer aux demandes manifestement abusives, notamment, par leur nombre et leur caractère répétitif¹.

Puis, le droit de rectification qui constitue selon l'article 8 de la loi 09-08 un complément essentiel du droit d'accès. En effet, les personnes concernées peuvent obtenir du responsable du traitement, l'actualisation, la rectification, l'effacement ou le verrouillage des données personnelles collectées. Cette procédure de rectification se fait par le biais d'une requête destinée à la personne chargée du traitement. Cette dernière est obligée de répondre dans un délai franc qui ne dépasse pas 10 jours². En cas de refus ou de non réponse dans le délai précité, une demande de rectification est introduite auprès de la CNDP, qui charge, l'un de ses membres pour faire les investigations nécessaires et procéder aux rectifications requises dans les plus brefs délais.

Enfin, le droit d'opposition à la prospection directe introduit par l'article 9 de la loi 09-08. Pour autant qu'elle justifie de motifs légitimes, la personne concernée pourra s'opposer, sans frais, au traitement des données la concernant. En effet toute personne peut refuser, sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection, en particulier commerciale. C'est une protection législative contre les messages publicitaires abusifs. Cette loi vise essentiellement à protéger la vie privée des personnes contre toute intrusion possible par exemple au niveau du téléphone portable, courrier électronique, etc. il faut noter que ce droit est réaffirmé par l'art. 10 de la dite loi.

II- Les obligations du responsable du traitement et du sous-traitant à l'égard des personnes.

La distinction entre les notions de responsable de traitement et de sous-traitant est parfois délicate tant il est facile de passer d'une fonction à une autre. Le responsable du traitement est défini par l'article premier de la loi 09-08. Il s'agit de la personne physique ou

¹Khalid ENNASHI, *Op.cit.*, p. 60.

²V. art. 8 de la loi 09-08.

morale, l'autorité publique, ou service ou organisme qui détermine les finalités et les moyens du traitement. Un responsable de traitement se caractérise donc par son autonomie et les choix qu'il peut opérer dans la mise en place et la gestion d'un traitement.

Au contraire, le sous-traitant est la personne physique qui traite des données à caractère personnel pour le compte du responsable du traitement. Il n'est a priori laissé aucune initiative au sous-traitant et celui-ci doit respecter les engagements pris pas le responsable de traitement. Par conséquent, le contrat liant le sous-traitant au responsable du traitement doit comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et prévoir que le sous-traitant ne peut agir sur instruction du responsable du traitement.

Dés lors qu'il met en œuvre un traitement de données à caractère personnel, le responsable du traitement doit respecter certaines obligations imposées par la loi. Il est tenu des obligations de confidentialité, de sécurité des traitements et de secret professionnel¹. Ces obligations qui incombent au responsable du traitement sont régies par l'article 23 et suivant de la loi 09-08. Ledit responsable est tenu de prendre toutes les précautions utiles, de nature technique et organisationnelle, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, surtout, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Le non respect de cette obligation est sanctionné.

Par ailleurs, et d'après l'article 24 de la même loi, le dispositif de protections doit être renforcé lorsqu'il s'agit des données sensibles² ou qui sont relatives à la santé. Aussi, le responsable du traitement doit s'assurer que les personnes placées sous son autorité, ainsi que les sous-traitants auxquels il confie le traitement respectent également les obligations de confidentialité et de sécurité. De plus, les mesures techniques et organisationnelles mises en œuvre doivent être, d'un niveau de sécurité, appropriées au regard des risques présentés par le traitement et de la nature des données à protéger. Enfin, le responsable du traitement et le

¹Sylvain CHATRY, *Op.cit.*, p.116.

²Selon l'article 1 de la loi 09-08 on entend par données sensibles toute donnée à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale de la personne concernée ou qui sont relatives à sa santé y compris ses données génétiques.

sous-traitant sont tenu au respect du secret professionnel¹, et même après avoir cessé d'exercer leurs fonctions.

III- Le rôle de la CNDP face aux traitements des données à caractère personnel.

Au Maroc, la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), a été mise en place en Février 2012 et créée² par la loi n°09-08 du 18 Février 2009, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Cette commission marocaine a pour mission principale de vérifier que les traitements des données personnelles sont licites, légaux et qu'ils ne portent pas atteinte à la vie privée, aux libertés et droits fondamentaux de l'Homme. Elle exerce aussi un pouvoir de contrôle, de conseil, de sensibilisation et de sanction. Mais sa mission principale consiste à veiller au respect des libertés et droits fondamentaux des personnes physiques à l'égard des traitements des données à caractère personnel³.

Par ailleurs, *« les actions de la CNDP ne se limitent pas uniquement au territoire marocain, mais elle mène aussi des actions à l'échelon international. Parmi d'autres, la Commission a saisi le MEAC en vue de l'adhésion à la Convention 108 de la CE relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Elle a déposé une demande d'adéquation au près de la Commission européenne. Elle a été accréditée à la 33^{ème} conférence internationale de la protection des données à caractère personnel et de la vie privée, ce qui permet à notre pays d'être membre de la conférence internationale des autorités nationales de contrôles des données personnelles »*⁴ et d'être ainsi le premier pays arabe, africain et musulman à être accrédité auprès de la Conférence internationale des commissaires à la protection des données et de la vie privée.

Sans s'étaler sur l'organisation institutionnelle de la CNDP, nous envisagerons ici l'approche juridique du traitement des données à caractère personnel et le rôle primordial que joue la CNDP pour réguler ce traitement. Ainsi le Chapitre III de la loi 09-08 dresse la liste de certaines formalités préalable à la mise en œuvre des traitements, qui doivent être effectuées

¹V. art. 26 de la loi 09-08.

²Décision du Premier ministre n°3-33-11 du 23 rabii II 1432 (28 Mars 2011) approuvant le règlement intérieur de la Commission nationale de contrôle de la protection des données à caractère personnel.

³Bouchaib RMAIL, criminalité informatique ou liée aux nouvelles technologies de l'information et de la communication, Imprimerie Somagram, 2005, p. 313, cité dans Khalid ENNASHI, *Op. cit.*, p. 65.

⁴Khalid ENNASHI, *Op.cit.*, p. 65.

auprès de la Commission nationale de la protection des données à caractère personnel et qui, selon la nature du traitement en cause, consiste en une déclaration ou ne demande préalable.

La déclaration préalable est prévue par l'article 13 et suivant de la loi 09-08. En effet cette déclaration traduit l'engagement du responsable à ce que le traitement des données sera effectué conformément aux dispositions de ladite loi et sera déposé au près de la Commission nationale. En principe, la déclaration préalable doit contenir certaines informations obligatoires, à savoir : l'identification du responsable du traitement, les finalités, le destinataire, la durée de conservation des données, etc¹. Ces informations doivent être reprises dans les formulaires types mis à dispositions par la CNDP. Une fois la déclaration préalable présentée auprès de la Commission nationale et après contrôle du respect des règles applicables au traitement, la CNDP délivre un récépissé dans les 24 heures suivant le dépôt de la déclaration. Conformément aux dispositions de la loi 09-08, la délivrance du récépissé atteste de l'enregistrement, d'une part, du dépôt de cette déclaration et, d'autre part, de l'engagement du responsable de traitement à respecter les dispositions de la loi 09-08, ses textes d'application ainsi que les délibérations en vigueur. Le responsable peut mettre en œuvre le traitement dès réception du récépissé.

Toutefois, la CNDP peut décider de soumettre le traitement à la procédure d'autorisation préalable dès lors qu'il existe un risque d'atteinte aux libertés fondamentales, au respect de la vie privée et aux droits fondamentaux de la personne dont les données sont connectées². Cette décision doit être notifiée au responsable du traitement dans les huit jours suivant le dépôt de la déclaration. Grâce à cette déclaration préalable, la CNDP contrôle le respect des dispositions légales contenues dans la loi 09-08 par le responsable du traitement. La procédure d'autorisation préalable est également requise lors de la mise en œuvre de flux transfrontaliers vers des pays dont le niveau de protection de la vie privée et des libertés n'est pas reconnu suffisant par la Commission. Cette dernière a établi la liste des Etats répondant au critère de protection requis³.

Paragraphe 4 : La preuve de l'écrit électronique.

A côté de la loi pure et simple, le droit a laissé aux parties d'aménager leurs relations contractuelles, selon la règle qui veut que les conventions valablement formées tiennent lieu de

¹V. art. 15 de la loi 09-08.

²V. art. 12 de la loi 09-08.

³V. art. 43 de la loi 09-08.

lois à ceux qui les ont faites. Mais qu'en est-il de la preuve ? En effet, l'importance de la preuve est constante, *idem est no, esse et non probari*¹. Cependant, il y a une divergence d'opinions compte au principe de la preuve écrite dans le contrat électronique (I), due aux risques de manipulation et falsification de cette preuve (II). C'est pourquoi, l'utilisation de la *blockchain* s'est avéré un outil efficace au service de la preuve électronique (III).

I- Le principe de la preuve écrite dans le contrat numérique.

La preuve est la démonstration de l'existence d'un fait ou d'un acte dans les formes admises par la loi, elle constitue un moyen déterminant pour l'application du droit par lequel le juge pourra trancher un litige et pour le justiciable un moyen d'appuyer ses allégations. Ceci implique que tout acteur raisonnable doit aménager au préalable une preuve pour ses transactions importantes, celui qui n'est pas indulgent aura recours à des moyens de preuve incertaine. En somme, la constitution écrite de tout acte juridique demeure importante, sous l'angle de la preuve².

Néanmoins, tout le monde s'accordait à penser que notre système probatoire des actes juridiques se fondait sur le papier. Pourtant, s'il est vrai que l'écrit papier était en situation de monopole, il est également bon de rappeler que cette prédominance n'était que de fait et non de droit ; vu que rien dans le droit marocain n'imposait que tous les écrits soient établis sous la forme d'un document papier, signé à la main. L'écrit était souvent confondu avec le support papier sur le quel il est apposé.

Au Maroc, comme ailleurs, la réforme était de mise. La loi 53-05 comporte une innovation fondamentale et de bon sens, c'est notamment l'ouverture du code des obligations et des contrats aux nouvelles formes et supports électroniques. Le législateur a décidé d'intégrer les données sans les subordonner à la primauté de l'écrit dans son sens traditionnel. De ce fait et suite à l'évolution de notre système juridique la définition de la preuve par écrit est devenue extensive, ce qui valide toutes les formes d'écrits, y compris et non exclusivement ceux sous forme électronique. La loi a mis fin donc à cette confusion, la preuve littérale est redéfinie afin de la rendre indépendante de son support, et elle ne s'identifie plus au papier et elle ne dépend ni de son support matériel ni de ses modalités de transmission. L'admissibilité d'un écrit sous forme électronique au même titre que l'écrit sur papier est soumise à deux

¹N'avoir pas de droit ou ne pas pouvoir le prouver sont choses équivalentes.

²Christiane FERAL-SCHUHL, *Op.cit.*, p. 1128.

conditions que puisse être identifié celui dont il émane et que les conditions dans lesquels il est établi et conservé en garantissant l'intégrité. Ce sont deux exigences capitales afin que les deux sortes de l'écrit en soient des versions également admissibles par le droit probatoire¹.

A présent, nul doute que la preuve ne s'identifie plus au papier, ne dépend ni de son support matériel, ni de ses modalités de transmission². Ainsi, l'article 417 du D.O.C dispose que la preuve littérale résulte d'un acte authentique ou d'une écriture sous-seing privé. Le texte ajoute qu'elle peut également résulter « de toute autres signes ou symboles dotés d'une signification intelligible quels que soient leur support et leurs modalités de transmission ». Dans ce contexte, la redéfinition de la preuve littérale n'est pas le seul apport de la loi 53-05, mais elle a également consacré, par le biais de son article 4³, la force probante de la preuve écrite électronique. Par conséquent cette loi, attribue à l'écrit sur support électronique la même force probante que l'écrit sur papier c'est ce qui découle de l'article 417-1 du D.O.C complété par la loi 53-05. Autrement dit, il est possible dans certains cas de prouver les transactions juridiques sans produire un écrit⁴. Il s'agit, en effet, d'une équivalence fonctionnelle entre l'écrit sous forme électronique et l'écrit sur papier⁵.

Par ailleurs, l'article 440 du D.O.C a complété ce dispositif de preuve en accordant la même force probante à la copie fiable qu'à l'original à condition toutefois que l'écrit électronique ait été conservé sous la forme dans laquelle il a été créé, envoyé ou reçu, de manière à être accessible pour être consulté à tout moment par toute personne intéressée, et que le procédé de conservation soit fiable. Ainsi, peu importe que l'original subsiste ou pas, dès lors que sa copie est fiable.

Il faut noter que l'admission de la valeur probante du document électronique est passée nécessairement par la reconnaissance de la validité juridique de la signature électronique, élément indispensable dans toutes les opérations effectuées par voie électronique. En effet, selon l'article 7 de la loi 43-20, l'effet juridique et la recevabilité d'une signature électronique qu'elle soit simple ou avancée comme preuve en justice ne peuvent être refusés

¹S. IZDI, « La preuve du contrat électronique en droit marocain », in *Revue Marocaine du droit commercial et des affaires*, N° 4-5, 2018, p.101.

²Ali El AZZOUZI, *La cybercriminalité au Maroc*, Bishops Solutions, 2010, Casablanca, p. 120.

³L'article 4 de la loi 54-05 dispose que « l'écrit sur support électronique a la même force probante que l'écrit établi sur support papier ».

⁴Ch. PISANI, « L'acte dématérialisé », in *Arch. Phil. Droit*, N° 43, 1999, p. 156.

⁵Khalid ENNASHI, *Op.cit.*, p. 71.

au seul motif que cette signature se présente sous une forme électronique ou qu'elle ne satisfait pas aux exigences de la signature qualifiée¹.

Il est courant que le fait d'apposer sa signature sur un acte implique d'assurer les obligations qui en découlent, pareille en matière électronique, c'est cette marque qui donne à l'écrit la qualité d'acte sous seing privé électronique, et sans laquelle ne peut être considéré qu'un commencement de preuve par écrit². La question s'est posée de savoir si un email constituait un écrit électronique pouvant servir de preuve. La réponse de la Cour de cassation marocaine a indiqué qu'un email est accepté comme preuve dès lors qu'il répond aux conditions exigées par l'article 417-1 du D.O.C³.

En revanche, la tâche du juge sera plus difficile lorsqu'il est appelé à se prononcer sur la question des conflits de preuve entre deux actes sous signature privées, l'un sur support papier, l'autre conservé sur support électronique. La difficulté provient du fait de l'absence, dans le droit marocain d'une stipulation organisant les conflits de preuve littérale. On peut prendre l'exemple des personnes de mauvaise foi qui pourraient archiver d'avance des écrits manuscrits contraires à leurs engagements électroniques, ou négocier des avenants électroniques à des contrats écrits dont elles savent par avance qu'elles ne les respecteront pas. Dans ce cas, il est intéressant de se demander quelle preuve littérale le juge pourrait-il prévaloir et quelle mode de preuve recevrait la qualification de force probante. Certainement, il faudra se remettre à la seule sagesse du juge pour limiter les risques de divorce entre les deux modes de preuve, et lui laisser le soin de trancher les conflits de preuve en fonction des circonstances de l'espèce. C'est ce que précise l'article 417 du D.O.C dans son 3^{ème} alinéa : « lorsque la loi n'a pas fixé d'autres règles et, à défaut de convention valable entre les parties, la juridiction statue sur les conflits de preuve littérale par tous moyens, quel que soit le support utilisé ». Ce renvoi au magistrat, auquel il appartiendra seul de trancher en fonction du cas d'espèce devrait rendre sa tâche encore plus difficile⁴. Sous ces réserves et à ces conditions, la signature électronique devient l'élément fondamental de l'écrit électronique. En apportant la preuve du contrat électronique, elle le sécurise.

¹Voir infra p. 123.

²S. IZDI, *Op.cit.*, p. 103.

³محمد اهتوت، شكلية الإثبات في العقود الإلكترونية، مجلة القانون التجاري، ع. 5 و 6، 2019، ص. 14.

⁴A. SLASSI MOUTABIR, « Le juge face à la preuve électronique », in *Revue du droit marocain*, N° 23, 2012, pp. 14-15.

II- La manipulation et la falsification de la preuve électronique.

La manipulation et la falsification sont deux techniques utilisées afin de contourner les règles de preuve. D'une part, la manipulation informatique des preuves électroniques consiste à prendre une preuve, ou ensemble de preuves, et à l'essor de toute substance significative dans le but d'affermir la preuve, ou d'en détériorer la force probante. Cette manipulation des éléments de preuve a nécessairement des incidences juridiques. Il s'agit d'inverser par tout moyen légalement admissible la charge de la preuve. Ainsi, par de telles manœuvres, on essaye de réduire la valeur probante des écrits adverses, afin de mettre en doute la conviction du juge, on encore de retarder les délais d'exécution des procédures judiciaires.

Pour illustrer mieux ces propos, prenons l'exemple de deux personnes Sami et Kamal. Sami qui a une créance sur Kamal, lui adresse un courrier électronique comportant une pièce jointe au format PDF, le mettant en demeure pour le paiement de la créance due. Sauf que pour envoyer ce mail, Sami a utilisé un ordinateur autre que celui par lequel il avait l'habitude de contracter Kamal. Kamal confirme à Sami la bonne réception du courrier et de sa lecture, mais fait savoir qu'il n'y donnera pas suite car il doute de l'identité réelle de son auteur. Furieux, et sans autre demande d'information devant un acte de telle mauvaise foi, Sami assigne Kamal en justice et produit l'e-mail envoyé ainsi que la réponse de mauvaise foi qui lui est parvenue.

La justice demande, alors, à Kamal de produire les éléments qui lui permettent de contester l'authenticité du courrier. Celui-ci démontre qu'en ouvrant le fichier PDF avec un logiciel spécialisé, il s'est aperçu que le nom de l'auteur du fichier était tout autre que celui de Sami parce que comme cité avant ce-dernier a utilisé l'ordinateur d'un collègue de travail. Karim ajoute qu'il avait un doute quant à la nature du courrier électronique, en ayant constaté un changement dans l'adresse internet IP de Sami¹, et qu'il est de notoriété publique que la messagerie internet n'est pas sécurisée, qu'il se prête avec facilité à des fraudes, et qu'en conséquence le motif de son refus était parfaitement légitime.

Devant c'est argumentations, le juge s'il manque de compétences techniques en la matière, il commandera une expertise judiciaire afin d'avoir quelques lumières sur la

¹Il faut préciser que les adresses IP ainsi que beaucoup d'autres informations sont véhiculées dans les courriers électroniques en plus des informations traditionnelles créées par leurs expéditeurs. Elles permettent d'assurer la traçabilité du courrier mais fournissent aussi des pistes permettant de vérifier, en partie, l'authenticité d'un courrier.

question. Dans ce cas, il y aura allongement du délai de procédure. En effet, le juge pourrait croire que Karim avait effectivement des raisons valables de douter de l'authenticité du courrier électronique d'autant plus que, dans d'autres cas, notamment ceux proches de la cybercriminalité, ces éléments pourraient être parfaitement justifiés.

Le jugement dans ce cas pratique peut basculer en faveur de Karim : même astreint par le juge à l'exécution de la mise en demeure, le délai d'exécution de celui-ci pourrait se faire à compter de la date du jugement et non de la date de réception par courrier électronique et sans qu'il ait des dommages moratoires, contrairement à ce que prévoit l'article 263 du D.O.C : « les dommages-intérêts sont dus soit à raison de l'inexécution de l'obligation, soit à raison du retard dans l'exécution, et encore qu'il n' y ait aucune mauvaise foi de la part du débiteur ». Ainsi, on vient de le constater, en manipulant la preuve avec exagération, afin d'appuyer une position de mauvaise foi, on peut contourner certaines règles de droit en toute légalité. Le principe de la preuve écrite électronique, ayant la même force probante que la preuve papier, se trouve sérieusement mis à mal : on peut trop facilement diffamer l'écrit électronique en tant que preuve¹.

D'autre part, le fait de falsifier constitue une infraction, étant donné qu'il s'agit d'un fait qui peut porter préjudice à l'acte, soit produire des effets de droit inexistant. De ce fait, la production d'un faux trouble le régime de la preuve². Cependant, si la falsification d'un écrit papier est une opération difficile à réaliser, dans l'univers numérique³, la pratique de la falsification de la preuve reste facile à réaliser en raison de l'existence de facteurs qui rendent faciles la production de faux ayant l'apparence manifeste de vrai. En effet, la falsification des fichiers informatiques reste un jeu d'enfant pour des informations avisés, parce que, contrairement au papier, la modification d'un écrit électronique n'entraîne pas modification apparente des autres données contenues dans ce fichier.

¹A. SLASSI MOUTABIR, *Op.cit.*, pp. 14-21.

²Jérôme AUBERT, *L'essentiel de l'introduction au droit*, ellipses, Paris, 2010, p. 126.

³A titre d'exemple, si l'on inscrit une ligne entre deux paragraphes sur un acte papier, l'ajout apparaîtra manifeste car l'esthétique et la présentation du document s'en trouvent altérées. Le papier lui-même subit la trace matérielle de l'écrit. Si l'on reproduit la preuve papier pour masquer cet ajout, on risque de perdre toutes les informations originales et il faut tenter de les reproduire au mieux ex : cacher de la société. En revanche, ajouter une ligne entre deux blocs de données en informatique, n'entraîne pas modification des autres données et le fichier va s'adapter en taille et en apparence. Si le fichier contenait des images celles-ci seront conservées sans nulle détérioration.

De ce fait, des personnes malfaiteurs peuvent altérer un procès soit en modifiant un écrit électronique existant, soit en créant de fausses preuves. Lorsqu'il s'agit de modifier l'acte électronique, la falsification de la preuve consiste à altérer le contenu en supprimant des informations ou en ajoutant de nouvelles. Lorsqu'il s'agit de créer une fausse preuve, la falsification consiste à produire une preuve inexistante sans partir d'un écrit original. Le problème avec l'écrit électronique c'est que la falsification d'une preuve ne laisse pas de trace matérielle apparente au sens propre du terme. La constatation de ces fraudes nécessite le recours à des techniques d'investigation très coûteuses qu'elles ne sont réalisées que pour des cas rares.

Face à ce constat, le juge se trouve confronté à des problèmes non négligeables. Il en résulte que le travail du magistrat reste très compliqué face à la présence de cet ensemble de techniques d'usurpation, de manipulation et de falsification de la preuve électronique.

III- Enjeux de la *blockchain* aux regards des règles relatives à la preuve électronique.

La *blockchain* est un registre sur lequel sont inscrit des transactions. Ces dernières sont regroupées à l'intérieur de blocs et chaque bloc contient des informations relatives au bloc précédent, de telle sorte qu'il est impossible de modifier une information sans modifier toute la chaîne de bloc. Ainsi, parmi les règles susceptibles d'être directement concernées par la *blockchain* figurent en bonne place les règles de preuve. Mais en l'absence d'une réglementation propre à la preuve par *blockchain*, subsiste un espace de liberté pour les parties, celui des conventions sur la preuve. Nous pouvons imaginer les parties à un contrat prévoir de pré-constituer une preuve de l'acte par *blockchain*. Les conventions sur la preuve relèvent de l'idée que le contrat peut venir compléter la règle de droit quand celle-ci ne dit pas tout¹. Une convention de preuve par *blockchain* sera efficace uniquement si les parties ont la libre disposition de leurs droits, ce qui suppose une étude au cas par cas concernant la charge de la preuve et le fait à prouver.

L'utilisation de la *blockchain* comme preuve d'un acte sous seing privé semble actuellement impossible pour plusieurs raisons. D'abord, les utilisateurs d'une *blockchain* étant sous pseudonymes, ils ne sont a priori pas identifiables. Or, il convient de pouvoir

¹V. MAGNIER, « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », in IP/IT, N° 2, Février 2019, Dalloz, p. 80.

identifier les personnes contractantes afin de bénéficier des régimes juridiques précités. Cette difficulté pourrait être neutralisée si les utilisateurs s'identifient dans les cas où ils souhaitent se prévaloir des contenus sauvegardés sur une *blockchain*.¹. En outre, la *blockchain* n'est pas sous le control exclusif du signataire, étant donné la présence des mineurs.

Plus largement, les écrits électroniques au sens du code civil doivent être établis et /ou certifiés par un tiers de confiance. Or, dans une *blockchain*, il n'y a pas de tiers de confiance. En effet, la *blockchain* se veut par principe un système de confiance décentralisé, et donc sans tiers de confiance. Elle est donc antinomique de la preuve électronique visée par le code civil, qu'il s'agisse d'une *blockchain* publique ou *blockchain* privée. Ainsi la *blockchain* ne peut pas actuellement constituer un écrit selon le D.O.C, pour prouver un acte juridique.

Cependant, son rôle de commencement de preuve est indéniable. En effet, selon l'article 334 du Code de commerce : « en matière commerciale la preuve est libre. Toutefois, elle doit être rapportée par écrit quand la loi ou la convention l'exigent ». La loi, donc, ne l'interdisant pas, la *blockchain* peut être utilisée dans ce cadre. Elle peut donc à nouveau, en application de ce texte être utilisée pour prouver un acte en matière commerciale, sous réserve qu'aucune exigence d'écrit ne soit ailleurs posée. La question est alors de savoir comment un juge va apprécier la valeur probante d'informations contenues dans une *blockchain*, notamment si la partie à qui le contenu de la *blockchain* est opposé, en conteste la fiabilité. Le juge pourrait alors recourir à un expert informatique pour vérifier l'absence d'altérité des contenus et confirmer l'identité de son auteur.

Sous-section 3 : L'exécution du contrat numérique : les *smart contracts*.

« Imaginez un monde dans lequel l'exécution forcée n'est plus une cause d'action parce que les contrats eux-mêmes exécutent automatiquement l'accord des parties » ²c'est ainsi que ce résume l'usage de ces technologies numériques appelées les *smart-contract*. En effet, lorsqu'on évoque la transformation des pratiques à l'ère du numérique et l'influence des technologies sur le droit, l'anglicisme *smart contract* est immédiatement cité. Peu connu des juristes, le *smart contract* n'est pourtant pas une nouveauté. La notion existe depuis une

¹I. GAVANON, « Blockchain et PI et mode : enjeux de la blockchain au regard des règles relatives à la preuve électronique », in IP/IT, N° 2, Février 2019, Dalloz, p. 93.

²A. HINKES, « Blockchains, smart contracts and the death of specific performance », consulté le 09-03-2022 à 10h sur <https://www.otcpm24.com/2019/05/22/blockchains-smart-contracts-and-the-death-of-specific-performance-inside-counsel/>

vingtaine d'années, même si c'est surtout aux Etats-Unis, chez les informaticiens, qu'elle a surtout été employée. Sa rencontre avec le monde du droit est relativement récente.

Si le champ d'application de la *blockchain* et les *smart contracts* est aussi large que l'on peut l'entendre, il est nécessaire de bien comprendre leur nature technique pour pouvoir traiter les nombreuses questions juridiques qui s'ouvrent inéluctablement¹. Ainsi le *smart contract* compris comme une technologie (Paragraphe 1), suscite une certaine perplexité quant à son régime juridique (Paragraphe 2).

Paragraphe 1 : La technologie de *smart contract*.

Face au flou des notions et aux raccourcis parfois trop rapidement faits, une première série de questions se posent d'emblée, s'agissant d'une technologie qui n'en est pour l'instant qu'au stade du développement : qu'est ce qu'un *smart contract* ? Et à quoi sert-il ? Ces considérations amènent donc, à porter sur les *smart contracts* un regard exploratoire (I) afin de découvrir la révolution contractuelle qu'il a conduit (II).

I- Regard exploratoire sur les *smart contracts*.

Le *smart-contract* est un programme informatique dont la fonction consiste à former, exécuter ou éteindre automatiquement un contrat qui, en toute hypothèse, ne se confond pas avec lui. Ce programme algorithmique se distingue par le fait qu'il fonctionne dans le cadre d'une *blockchain*. Il fait noter que le *smart contract* n'a rien, selon la traduction littérale, d'un contrat intelligent. Ce n'est pas un contrat mais un programme informatique car le programme ne fait que ce que le programmeur a prévu qu'il fasse, en attendant peut-être que l'intelligence artificielle change la donne. Il est une technologie dont la qualification juridique lui est étrangère. Pour l'instant, il s'agit d'un simple algorithme de gestion des opérations contractuelles, il reste la plupart du temps un *smart contract* de traduction.

En somme, le *smart contract* est un programme informatique fonctionnant dans la *blockchain* permettant d'exécuter automatiquement les termes d'un contrat, opérant sous le mode de la condition (si.../donc..). Il également question de contrats qui s'auto-exécutent². Ceci implique qu'il y ait déjà un contrat conclu auparavant ; il devrait être encadré pas une

¹J. GOSSA, « Les Blockchains et Smart contracts pour les juristes », in IP/IT, N° 7-8, Juillet-Aout 2018, Dalloz, p. 393.

²G.M. HYMA et M.P. DIGESTI, « New Nevada Legislation Recognizes Blockchain and Smart contracts Technologies », Nevada Lawyer, Nevada, August 2017, p. 17.

convention qui en fixerait les modalités de fonctionnement et prévoirait les conséquences juridiques de son utilisation.

En effet, le *smart contract*, programme qui s'auto-exécute sans intervention d'un tiers n'est pas nouveau. Il se rapporte à un courant des années 1950 dit mécaniciste. Le *smart contract* a donc précédé la blockchain. La consommation de produits par l'utilisation d'un distributeur automatique est un *smart contract*, le programme s'auto-exécutant sans l'intervention d'un tiers. La nouveauté est l'association de ce processus automatique à la technologie des *blockchains*¹ par Nick Szarbo dans les années 1990. Informaticien, juriste et cryptographe, Nick souhaitait mettre en place un protocole permettant à des étrangers, entre lesquels il n'existe à priori aucun lien de confiance² et ne se connaissent pas, d'effectuer des transactions en toute sécurité.

Juridiquement, ce sont des chercheurs américains qui ont entrepris de traduire des normes juridiques dans un langage informatique, de les coder pour en assurer l'exécution par le biais d'un ordinateur. C'est dire que le projet est ancien tout au moins dans sa conceptualisation. Ce qui est récent, bien évidemment, c'est sa concrétisation, rendue possible par l'ère numérique. Ainsi sont nés, progressivement les *smart contracts*, ces algorithmes de gestion des opérations contractuelles.

A vrai dire, pour appréhender au mieux les virtualités des *smart contracts*. Il convient de partir de ses différents cas d'usage. Pensons, au contrat de location saisonnière. Dès lors que le locataire a viré le montant du loyer, le *smart contract* détecte le paiement et déverrouille automatiquement la porte d'entrée du logement. Dans ce cas, le *smart contract* fonctionne avec une serrure connectée, qui s'ouvre que lorsque le locataire a payé. Cet exemple vaut autant pour le contrat de location automobile. Si le locataire manque une mensualité, un message s'active dans le véhicule. Le chauffeur a alors 48 heures pour réguler le loyer, à défaut de quoi le *smart contract* immobilise le véhicule géolocalisé. Ces illustrations montrent la diversité des fonctions assignées au *smart contract*, qui permet notamment d'exécuter des obligations ou de sanctionner un débiteur défaillant.

¹Le rattachement du smart contract à la blockchain se fait par l'émission d'une adresse formulée en hexadécimal. Cette adresse est celle où les transactions seront envoyées pour déclencher un smart contract.

²Laurent LELOUP, *Blockchain : La révolution de la confiance*, Eyrolles, Paris, 2017, p. 31.

II- La révolution contractuelle des *smart contracts*.

En effet, de nombreux débats sont nés autour des *smart contracts* qui constituent une révolution contractuelle¹. D'une part, le smart contrat est considéré comme un processus plus sécurisé ; sans aucun doute, l'utilisation de la technologie des *blockchains* en général et du *smart contract* en particulier permet de renforcer la sécurité de l'exécution du contrat. On connaît les risques liés à l'intervention de nombreux acteurs et à l'échange de nombreux documents lors de l'exécution de certains contrats. Les documents peuvent être égarés, expédiés aux mauvaises personnes, falsifiés, incomplets. De plus, une réduction des erreurs, des délais et des coûts font du *smart contract* un moyen de renforcer l'efficacité économique du processus contractuel. D'autre part, comme cité tout à l'heure, les smart contrats sont un processus totalement désintermédié. En effet, il est souvent dit du *smart contract* qu'il entraîne une désintermédiation et permet de penser un monde sans tiers de confiance. C'est le cas des professionnels du droit tels que le notaire, l'avocat et le juriste d'entreprise. L'esprit qui règne autour de cette technologie est que l'algorithme renforce le contrat là où l'intervention humaine l'affaiblit².

La question qui se pose est de savoir si on peut aller plus loin et défendre également la disparition du juge étatique. La saisine du juge pourrait causer des lenteurs et puisque le *smart contract* suppose d'aller vite sans retarder l'exécution du contrat, nous pouvons supposer de prévoir de court-circuiter le premier *smart contract* par un autre *smart contract* en cas de contestation. Le différend pourrait alors être soumis, toujours en conformité avec cette technologie qui veut accélérer le temps et réduire l'intervention de tiers, à un processus de médiation numérique ou à un arbitrage numérique qui permettrait de résoudre dans des délais très courts le différend né de la mise en œuvre d'un *smart contract*. Ce processus ne devrait pas empêcher celui qui n'est pas satisfait de saisir un juge, même si probablement dans ce cas ses chances de succès seront réduites s'il est établi que le *smart contract* a été mis en œuvre de manière légitime. Néanmoins, la fin du tiers de confiance et le phénomène de désintermédiation totale demeurent à vrai dire une vue de l'esprit. Le *smart contract* ne remplacera pas l'intervention d'un tiers.

¹C. BARREAU, « La régulation des smart contracts et les smart contracts des régulateurs », in Annales des Mines- Réalités industrielles, N° 3, Aout 2017, p. 27.

²M. MEKKI, « Le contrat, objet des smart contracts (Partie 1) » in IP/IT, N °7-8, Juillet- Aout 2018, Dalloz, pp. 415-416.

Paragraphe 2 : La valeur juridique des *smart contracts*.

Plusieurs obstacles semblent rendre difficile l'utilisation des *smart contracts* en raison du vide juridique en la matière. En attendant, il faut traiter les *smart contracts* avec les outils juridiques consacrés. Or, dans la plupart des systèmes juridiques, il n'existe pas de consécration légale. La détermination de leurs effets est donc délicate et incertaine¹. En dépit que les *smart contracts* jouent un rôle dans l'optimisation de la phase d'exécution du contrat numérique (I) cependant, les difficultés liées à sa réglementation semblent freiner ce rôle (II).

I- Les *smart contracts* : une optimisation de la phase d'exécution du contrat.

La technologie des *smart contracts* appliquée aux contrats permet à la fois de renforcer leur exécution mais également leur sanction. D'abord, le *smart contract* permet de renforcer l'exécution du contrat ceci en automatisant le transfert de fonds. En effet, la force du *smart contract* réside dans son automaticité en dehors de toute intervention humaine. Par le protocole informatique des *smart contracts*, les parties peuvent automatiser un transfert de fonds après que des documents aient été remis, des faits établis ou des actes accomplis, l'ensemble étant authentifié au moyen de la technologie *blockchain*. L'exemple classique est le *smart contract* automatisant la remise d'une indemnité d'assurance lorsque le retard est établi ou l'état de catastrophe naturelle reconnu. Si cette situation de fait est établie, alors la somme est automatiquement versée au moyen par exemple de *bitcoin*, à l'assuré, sans demande ni intermédiaire². Pensons aussi au droit des sociétés. Les pactes d'actionnaires, pour la mise en œuvre d'un droit de préemption ou de préférence, peuvent utiliser la technologie des *smart contracts*. L'organisation d'une société dans sa globalité peut s'appuyer sur une série de *smart contracts* pour le versement par exemple des dividendes. On peut même dans ce dernier cas envisager une sorte de société entièrement algorithmée par un réseau de *smart contract*.

Par ailleurs, et indépendamment de toute idée de sanction, le *smart contract* peut servir à fixer les limites temporelles d'un contrat en déterminant son débit d'exécution et la

¹E. MARIQUE, « Les smart contracts en Belgique : une destruction utopique du besoin de confiance », in IP/IT, N° 1, Janvier 2019, Dalloz, p. 22.

²Le groupe Axa utilise déjà la technologie des smart contracts d'Ethereum pour la gestion de l'assurance retard d'avion. Le contrat d'assurance est connecté aux bases de données du trafic aérien mondial et dès qu'un retard d'avion de plus de deux heures est enregistré, le contrat s'exécute automatiquement sans aucune formalité et sans intervention humaine.

fin de son exécution. On pense surtout à la location ou le prêt d'un appartement, ne passerait plus par une plateforme numérique, qui jouerait le rôle d'intermédiaire, mais fonctionnerait au moyen d'un *smart contract*. La confirmation du versement des fonds permettrait, au moyen d'un *smartphone* par exemple, de débloquent une serrure ou en cas de non paiement ou à l'issue du contrat de bloquer la serrure¹. Enfin, le *smart contract* renforce certaines sanctions en droit des contrats. Dans toutes ces hypothèses, le *smart contract* ne s'est pas substitué au contrat mais il s'est superposé à lui pour en optimiser l'exécution.

II- Les difficultés liées à la réglementation des *smart contracts*.

Le *smart contract* est une technologie naissante qui laisse pour l'heure ouverte la question de son encadrement juridique. Les premières observatrices ont déjà noté certaines difficultés, qui tiennent notamment au caractère transfrontalier du cyberspace. Les spécialités du droit international privé ne manqueront pas d'être sollicitées pour réguler les conflits de lois et de juridictions soulevés par les *smart contracts*. Dans le cadre de ce propos limité, nous voudrions simplement confronter l'usage de ces algorithmes au droit commun des contrats. Si l'on veut bien admettre l'hypothèse qu'une difficulté d'application d'un *smart contract* sera demain soumise à un juge marocain. Il faut en effet, prendre la mesure des problématiques futures. De ce fait, plusieurs obstacles juridiques semblent rendre difficile l'utilisation des *smart contracts*, tel qu'ils viennent d'être présentés. L'automaticité qu'ils impliquent s'adapte mal avec plusieurs pans du droit marocain.

Si l'on prend l'exemple du preneur ou de l'utilisateur qui serait privé de l'usage d'un bien qu'il loue parce qu'il connaît un retard de paiement. Ce type de sanction apparaît très brutal dans un contexte où le droit se montre protecteur à l'égard des débiteurs. En amont, le droit du surendettement des particuliers pourrait sans doute être mobilisé. Un mécanisme qui ne laisse pas la possibilité au consommateur de plaider sa cause ou de demander un étalement des échéances semble difficilement compatible avec la philosophie du droit de la consommation ou du surendettement. On pourrait même se demander si, en lui-même, le mécanisme de *smart contract* prévu dans le contrat de consommation ne heurterait pas l'ordre public et s'il ne pourrait pas être analysé comme une modalité abusive.

¹G. GUERLIN, « Considérations sur les smart contracts », in IP/IT, N°10, Octobre 2017, Dalloz, p. 515.

Dans un même ordre d'idées, les *smart contracts* semblent, mal se combiner avec le droit des procédures collectives. Il suffit d'imaginer une entreprise au bord de la cessation des paiements. Si le *smart contract* déclenche des pénalités pour chaque retard de paiement, ou empêche l'utilisation du bien loué, celui-ci peut se muer en facteur d'accélération des difficultés. Surtout, on se demande comment concilier les règles de paralysie des créanciers, avec l'automatisme d'une technologie *smart contract*. S'agissant là encore d'un droit d'ordre public, celui-ci devrait primer sur la logique individuelle de sécurisation des paiements¹.

Au Maroc, en l'absence de toute définition des *smart contracts*, il semble difficile d'envisager les perspectives contractuelles qu'ils recouvrent. Pour pallier à cette difficulté, il convient dans un premier lieu de se demander si, tout simplement, le *smart contract* pourrait être qualifié de contrat au sens du droit marocain. Le droit marocain dénombre quatre conditions de validité du contrat à savoir : la capacité, le consentement, l'objet et la cause. Si l'on s'attarde à l'adaptation de ces conditions au contexte spécial du smart contrat, on constate sans difficulté qu'il n'est pas besoin d'effectuer de grands changements. Dès lors, il serait possible de considérer le smart contrat comme un contrat. Le contrat électronique à titre d'exemple, se distingue du contrat normal en matière de support et d'expression des consentements qui sont tous deux manifestés dans l'univers digital. Sur ces points, les *smart contracts* ne diffèrent guère puisque le support est un réseau et les consentements, sur lesquels un point précis sera consacré, peuvent être exprimé par un « clic » ou par la transmission à l'autre partie de sa clé publique. En deuxième lieu, l'intégration des *smart contracts* dans notre ordre juridique soulève plusieurs interrogations. Les principes de la *blockchain* et les principes de notre droit contractuel semblent s'opposer².

Le *smart contract* permet d'éteindre automatiquement le contrat lorsqu'une condition n'est pas respectée par l'une des parties. Ainsi lorsqu'un locataire voit sa serrure verrouillée en raison d'un retard de paiement de loyer, le *smart contract* met alors en œuvre une exception d'inexécution. Or, l'article 235 du D.O.C prévoit expressément ce qui suit : « l'une des parties refuse d'accomplir son obligation jusqu'à l'accomplissement de l'obligation corrélatrice de l'autre partie, à moins que, d'après la convention ou l'usage, l'un des contractants ne soit tenu d'exécuter le premier sa part de l'obligation ». La mise en application de l'exception d'inexécution n'obéit à aucune condition spécifique. Il n'est pas

¹J-Ch. RODA, « Smart contracts, Dumb Contracts », in IP/IT, N° 7-8, Juillet-Aout 2018, Dalloz, p. 401.

²Sh. EL KASSIMY, « Les smart contracts : la révolution de la confiance », in Revue de Droit Commercial, N° 7, 2020-2021, p. 27.

nécessaire de demander l'autorisation du juge, ni d'adresser à son contractant une mise en demeure. On peut également envisager le problème sous l'angle de la résolution unilatérale prévue par l'article 120 du D.O.C qui dispose que « ... le créancier a le choix, ou de recevoir la chose en l'état ou elle se trouve, ou de résoudre le contrat, sauf son droit aux dommages-intérêts ». Résoudre un contrat avant l'exécution du terme n'apparaît pas envisageable.

Ces mises en situation suffisent pour observer les difficultés liées à l'utilisation des *smart contracts*. Cependant, confronté à l'avènement des *smart contract*, le juriste doit adopter une attitude tenant compte de ces différentes tendances. D'un côté, l'attrait de la nouveauté ne doit pas aveugler et il faut se garder de vouloir absolument adopter des règles. De l'autre, il est essentiel de ne pas se réveiller après la bataille. L'expérience du *Bitcoin* et d'autres monnaies virtuelles rappelle combien il est important de savoir anticiper l'apparition d'un phénomène au risque sinon, d'éprouver les pires difficultés pour réguler celui-ci.

Pour reprendre la formule du doyen Jean Carbonnier lorsqu'il qualifiait l'inflation législative, le *smart contract* est un mal nécessaire. S'en détourner serait irréaliste, mais s'y soumettre serait une erreur. Le *smart contract* doit être appréhendé par le juriste de telle sorte qu'il permette de construire un contrat augmenté et pas seulement machinisé¹. Comme tout phénomène où règne une forte incertitude, nous devons être sur nos gardes. La démarche du juriste à l'égard de ces technologies qui promettent de réduire les couts, d'accélérer le temps et de surmonter les faiblesses de l'homme au plus grand profit des créanciers, est de chercher les moyens de profiter pleinement de ses vertus sans souffrir de ses vices. A l'instar des questions de santé publique ou d'environnement ou l'incertitude scientifique règne en maître. Il faut promouvoir un développement durable des *smart contracts*.

Section 2 : Les contrats relatifs à l'Internet.

Nous avons songé, dans les développements qui suivent, aux contrats relatifs à l'internet entre entreprises, l'une fournisseuse l'autre cliente, qui présente le plus intérêt et la plus grande spécificité. Cependant, les contrats les plus nombreux sont conclus par des particuliers ; les règles protectrices des consommateurs s'appliquent donc à tous les égards. La présente étude se bornera aux contrats de droit privé. L'internet est depuis ses origines un territoire propice à l'accord de volontés entre les parties. Au fil des années, s'est développée une très grande variété de contrats.

¹Gilles BABINET, Big data, penser l'homme et le monde autrement, Le passeur, Paris, 2015, p. 6.

Les contrats de l'internet ont la particularité d'être évolutifs et très divers. Ils sont également fortement impactés par le caractère fondamentalement international de l'internet. Nous nous contenterons d'étudier certains contrats parmi les plus emblématiques du droit de l'internet, à savoir les contrats du site internet (Sous-section 1), le contrat de publicité sur internet (sous-section 2) et les contrats de commerce électronique (B/B et B/C) (sous-section 3).

Sous- section 1 : Le contrat du site Internet.

Le contrat relatif au site internet, quel qu'il soit est souvent dit clés en mains. En effet, le prestataire conçoit et réalise le site internet (Paragraphe 1), assure l'hébergement et le référencement (Paragraphe 2), tout en assurant la maintenance selon une périodicité prévue (Paragraphe 3).

Paragraphe 1 : Le contrat de conception et de réalisation de site Internet.

Le contrat de conception du site internet rentre dans la catégorie générale des contrats d'entreprise. Les parties doivent définir très précisément l'objet du contrat (I) ainsi que les étapes de création du site internet (II) pour que chaque partie connaisse les obligations qui lui incombent (III).

I- L'objet du contrat.

Les parties doivent définir très précisément l'objet du contrat afin d'éviter toute difficulté d'interprétation ultérieure. La définition de l'objet est en grande partie liée aux documents techniques et commerciaux à annexer au contrat. Tout d'abord, la proposition commerciale, autrement dit l'offre commerciale et technique du prestataire avant validation par le client. Ensuite le cahier des charges, il s'agit de l'expression par le client de ses besoins, en termes techniques et commerciaux.¹ Il peut décrire ; l'orientation générale du site, le public visé, le style de la ligne graphique (choix des couleurs...), les caractéristiques techniques du site, la description de l'arborescence du site et de sa mise en page.... Enfin le planning, celui-ci est exprimé le plus souvent sous forme d'un calendrier glissant, le planning présente les

¹Le caractère incomplet d'un cahier des charges est susceptible d'exonérer un prestataire de sa responsabilité dans l'inexécution de ses prestations. La Cour d'appel de Paris l'a rappelé dans une affaire Uzik C/ Moralotop en relevant que « que le cahier des charges dont l'objet est de définir avec une grande précision toutes les fonctionnalités attendues du produit, pour permettre, notamment, au prestataire de facturer son travail, laisse trop de zones d'ombres ». CA Paris, pole5, ch.11, 16 Mars 2012.

grandes étapes de la conception et de la réalisation du site, lesquelles conditionnent le paiement. Par ailleurs, le planning doit prévoir les grandes étapes de la conception et de la réalisation du site qui sont : la rédaction du cahier des charges, la réalisation de la maquette du site, la remise des pages-écrans, la recette provisoire du site¹.

Plusieurs méthodes sont en pratique mises en œuvre pour déterminer l'objet du contrat de conception ou de réalisation de site internet. La première méthode qui procure un maximum de sécurité c'est lorsque la rédaction du cahier des charges et du planning est préalablement à la signature du contrat. Le plus souvent, le cahier des charges et le planning sont rédigés préalablement à la signature du contrat auquel ils sont annexés. Cette formule présente une sécurité maximum pour les parties dans la mesure où elle limite toute incertitude sur l'objet de la prestation, son calendrier et le prix correspondant.

La deuxième méthode permet une sécurité moyenne. Consiste en la rédaction du cahier des charges et du planning postérieurement à la signature du contrat. Ce système présente l'avantage au prestataire de fracturer en toute hypothèse la rédaction du cahier des charges à son client. En revanche, il présente l'inconvénient pour les parties d'une indétermination relative de l'objet du contrat, le cahier des charges pouvant révéler des prestations supplémentaires, non envisagées dans le devis initial : un mécanisme contractuel d'ajustement du prix devra donc être prévu.

La troisième méthode qui est la moins sécurisée. C'est lorsqu'il y a absence de rédaction du cahier des charges et du planning ou insuffisance de ces documents. Cette formule, qui engendre un risque important de désaccord sur l'objet du contrat a posteriori, doit être évitée, sauf lorsque les prestations sont facturées sur la base du temps passé². Il faut noter qu'il est recommandé d'exclure du contrat de conception ou de réalisation de site des prestations qui, bien que connexes, sont d'une nature juridique différente, et en particulier les prestations d'hébergement du site, de maintenance technique et éditoriale du site, et de référencement du site. Ces prestations doivent faire l'objet de contrats séparés, à conclure soit avec le prestataire (qui assure lesdites prestations directement ou en sous-traitance), soit avec un ou plusieurs prestataires tiers.

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 141.

²Ibid., p. 142.

II- Les étapes de création du site Internet.

La création du site internet comprend généralement plusieurs étapes, prévues par le contrat, ou annexées dans un cahier des charges qui servira référentiel de conformité, leurs résultats doivent être validés par le client dans un procès-verbal, avant de passer à l'étape suivante. Ce contrat implique donc une participation active du donneur d'ordre¹. Comme dans tout contrat comportant des étapes pour la réalisation de son objet il est bienvenu de prévoir que le client désignera une personne déterminée chargée de s'occuper du suivi du projet.

Les étapes de création peuvent être comme suit ; d'abord, l'établissement après analyse du cahier des charges, établit un dossier de production contenant les aspects graphiques, de navigations, fonctionnelles et informationnelles. Ensuite, il y a réalisation du site avec notamment le développement informatique du système de gestion qui abritera le contenu du site, son architecture et son esthétique. Puis, il y a mise en ligne provisoire du site et la réalisation d'une série de test. Après les corrections effectuées à la suite des tests, il y a réception de la part du client. Dans ce cas, la procédure et les modalités de la réception donnent parfois lieu à des clauses détaillées dans le contrat. Enfin, la mise en ligne du site est définitive.

III- Les obligations du prestataire et du client.

D'une part, l'obligation de la réception des prestations. Celle-ci doit être organisée dans l'intérêt des deux parties. Celui du prestataire, d'abord, car elle lui permet de rapporter la preuve de l'achèvement de ses obligations. Celui du client, ensuite, afin qu'il puisse exprimer ses éventuelles réserves, et faire corriger les prestations dans le sens souhaité. La réception définitive du site peut comporter des réserves sur des points mineurs. Lorsqu'il existe un système complexe, l'obligation de délivrance n'est considérée comme satisfaite qu'à partir du moment où l'ensemble est opérationnel, autrement dit lorsque le site est en mesure de fonctionner pour remplir l'usage pour lequel il a été conçu ; c'est-à-dire pas au moment de sa mise à disposition et de sa réception mais ultérieurement. La délivrance matérielle se distingue de la délivrance opérationnelle. Chaque réception donne lieu à un procès verbal.

¹Philippe LE TOURNEAU, *Op.cit.*, p. 573.

Le client est évidemment libre de refuser de réceptionner un site non conforme¹ sans rime ni raison est une défaillance contractuelle déchargeant d'autant son partenaire².

D'autre part, il est dans l'intérêt du prestataire de décrire très précisément les diligences qui sont attendues du client pour la bonne fin des prestations. En général, le client s'engage à fournir au prestataire, dans le respect du calendrier, toutes données destinées à être intégrées au site pour lesquelles il doit détenir les droits de propriété intellectuelle correspondants. Il faut noter que l'obligation du créateur est de résultat quant à l'existence de la création elle-même. En revanche, l'obligation est seulement de moyens quant à la qualité du site, et donc à son efficacité³. Par ailleurs, il pèse également sur le client l'obligation de collaboration active et régulière avec le prestataire, l'obligeant à mettre à sa disposition tout document ou information nécessaire, ainsi qu'à le mettre en relation avec toute personne utile au sein de son propre personnel.

Lors du paiement, plusieurs formules sont envisageables. Il est ainsi possible de prévoir soit le paiement d'un prix global et forfaitaire, toute demande additionnelle donnant lieu à la facturation additionnelle (sur devis accepté ou au temps passé), soit le paiement au temps passé (système dit « en régie »). Dans la première hypothèse, des paiements fractionnés doivent intervenir à la signature du contrat, à la remise d'éléments significatifs (ou à l'échéance d'une étape significative de la réalisation, pouvant être constatée objectivement et simplement), ainsi qu'à la livraison de la version définitive du site. Dans la seconde hypothèse, il convient de prévoir un barème de prix exprimé en jours variant selon la qualification du personnel intervenir. Ce barème doit être joint en annexe du contrat⁴.

Enfin, il est indispensable pour le prestataire de disposer de la plus grande liberté pour sous-traiter tout ou partie des prestations. Néanmoins, il doit veiller à ce que les conditions qui lui sont imposées par ses sous-traitants ne soient pas plus rigoureuses que celles qu'il pratique à l'égard de son client (délais, propriété intellectuelle, garanties, etc.) et contractualiser impérativement sa relation avec ses sous-traitants pour définir clairement les responsabilités

¹La Cour d'appel de Douai, dans une décision du 11 Avril 2011, a précisé que : « la réception sans réserve ne couvre que les défauts apparents de conformité alors qu'ainsi que le tribunal 'a relevé, certaines prestations prévues au contrat entre M.X et la société Cometik ne pouvaient s'apprécier qu'à l'usage à plus long terme »

²Philippe LE TOURNEAU, *Op.cit.*, p. 572.

³C. Appel, ch. Com., décision n° 15/00172, 29 Mars 2016, Grenoble: résiliation du contrat aux torts du client qui avait refusé toute réception provisoire, alors qu'elle aurait été de nature à lui permettre de faire état de la non-conformité du site.

⁴Philippe LE TOURNEAU, *Op.cit.*, p. 572.

⁵Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 147.

de chacun. Il pourra également standardiser, dans la mesure du possible, son mode de collaboration avec ses prestataires externes.

Paragraphe 2 : Le contrat de maintenance du site Internet.

Le terme maintenance, issu de l'anglais, recouvre un grand nombre de prestations qui visent toutes à maintenir le système à son meilleur niveau de performance : entretien, dépannage, assistance, améliorations, soutien logistique, etc. Le contrat de maintenance dont la signature doit être envisagée concomitamment à celle du contrat de réalisation de site Internet est, à l'instar de ce dernier contrat, également un contrat d'entreprise. Il convient de traiter l'objet de ce contrat (I) avant de préciser les obligations des parties (II).

I- Définition et objet du contrat.

Il existe deux types de maintenance. D'une part, la maintenance technique qui consiste à entretenir le site sur le serveur ainsi que de réparer ses défaillances techniques. D'autre part, la maintenance éditoriale qui a pour objet de mettre à jour, faire évoluer ou corriger le contenu éditorial du site (texte, iconographie, etc.). Chaque type de maintenance correspond à des niveaux d'engagements variables avec des implications juridiques différentes. Le contrat doit donc être explicite quant au type de maintenance choisi par les parties.

Il est recommandé d'exclure du contrat les prestations qui, bien que connexes, ne seront pas fournies dans le cadre du contrat de maintenance, et notamment la conception et la réalisation du site, l'hébergement du site, le référencement du site, l'assistance aux utilisateurs, la formation du personnel du client. Par ailleurs, le client paie en général en redevance annuelle au prestataire. Le prestataire est libre de facturer selon ses propres modalités. Le plus souvent, la facturation se fait mensuellement, le règlement s'effectuant à la réception de la facture par le client. Enfin le contrat de maintenance est conclu généralement pour une durée d'un ou deux ans, tacitement reconductible pour une période d'égale durée. Les parties restent naturellement libres de prévoir une autre durée plus ou moins longue¹.

¹Ibid., p. 148.

II- Les obligations des parties : prestataires et clients.

Le prestataire est tenu d'un certain nombre d'engagement. Il doit en effet veiller sur la maintenance technique curative. Celle-ci a pour objet la correction des dysfonctionnements techniques affectant le site. L'obligation de disponibilité du maintenant et une obligation de résultat. C'est pourquoi, le contrat doit préciser les modalités d'intervention (déplacement éventuels, interventions en ligne, etc.), les délais d'intervention et la nature juridique de l'obligation souscrite (obligation de moyens ou de résultat). Aussi il est tenu d'une maintenance technique évolutive qui a pour objet la réalisation de prestations techniques garantissant que le site demeure performant, en dépit des évolutions technologiques. Dans ce cadre, le contrat peut couvrir la veille technologique, la création de nouvelles applications logicielles ou fonctionnalités, ainsi que le développement d'une nouvelle ergonomie du site, etc. De plus, le prestataire doit garantir une maintenance éditoriale. Cette prestation peut couvrir la conception et la réalisation de nouvelles rubriques, la création de nouvelles pages-écrans, l'actualisation rédactionnelle ou graphique, ou encore la mise à jour des bases de données, etc.

Le prestataire cède généralement ses droits d'exploitation, de reproduction, de représentation et d'adaptation sur les créations et contenus fournis au client dans le cadre d'une maintenance éditoriale. Le transfert de propriété s'opère au fur et à mesure de l'achèvement des travaux, et sous réserve du paiement de la prestation par le client. Le prestataire doit enfin veiller à ce que le client lui remette les informations nécessaires à la réalisation de ses prestations¹.

Paragraphe 3 : Le contrat de fourniture d'accès.

Un fournisseur d'accès à internet (FAI), est un organisme (généralement une entreprise) offrant une connexion au réseau informatique Internet. Le terme anglais désignant un FAI est *Internet Service Provider (ISP)*². Le fournisseur d'accès met à la disposition de son partenaire une d'accès pour parvenir à un serveur est ainsi pourvoir se connecter à un réseau. Cette opération se fait dans le cadre d'un contrat qu'il convient d'en préciser l'objet (II) ainsi que les obligations de chacune des parties (II).

¹Ibid., p. 149.

²« Fournisseur d'accès à Internet –Définition », consulté le 02-06-2022 à 16h sur <https://www.techno-science.net/definition/10925.html>

I- Définition et objet du contrat.

Le contrat de fournisseur d'accès est aujourd'hui l'un des principaux contrats de consommation de masse au Maroc à travers lequel le fournisseur d'accès au réseau internet permet à l'internaute de relier son ordinateur au réseau de communication afin d'y accéder pour y collecter des informations et envoyer des messages ou de l'information. Il n'y a donc pas, en principe, d'intervention de ce prestataire sur le contenu de l'information¹. Donc, le fournisseur d'accès à l'internet met à la disposition de son partenaire une clé d'accès pour parvenir à un serveur et pouvoir se connecter à un réseau et bénéficier des services qu'il offre. Cette clé permet d'accéder au réseau mais rien de plus c'est-à-dire que le fournisseur ne prend aucun engagement au regard du contenu. Le contrat ne porte donc pas sur la communication d'information mais sur l'acheminement de celle-ci².

On peut considérer la nature juridique de ce contrat comme étant un contrat d'entreprise, ou encore la considérer comme une location du fait que le client bénéficie d'un droit d'usage intermittent d'un réseau pour parvenir à un serveur, par abonnement, exactement comme pour le téléphone. Si aucun prix n'est exigé par le fournisseur donc il s'agit de prêt. Force est de constater que les fournisseurs d'accès aux travers les contrats qu'ils proposent aux internautes prévoient de nombreuses clauses limitatives de responsabilité.

II- Les obligations du fournisseur d'accès et du client.

Le contrat précise les obligations du fournisseur. Il existe une obligation spéciale d'information à la charge du fournisseur d'accès. Le fournisseur s'engage généralement à rendre disponible en permanence son centre serveur, sous réserves des périodes de maintenance. A cet égard son obligation est de résultat. Toutefois, le contrat peut ne fournir aucune garantie de service interrompu et ne pas garantir le taux de disponibilité à 100% ; dans ce cas, l'obligation est de moyens.

Par ailleurs, l'obligation du fournisseur d'accès est de moyens sauf clauses contraires, notamment quant à l'accès aux informations circulant sur le réseau, aux services, aux taux de transfert et aux temps de réponse des informations circulant à partir de son centre de serveur

¹Luc GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, Droit des activités numériques, Dalloz, 1^{ère} éd., Paris, 2014, p. 230.

²Philippe LE TOURNEAU, *Op.cit.*, p. 525.

vers l'internet dans la mesure où il n'a pas la maîtrise de celui-ci. Les performances du réseau ne dépendent pas de lui. Le contenu du réseau n'entre pas dans l'objet du contrat passé avec le fournisseur, d'autant moins qu'il se trouve dans l'impossibilité de contrôler les données circulant sur les autoroutes de l'information. Toutefois, les prestations qu'il assure personnellement doivent correspondre à celles qu'il a promises dans son offre. De l'importance, une fois encore, d'une rédaction réfléchie des contrats¹.

En outre, le fournisseur d'accès délivre généralement un logiciel permettant la connexion et la navigation, voire, plus rarement, du matériel, vendu, loué ou prêté. Il s'engage souvent à assurer une assistance technique à ses clients, à permettre l'accès à des services en ligne. Au surplus, le fournisseur d'accès doit recueillir les demandes de clients qui se plaignent de *spamming* et d'en joindre à l'abonné qui s'est livré au *spamming* de mettre fin à cette pratique sous peine de suspendre l'accès au réseau².

Les fournisseurs d'accès à l'internet sont tenus de détenir et de conserver des données de nature à permettre l'identification de quiconque a contribué à la création de contenu des services dont ils sont prestataires³. Leur activité implique la collecte et l'utilisation de données à caractère personnel, la protection de celles-ci est assurée par la loi 09-08. Conformément à ladite loi le client dispose à tout moment d'un droit individuel d'opposition, d'accès, de modification, de rectification et de suppression des données le concernant auprès du fournisseur.

Le client utilisateur doit se procurer et maintenir en état les matériels informatiques, les logiciels et le modem qui sont nécessaire à sa connexion à l'internet, sauf clause prévoyant que le fournisseur mettra à la disposition de son partenaire tel ou tel de ses éléments, de façon accessoire. Il lui appartient de veiller à sa propre sécurité informatique. Il doit choisir un mot

¹Christiane FERAL-SCHUHL, *Op.cit.*, p. 1287.

²Mohamed Diyaa TOUMLILT, *Le commerce électronique au Maroc aspects juridiques*, Editions Maghrébines, Casablanca, 2008, p.104.

³Le fournisseur d'accès à internet collecte plusieurs types d'informations via l'utilisation en ligne du service notamment : l'état civil du client (nom, prénom), adresse de courrier électronique. En aucun cas le fournisseur n'a connaissance des données bancaires du client. Les informations conservées par le fournisseur ne sont transmises qu'aux seules personnes physiques et morales qui sont habilitées à les connaître. Néanmoins, le fournisseur pourra les communiquer, par tout moyen ou support, à ses sous-traitants pour des besoins de gestion et ou de recouvrement. Dans des circonstances très exceptionnelles, le fournisseur peut être amené à communiquer ces données lorsque cette démarche est imposée par la loi, ou qu'elle est nécessaire à l'identification, à l'interpellation ou à la poursuite en justice de tout individu susceptible de porter préjudice ou atteinte, intentionnellement ou non, aux droits ou à la propriété du fournisseur ; à d'autres utilisateurs du site du fournisseur ; à toute autre personne qui pourrait être pénalisée par de telles activités.

de passe lors de son abonnement, sur la confidentialité duquel il devra veiller, avec d'autant plus de vigilance. Un prix est généralement prévu, mais pas toujours, certains fournisseurs assurant un accès à titre gratuit, se rémunérant par la publicité.

Le contrat comporte presque toujours une clause résolutoire expresse en cas de manquement du client à ses obligations, mais qui ne peut être valide que si elle prévoit avec précision quel manquement à quelle obligation déterminée entraînera son application. Le contrat comporte une annexe de savoir-vivre sur le réseau et au minimum s'y référer. Le client s'engage alors à respecter les prescriptions et à ne pas commettre d'actes illicites. Le contrat est généralement conclu en ligne, l'internaute est réputé lié par ses dispositions, leur acceptation expresse conditionnant son inscription.

Paragraphe 4 : Le contrat d'hébergement du site Internet.

Le contrat d'hébergement est le prolongement naturel de l'accès, du moins pour un professionnel qui ne se contente pas de butiner sur le réseau. Dès lors, il convient d'en définir l'objet (I) avant de préciser les obligations découlant de ce contrat (II).

I- L'objet du contrat d'hébergement de site Internet.

Le contrat d'hébergement consiste à héberger virtuellement sur ses appareils le site du client, ce qui revient à stocker des données et à les rendre accessibles sur la toile mondiale. L'hébergeur est un stockeur d'informations que le fournisseur d'accès achemine dans ses centres de stockage. Particuliers et entreprises recourent de plus en plus à ces centres. Ces derniers présentent plusieurs avantages, notamment de préserver ses données des attaques et de désencombrer leurs systèmes informatiques. Le contrat d'hébergement comprend une location d'un espace dans le disque dur de l'hébergeur et une mise à disposition des capacités de traitement. De ce fait, il semble possible de qualifier ce contrat de location. Très souvent, le contrat d'hébergement est passé avec le fournisseur d'accès par un contrat unique. La nature juridique de ces deux contrats est identique¹.

Il existe deux grands types d'hébergement. D'une part, l'hébergement dit « mutualisé » implique le partage par plusieurs clients d'un même serveur d'hébergement appartenant à l'hébergeur. D'autre part, l'hébergement dit « dédié » qui implique la présence d'un seul client sur un serveur d'hébergement appartenant à l'hébergeur, qui lui est réservé,

¹Philippe LE TOURNEAU, *Op.cit.*, p. 532.

ou bien au client, laissé en dépôt par ce dernier à l'hébergeur. Chaque type d'hébergement présente des implications juridiques spécifiques nécessitant la conclusion de contrats distincts, avec des niveaux d'engagement variables. Par exemple, dans le cas d'un hébergement dédié sur les machines au client, le prestataire pourra se limiter à l'installation physique des équipements au client dans son centre d'hébergement, ainsi qu'à leur raccordement au réseau Internet et au réseau électrique. En revanche, dans le cadre d'un hébergement mutualisé, le prestataire d'hébergement assurera seul l'installation, la configuration, la maintenance, la gestion et l'administration des technologies mutualisées, le client n'ayant en principe pas d'accès aux équipements et logiciels d'hébergement du prestataire. Le contrat doit donc être explicite sur le type d'hébergement retenu par les parties¹.

La clause de force majeure du contrat d'hébergement doit notamment couvrir le blocage total ou partiel des moyens de télécommunications et de communication. Par exemple défaillance du réseau internet, non imputable à l'hébergeur. Si la force majeure perdure au-delà d'une certaine durée à déterminer, à compter de la survenance de l'événement, le client dispose généralement de la faculté de confier tout ou une partie des prestations à réaliser à des tiers.

La durée du contrat peut être déterminée ou non. Lorsqu'elle est indéterminée, elle est favorable au client puisque le contrat peut être résilié à tout moment, sous réserve d'un préavis suffisant. Dans cette hypothèse, le client n'est jamais « captif » de son prestataire et il peut se dégager aisément d'une solution d'hébergement qui deviendrait trop onéreuse, techniquement défaillante, etc. En cas de durée déterminée, cette situation est favorable au prestataire puisqu'elle permet à ce dernier de pérenniser ses revenus sur le long terme et de couvrir son investissement initial d'installation du site du client sur ses serveurs.

En général, la prestation d'hébergement est facturée sous la forme d'un loyer mensuel ou trimestriel payable à réception de facture pour des termes à échoir. Dans certains contrats, un droit d'entrée est facturé en sus au client pour couvrir les coûts initiaux d'installation du site au client sur le serveur d'hébergement. Compte tenu de la durée du contrat, un mécanisme de révision de prix doit être prévu². Finalement, il est utile de prévoir que les fichiers conservés dans les systèmes informatiques de chaque partie dans des conditions raisonnables

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 142.

²Philippe LE TOURNEAU, *Op.cit.*, p. 534.

de sécurité, les enregistrements vidéo d'accès aux salles d'hébergement et liste des codes d'accès seront considérés comme des moyens de preuve en cas de litige.

II- Les obligations découlant du contrat d'hébergement.

Le prestataire se trouve soumis d'un certain nombre d'engagement ; tout d'abord l'engagement de disponibilité, l'hébergeur s'engage à ce que le site du client soit accessible 24h/24h et 7i/7j, avec l'indication d'un pourcentage de disponibilité. L'accessibilité du site est une obligation de moyens. Certains événements peuvent justifier une interruption de cette disponibilité par exemple la maintenance, la survenance d'un cas de force majeure ou bien la mise en œuvre d'améliorations sur le serveur. Ces causes d'interruption autorisées seront en général définies limitativement par le client et largement par le prestataire. L'engagement de disponibilité n'est effectif que s'il est assorti de sanctions contractuelles¹.

Ensuite, l'hébergeur doit assurer une sécurité, d'une part le prestataire est tenu de la sécurité des serveurs et des locaux. Ainsi, il s'engage le plus souvent à mettre en œuvre les moyens les plus performants pour une parfaite sécurité et intégrité du site du client selon des caractéristiques techniques précises afin notamment d'empêcher l'intrusion de tiers non autorisés, de détournements éventuels et l'intrusion de virus. La sécurité doit également être assurée par des sauvegardes. D'autre part, et selon les dispositions de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et ses textes d'application, l'hébergeur doit s'engager à mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, ainsi que contre toute forme de traitement illicite. Enfin, en cas de fin du contrat, le prestataire s'engage le plus souvent à fournir toutes prestations permettant de maintenir, sans rupture, l'accessibilité du site du client et d'assurer le passage d'un prestataire à un autre sans dommage pour ce dernier. La remise des données et programmes stockés sur les serveurs au nouveau prestataire peut être organisée contractuellement².

¹En général, l'hébergeur s'engage à indemniser le client par l'application de pénalités contractuelles, venant en déduction du prix de l'hébergement (par ex, à partir d'un taux d'indisponibilité supérieur à quatre heures, une déduction sera faite sur le montant du loyer mensuel selon un pourcentage déterminé et au-delà de 24heures, ce loyer ne sera pas dû), et à remettre périodiquement au client des tickets d'incident précisant l'origine de chaque dysfonctionnement, sa durée et les mesures prises pour y remédier.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, pp. 152-153.

Le client doit fournir en temps utile ses spécifications, et toutes les données nécessaires à l'hébergement du site. Il s'engage aussi, notamment, à coopérer avec l'hébergeur et à posséder un système informatique permettant l'accès aux serveurs internet et compatible avec les prestations de l'hébergeur¹. Le client est souvent tenu de payer un prix mais le contrat d'hébergement peut être gratuit. Le contrat d'hébergement comme cité ci-dessus est généralement forfaitaire et par abonnement.

Sous-section 2 : Le contrat de commerce électronique.

L'air du temps fait du droit de la consommation une préoccupation constante de différentes législations nationales et des institutions et organismes internationaux qui se sont penchés sur la question des utilisations de l'internet, notamment, en matière de commerce électronique. En effet, l'internet offre un nouvel espace de commerce, dans la mesure où elle permet aux entreprises, quelle que soit leur situation géographique, de s'adresser aux consommateurs. Dans ce contexte et dans un souci de protection de ces derniers, de nombreuses lois ont vu le jour, dans le but d'établir, au niveau international, des dispositions communes en matière de passation de contrats en ligne.

La loi type CNUDCI sur le commerce électronique adoptée en 12 Juin 1996 constitue pour une grande partie des Etats, la principale inspiration des législateurs dans le domaine du commerce électronique. L'Assemblée générale des Nations unies le reconnaît elle-même puisqu'elle déclare dans sa résolution à propos de la loi type sur les signatures électroniques que la loi type sur le commerce électronique est universellement tenue pour une référence indispensable en droit du commerce électronique Cette loi type a ainsi promu l'utilisation des communications sans support papier en définissant les principaux concepts du commerce électronique et en incitant à l'équivalence entre données informatisées et données papier. La loi type sur le commerce électronique peut être considérée comme le fondement du droit du commerce international électronique².

Le commerce électronique ou commerce en ligne est celui qui est réalisé sur internet. C'est l'activité économique par laquelle une personne propose ou assure à distance et par voie électronique, la fourniture de biens ou services³. Il comprend le commerce entre entreprises (*Business to Business* ou *B to B*) et le commerce entre entreprise et consommateur (*Business*

¹Philippe LE TOURNEAU, *Op.cit.*, p. 534.

²Eric CAPRIOL, *Op.cit.*, p. 81.

³V. art. 65-4 de la loi 53-05.

to Consumer ou B to C). Le commerce électronique constitue une technique de vente qui se caractérise par trois mots : l'immatérialité, l'interactivité et l'internationalité, puisqu'il possède des normes mondiales et ignore les frontières¹.

La crise liée à la pandémie de la Covid-19 a accéléré l'expansion du commerce électronique vers de nouvelles catégories d'entreprises, de consommateurs et de produits. Les estimations indiquent que les commandes en ligne ont augmenté dans plusieurs régions au premier semestre de 2020, notamment en Europe, en Amérique du Nord et dans la région Asie-Pacifique². Au Maroc, depuis ces dernières années le e-commerce a connu une véritable évolution notamment avec la pandémie qui a été perçue comme accélérateur du développement du secteur. Dans son dernier rapport sur l'activité monétique marocaine en Septembre 2021, le CMI indique que l'activité du e-commerce marocaine ressort en progression de 48,4% en nombre et 30,5% en montant par rapport à la même période de l'année 2020 ; il faut dire que le Maroc a été particulièrement profitable en termes de e-commerce ces dernières années, il se place à la 95^{ème} place sur 152 pays couverts par l'indice 2019 du e-commerce entre entreprises et consommateur, publié annuellement par la conférence des Nations Unies sur le Commerce et le Développement.

Dans les rapports entre un vendeur sur internet exploitant un site de commerce électronique et l'internaute consommateur lui commandant un produit et avec lequel un contrat va donc être conclu, l'ensemble du dispositif juridique applicable est construit pour organiser un rééquilibrage, en protégeant la partie faible. Au Maroc, en plus de la loi 53-05 relative à l'échange électronique de données juridique, la loi relative à la consommation à savoir la loi 31-08 régit l'opération de vente à distance.

Constitue une vente à distance, la fourniture d'un produit, d'un bien ou la prestation d'un service au consommateur par un moyen électronique ou au moyen de communication à distance³. En matière de vente, la mise en œuvre de ces techniques aboutit à la vente par correspondance, la vente par téléphone ou encore certaines formes de du commerce

¹Philippe LE TOURNEAU, *Op.cit.*, p. 485.

²OCDE, « Le commerce électronique au temps de la pandémie de Covid-19 », Les réponses de l'OCDE face au coronavirus (Covid-19), 7 Octobre 2020.

³V. art. 27 de la loi 31-08.

électronique. Le législateur n'énumère pas expressément ces modalités de vente, il les englobe dans l'expression technique de communication à distance¹.

Les nouvelles technologies soulèvent des difficultés spécifiques, notamment au regard de leur licéité, de la manifestation du consentement, du paiement et plus largement de la protection du consommateur². Le problème qui se pose est celui de la prise de compte des intérêts du consommateur par le législateur marocain. Il s'agit de se demander si la réponse apportée par le législateur marocain à travers la loi 31-08 édictant des mesures de protection du consommateur est suffisante et adaptée pour protéger le consommateur, notamment dans l'hypothèse de la vente à travers les nouvelles technologies.

Nous évoquerons successivement l'obligation d'information loyale claire et transparente du consommateur (Paragraphe 1) ; Les modalités d'acceptation de l'offre par le consommateur et de formation du contrat (Paragraphe 2) ; la faculté de rétractation du consommateur (Paragraphe 3).

Paragraphe 1 : L'obligation d'information loyale, claire et transparente.

La loi marocaine relative à la consommation prévoit, dans le chapitre premier consacré à l'obligation générale d'information, que le professionnel doit communiquer de manière lisible et compréhensible au consommateur avant la conclusion d'un contrat de vente ou de fourniture de service, certaines informations obligatoires. Il s'agit des principales caractéristiques du bien ou du service ainsi que de son prix³. En effet, l'article 3 de la loi 31-08 indique que l'information doit porter sur la date de péremption, et lui fournir les renseignements par voie de marquage, d'étiquetage, d'affichage ou par tout autre procédé. Le texte ajoute que le fournisseur doit fournir les informations relatives au mode d'emploi du produit ou service, le manuel d'utilisation, la durée de garantie et ses conditions ainsi que les conditions particulières de la vente ou la réalisation de la prestation.

L'article 5 de la loi 31-08 exige que la mention d'un prix ou du tarif soit obligatoire. Le texte précise que le contrat doit inclure le prix global à payer par le consommateur y

¹Les techniques de communication à distance sont définies par l'article 25 de la loi 31-08 comme : « tout moyen utilisé pour la conclusion d'un contrat entre un fournisseur et un consommateur sans la présence simultanée des parties ».

²François COLLART DUTILLEUL et Philippe DELEBECQUE, Contrats civils et commerciaux, Dalloz, 10^{ème} éd., Paris, 2015, p. 116.

³V. art. 29 de la loi 31-08.

compris la taxe sur la valeur ajoutée, toutes autres taxes, ainsi que le coût de tous les services à payer obligatoirement en supplément par le consommateur. Lorsque le contrat est conclu à distance, l'article 29 de la présente loi ajoute qu'il faut inclure le coût de la technique de communication à distance. De plus, l'article 31 de la loi 31-08 exige que s'il s'agit d'une vente à distance, le professionnel doit indiquer expressément au début de la conversation avec le consommateur, son identité et l'objet commerciale de la communication.

Ajoutons que, la conclusion d'un contrat en ligne nécessite que le professionnel connaisse l'identité de celui qui lui commande un produit ou un service, aux fins de l'exécution du contrat conclu, pour le paiement en ligne et pour la livraison du bien commandé, ainsi que, notamment, pour vérifier que la personne qui accepte son offre dispose de la capacité juridique de contracter. De même, certain produits ou services étant interdits à des catégories définies de personnes tels les mineurs, le professionnel peut être amené à s'assurer que l'utilisateur est en droit de consommer ces biens ou services. L'utilisateur doit ainsi habituellement indiquer son nom et son adresse, ainsi que son adresse électronique. En retour, puisque l'identité des consommateurs est ainsi collectée, enregistrée et stockée par le commerçant sur son serveur, ce dernier doit se soumettre aux contraintes de la loi 09-08 sur la protection des données à caractère personnel¹.

En l'absence d'exécution immédiate du contrat, la date ou le délai auquel le professionnel s'engage à livrer le bien ou à exécuter le service doit être indiqué². Il se dégage dès lors une amélioration de la sécurité du consentement du consommateur. Le législateur marocain a opéré une avancée remarquable puisque le devoir précontractuel d'information, imposé à la personne avec qui le consommateur contracte, permettra à ce dernier d'avoir des détails non seulement sur le bien mais surtout sur son cocontractant à qui il pourra adresser des questions ou des demandes si le besoin s'en fait sentir. Ainsi, les incertitudes relatives aux litiges semblent être supprimées par le droit de dénonciation conféré implicitement au consommateur³.

En revanche, le législateur marocain n'a pas élargit cette obligation d'information précontractuelle aux opérateurs de plateforme en ligne. Ces derniers ne sont plus seulement l'apanage des pays développés puisqu'elles existent désormais au Maroc. En effet, tout

¹Voir supra p. 128.

²V. art. 12 de la loi 31-08.

³Geoffray BRUNAUX, Le contrat à distance au XIXème siècle, LGDJ, Paris, 2010, p. 25.

comme *eBay* ou *Le boncoin*, il existe au Maroc des sites d'annonces¹ destinés au marché marocain et qui échappe à toute réglementation. Ces plateformes électroniques sont des comparateurs, des moteurs de recherche, des plateformes collaboratives et des réseaux sociaux. Ces sites internet de vente, location ou partage entre particuliers qui mettent en relation par voie électronique, des personnes en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un bien ou d'un service doivent fournir une information loyale et claire au consommateur sur le bien ou service, le prix, la date ou le délai auquel le professionnel s'engage à livrer le bien ou à exécuter le service, les informations relatives à son identité, à ses coordonnées électroniques et téléphoniques et à ses garanties légales.

L'obligation d'information précontractuelle s'analysant en une obligation de loyauté du professionnel, le législateur marocain devrait consacrer cette obligation en l'adaptant aux réalités économiques actuelles. En le faisant, le législateur aura le mérite de créer des règles de transparence et de loyauté qui doivent présider à toute relation contractuelle.

Paragraphe 2 : Les modalités d'acceptation de l'offre par le consommateur et de formation du contrat.

Comme cité précédemment, l'article 65-3 du DOC tel que complété par la loi 53-05 relative à l'échange électronique de données juridiques autorise la voie électronique à être utilisée pour mettre à disposition du public des offres contractuelles ou des informations en vue de la conclusion d'un contrat. Cette offre, exposée par le site, doit être claire et explicite. Elle doit notamment comporter des conditions générales de vente, la disponibilité du bien et les délais de livraison et le prix. Toutes les informations précontractuelles habituelles doivent aussi être données². Ne pas omettre de mentionner la durée de l'offre étant donné qu'un site peut être consulté du monde entier, les territoires pour lesquels elle est valable. Ces informations doivent apparaître et sont communiquées au consommateur de manière claire et compréhensible, par tout moyen adapté à la technique de communication à distance.

Dans le commerce électronique la détermination du moment de la formation du contrat est liée à des questions purement techniques³. Avant la conclusion du contrat, le fournisseur doit rappeler au consommateur ses différents choix et lui permettre de confirmer sa demande

¹Citons entre autres, Avito et Jumia.

²V. art. 29 de la loi 31-08.

³Philippe LE TOURNEAU, *Op.cit.*, p. 504.

ou de la modifier selon sa volonté. Par ailleurs, toute commande doit faire l'objet d'un accusé de réception par le vendeur. Ainsi, dès réception de l'acceptation, l'auteur de l'offre doit accuser réception de l'acceptation de l'offre qui lui a été adressée. Cette obligation doit être remplie sans délai injustifié et par voie électronique¹. Ce processus transparent a pour corollaire l'interdiction faite aux professionnels d'ajouter, par défaut, des éléments complémentaires ou accessoires non commandés par l'internaute. Donc, l'acceptation de l'offre, sa confirmation et l'accusé de réception sont réputés reçus lorsque les parties aux quelles ils sont adressés peuvent y avoir accès.

Enfin, l'exécution de la commande doit être faite dans un délai maximum de 3 à 30 jours à compter du jour où le fournisseur a confirmé la réception de la commande de la part du consommateur. A défaut d'exécution du contrat suite à l'indisponibilité du contrat. Le consommateur doit être informé de cette indisponibilité pour pouvoir être remboursé.

Paragraphe 3 : Le droit de rétractation.

La rétractation est une manifestation de volonté par laquelle l'auteur entend revenir sur volonté précédemment manifestée et la retirer comme si elle était non avenue, afin de la priver de tout effet passé ou à venir. L'objectif est de permettre au consommateur de revenir sur son consentement, en particulier lorsqu'il a été donné précipitamment, ou lorsqu'il a été exprimé dans un contexte où sa réflexion était mise en mal. C'est un droit discrétionnaire pour la partie qui le détient. A cet égard, le droit de rétractation conduit à sanctionner le manquement aux obligations précontractuelles d'information qui pèsent sur les professionnels. Le droit de rétractation est donc au cœur du dispositif de protection du consommateur.

Le droit ou du moins la faculté de rétractation se situe en aval de l'échange des consentements². Il se distingue ainsi du délai de réflexion qui intervient en amont de la conclusion du contrat, en reportant le moment où le consommateur peut donner son consentement. Le fondement principal de ce droit reconnu au consommateur est la protection contre sa propre précipitation. Selon l'article 36 de la loi 31-08, le consommateur commandant un produit ou un service bénéficie d'un délai de 7 jours pour se rétracter, sans avoir à justifier de motifs. Ce délai court à compter de la réception pour les biens ou

¹V.art. 65-5 du D.O.C complété par la loi 53-05.

²Eric BAZIN, Le droit de repentir en droit de la consommation, Dalloz, Paris, 2008, p. 3028.

l'acceptation de l'offre pour les services. Ce délai est prolongé à 30 jours si les informations que le fournisseur est censé fournir sur le fondement des articles 29 et 32 de la même loi n'ont pas été communiquées au consommateur. D'une part, lorsque le droit de rétractation est exercé, le fournisseur est tenu de rembourser, sans délai, au consommateur le montant total payé et au plus tard dans les 15 jours suivant la date à laquelle ce droit a été exercé. D'autre part, l'article 38 de la loi 31-08 exclut certains biens et services¹ du champ d'application de l'article 36.

En droit marocain, le droit de rétractation est d'ordre public. Une règle d'ordre public est obligatoire et les parties ne peuvent y déroger, c'est ce qui ressort de l'article 62 du D.O.C. Par conséquent, toute clause par laquelle le consommateur renoncerait de manière anticipée à ce droit est nulle. La protection du choix du consommateur dépend certes, du fruit du caractère discrétionnaire qui permet au consommateur de ne jamais donner de motifs quant à sa décision de se rétracter, mais également celui du caractère d'ordre public qui lui est conféré par le législateur. L'exercice du droit de repentir est d'ordre public. Le consommateur ne peut en aucun cas y renoncer ni de manière expresse ni de manière tacite. Les parties ne peuvent y déroger.

Lorsque le consommateur exerce son droit de rétractation, il est tenu de renvoyer les biens au professionnel dans les meilleurs délais et au plus tard dans les 7 jours qui suivent la livraison de la commande. En l'absence de précisions légales formelles, des questions se posent, par exemple, le cas où le produit est détérioré du fait de l'ouverture de son emballage. En outre, s'agissant d'un contrat de service déjà exécuté, une restitution serait difficile. En dépit du silence de la loi marocaine sur l'hypothèse de la détérioration du produit, la faute de l'acheteur justifie qu'il supporte les conséquences liées à la détérioration du produit. Ainsi, les vendeurs ont le droit de refuser la reprise du produit détérioré sans toutefois obliger l'acheteur au paiement d'une indemnité. En effet, la sanction de la détérioration du produit sera soit le refus dudit produit, soit sa reprise moyennant réparation aux frais de l'acheteur.

¹Ces exceptions concernent les contrats : fourniture de services dont l'exécution a commencé, avec l'accord du consommateur, avant la fin du délai de rétractation ; fourniture de produits, biens ou de services dont le prix est fonction de fluctuations des taux du marché financier ; fournitures de biens confectionnés selon les spécifications du consommateur ou nettement personnalisés¹ ou qui, du fait de leur nature, ne peuvent être réexpédiés ou sont susceptibles de se détériorer ou de se périmérer rapidement ; fourniture d'enregistrements audio ou vidéo ou de logiciel informatiques lorsqu'ils ont été descellés par le consommateur ; fourniture de journaux, de périodiques ou de magazines. De même, sont exclus les services d'hébergement, de transport, de restauration, de loisirs qui doivent être fournis à une date ou selon une périodicité déterminée. V. art. 42 de la loi 31-08.

Cette proposition, qui a pour but de clarifier les conditions de la restitution des produits encore obscures dans la législation marocaine, doit pouvoir s'étendre à la restitution d'un service rendu.

Sous-section 3 : Le contrat de publicité numérique.

Internet constitue un support publicitaire, au même titre que la télévision, la presse ou la radio. La particularité de ce support est de permettre aux annonceurs d'atteindre plus efficacement un public ciblé. En effet, à la différence des grands médias traditionnels, le support internet permet de garantir aux annonceurs un contact entre le message publicitaire et à leur cible. Il leur permet également de connaître le nombre d'internautes ayant visionné ou cliqué sur une publicité affichée sur leur écran, et même de suivre le comportement des internautes postérieurement à l'affichage jusqu'à l'acte d'achat ou à la réalisation d'une action déterminée par l'annonceur. Ainsi, à la fin de l'année 2020, les dépenses en publicité digitale ont représenté à l'échelle mondiale plus de 200 milliards d'euros. Les géants du web ne s'y sont pas trompés et la publicité en ligne constitue la source principale de leurs revenus. Ce mode de publicité suscite des difficultés juridiques de plus en plus nombreuses¹. Les spécificités d'Internet en tant que support publicitaire ont poussé à délimiter un marché pertinent de la publicité en ligne distinct des marchés liés à la publicité hors ligne. On distingue trois principaux segments de marché, à savoir la publicité par affichage (*display*)², la publicité liée aux recherches (*search*)³, et la publicité dans les annuaires⁴.

¹H. GUYADER, « Avant-propos sur les enjeux de la publicité digitale », in IP/IT, N° 9, Septembre 2021, Dalloz, p. 430.

²La publicité dite « display » est la forme la plus ancienne de publicité digitale : les premières bannières publicitaires datent du milieu des années 1990. Aujourd'hui, ce levier pèse pour 17% des investissements publicitaires en ligne. Bien que le format emblématique de la publicité display reste la bannière publicitaire sous ses multiples formes, il n'est pas rare de voir regroupés sous le nom de display des formes publicitaires très variées, comme la vidéo, qui a aujourd'hui dépassé la bannière, ou même les formats audio (diffusés sur les podcasts, notamment), qui sont en forte progression.

³Le principe est assez connu : positionner une publicité sur les moteurs de recherche en « achetant » des mots-clés, qui correspondent au produit que l'on souhaite promouvoir, par exemple « canapé clic-clac », ou « vol Casablanca-Paris ». Le positionnement se fait sur un système d'enchères pour un mot-clé donné, on détermine un montant d'enchère, qui représente le montant maximal que l'annonceur est prêt à payer pour un clic sur sa publicité. La plupart du temps, plus le montant de l'enchère est élevé, plus l'annonce sera visible au sein des résultats de recherche.

⁴Ce levier consiste à annoncer sur les réseaux sociaux, comme Facebook, Instragram, Snapchat, ou plus récemment TikTok. Ces acteurs bénéficient d'une connaissance très fine de leurs utilisateurs, ce qui permet un ciblage très fin de leurs utilisateurs, ce qui permet un ciblage très précis, que ce soit par critères

Internet est essentiellement un espace d'expression d'accès gratuit. La publicité y revêt donc structurellement un aspect crucial. Cela n'est pas nouveau, mais ce qui l'est, ce sont les techniques publicitaires sur internet, et plus spécifiquement les modalités d'achat et de vente d'espace publicitaire, qui se distinguent assez nettement de ce qui peut s'observer sur les médias classiques¹. La publicité par voie électronique qu'il revient de traiter sous l'angle juridique présente une grande complexité et soulève pour le juriste des difficultés. Il ya celle qui relèvent du contrat d'achat d'espace publicitaire (Paragraphe 1). Il y aussi celles qui relèvent de la protection des personnes qui utilisent les réseaux numériques (Paragraphe 2). Il ya aussi des perspectives plus globales tenant au fonctionnement du marchés (Paragraphe 3).

Paragraphe 1 : L'achat d'espace publicitaire.

Traditionnellement, les contrats d'achat et de vente d'espace publicitaire mettent en relation trois parties : l'annonceur qui souhaite diffuser une information (faire de la publicité pour sa marque), vendre un service ou produit ; le support, qui vend des espaces publicitaires aux annonceurs ; et l'intermédiaire entre l'annonceur et le support (l'agence de publicité), qui aide le support à trouver des clients et les annonceurs à trouver des supports. L'achat d'espace peut aussi être réalisé directement par l'annonceur auprès du support, sans recours à un intermédiaire.

Le développement d'internet a complexifié les activités de publicité, et le rôle des différents intervenants, ce qui n'est pas sans poser de difficultés eu égard à l'application de certaines dispositions relatives aux contrats de vente et d'achat d'espace publicitaire.² Incontestablement, l'essor de la publicité en ligne a contribué à effacer la frontière jusqu'ici très clair entre, d'une part, les supports et leurs régies et, d'autre part, les annonceurs et leurs mandataires à l'achat d'espace publicitaire.

Les nouvelles modalités d'achat en ligne d'espaces publicitaires sur des places de marché dites *Ad exchanges*, permettant d'optimiser et d'automatiser la vente d'espaces

sociodémographiques par centre d'intérêt ou par comportement. Au premier trimestre 2020, les réseaux sociaux représentaient 25% des investissements digitaux.

¹Frédéric DUMONT, « Les contrats de publicité. Les nouvelles techniques d'achat publicitaire sur internet » in L'entreprise à l'épreuve du droit de l'Internet, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014, p. 45.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 155.

publicitaires sur une logique d'enchères en temps réel *RTB*¹, ont considérablement changé le rôle des agences médias et multiplié les intermédiaires. Ce procédé constitue une innovation plus structurante, à plusieurs points de vue. Il serait difficile ici d'entrer dans le détail technique, particulièrement complexe, de l'opération, mais l'on peut tout de même identifier quelques spécificités. Les achats s'y font en général à l'aveugle, c'est-à-dire que l'annonceur ne sait pas à l'avance sur quel site son annonce paraîtra. Aussi, la vente se fait quasi instantanément, selon un mécanisme d'enchères. L'opération se déroule comme suit : du côté de la vente, un certain nombre d'éditeurs de sites internet mettent en commun leurs espaces disponibles et les proposent aux enchères ; du côté de l'achat, un certain nombre d'annonceurs répondent aux enchères. L'offre détermine la cible publicitaire, l'audience souhaitée² ; le groupe d'annonceurs qui remporte l'enchère fait diffuser ses publicités, quasiment en temps réel³.

Dans ce schéma, pas moins de cinq intermédiaires interviennent entre l'annonceur et le support de sorte qu'il est très délicat de déterminer qui dans cette chaîne doit être réputé agir pour le compte de l'annonceur, en qualité de mandataire de ce dernier (I), soumis de ce fait aux obligations de transparence et qui doit être réputé agir pour le compte du support en qualité de régie (II).

I- Le contrat d'achat d'espace publicitaire.

Le contrat d'achat d'espace publicitaire peut être insérer sous diverses formules. Plusieurs alternatives pourront être envisagées notamment le contrat de commissionnaire, le contrat de courtage, le contrat de manda, etc. Nous allons essayer de détailler le cas où le contrat d'achat d'espace publicitaire prendra la forme d'un contrat de mandat réglementé. Le contrat de mandat doit nécessairement faire l'objet d'un écrit et respecter les dispositions de droit commun des contrats⁴. Un contrat de mandat pour l'achat d'espace publicitaires pourrait avoir comme objet : le mandat de procéder en son nom et pour son compte à la négociation et à l'achat d'espaces publicitaires nécessaires à la diffusion de ses compagnes

¹Cet acronyme anglais signifie "Real-Time Bidding", ou enchères en temps réel en français. C'est un mot que l'on retrouve principalement dans le domaine de la publicité en ligne et qui caractérise la manière dont les espaces publicitaires sont achetés et vendus selon un système d'enchères. Google a été le premier à mettre en place un système de RTB pour ses liens sponsorisés. Sur un même mot clé, si plusieurs annonceurs souhaitent diffuser leur publicité, c'est celui qui aura l'enchère la plus élevée qui gagnera la mise.

² G. GIUDICELLI, « La publicité digitale en France », in IP/IT, N° 9 Septembre, 2021, Dalloz, p. 435.

³Frédéric DUMONT, *Op.cit.*, p. 46 ;

⁴Philippe LE TOURNEAU, *Op.cit.*, p. 597.

publicitaires. Le contrat de mandat doit impérativement mentionner les conditions de la rémunération du mandataire détaillant, s'il y a lieu, les diverses prestations qui seront effectuées dans le cadre de ce contrat de mandat de leur rémunération respectives, ainsi que les autres prestations rendues par l'intermédiaire en dehors du contrat de mandat et le montant global de leur rémunération¹.

Le mandataire (l'intermédiaire) est soumis à deux obligations principales. Il est soumis en premier lieu à une obligation de loyauté. Il est interdit au mandataire de recevoir d'autre paiement que celui qui est versé par son mandat, pour la rémunération de l'exercice de son mandat, ni aucune rémunération ou avantage quelconque de la part du vendeur. En second lieu, il est soumis à une obligation de reddition des comptes. En droit commun l'obligation de reddition des comptes se manifeste par l'obligation d'informer le mandant de l'accomplissement de sa mission et de restituer à ce dernier les sommes reçues en vertu de sa procuration.

Les obligations du mandat (l'annonceur) sont de deux ordres. A l'égard des tiers, en vertu du principe de la représentation, le mandant est tenu d'exécuter les engagements contractés par son mandataire, mais n'est pas tenu par les actes du mandataire qui excéderaient le mandat qui lui a été conféré. A l'égard du mandataire, le mandant est tenu de régler la rémunération du mandataire et de le rembourser des avances et frais qu'il aura fait dans le cadre de l'exécution du mandat. Le support est tenu, d'une part de communiquer à tout professionnel qui en fait la demande son barème de prix et ses conditions de vente, d'autre part, de faire figurer la facture délivrée à l'annonceur et, enfin, de communiquer directement sa facture de vente à l'annonceur, même si la prestation est réglée par l'intermédiaire².

II- Le contrat de régie publicitaire.

Le régisseur de publicité est un acteur traditionnel des opérations d'achat et de vente d'espace publicitaire. Il se définit comme « *l'entreprise qui a la charge de recueillir la publicité pour le compte d'un support quel qu'il soit* »³, ou comme le professionnel dont la fonction consiste à commercialiser, auprès des annonceurs et des agences, les espaces dont dispose le support. La régie publicitaire apparaît donc juridiquement comme une émanation

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 158.

²Ibid., pp. 159-160 ;

³François GREFFE et Pierre GREFFE, *La publicité et la loi*, Litec, 11^{ème} éd., Paris, 2009, p. 59.

du support, même si elle n'est pas nécessairement l'émanation économique de celui-ci. Cette caractéristique a pour conséquence de soustraire la régie publicitaire aux règles très contraignantes du statut de mandataire.

Un contrat de régie publicitaire a pour objet de mettre à la charge du régisseur l'obligation de prospecter, de recueillir et de promouvoir, par tous les moyens à sa convenance, la publicité à insérer sur le support, de la facturer et d'encaisser le montant auprès des annonceurs, et de tout agent intermédiaire, aux termes et conditions définis dans le contrat. Le régisseur de publicité intervient généralement en qualité de mandataire, sauf dans les cas, relativement rares, où il agit ses seuls risques.

C'est dans ce schéma traditionnel de l'activité publicitaire que s'est développée l'activité de régie publicitaire en ligne. Le contrat de régie publicitaire est généralement conclu pour un ou plusieurs sites internet. Ce couplage de sites constitue une nouvelle catégorie de support publicitaire qui est, en fait, élaboré et composé par le régisseur. Il y a là une originalité manifeste par rapport à la situation traditionnelle où le régisseur se borne le plus souvent à intervenir pour le compte du support. S'il demeure le mandataire des titulaires de sites internet qui composent de bouquet, le régisseur a un rôle propre qui est fondamental, puisque c'est lui qui va être en mesure de bâtir le support.

Internet est un univers par essence changeant, difficilement compatible avec la durée, en général relativement longue, des contrats de régie publicitaire. Les parties sont ici libres de se soumettre à une durée déterminée ou indéterminée. Le tarif de la publicité est généralement déterminé, selon des calculs plus ou moins sophistiqués, en fonction de la durée de l'insertion et de l'audience du site. En ce qui concerne la commission du régisseur, le partage entre l'éditeur et le régisseur des revenus publicitaires provenant d'annonceurs ou d'intermédiaires est toujours calculé sur le montant net encaissé, c'est-à-dire sur le montant brut facturé en fonction de la grille tarifaire, duquel sont soustraites les éventuelles réductions du montant facturé au client lié à un escompte de volume ou de fréquence, ainsi que toute remise à un intermédiaire, particulièrement à une agence de publicité ou à une centrale d'achat d'espace. Le régisseur s'engage aussi à prospecter les annonceurs potentiels.

Le contrat de régie met à la charge du titulaire du site une obligation d'information du régisseur particulièrement étendue. Ces dispositions ont pour objet principal d'assurer au régisseur, et donc indirectement aux annonceurs, la meilleure connaissance possible du site sur lequel ces derniers insèrent leurs publicités. Cette spécificité du contrat de régie en ligne

s'explique très logiquement par le caractère essentiellement évolutif d'un site web. L'éditeur du site internet est également soumis à une obligation de mentionner l'identité de son régisseur. En effet, traditionnellement, le support presse s'engage contractuellement, à l'égard de son régisseur de publicité, à imprimer dans le corps de la publication une mention relative aux coordonnées de son régisseur. Sous une nouvelle forme, le titulaire du site s'engage à mentionner le régisseur comme son unique représentant pour la vente d'espace publicitaire sur son site web.

Paragraphe 2 : Le référencement.

Le référencement est de la nature de la toile, sa clé de voute, car seul, il permet d'assurer la publicité de son contenu au sein de l'immensité des données qu'elle véhicule. Il assure la diffusion des informations dans le commerce par voie électronique. Etre référencé, et bien placé sur un moteur de recherche, est d'une importance capitale pour les entreprises. Un site mal référencé ou pas référencé n'a aucune existence réelle. Le référenceur assure un service ; comme celui-ci ne consiste pas à accomplir un acte juridique il s'agit forcément d'un contrat d'entreprise. Lorsque le contrat est conclu par internet il est soumis à diverses règles envisagées précédemment.

Des intermédiaires interviennent dans les divers référencement parfois comme courtiers mais dans d'autres cas en représentant l'une des parties donc en tant que mandataire. Cependant, ils assurent généralement un certain nombre de prestations par exemple, la création des références dans le code source du référencé. Les éditeurs cherchant à accroître la visibilité de leurs sites Internet peuvent soit opter pour un référencement par un moteur de recherche ou un annuaire (I), soit choisir un référencement par affiliation (II).

I- Le référencement par un moteur de recherche ou un annuaire.

Le référencement naturel permet à un site internet d'être référencé dans les résultats des recherches effectuées par un internaute sur un moteur de recherche ou dans un annuaire. Par exemple, les mots clés contenus dans le nom de domaine, dans le titre du site, dans le site lui-même, ou encore à partir de la popularité du site de son ancienneté, du nombre de liens

hypertextes pointant vers ce site, etc. Le référencement est ici automatique, il résulte de l'algorithme conçu par les éditeurs de moteur de recherche¹.

Lorsqu'il existe un véritable accord, conclu généralement en ligne, des obligations naissent à la charge des parties. La prestation est tantôt à titre gratuit tantôt à titre onéreux. La pratique du référencement payant permet à l'éditeur d'un site internet de réserver, auprès d'un moteur de recherche ou d'un annuaire sur internet, un espace publicitaire qui s'affichera en marge des résultats de recherches effectuées par les internautes, sous forme de lien promotionnel renvoyant directement à son site. Pour cela, il choisira les mots-clés qui, une fois entrés par l'internaute dans l'outil de recherche en ligne, engendreront l'apparition automatique d'une annonce au profit du site Internet de l'annonceur. L'achat du mot-clé relève en pratique d'un système d'enchères, puis d'un cout par clic².

Les exploitants d'annuaires et de moteurs de recherche s'engagent seulement à assurer le site du demandeur dans un délai assez bref. A défaut de précision contractuelle contraire, l'obligation de référencement constitue une obligation de moyens ce qui est la solution raisonnable dans ce domaine ; néanmoins le contrat peut prévoir une obligation de résultat, avec les conséquences qui s'y attache. Les moteurs de recherche proposent généralement leurs services pour mettre en place les liens commerciaux, en suggérant de des mots clés. Il est prudent de rappeler dans le contrat au titulaire du site de référencé que le contenu de son site doit être licite³.

II- Le référencement par affiliation.

Le référencement par affiliation est un référencement à un degré au-dessus du référencement envisagé précédemment. En effet, l'affiliation est une technique commerciale permettant à un éditeur de site internet (l'affilié), d'envoyer du trafic de son site vers un autre, la cible, appartenant à un autre éditeur (l'affileur). Le premier est donc prescripteur pour le compte du second. Ce mode de référencement s'effectue de diverses manières. Selon la plus simple et la plus fréquente. Il se traduit par l'insertion sur le site de l'affilié de dispositifs techniques tels des liens hypertextes ou des bandeaux publicitaires, permettant aux internautes le visionnement d'avoir un accès direct aux pages du site cible.

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 185.

²Ibid., pp. 186-188.

³Philippe LE TOURNEAU, *Op.cit.*, p. 557.

Dans un autre procédé, l'affilié acquiert d'un moteur de recherche le droit d'usage de mots-clés, établissant des liens commerciaux ; ceux-ci permettent de renvoyer l'internaute cliquant sur eux soit sur le site de l'affilié soit directement sur le site de l'affilieur. L'affiliation prend généralement la forme d'une convention conclue directement entre l'affilieur et chacun des affiliés. Le contrat d'affiliation s'apparente à une prestation de service de publicité¹.

Paragraphe 3 : La protection des données à caractère personnel en matière de publicité ciblée.

Le régime juridique de l'exploitation des données à caractère personnel exerce une influence considérable sur l'activité publicitaire et suscite quelques inquiétudes et des critiques². Sur internet, les possibilités de ciblage sont beaucoup plus développées que sur les médias audiovisuels traditionnels ; ce qui justifie que l'expression « publicité ciblée » soit habituellement employée en référence à ce support. La publicité ciblée impliquant l'exploitation de données concernant les personnes auxquelles elle s'adresse pose directement la question des finalités de ces traitements et des atteintes possible à la vie privée.

La publicité ciblée désigne les facultés d'adaptation d'un contenu publicitaire à des informations de navigation ou à des données à caractère personnel. On identifie trois niveaux de publicité ciblée sur internet : La publicité personnalisée « classique », choisie en fonction des caractéristiques connues de l'internaute (âge, sexe, etc.) qu'il a lui-même renseignée par exemple en s'inscrivant sur un service ; la publicité contextuelle choisie en fonction du contenu immédiat fourni à l'internaute (par ex., en fonction d'un statut sur *Facebook* ou d'un message dans *Twitter*) ; et la publicité comportementale choisie en observant le comportement de l'internaute à travers le temps (visites successives de sites, interactions, achats, mot-clé, etc.) pour en déduire son profil et lui proposer des publicités adaptées³.

Face aux enjeux économiques très importantes et dans un contexte de concurrence internationale exacerbé par la nature transfrontière d'internet, la tentation peut être grande pour les acteurs de s'approprier le maximum de données et de constituer des bases de référence

¹Ibid., p. 567.

²Jean-Pierre CLAVIER, « La publicité par voie électronique », in *L'entreprise face aux défis du numérique*, Ouvrage collectif sous la direction de Jean-Marc MOULIN, Sylvain CHARTRY et Alexandre RIERA, Mare&Martin, Paris, 2018, p. 175.

³Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 181.

les plus importantes possible. Dès lors, il semble légitime d'envisager les différentes techniques d'identification et de suivie de navigation (II), avant de présenter le cadre légal applicable aux traitements des données personnelles collectée lors de la publicité ciblée (I).

I- Les techniques d'identification et de suivie de navigation.

Les stratégies de ciblage et la précision des profils obtenus reposent sur le recoupement du maximum d'informations concernant une personne déterminée. La mise en œuvre de la publicité ciblée implique donc le suivi de la navigation de l'internaute et éventuellement son identification. Dans l'hypothèse la plus simple, l'internaute s'identifie lui-même sur le service. C'est le cas par exemple des sites qui imposent une identification préalable avant l'accès au service, à un espace personnel dédié, ou à certaines fonctionnalités. L'internaute peut également être identifié par un service par le biais d'une connexion via un service ou un compte utilisateur tiers. Les informations de connexion sont dans ce cas collectées par le réseau social et, éventuellement et de manière limitée, par le site intégrant cette fonctionnalité. Troisième possibilité est celle relative au le suivi de la navigation de l'internaute par le recours aux cookies appelés aussi témoins de connexion¹. Un cookie peut être installé sur le poste d'un internaute par l'éditeur du site, ainsi que par la régie publicitaire qui gère l'affichage des contenus publicitaires au sein de ce site². Une régie pourra ainsi, grâce aux cookies insérés dans ces espaces publicitaires, suivre la navigation d'un internaute sur les différents sites où ses publicités sont affichées et proposer des publicités ciblées sur l'ensemble de ces sites. Néanmoins, en Janvier 2020, Google a annoncé que, d'ici deux ans son navigateur Chrome bloquerait par défaut les cookies, emboitant le pas à d'autres tel Apple. Chrome représentant 60% du marché des navigateurs, cette annonce a fait l'objet d'une grande attention des acteurs publicitaires³.

Si la promesse de la publicité ciblée est d'épargner à l'internaute des annonces sans rapport avec ses goûts et ses attentes, celle-ci est aujourd'hui mal accueillie par le public. Ainsi une grande partie de la population n'est pas favorable au principe de l'utilisation de ses données personnelles (même sous une forme anonyme), notamment en raison de son caractère

¹Techniquement, un cookie est un fichier texte qui contient systématiquement un numéro d'identifiant unique de l'internaute et des informations relatives au serveur ayant procédé à l'installation. Certaines peuvent contenir des données purement personnelles ; d'autres sont exclusivement techniques.

² Christiane FERAL-SCHUHL, *Op.cit.*, p. 597.

³G. GIUDICELLI, *Op.cit.*, p. 436.

intrusif¹. Cette méfiance du public est révélatrice d'un manque de confiance global envers les acteurs de la publicité ciblée quant à l'utilisation réelle qui peut être faite de leurs données et l'opacité des transferts et des échanges d'informations. Ce manque de confiance traduit également le sentiment d'insécurité juridique qui peut résulter d'un cadre légal encore sujet à débats et en évolution régulière.

II- Le cadre légal applicable à la publicité ciblée.

L'accumulation et le traitement intensifs de grandes quantités de données à caractère personnel ne constituent pas en tant que tels des infractions². Néanmoins, l'exploitation des données à caractère personnel aux fins de la publicité ciblée est anonyme, la législation sur la protection des données à caractère personnel à savoir la loi 09-08 se voit appliquer. En dehors du cas évident où la publicité est ciblée sur la base d'un profil explicite d'un internaute identifié, la question de l'anonymat des données exploitées peut être posée. En effet, l'essentiel de la publicité ciblée mise en œuvre sur internet ne requiert pas, à ce jour, l'identification d'une personne déterminée. Autrement dit, pour une régie publicitaire ou un annonceur, l'identité de la personne visée importe peu dès lors que son profil de consommation est en adéquation avec l'offre³.

Les lignes directrices relatives à la conformité des sites web à la loi 09-08 constitue un outil pratique au service des entreprises et des organismes qui exploitent un site web utilisant des données personnelles. Les recommandations exposées dans ce texte sont élaborées à partir des dispositions de la loi 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et ses textes d'application. Il en résulte que tout responsable de site web qui collecte et traite des données à caractère personnel est tenu par la loi 09-08 de notifier à la CNDP les traitements mis en œuvre sur ledit site.⁴ Conformément au principe de proportionnalité, il ne faut collecter et traiter que les données strictement nécessaires à la réalisation des finalités du traitement poursuivies par le responsable du site web. Des mesures doivent être mises en œuvre afin d'assurer la confidentialité et la sécurité

¹Jean-Pierre CLAVIER, *Op.cit.*, p. 65.

²N. LANERET et A. BAUDEQUIN, « Données personnelles quelle circulation demain », in IP/IT, N° 12, Décembre 2017, Dalloz, p. 240.

³Valérie-Laure BENABOU, « Essai de prospective juridique sur les modes de valorisation des données : fonds informationnel, droit à la probabilité et dividende de la donnée » in *Le Big Data et Le Droit*, Ouvrage collectif sous la direction de Florence G'SELL, Dalloz, Paris, 2020, p. 219.

⁴Khalid ENNASHI, *Op.cit.*, p. 61.

des données personnelles enregistrées pour éviter qu'elles soient détruites, déformées, endommagées ou accessibles à des tiers non autorisés.

Lorsque le responsable du site web fait appel à un sous-traitant pour traiter des données personnelles, il est tenu de choisir un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité techniques et organisationnelles. D'autre part, la réalisation des traitements en sous-traitance doit être régie par un contrat ou un acte juridique qui lie le sous-traitant au responsable du site web. Quand un site est amené à traiter les données personnelles, celles-ci ne doivent être conservées que le temps nécessaire à la réalisation de la finalité du traitement.

Une campagne de contrôle a été entamée par la CNDP en 2014. Cette campagne qui a visé 104 sites web s'est déroulée en deux phases. Les chiffres obtenus montrent que 22% des sites web affichent une mention conforme aux exigences de la loi. La mention est présente, mais incomplète, dans 28% des cas. Par contre, 50% des sites contrôlés n'affichent pas de mention relative à la protection des données à caractère personnel. Il est constaté que 1% des sites web au Maroc se soucient de recueillir le consentement des internautes à collecter et traiter leurs données personnelles. Dans 80% des cas, le site web n'évoque nulle part la demande de consentement, et dans 19% des cas, la présence de la demande est aléatoire, puisqu'elle ne figure pas sur la totalité des formulaires de collecte des données. L'opération de contrôle de la Commission nationale montre que l'obligation d'informer les personnes concernées au moment de la collecte de leurs données personnelles dans les termes prévus par la loi est très rarement respectée (1%). Les informations sur l'identité du responsable du site web, les finalités du traitement, les destinataires des données collectées et autres renseignements ne sont que communiquées que dans 28% des cas. Ces informations sont totalement absentes dans 71% des sites web.

Enfin le contrôle a révélé d'autres irrégularités par rapport à la loi. Elles concernent le principe de proportionnalité (collecte excessive de certaines données et injustifiée par le traitement), les règles de la prospection directe et l'utilisation des cookies¹. En effet, un site internet qui utilise des cookies faisant appel à des données personnelles doit recueillir le consentement de l'internaute avant le dépôt de ces cookies². De même qu'il doit préciser la

¹Communiqué de presse du 19/09/2014 sur l'opération de contrôle de sites web consulté 19-10-2021 à 10h sur <https://www.cndp.ma/fr/presse-et-media/communiqu%C3%A9-de-presse/253-communiqu%C3%A9-de-presse-19-09-2014.html>

²Plusieurs solutions existent en pratique pour gérer efficacement l'installation des cookies et les échanges d'informations permis par ces derniers. Ces derniers peuvent être mises en place soit par les professionnels à

finalité de l'utilisation des cookies et expliquer à l'internaute les moyens de s'y opposer. Plusieurs solutions existent en pratique pour gérer efficacement l'installation des cookies et les échanges d'informations permis par eux. Ces derniers peuvent être mises en place soit par les professionnels à destination des utilisateurs, soit par les internautes eux-mêmes¹.

A partir de 2016, un deuxième contrôle a été opéré qui a concerné 340 sites internet. Sur ces 340 sites, 33 sites ont fait l'objet de lettres d'avertissement aux opérateurs concernés, et 7 sites ont fait l'objet de procès-verbaux adressés aux tribunaux de commerce compétents. Les contrôles effectués ont fait apparaître des écarts par rapport à la réglementation comme l'absence de l'identité et des coordonnées du fournisseur, la présence d'une publicité trompeuse ou de nature à induire en erreur, l'absence de rappel des conditions contractuelles de vente avant validation de l'offre et autres irrégularités. D'où la nécessité de s'intéresser à ce domaine dans le processus de garantir une confiance numérique².

Sous-section 4 : Le contrat de *Cloud computing*.

Le *Cloud computing* qui signifie littéralement en français « informatique en nuage », désigne le transfert, vers le « nuage Internet », de données et d'applications qui étaient jusqu'alors situées sur les serveurs et ordinateurs des professionnels et des particuliers. Selon la Norme ISO/IEC le *Cloud computing* est : « *Un modèle qui permet d'accéder par le réseau à une masse évolutive et élastique de ressources physiques ou virtuelle et qui implique un service à la demande et une administration à la demande*³ ». Autrement dit, le *Cloud*

destination des utilisateurs, soit par les internautes eux-mêmes. Nous nous limiterons à deux exemples qui illustrent bien les solutions techniques qui existent aujourd'hui. Le premier type consiste en une plateforme tierce et indépendante permettant à l'internaute d'exprimer ses choix pour l'ensemble des cookies installés sur son poste. Une connexion à ce site sans identification préalable, permet un scan de l'ensemble des cookies présents sur le poste et l'identification de ceux permettant une publicité comportementale. Un clic sur chaque cookie permet d'obtenir plus d'informations sur la société émettrice. L'internaute peut autoriser ou refuser au cas par cas, ou la totalité des cookies installés. Le deuxième type consiste à proposer à l'internaute un espace cliquable dans la bannière publicitaire qui permet d'accéder à l'espace de configuration des publicités ciblées. Certaines régions disposent de leurs propre système (Google, Microsoft..) ; d'autres ont recours à ces technologies dans le cadre de licences.

¹Jean-Baptiste AUROUX, « La publicité ciblée sur internet à l'épreuve du droit des données à caractère personnel » in L'entreprise à l'épreuve du droit de l'Internet, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014, p. 78.

²H.G., « Protection du consommateur: ce qui va changer dans la loi », in Media24, 26 Novembre 2019 consulté le 14-10-2021 à 15h sur <https://medias24.com/2019/11/26/protection-du-consommateur-ce-qui-va-changer-dans-la-loi/>

³La norme ISO 17788 définit les cinq types d'intervenant sur le marché du cloud computing (auditeurs, partenaires, clients, fournisseurs, intermédiaires), les trois types de services proposés (infrastructure as a service

computing offre la possibilité de concevoir une architecture réseau et applicative sur mesure ainsi qu'un traitement des données quasi instantané.

Le *Cloud computing* permet de limiter les ressources internes de l'entreprise en les mutualisant. Pour certains, le Cloud serait la solution pour disposer d'une puissance sans limite et adaptable immédiatement à la demande. Le *Cloud computing* constitue une évolution majeure dans la gestion des systèmes d'information. Il présente plusieurs avantages : la simplicité du service à la demande, la flexibilité, l'accès léger, la vitalisation des ressources, et paiement proportionnel à l'usage qui est fait¹.

Néanmoins, comme toute technique, le *Cloud computing* présente des dangers et a des inconvénients, dont une illustration spectaculaire a été donnée le 12 Décembre 2014 lorsqu'une panne informatique a touché l'une des installations du contrôle aérien britannique *Nats*, basée à *Swanwick* dans le sud-est de l'Angleterre ; l'ensemble des aéroports britanniques ont été paralysés pendant plusieurs heures et, par contre-coup, de nombreux aéroports d'autres pays ont été perturbés. La commodité du *Cloud* conduit à négliger les sauvegardes par des moyens simples².

Il faut tout d'abord noter qu'une entreprise qui se lance dans l'aventure du *Cloud* doit en tirer les conséquences comptables et fiscales³. Les offres de *Cloud* prennent généralement la forme d'abonnements, modifiant ainsi la gestion des immobilisations corporelles et incorporelles au sein d'une entreprise⁴. Le *Cloud computing* n'est pas sans bouleverser les contrats traditionnels du droit de l'internet tels que le contrat de licence de logiciel. Ainsi, il permet aux entreprises de disposer de leurs applications via internet, sans que le logiciel soit

ou « IaaS », platform as a service ou « PaaS » et Software as a Service ou « SaaS ». Cette norme a été publiée en Octobre 2014 par ISO/IEC JTC 1/SC 38 Plateformes et services d'applications distribuées.

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 134.

²Philippe LE TOURNEAU, *Op.cit.*, p. 461.

³B. DELMAS-LINEL, B. SABAILA et F. LIZZIT, « Promesses du cloud computing et protection des données à caractère personnel : la remise en question du cadre juridique français et européen », in Lexbase Hebdo, N° 292, 12 avril 2012, éd. Affaires, p. 113.

⁴Il existe trois types de services de Cloud :

- Software (SaaS) : Le prestataire fournit des applications directement utilisables à distance. Le client consomme le logiciel à la demande. Le logiciel est hébergé chez le fournisseur.
- Platform as a Service (PaaS): Le prestataire met à disposition un environnement de développement, permettant à une direction des services informatiques de développer ses applications.
- Infrastructure as a Service (IaaS) : Le prestataire met à disposition une infrastructure à distance avec des capacités de traitement à géométrie variable permettant de ne pas anticiper ses besoins plusieurs mois à l'avance. Afin de choisir l'offre la plus appropriée, l'entreprise doit réaliser en amont un important travail de définition du périmètre de ses besoins. Généralement appelé audit ou mission de cadrage, ce travail préalable ne doit pas être négligé car changer de modèle en cours d'élaboration peut s'avérer compliqué et coûteux.

préalablement installé sur le poste de chacun des utilisateurs. De ce fait, nous allons essayer d'étaler tous les éléments essentiels composants du contrat *Cloud* (Paragraphe 1) ainsi que les données hébergées dans le *Cloud* (Paragraphe 2).

Paragraphe 1 : Les éléments du contrat de *Cloud computing*.

La préparation du contrat *Cloud* commence par un audit. Celui-ci détermine d'abord les applications, services ou traitement devant bénéficier du service. Puis il identifie les traitements sensibles qui seront effectuées à distance, ainsi que les garanties à obtenir. Un cahier des charges détaille les spécificités techniques et fonctionnelles attendues, il mentionne également les exigences relatives à la maintenance, à la traçabilité et à la reprise des données, ainsi qu'à leurs confidentialité et à leur sécurité. Pour une société importante, le contrat sera évidemment individualisé. Mais la majorité des contrats *Cloud computing* sont des contrats types, à prendre ou à laisser, avec tout au plus quelques modifications marginales.

Les obligations du prestataire sont généralement qualifiées de moyens. En effet, face à la rapidité des évolutions technologiques et à la complexité des réseaux de communication, il est difficile pour le prestataire de garantir que son service fonctionnera sans discontinuité et sans aucune anomalie. Cette obligation de moyen limitera en conséquence la responsabilité du prestataire aux seuls dommages directs résultant d'un manquement de sa part, il est d'ailleurs stipulé une clause limitative de responsabilité¹. Le principal engagement du prestataire est d'assurer la disponibilité et l'accessibilité des données externalisée.

Dans le cas où le client souhaite que le service fonctionne en permanence (24h/24H - 7j/7j), il pourra être envisagé de négocier des garanties de niveaux de service précis qui pourront être annexées au contrat de *Cloud computing*. Dans les cas où les serveurs ne seraient pas directement hébergés par un éditeur, le niveau d'obligation de l'hébergeur peut avoir des conséquences sur la responsabilité de l'éditeur vis-à-vis de l'utilisateur final. Dans cette hypothèse, les éditeurs auront le plus grand intérêt à prévoir une convention de niveau de service avec pénalités, qui pourra être annexée au contrat². Le contrat doit indiquer en cas de recours à des sous-traitants, les noms de ceux-ci et garantir qu'ils respecteront les engagements, tant de sécurité que de performance. Un plan de sécurité peut être élaboré.

¹Philippe LE TOURNEAU, *Op.cit.*, p. 462.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 137.

De plus, un système de secours doit permettre d'assurer la continuité de l'activité ou, à tout le moins, sa reprise rapide. Il peut être prévu un comité de pilotage.

La détermination du prix et des modalités de paiement dans un contrat de *Cloud* est très variable. Les prestataires prévoient généralement des formules de type *pay as you go*, qui font varier le prix en fonction de la capacité consommée, du nombre d'utilisateurs, du nombre de boîtes de messagerie, etc. Le client pourra préférer un forfait, dont le montant sera fixé au regard des mêmes critères que ceux précités. La clause de prix devra également anticiper les éventuels coûts additionnels liés notamment à l'évolution de la qualité de la prestation ou au contraire aux besoins du client. Le client aura intérêt à prévoir une clause de *benchmarking* lui permettant de procéder régulièrement à des comparaisons de prix entre ceux pratiqués par son prestataire et ceux affichés par ses concurrents pour les mêmes services.

Dans le cas d'un contrat international, il sera également pertinent de prévoir des dispositions fiscales, relatives notamment aux questions de retenue à la source¹. Par ailleurs, la dimension internationale du contrat de *Cloud* nécessite impérativement de préciser quelle loi régit le contrat. Par automatisme, le client sera tenté de recourir à la loi nationale. Cependant, en fonction des enjeux du contrat, d'autres législations peuvent s'avérer plus intéressantes.

Concernant la durée du contrat, il est possible de prévoir une durée déterminée, par exemple pour quelques mois seulement. Une durée indéterminée peut aussi être stipulée, moyennant un préavis dont la durée peut varier. Il est en outre possible de prévoir que la date d'entrée en vigueur du contrat et celle de sa prise d'effet diffèrent, notamment si le client doit procéder à des modifications d'ordre technique, par exemple pour mettre son système en conformité avec le réseau du prestataire. Aussi, il est d'usage dans les contrats de *Cloud* que le client puisse résilier le contrat en cas de manquement répété du prestataire à ses obligations d'accessibilité et de disponibilité². Enfin, le contrat de *Cloud computing* comporte souvent dans leurs conditions générales une clause de suspension de service, autorisant le prestataire sous certaines conditions à suspendre son service tant que le client n'exécute pas ses obligations, application de l'exception d'inexécution.

¹Voir infra p. 225.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, pp. 139-140.

Paragraphe 2 : Les données hébergées dans le *Cloud*.

Le recours au *Cloud computing*, dans le cadre des services proposés par les prestataires informatiques, présente des avantages considérables. Cependant, les risques liés à l'usage du *Cloud* nécessite de faire preuve d'une vigilance particulière, afin de tenir notamment compte des contraintes réglementaires relatives aux données personnelles¹. Le *Cloud computing* a introduit l'idée de mutualisation, et l'utilisation de ressources matérielles diverses et disséminées dans d'innombrables *data centers* situés dans différents pays du monde. De telles solutions constituent un facteur d'aggravation des risques d'atteinte à la confidentialité des données. En droit, ce sont les garanties apportées par le cadre juridique d'un pays désigné qui déterminent les formalités préalables à la mise en œuvre d'un traitement de données et donc les conditions de sa licéité. Qu'il s'agisse de niveau de service, d'interopérabilité de plan de réversibilité de portabilité des données, la loi 09-08 apporte une vision pragmatique aux acteurs².

Le stockage des données dans le *Cloud* est un moyen facilitant l'accès aux données à distance, et ce quel que soit le point d'accès aux données par *smartphone*, une tablette ou différents postes informatiques. Toutefois, ce stockage génère des risques. Ces risques spécifiques peuvent en effet avoir des effets d'autant plus dommageables que les données susceptibles d'être traitées via le *Cloud computing* peuvent être des données à caractère personnel, des données issues du *big Data*, dont l'exploitation et l'association à d'autres données peuvent présenter des enjeux commerciaux majeurs, des données critiques pour l'activité du client, ou encore des données couvertes par le droit du producteur de base de données ou tout autre droit de propriété intellectuelle.

Bien évidemment, les parties à un contrat de prestations de services informatiques mise en œuvre par le *Cloud* devront s'assurer que leurs relations contractuelles sont suffisamment encadrées pour prévenir toute difficulté découlant de la spécificité du *Cloud*. Et afin de vérifier le respect des critères de sécurité et de géolocalisation des données, une clause imposant l'audit pourra être stipulée. De même, le client pourra prévoir une clause imposant au prestataire de lui transmettre une information complète concernant les aspects techniques

¹G. VERCKEN, « La révolution du Cloud : A quoi sert encore le contrat ? », in IP/IT, N° 10, Octobre 2016, Dalloz, p. 451.

²C. ZOM, « Contrats de Cloud computing et Données personnelles : éléments de rénovations des techniques contractuelles », in IP/IT, N° 10, Octobre 2016, Dalloz, p. 454.

de la prestation¹. Le client devra mesurer les risques que constitue l'externalisation de données particulièrement sensibles dans certains pays². La perte de ces données, ou encore l'éventualité d'une attaque informatique sont autant de situations qu'il convient de prévoir dans un contrat de *Cloud computing*.

Dans l'environnement *Cloud*, la question des données personnelles doit faire l'objet d'une attention renforcée de la part du bénéficiaire de la prestation informatique comme de la part du prestataire. En effet, le traitement de données personnelles via le *Cloud* peut notamment impliquer d'une part la circulation des données personnelles en dehors du Maroc et d'autre part des risques accrus d'atteinte à la sécurité et à l'intégrité des données personnelles en dehors de l'entreprise.

S'agissant de la circulation des données personnelles en dehors du territoire marocain. La loi 09-08 prévoit l'obligation à la charge du responsable de traitement d'informer la personne concernée que des données personnelles la concernant sont susceptibles d'être transférées en dehors du Maroc³, et restreint le droit de transférer des données personnelles qu'aux seuls pays figurant sur la liste établie par la CNDP⁴. A défaut de présence sur la liste il faut un consentement exprès de la personne concernée par le transfert, une application d'un accord international auquel le Maroc fait partie et une autorisation expresse de la CNDP. Or, la mise en œuvre de prestations informatiques par le biais du Cloud implique généralement que le bénéficiaire de la prestation n'a pas connaissance de la localisation géographique des données stockées sur le Cloud et n'est pas en mesure de vérifier ou d'empêcher techniquement que les données soient transférées en dehors du Maroc, et

¹Une attention particulière pourra être portée par le client aux règles contraignantes d'entreprise (Binding Corporate Rules, « BCR ») éventuellement mises en place par le prestataire au sein de son groupe. Ces BCR, qui ont vocation à être préalablement validées par les autorités nationales en charge de la protection des données vers un pays tiers n'assurant pas un niveau de protection.

²B. DELMAS-LINEL et C. MUTZ, « Le cloud computing à l'épreuve des souverainetés nationales. Faut-il avoir peur du USA Patriot Act ? », in RLDI, N° 090, 2013, p. 53.

³V. art. 43 de la loi 09-08.

⁴La liste établie par la CNDP désignant les pays offrant un niveau de protection suffisant et conforme aux exigences de la législation marocaine comprend les pays suivants : Allemagne, Autriche, Belgique, Bulgarie, Canada, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Liechtenstein, Lituanie, Luxembourg, Malte, Norvège Pays-Bas, Pologne, Portugal, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse. Délibération N°236-2015 du 18 Décembre 2015 portant modification de la délibération n°465-2013 du 06 Septembre 2013 établissant la liste des Etats assurant une protection suffisante de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel.

potentiellement vers des pays n'offrant pas un niveau de protection adéquat¹. En pratique, il est donc fortement recommandé au bénéficiaire des services informatiques de prévoir contractuellement quels seront les lieux de stockage des données, ou à tout moins quels sont les pays dans lesquels les données seront susceptibles d'être stockées. Au minimum, il est fortement recommandé d'exclure toute possibilité de stockage dans des pays n'offrant pas un niveau de protection adéquat au sens de la loi 09-08.

S'agissant de la sécurité et de l'intégrité des données personnelles en dehors de l'entreprise, tout transfert de données en dehors des locaux d'une entreprise soulève la question du respect de la confidentialité. En fonction du degré de confidentialité ou plus généralement du secteur d'activité, les informations transférées nécessiteront des niveaux de protection différents, qu'il sera indispensable de préciser contractuellement. Il est toutefois souhaitable de ne pas figer ces niveaux de sécurité afin de garantir une adaptabilité rapide de la protection des données en l'absence même de tout avenant contractuel.

Le client devra prévoir non seulement le niveau d'engagement de son prestataire, mais également, afin d'éviter des mécanismes de responsabilité en chaîne, celui de ses salariés, de ses éventuels, sous-traitants ou fournisseur. A cet effet, il est recommandé d'indiquer une durée de protection et de sécurisation des données supérieure à la durée du contrat. En cas de rupture du contrat par l'une ou l'autre des parties, le client devra disposer d'une période de protection supplémentaire afin d'envisager sereinement les nouvelles modalités de protection de ses données. Une clause d'audit pourra aussi être prévue afin d'évaluer régulièrement les niveaux de sécurité et de confidentialité. Enfin il est possible de stipuler une clause de réversibilité, avec pour objectif fixer les modalités de restitution des données, les transferts de connaissance, la comptabilité des données entre l'ancienne et la nouvelle structure, etc.

.

¹T. LANGE, « Cloud computing et Données personnelles : Les clauses à maîtriser », in IP/IT, N° 10, Octobre 2016, Dalloz, p. 459.

Chapitre II

La propriété intellectuelle et la transformation digitale de l'entreprise

Le numérique apparaît comme un levier déterminant de la compétitivité des entreprises par les économies des coûts qu'il peut engendrer, mais surtout parce qu'il révolutionne l'innovation. Cette innovation a un rapport direct avec la propriété intellectuelle de l'entreprise. En effet, dans cette économie numérique, la propriété intellectuelle n'a jamais été aussi importante. Les droits de propriété intellectuelle constituent de véritables droits économiques. Or le caractère exclusif qui les distingue et les contrats dont ils sont l'objet soulèvent des interrogations sur les rapports entre le numérique et le droit de la propriété intellectuelle¹.

Dans sa diversité, la propriété intellectuelle, à travers la notion de marque de droit d'auteur de traçabilité des contributions et des technologies, peut être un formidable outil de transition numérique des entreprises. Cependant, les liens entre la transformation digitale et la propriété intellectuelle ne se réduisent pas à la question de savoir si la propriété intellectuelle constituerait un frein ou un levier pour la transformation digitale des entreprises. Les deux sujets sont intrinsèquement liés. La propriété intellectuelle se révèle être une des composantes de la transformation digitale de l'entreprise en étant tout à la fois un actif immatériel et un instrument de protection².

De plus, la propriété intellectuelle est un levier complexe. La notion de propriété intellectuelle repose sur l'attribution de droits exclusifs accordés sur des créations intellectuelles³. En effet, lors de la transformation numérique de l'entreprise, nombreux sont les créations intellectuelles numériques qui doivent faire l'objet d'une protection juridique suffisante (Section 2) c'est le cas par exemple de la création d'un site web, celle-ci ne relève pas uniquement de la conception et de la réalisation de pages html encore faut-il lui donner un nom qui désignera son adresse et permettra ainsi aux utilisateurs de l'identifier sur le

¹S. EL HAJOU, « Les interférences entre le droit de la concurrence et le droit de la propriété intellectuelle », in *Revue marocaine de droit économique*, N° 1 Octobre, 2007, p. 79.

²C. BAUJARD, « Formation numérique : quel dispositif juridique de protection des savoirs ? », in *Revue Recherches en Sciences de Gestion-Management*, N° 94, 2013, p. 162.

³Alain GIRARDET, « Articuler les droits de propriété intellectuelle sans les confondre ou la difficile recherche de frontières ! » in *L'articulation des droits de propriété intellectuelle*, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2011, p. 116.

réseau internet afin de pouvoir y accéder. C'est ce que l'on appelle le nom de domaine (Section 1).

Section 1 : Le nom de domaine.

Les noms de domaines constituent un type de signe spécifique à l'environnement numérique, apparu au sein des valeurs immatérielles. Le système des noms de domaines a pour fonction d'aider à la navigation les utilisateurs sur le réseau internet¹. L'origine des noms de domaines est avant tout technique. En effet, le réseau internet relie différentes ressources tant matérielles (serveurs) qu'intellectuelles (documents). Or, chacune de ces ressources est identifiée de manière unique, au moyen d'une adresse dite IP (Internet Protocol)² composée d'une suite de chiffres séparée par des points. A titre d'exemple, l'adresse IP de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) est 195.92 249,55, mais vu que cette adresse est difficilement mémorisables et utilisables par les internautes, elle a été traduite en langage logique qui est www.wipo.int et cela par des serveurs composant le *DNS*³ qui assurent la correspondance entre ces noms de domaines et les adresses numériques⁴.

On peut donc définir un nom de domaine comme une dénomination unique à caractère universel qui permet de localiser une ressource ou un document sur internet, et qui indique la méthode pour y accéder, le nom du serveur et le chemin à l'intérieur du serveur. Autrement dit, le nom de domaine est la dénomination électronique de l'entreprise et son adresse sur la toile. Il remplit la double fonction du nom commercial et de l'enseigne⁵.

Le nom de domaine se compose de deux parties : le radical (nom de second niveau, *Second Level Domain* ou *SLD*) c'est la partie figurant avant le point composé d'un nom commercial ou d'une marque préexistante qui permet son identification, et l'extension (nom de second niveau, *Top Level Domain* ou *TLD*) c'est la partie finale figurant après le point. Par exemple, dans le nom de domaine www.wipo.int « wipo » est le domaine de second

¹Jacques AZEMA et Jean-Christophe GALLOUX, Droit de la propriété industrielle, Dalloz, 8^{ème} éd. Paris, 2017, p. 314.

²Rappelons que, techniquement une adresse IP n'identifie pas une personne, mais un ordinateur. Seul le fournisseur d'accès est en mesure d'associer une adresse IP et le titulaire de l'abonnement. L'identification par le fournisseur d'accès demeure au surplus approximatif la personne utilisant l'ordinateur n'étant pas nécessairement l'utilisateur de l'abonnement.

³Domain Name Système est un serveur utilisé pour héberger les données nécessaires à la mise en correspondance des adresses IP et des noms de domaine.

⁴Luc GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, *Op.cit.*, p. 632.

⁵Philippe LE TOURNEAU, *Op.cit.*, p. 579.

niveau et « .int » est le domaine de premier niveau. La mention « www. » signifie *World Wide Web*, indique quant à elle que le nom de domaine donne accès à un service web.

En effet, l'explosion de l'internet grand public et du commerce électronique ont propulsé le nom de domaine à l'avant de la scène numérique. Il s'agit désormais d'un actif de l'entreprise précieux et convoité qui nous pousse à étudier ses modalités d'attribution (sous-section 1). Mais, au-delà de l'attribution, ce pose le problème de la réglementation des noms de domaine (Sous-section 2).

Sous-section 1 : Attribution du nom de domaine.

Le système des noms de domaines appelé système de nommage comprend des *generis top level domains* (*gTLD*) et les *country code top level domains* (*ccTLD*)¹. Les *gTLD* sont assortis d'un suffixe générique correspondant à la nature de l'organisme réservataire et à son activité. Ainsi, les plus connus sont « .com » pour les sites à caractère commercial, « .org » pour les organisations à but non lucratif et « .edu » pour les institutions d'éducation. Les *ccTLD* comportent un suffixe géographique indiquant le pays d'où est originaire le site, ainsi « .ma » pour le Maroc, « .fr » pour la France, « .de » pour l'Allemagne, etc. chaque extension comporte un organisme gestionnaire qui met en place une charte de nommage et enregistre les noms de domaine qu'il répertorie dans une base de données. Dans certains cas, une zone géographique recouvre plusieurs pays appelée extensions régionales telles que « .eu » pour les pays européens ou encore « .asia » pour les pays asiatiques.

Suite à l'encombrement des noms de domaines, la création de nouveaux domaines génériques s'est imposée. Ainsi, il y a eu la délocalisation des noms de domaines *gTLD* « .edu », « .gov », « .int » de manière à en faire des noms de pays et, d'autres parts, de créer sept nouveaux domaines génériques de premier niveau (*gTLD*) pour permettre une meilleure identification du caractère du site et pour diminuer les enregistrements sous « .com ». Ainsi à titre de solution alternative au choix du « .com », il proposait « .store » pour les activités liées à la vente de biens, « .web » pour les entités dont l'activité principale s'exerce sur l'internet.

En parallèle avec ces créations, l'Organisation Mondiale de la Propriété Intellectuelle (OMPI) a publié dans un rapport en date du 30 Avril 1999² une série de recommandations à

¹Plus de 370 millions de noms de domaine sont déposés dans le monde auprès de bureaux d'enregistrement.

²OMPI, Rapport final concernant le premier processus de consultations de l'OMPI sur les noms de domaines de l'internet, Genève, 30 avril 1999.

l'intention de l'ICANN¹. L'OMPI s'est montrée très réservée sur la création de nouveaux noms de domaines génériques, estimant qu'une telle introduction risquerait d'amplifier le phénomène du *cybersquat*². C'est pourquoi elle ne l'a préconisée qu'à la double condition que l'ensemble des recommandations³ formulées dans son rapport soient adoptées et que cette introduction de nouveaux *gTLD* se fasse de manière progressive et réfléchie, permettant d'en contrôler et d'en évaluer les conséquences⁴.

En 2008, à l'occasion de sa réunion internationale, l'ICANN a annoncé une nouvelle étape dans le processus de libéralisation des choix des noms de domaine pour que les internautes puissent créer l'extension d'adresses internet de leur choix, en caractères latins ou non latins. Elle a finalement autorisé pour la première fois, en Mai 2010, l'écriture des adresses *URL*⁵ avec des alphabets non latins. Quatre extensions géographiques ont déjà été acceptées avec la capacité d'écriture dans leurs alphabets. Il s'agit de l'Egypte, la Russie, l'Arabie saoudite et les Emirats arabes unis⁶. De ce fait, nous allons procéder à l'étude des organismes attributifs des noms de domaine sur internet (Paragraphe 1) ainsi que leurs modalités d'attribution (Paragraphe 2).

Paragraphe 1 : Les organismes attributifs des noms de domaines sur Internet.

A l'échelle internationale, l'organisme chargé de l'administration du réseau internet est une société privée américaine à but non lucratif dénommée *Internet Corporation for Assigned Names and Numbers (ICANN)*, seule compétente pour administrer le système au plan mondial⁷. Fondée en 1998, elle fut chargée par le département du commerce du gouvernement des Etats-unis⁸ pour l'attribution des adresses IP et la gestion du système des noms de domaines¹.

¹Internet Corporation for Assigned Names and Numbers.

²Voir infra p. 286.

³Ces recommandations se résume dans : les procédures améliorées d'enregistrement des noms de domaine, résolution efficace des différends, et mécanisme d'exception ou d'exclusion pour les marques déposées célèbres ou notoirement connues.

⁴Christiane FERAL-SCHUHL, *Op.cit.*, p. 975.

⁵Uniform Resource Locator : Une URL est simplement l'adresse d'une ressource donnée, unique sur le Web.

⁶Pour la première fois, l'organe de régulation acceptait des mots dans toutes les langues non latines, telles que le chinois ou l'arabe.

⁷Christiane FERAL-SCHUHL, *Op.cit.*, p. 971.

⁸Cette organisme a fait, depuis 2003, date du Sommet mondial sur la société de l'information organisé par l'Union internationale des télécommunications, l'objet de critiques, certains considérant qu'il est sous contrôle du gouvernement américain. Le 14 Mars 2014, la National Télécommunications and Information Administration, agence du ministère du Commerce américain, a indiqué qu'elle ne renouvellerait pas le contrat avec l'ICANN fin 2015. L'agence précise que la nouvelle régulation ne devra dépendre des gouvernements mais être organisée par

L'ICANN délègue la fonction d'encadrement et de gestion de l'attribution des noms de domaines à des registres régionaux, répartis dans cinq zones au niveau mondial, chacun étant gérée par un registre particulier ; la zone Europe est gérée par le RIPE-NCC², la zone Asie-Pacifique est gérée par l'APNIC³, la zone Amérique est gérée par l'ARIN⁴, la zone Afrique est gérée par l'AFRINIC⁵ et la zone Amérique Latine et Caraïbes est gérée par la LACNIC⁶. L'ICANN a également une fonction de résolution des litiges relatifs aux noms de domaines. Elle a ainsi créé un système de résolution des litiges non contentieux dénommé UDRP⁷. Enfin, l'ICANN gère le système de nommage internet et sa disponibilité. Elle participe aux créations de noms de domaines internationalisés⁸ et accrédite les offices d'enregistrements des noms de domaines appelé *registrars*.

A l'échelle nationale, originellement, l'ANRT est l'administrateur du domaine «.ma» auprès de l'ICANN⁹. C'est un établissement public doté de la personnalité morale et de l'autonomie financière dont la mission est de représenter les titulaires des adresses internet correspondant au territoire national auprès des instances internationales gouvernementales ou non gouvernementales en charge de la gestion internationale des noms de domaines internet. L'ANRT assure la gestion administrative, technique et commerciale des noms de domaine

la communauté des utilisateurs, les gouvernements et les entreprises. Mais cette décision a fait l'objet d'un moratoire faute pour l'ICANN de vouloir se soumettre à une autre forme de contrôle. Puis, en Mars 2016 à la Conférence de Marrakech, l'ICANN a présenté un plan de transition. Le 30 Septembre 2017, le Sénat américain a finalement accepté qu'il soit mis un terme au contrat, actant ainsi le transfert à la communauté internet mondiale à la supervision de l'ICANN. La fin du contrat liant l'ICANN au gouvernement américain a ainsi pris fin le 30 Septembre 2016.

¹L'objet social de l'ICANN définit sa mission : « Réduire la charge des gouvernements et promouvoir la stabilité institutionnelle de l'Internet : en coordonnant l'allocation de paramètres techniques dans le but de préserver la connectivité internationale de l'Internet ; exécutant et supervisant les fonctions associées à la coordination de l'espace des adresses Internet (IP) ; exécutant et supervisant les fonctions associées à la coordination du système, de noms de domaine, y compris le développement des règles définissant les circonstances dans lesquelles de nouveaux noms de domaine de premier niveau sont ajoutés aux serveurs racines ; supervisant l'exploitation du serveur gérant la racine principale DNS ».

²Réseaux IP Européens - Network Coordination Centre.

³Asia-Pacific Network Information Centre.

⁴American Registry for Internet Numbers.

⁵African Network Information Centre.

⁶Latin America and Caribbean Network Information Centre.

⁷ Voir infra p. 369.

⁸ Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, pp. 34-35.

⁹V. art. 7 de la décision ANRT/DG/N°12/14 du 21 Novembre 2014 relative aux modalités de gestion administrative, technique et commerciale des noms de domaine Internet «.ma».

«.ma»¹. Sa mission est formellement établie par la loi 24-96 relative à la poste et aux télécommunications du 7 août 1997, telle qu'elle a été modifiée et complétée par la loi 29-06 du 17 avril 2007.

L'ANRT assure plusieurs missions à savoir ; la définition de la réglementation régissant la gestion du domaine national «.ma» et le suivi de sa mise en œuvre, la mise en place de règles de gestion administrative et technique, dans des conditions transparentes et non discriminatoires, la mise en place des spécifications techniques nécessaires pour une gestion technique du domaine «.ma» répondant aux besoins de tous les utilisateurs et des prestataires, et facilitant l'enregistrement de nouveaux noms de domaine, la protection des utilisateurs finaux quant aux usages abusifs des noms de domaine «.ma» , la mise en place de règles régissant la gestion de conflits autour de l'utilisation de noms de domaine «.ma» , enfin la garantie de la continuité des services d'enregistrement des noms de domaine «.ma»².

Paragraphe 2 : Les modalités d'attribution des noms de domaines.

La première action de l'ICANN depuis sa création a été de mettre en place la privatisation des *gTLD* qui sont «.com», «.org» et «.net» en Avril 1999, ouvrant ainsi le marché de l'enregistrement de ces *gTLD* à la concurrence. A cet effet, près d'un millier de *registrars* ont été agréés par l'ICANN et sont habilités à attribuer des noms de domaines. L'enregistrement d'un nom de domaine, soumis au respect de conditions de fond, intervient à l'issue d'une procédure particulière³.

A coté de ces conditions techniques, il existe un certain nombre de conditions juridiques relatives à l'enregistrement des noms de domaines. Ces conditions sont essentiellement issues des règles applicables aux *ccTLD*, l'ICANN n'imposant que peu de restrictions à la liberté d'enregistrement pour les *gTLD*. On peut les classer en deux catégories, les noms de domaines ne doivent pas porter atteinte aux droits des tiers d'une part, d'autre part ils doivent être licites.

¹H. BOUAYAD, « Autorité de concurrence et autorités de régulation du secteur des technologies de l'information et des communications « TIC » », in Revue Marocaine de Droit Economique, N° 1, Octobre 2007, p. 68.

² ANRT, « Présentation », consulté le 02-04-2022 à 10h sur <https://www.anrt.ma/e-services/presentation>

³المختار لمجردي، الحماية القانونية للمصنفات الرقمية، رسالة لنيل الدكتوراه في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، اكدال الرباط، السنة الجامعية 2016-2017، ص. 200.

L'ICANN confie la gestion des TLD à des organismes appelés registres, choisis sur la base de leur fiabilité, par le biais de contrats de nature variable, qualifiés de *Memorandum of understanding*¹ ou de *Sponsorship Agreement*². L'exploitation des ccTLD est dans la plus part des cas confiée à des organismes publics des Etats concernés. C'est ainsi que le registre choisi par l'ICANN pour la gestion du domaine «.ma» est l'ANRT. A leur tour, les registres concluent des contrats avec les *registrars* ou bureaux d'enregistrement, qu'ils accréditent. Ces bureaux, qui jouent le rôle d'intermédiaires entre l'office d'enregistrement et les titulaires de noms de domaines, sont chargés de traiter les demandes d'enregistrement, de renouvellement, de transfert ou de suppression de noms de domaines. Ils proposent souvent, par ailleurs, d'autres prestations telles que l'hébergement de ressources internet ou encore la création de sites web³.

Comme chaque nom de domaine est unique, il convient de procéder à une recherche d'antériorité pour vérifier sa disponibilité. A cet effet, le déposant dispose de la base de données WHOIS⁴. Une fois la disponibilité vérifiée, il est possible d'enregistrer le nom de domaine en se conformant aux stipulations contractuelles imposées au déposant. S'agissant des principaux *gTLD* notamment le «.com», la règle applicable est celle du premier arrivé, premier servi. Ceci veut dire que chaque requérant peut choisir le nom qu'il souhaite, à condition qu'il n'ait pas déjà été enregistré. C'est-à-dire que le premier qui a choisi un nom de domaine déterminé sera le seul à pouvoir l'utiliser à l'avenir.

En effet, aucune formalité préalable à l'enregistrement d'un nom de domaine générique n'est exigée du déposant. Ce dernier n'a donc à produire aucun justificatif pour le nom de domaine qu'il a choisi et qui lui sera attribué si personne d'autre ne l'a demandé avant lui. Le formulaire d'enregistrement qu'il doit remplir prévoit seulement une mention du demandeur qui déclare qu'à sa connaissance, il ne préjudicie pas aux droits d'un tiers⁵. Enfin, l'enregistrement d'un nom de domaine de second niveau s'effectue par le biais d'un contrat

¹Il se traduit par protocole d'accord. Il s'agit d'un accord signé entre deux ou plusieurs parties, pour définir les liens qui les unissent et leurs objectifs communs.

²Il se traduit par l'accord de parrainage. Il fait référence à un contrat écrit dans lequel les parrains et les candidats se font des promesses. Le parrain soumettra généralement une entente de parrainage dûment remplie et signée (photocopie ou télécopie) avec la demande de parrainage.

³Luc GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, *Op.cit.*, p. 637.

⁴Service de base de données publique permettant d'effectuer des recherches afin d'obtenir des informations sur un nom de domaine comme la date d'enregistrement, les contacts administratifs et techniques associés ainsi que les serveurs DNS.

⁵Christiane FERAL-SCHUHL, *Op.cit.*, p. 982.

conclu entre le demandeur et l'un des bureaux d'enregistrement désignés par le registre. Par ce contrat, le registre s'engage, contre le paiement d'une somme, à faire enregistrer le nom de domaine dans l'extension demandée auprès du registre compétent, sans pouvoir toutefois en garantir l'attribution, la décision relevant du registre¹.

Les règles pour le choix d'un nom de domaine dans la zone «.ma », sont définies par la décision n° 12-14 du 21 Novembre 2014 émanant de l'ANRT relative aux modalités de gestion administratives, technique et commerciale des noms de domaine Internet «.ma »². Selon l'article 5 de ladite décision, l'attribution et l'enregistrement d'un nom de domaine est soumis à des contraintes syntaxiques. Comme les noms de domaines ne peuvent exister qu'une seule fois au niveau mondial, leur attribution se fait selon la règle du premier arrivé premier servi. Il y a toutefois quelques réserves, c'est le cas de certains termes dont l'enregistrement en tant que nom de domaine est soumis à des conditions particulières liées à l'identité et au droit du demandeur. La liste des termes réservés est disponible sur le site web du registre et est régulièrement mise à jour par l'ANRT. La décision de l'ANRT dispose en outre dans son article 6 que l'enregistrement d'un nom de domaine peut être refusé si celui-ci porte atteinte à la sûreté nationale ou à l'ordre public ou au contraire à la morale ou aux bonnes mœurs. De même, il ne doit pas porter atteinte à la religion, la langue, la culture, les opinions politiques, ni utiliser des termes à connotation racistes.

Une convention appelée prestataire est conclue entre l'ANRT et tout prestataire déclaré. Cette convention définit les droits et les obligations des deux parties et les conditions administratives et techniques d'accès au registre par les prestataires³. La commercialisation des noms de domaine «.ma» est assurée exclusivement par les prestataires. Dans ce cas toute personne souhaitant enregistrer un nom de domaine « .ma » doit s'adresser à un prestataire. Le titulaire du nom de domaine procède à l'enregistrement sur une base annuelle allant de 1 à 5 ans renouvelable. Le prestataire est tenu d'enregistrer ledit nom de domaine au niveau du registre pour la même période demandée par le titulaire⁴. Ainsi, est composée la chaîne de contrats qui gouverne le système des noms de domaine. La multiplicité des acteurs

¹GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, *Op.cit.*, p. 638.

²Selon un Observatoire annuel des noms de domaine sous .ma l'arrêté au 31 décembre 2021 par l'ANRT, le parc .ma a franchi le seuil symbolique des 100.000 noms de domaine .ma enregistrés, avec une Croissance de +13.61% entre 2020 et 2021 et Croissance annuelle moyenne de 9,68% depuis 2011.

³V. art 9 de la décision ANRT/DG/N°12/14 du 21 Novembre 2014 relative aux modalités de gestion administrative, technique et commerciale des noms de domaine Internet «.ma».

⁴ V. art. 26 de la décision ANRT/DG/N°12/14 du 21 Novembre 2014 relative aux modalités de gestion administrative, technique et commerciale des noms de domaine Internet «.ma».

intervenant dans cette chaine contractuelle est source de complexité. Elle conduira notamment à s'interroger sur le statut juridique du nom de domaine.

Sous-section 2 : La réglementation des noms de domaines.

Bien plus qu'une seule adresse, le nom de domaine est devenu une véritable enseigne virtuelle, dotée d'une forte valeur économique, ainsi qu'un prolongement naturel de la marque. Il a acquis en quelques années un véritable statut de signe distinctif de sorte qu'il est désormais impossible, voire dangereux, de concevoir une stratégie de protection de marque sans mettre en place une stratégie équivalente pour les noms de domaines. Ainsi, protéger un nom de domaine est essentiel pour toute entreprise disposant d'un site internet et pour ce faire une réglementation des noms de domaines s'avère indispensable. Il paraît donc opportun de s'arrêter sur le statut juridique des noms de domaines (Paragraphe 1) avant d'étudier les outils juridiques mis en place pour leur protection (Paragraphe 2).

Paragraphe 1 : Le statut juridique des noms de domaines.

La question du statut juridique des noms de domaines n'est toujours pas réglée et reste délicate et débattue. La première raison à ce défaut de statut qui peut être invoquée réside dans l'absence de dispositions légales et réglementaire. La loi 24-96 relative à la poste et aux télécommunications du 7 août 1997, telle qu'elle a été modifiée et complétée par la loi 29-06 du 17 avril 2007, ainsi que la décision n° 12-14 du 21 Novembre 2014 émanant de l'ANRT ont certes été adoptés en vue de réglementer l'attribution et la gestion administrative et commerciale des noms de domaine. Cependant, ce corpus normatif ne concerne que les noms de domaine qui relèvent de l'extension «.ma ».

La seconde raison qui préside à ce flou s'explique par la pluralité des fonctions que remplissent les noms de domaines. Si, initialement, les noms de domaines ont été créés afin de jouer le rôle d'adresse numérique, par la suite, ce rôle a évolué à mesure que le web s'est ouvert au public, les internautes, notamment les sociétés commerciales, ont très vite compris que les noms de domaines étaient plus que de simples adresses permettant d'accéder à un serveur distant. Ils ont vu dans ces derniers un formidable moyen d'affirmer leur identité,

voire leur raison sociale, et de distinguer leur plateforme des sites web concurrents. Partant, les noms de domaines ont rapidement rempli la fonction de signe distinctif¹.

C'est ainsi que l'incertitude quant à leur statut est née. En raison du caractère distinctif que la plupart revêtent, l'analogie avec les marques vient facilement à l'esprit². Comme celles-ci les noms de domaines semblent, à première vue constituer des signes distinctifs, dont la fonction serait désignée, indirectement, des produits ou services proposés sur les sites web des entreprises correspondantes. Le nom de domaine a ainsi été successivement qualifié de signe de ralliement de la clientèle vers le site qu'il identifie, de magasin virtuel ou encore d'équivalent électronique de l'enseigne.

Pourtant, ces comparaisons doivent être nuancées pour plusieurs raisons. D'une part, tous les noms de domaines ne s'apparentent pas à des signes distinctifs, en ce sens que certains d'entre eux, par leur caractère descriptif ou générique ne permettent pas d'identifier l'origine des produits ou services auxquels ils sont associés par exemple « hotel.com ». En d'autres termes, tandis que les marques désignent les produits ou services d'une entreprise déterminée, les noms de domaines non distinctifs fonctionnent, pour le public, comme un outil de recherche de produits ou services sans référence à une entreprise particulière. D'autre part, même dans l'hypothèse où ils sont distinctifs, les noms de domaine ne peuvent être assimilés aux marques. En effet, au-delà de leur ressemblance, qui tient particulièrement au monopole conféré au titulaire du signe, il existe entre ces deux types de signes des différences fondamentales qui s'opposent à l'application aux noms de domaines des règles propres aux marques³. Tandis que la marque est un titre de propriété, à la portée territoriale, délivré par l'autorité publique, la titularité du nom de domaine, signe par essence international, résulte d'un enregistrement contractuel.

Par ailleurs, une partie de la doctrine préconise la qualification du nom de domaine en tant qu'objet de propriété. Elle s'appuie essentiellement dans ses arguments sur le caractère exclusif du droit que confère l'enregistrement d'un nom de domaine à son titulaire. Pourtant si l'exclusivité est bien de l'essence de la propriété, le caractère exclusif du nom de domaine ne suffit pas à emporter la qualification de propriété. En effet, la qualification de propriété est

¹G. HASS et A. BAMDE, « Un statut juridique pour le nom de domaine », in IP/IT, N° 2, Février 2016, Dalloz, p. 63.

²Philippe LE TOURNEAU, *Op.cit.*, p. 579.

³F. HONORAT, « La marque face au nom de domaine », in LEGICOM, N° 44, 2010, Victoires, p. 92.

soumise à plusieurs conditions parmi lesquelles l'exigence d'un risque de confusion. Aussi, au soutien de la réfutation de la qualification de propriété désormais partagée par une large partie de la doctrine, il faut observer que l'exclusivité de la jouissance temporaire d'un nom de domaine, due à son enregistrement, n'implique pas l'existence d'un droit de propriété sur le nom de domaine parce qu'il n'y a pas de propriété sans autorisation de la loi. Pour toutes ces raisons la qualification de nom de domaine en tant que propriété s'avère inadapté.

Ainsi, se révèle la nature juridique complexe du nom de domaine qui n'est pas l'objet d'un droit de propriété intellectuelle mais qui confère un monopole à son bénéficiaire. On peut donc conclure que l'enregistrement d'un nom de domaine confère à son titulaire un droit exclusif d'occupation sur un signe dont ni lui-même ni l'agence ne sont propriétaire. A défaut d'une qualification d'élément du domaine public, les noms de domaines tendent vers la catégorie des choses communes, définies comme des choses n'appartenant à personne mais faisant l'objet d'un usage réglementé¹. Le statut ambigu des noms de domaines, illustré par leur difficile qualification juridique soulève la question de leur protection.

Paragraphe 2 : La protection des noms de domaines.

Comme cela a été souligné plus haut, ni le caractère distinctif d'un nom de domaine ni son enregistrement ne sont suffisants pour lui conférer une protection juridique. Dès lors, en l'absence de droit privatif et de dispositions spécifiques régissant le statut des noms de domaines². Leur protection ne peut être assurée que sur le fondement de la responsabilité civile dont la mise en œuvre suppose la caractérisation d'une faute dommageable. Pour ce faire, les juges examineront au préalable, l'existence d'une exploitation du nom de domaine auquel il est porté atteinte. Le seul enregistrement ne suffit pas. Il faut la démonstration du risque de confusion engendré par le signe distinctif litigieux. La protection du nom de domaine est, de la sorte, subordonnée à l'usage qui en est fait. Autrement dit, le seul enregistrement d'un nom de domaine ne confère à son titulaire aucune protection. Le signe ne devient protégeable que s'il fait l'objet d'une exploitation effective. De plus, un nom de domaine pour être effectivement exploité doit conduire à un site internet actif, présentant des produits ou services, et non pas à une simple page en construction.

¹Luc GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, *Op.cit.*, p. 643.

²Jacques AZEMA et Jean-Christophe GALLOUX, *Op.cit.*, p. 1167.

Une fois démontrée l'exploitation effective du nom de domaine, son titulaire sera fondé à engager une action en concurrence déloyale. Pour que son action aboutisse il lui faudra néanmoins rapporter la preuve d'une faute, d'un nom de dommage et d'un lien de causalité. Toute la difficulté résidera alors dans la caractérisation du premier élément de ce triptyque : la faute. Cette dernière consiste en la production, par le signe distinctif contesté, d'un risque de confusion dans l'esprit du public. Pour démontrer l'existence de ce risque de confusion, il appartiendra au demandeur de démontrer la réunion de deux conditions : l'antériorité et l'imitation du nom de domaine dont il recherche la protection.

Concernant, tout d'abord la condition d'antériorité, elle va de soi. Celui qui revendique l'appropriation d'un nom de domaine ne saurait reprocher à son adversaire une concurrence déloyale que s'il établit que son exploitation est antérieure à celle du signe distinctif dont il conteste l'usage. L'existence d'une antériorité s'appréciera à la lumière du principe de spécialité. La raison en est que la protection des signes distinctifs est, quelle que soit leur nature, toujours relative, sauf à ce qu'il s'agisse d'une marque notoire. Autrement dit, ils ne bénéficient d'une protection que pour la classe de produits ou services auxquels ils sont associés. Ainsi la Cour de cassation française a eu l'occasion d'affirmer dans un arrêt du 13 Décembre 2005 qu' « *un nom de domaine ne peut contrefaire une marque antérieure que si les produits et services offerts sur ce site sont, soit identiques, soit similaires à ceux visés dans l'enregistrement de la marque et de nature à entraîner un risque de confusion dans l'esprit du public* »¹. Le même raisonnement peut être tenu dans l'hypothèse où l'antériorité consisterait en un signe distinctif autre qu'une marque².

La preuve de l'antériorité n'est pas suffisante pour caractériser le risque de confusion ; elle doit s'accompagner de la démonstration d'une limitation du nom de domaine. S'agissant de cette seconde condition, elle suppose, plus précisément, que le demandeur établisse que l'imitation d'un nom de domaine dont il est titulaire est de nature, soit parce que les signes sont identiques, soit parce qu'ils sont similaires, à induire le client en erreur sur l'origine des produits ou services désignés, tant et si bien qu'il en résulte un détournement de clientèle³.

¹C. Cass. ch. Civile, décision n° 02-21.259, 13 Décembre 2005.

²Philippe LE TOURNEAU, *Op.cit.*, pp. 585-586.

³G. HASS et A. BAMDE, *Op.cit.*, p. 66.

Section 2 : Les créations numériques de l'entreprise.

Dans le monde du numérique, exister signifie être visible. L'enjeu de la visibilité d'une entreprise est majeur et ses créations numériques sont au cœur de cette problématique. Le défi est de conjuguer harmonieusement le monde réel et le monde numérique en conservant les créations des entreprises au cœur du système de protection (Sous-section 1). Dans ce contexte, la technologie de la *blockchain* connaît un engouement notamment dans le domaine de la propriété intellectuelle en l'occurrence les créations numériques, car cette technologie pourrait faciliter la preuve de l'antériorité des droits et permettrait de prouver les droits sur les créations et assurerait la traçabilité des transactions. Un débat sur les enjeux et les bienfaits apportés par la *blockchain* s'impose (Sous-section 2).

Sous-section 1 : La protection de l'œuvre numérique de l'entreprise.

La forme actuelle du droit d'auteur est issue de la loi 2-00 relative aux droits d'auteur et droits voisins. Selon l'article 2 de ladite loi : « Tout auteur bénéficie des droits prévus dans la présente loi sur son œuvre littéraire et artistique. La protection résultant des droits prévus au précédent alinéa comme dès la création de l'œuvre, même si celle-ci n'est pas fixée sur un support matériel ». La notion d'œuvre numérique n'existe pas en tant que telle dans le droit positif. Elle recouvre pourtant dans la pratique une réalité omniprésente. La majorité des œuvres produites aujourd'hui au sein des entreprises comprennent une dimension numérique, même les créations les plus traditionnelles sont désormais exposées à l'univers de l'interactivité, par exemple ; un texte sera enrichi par des liens renvoyant à d'autres contenus numériques¹.

La notion d'œuvre numérique se situe à la frontière entre l'œuvre logicielle, l'œuvre audiovisuelle et la base de données, pour se rapprocher de ce que l'on appelle également l'œuvre multimédia. L'œuvre numérique ne peut être confondue en tant que telle avec l'œuvre logiciel, même si par exemple, un site web ne peut être créé et consulté qu'à l'aide

¹Viviane GELLES et Blandine POIDEVIN, « Réflexions autour de la création numérique dans l'entreprise : problématiques juridiques, enjeux et pistes de réforme » in La propriété intellectuelle et la transformation numérique de l'économie, Ouvrage collectif sous la direction de Fatima GHILASSENE et Laurence JOLY, INPI, 1^{ère} éd., France, 2015, p. 114

d'outils logiciels, dans la mesure où lesdits logiciels restent des instruments et non la finalité poursuivie par le créateur.

La notion se rapproche également de celle de base de données, définie à l'article premier de la loi 2-00 comme : « Tout recueil d'œuvres, de données ou d'autres éléments indépendants, disposer de manière systématique ou méthodique et individuellement accessibles par des moyens électronique ou toutes autres manières ». Dans la mesure où le site internet fournit un contenu présenté comme un ensemble d'éléments auxquels l'internaute peut accéder selon les principes de navigation retenus par le créateur du site concerné, il constitue bien une base de données au sens de l'article précité de la loi 2-00 relative aux droits d'auteur et droits voisins. L'œuvre numérique emprunte également certaines caractéristiques à l'œuvre audiovisuelle, en présentant également des éléments textuels associés à des aspects sonores et visuels.

En définitive l'œuvre numérique peut être définie comme toute œuvre de création incorporant sur un même support un ou plusieurs éléments suivants : texte, son, images fixes, images animées, programmes informatiques, dont la structure et l'accès sont régis par un logiciel permettant l'interactivité¹. Le problème est qu'il n'existe à ce jour, aucun régime juridique propre à l'œuvre numérique et que cette dernière emprunte ses principes de protection à différents types d'œuvres dont nous avons fait référence à savoir l'œuvre logicielle (Paragraphe 1) et les bases de données notamment le site internet (Paragraphe 2). Or, ces œuvres sont souvent créées par des salariés dans le cadre de l'exécution de leur contrat de travail. Dans ce contexte, l'une des problématiques prioritaires qui préoccupe les entreprises est celle de l'insécurité juridique affectant la création, par leurs salariés, d'œuvres numériques (Paragraphe 3).

Paragraphe 1 : La protection du logiciel.

La question du choix de la protection du logiciel a toujours fait osciller cet objet singulier entre propriété industrielle et propriété littéraire et artistique. Logique industrielle de son mode de création d'une part, mais également création de forme de par son écriture d'autre part. L'oscillation est également conceptuelle, puisque le droit d'auteur dont il est question est

¹SNE, questions juridiques relatives aux œuvres multimédia, Livre blanc du Groupe de travail audiovisuel et multimédia, 1994.

un droit très spécifique¹. Appliqué au logiciel, il peut sans abus être qualifié de droit voisin du droit de brevet². En ce sens, le logiciel se situe entre brevet et droit d'auteur. Mais à la vérité, un logiciel peut être à la fois qualifié d'œuvre de l'esprit et protégée par le droit d'auteur et d'invention brevetable.

Au Maroc, la loi 2-00 tel que modifié et complétée par la loi n° 34-05 et la loi n°72-12 vient trancher la question en ajoutant les programmes informatiques à la liste des œuvres protégeables par le droit d'auteur³. La loi sur la propriété littéraire et artistique ne précise pas que pour bénéficier de la protection du droit d'auteur, le logiciel doit présenter un caractère d'originalité. Néanmoins, cette condition découle des principes mêmes de la propriété littéraire et artistique. Donc seuls les logiciels présentant un caractère original sont protégés par le droit d'auteur. Le critère d'originalité est la seule condition de fond nécessaire à la protection du logiciel par le droit d'auteur⁴. Mais en absence de définition légale, on peut considérer qu'une œuvre n'est protégeable qu'à partir du moment où elle porte l'empreinte de la personnalité de son auteur. Cette condition, peu adapté aux logiciels, a toutefois évolué. En effet, le logiciel est protégeable si son code source porte la marque de l'apport intellectuelle de son auteur. *« L'originalité doit donc s'entendre d'un effort personnalisé allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante et la matérialisation de cet effort réside dans une structure individualisée »*⁵. L'originalité est appréciée à l'une des choix de conception propres à l'auteur.

La protection du logiciel ne s'étend pas aux idées, seule l'expression littérale et mathématique des programmes qui sont à la base du logiciel l'est. Seule la mise en forme de ces idées peut faire l'objet d'une protection par le droit d'auteur, c'est-à-dire la matérialisation de l'auteur de son œuvre. Parfois, ils sont intégrés dans les appareils électroménagers ou voitures, mais en général ils sont insérés dans des supports physiques comme par exemple

¹Frank MACREZ, « Logiciel : le cumulard de la propriété intellectuelle » in L'articulation des droits de propriété intellectuelle, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2011, p. 47.

²Joanna SCHMIDT-SZALEWSKI et Jean-Luc PIERRE, Droit de la propriété industrielle, Litec, 4^{ème} éd., coll. Manuels, Paris, 2007, p. 132.

³V. art. 3 de la loi 2-00.

⁴O. PIGNATARI et A. COUSIN, « L'originalité des logiciels », in IP/IT, N° 5, Mai 2016, Dalloz, p. 248.

⁵C. Cass., Ass. Plén., décision n° 83-10477, 7 Mars 1986, la Société anonyme BABOLAT MAILLOT WITT contre Monsieur Jean X.

dans un *CD* ou une clé *USB*. A ce titre il est à noter que c'est la partie du logiciel qui fait l'objet de protection¹.

Quant à la titularité des droits d'auteur. Les droits moraux sur les logiciels reviennent à leur auteur. L'auteur du logiciel pourra exiger que l'œuvre porte la mention de son nom. En pratique, le nom de l'auteur sur le support du logiciel ou sur la documentation technique accompagnant celui-ci. De même, dans le cadre du respect de l'œuvre, l'auteur peut s'opposer à toute modification qui est préjudiciable à son honneur ou à sa réputation. Aux Etats-Unis, c'est la mention *Copyright* qui est apposée sur les œuvres et lui confère une protection internationale. Ensuite l'auteur d'un logiciel a le choix de livrer son logiciel au public. Toutefois dans le cadre des créations des salariés au sein d'une entreprise, les droits patrimoniaux relatifs au logiciel sont obligatoirement conférés à l'employeur.

Outre les droits moraux, l'auteur jouit sur son programme des droits patrimoniaux. Le droit d'exploitation appartenant à l'auteur d'un logiciel comprend le droit de faire et d'autoriser à savoir, la reproduction permanente ou provisoire d'un logiciel en tout ou partie, par tout moyen et sous toute forme. Dans la mesure où le changement, l'affichage, l'exécution, la transmission et le stockage de ce logiciel nécessitent une reproduction, ces actes ne sont possibles qu'avec autorisation de l'auteur, la représentation est soumise elle aussi à l'autorisation préalable de l'auteur du logiciel, et consiste dans la communication du logiciel au public par tout procédé possible, la traduction ou toute adaptation du logiciel ou encore la vente, la distribution gratuite ou la location de ce logiciel.

Nous ne pouvons pas parler de logiciel sans faire référence aux algorithmes. Ces derniers constituent une valeur essentielle du capital de certaines entreprises impliquées dans l'exploitation des données numériques et, à ce titre, ils méritent protection. Pourtant, ils ne jouissent, en tant que création immatérielle, que d'une protection limitée, voire incertaine. L'algorithme est un principe mathématique. Il relève du champ des idées, lesquelles ne sont pas protégeables. En pratique, les algorithmes sont des créations intégrées au code source d'un logiciel². Or comme cité ci-dessus les logiciels sont protégeables par le droit d'auteur du moment qu'il présente une originalité. S'agissant des algorithmes, la condition d'originalité sera difficile à prouver comme l'illustre un arrêt de la Cour de

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 270.

²M. BOIZARD, « La valorisation des données numériques par la protection juridique des algorithmes », in IP/IT N° 2, Février 2018, Dalloz, p. 100.

cassation française du 14 Novembre 2013¹. Un éditeur agissait en contrefaçon contre la société *Microsoft Corporation* pour reproduction d'un logiciel de comptabilité qu'il avait conçu. La Cour écarte la contrefaçon en raison de l'absence de fourniture d'éléments permettant de justifier de l'originalité du logiciel tels que les lignes de programmation, les codes ou l'organigramme, ou du matériel de conception préparatoire. Cette décision met le doigt sur la limite d'une protection par le droit d'auteur qui ne protège pas le logiciel dans sa globalité : les fonctionnalités d'un logiciel ne sont pas protégées en elles-mêmes.

Concernant le logiciel, le panorama est, finalement et schématiquement, le suivant. D'un côté, un droit d'auteur au critère de qualification et au régime juridique très spécifiques mais qui a été codifié au sein des dispositions générales du droit auteur. De l'autre, un brevet délivré illégalement, ou à tout le moins selon une interprétation du donné légal qui peut être sérieusement contestée, notamment devant le juge judiciaire. Autrement dit, droit d'auteur *sui generis* et brevet contrat *legem*, mais présumé valable². Il faut noter qu'à côté de la protection juridique, il existe une protection basée sur des mesures techniques³.

Il est interdit d'une part la promotion des outils de déplombage⁴. Ainsi toute publicité ou notice d'utilisation relative aux moyens permettant la suppression ou la neutralisation de tout dispositif technique protégeant un logiciel doit mentionner que l'utilisation illicite de ces moyens est passible des sanctions de contrefaçon. D'autre part, il est interdit d'utiliser des outils de « déplombage ». Il est interdit toute détention pour un usage personnel ou l'usage d'outils d'atteinte aux mesures de protection des œuvres. C'est le cas d'un étudiant en informatique, qui a développé un logiciel permettant de recopier sans autorisation des œuvres sur *Deezer.com*, en contournant les mesures de protection, et qui avait créé un site web pour diffuser ce logiciel⁵. L'étudiant a été reconnu coupable d'accès frauduleux au système de *Deezer*, d'atteinte à une mesure efficace de protection et de mise à disposition du public de moyens contournement encourant ainsi des amendes et des dommages intérêts.

¹C. Cass., Civile, ch. Civile, décision n° 12-20.687, 14 Novembre 2013, MM. X et Y contre la Société Microsoft corporation.

²Frank MACREZ, *Op.cit.*, p. 48.

³Fabrice MATTATIA, *Droit d'auteur et propriété intellectuelle dans le numérique*, Eyrolles, 3^{ème} éd., Paris, 2021, p. 117

⁴Le piratage de logiciels peut prendre la forme de déplombage du logiciel qui consiste à supprimer les protections interdisant les copies illégales.

⁵TGI, ch. Correctionnel, 28 Juin 2013, Blogmusik, Sacem et autres (Deezer) contre M. Jérôme G., Nîmes.

Néanmoins, il est reconnu à l'utilisateur d'un logiciel un certain droit à la décompilation, notamment en vue d'assurer l'interopérabilité de ce logiciel, même en cas de protection par un dispositif technique. Il découle de l'article 21 de la loi 2-00 le droit de la libre reproduction et adaptation de programmes d'ordinateur : « le propriétaire légitime d'un exemplaire d'un programme d'ordinateur peut, sans l'autorisation de l'auteur et sans paiement d'une rémunération séparée, réaliser un exemplaire ou l'adaptation de ce programme à condition que cet exemplaire ou cette adaptation soit nécessaire à l'utilisation du programme d'ordinateur à des fins pour lesquelles le programme a été obtenu, soit nécessaire à des fins d'archivage et pour remplacer l'exemplaire licitement détenu dans le cas où celui-ci serait perdu, détruit ou rendu inutilisable ». Le texte ajoute qu'« aucun exemplaire ni aucune adaptation ne peuvent être réalisés à des fins autres que celles prévues aux deux précédents paragraphes du présent article et tout exemplaire ou toute adaptation seront détruits dans le cas où la possession prolongée de l'exemplaire du programme d'ordinateur cesse d'être licite ».

Paragraphe 2 : La protection des bases de données : exemple du site Internet.

L'internet expose le juriste spécialiste du droit d'auteur à de nombreuses difficultés. En effet l'internet se nourrit de nombreuses créations de l'esprit et suscite aussi la création de nouvelles œuvres : jeux en ligne, site web...¹ Se pose donc ici la question des moyens de protection de ces nouvelles richesses. Nous nous attacherons donc à la manière de protéger les bases de données en prenant l'exemple des sites web. La loi 2-00 relative aux droits d'auteur et droits voisins dans son troisième article énumère une liste de créations considérées comme des œuvres de l'esprit protégeable au titre du droit d'auteur. Bien que non expressément visé par ce texte, le site internet est susceptible d'être protégé par le droit d'auteur sous certaines conditions.

Le site web peut être protégé par le droit d'auteur de diverses manières. Son titre, tout d'abord, peut l'être, dans les mêmes conditions que les titres des autres œuvres, ceci venant s'ajouter aux noms de domaines². Au niveau du contenu, ensuite, le site est animé par un logiciel qui mérite une protection juridique. La création recèle encore des textes, images et

¹Tristan AZZI, « Les créations multimédias (bases de données, jeux vidéos...) » in L'articulation des droits de propriété intellectuelle, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2011, p. 32.

² Voir supra p. 186.

sons qui sont autant d'éléments protégeables. Il en est de même pour la ou les bases de données que comporte le site, quand celui-ci, dans sa globalité n'est pas appréhender comme une base. Le site contient, enfin, des liens hypertextes qui non seulement sont susceptibles de porter atteinte au droit d'auteur en permettant des téléchargements indus, mais peuvent encore être envisagés comme objets de droits. On ne s'étonnera donc pas que l'on ait qualifié ces sites de « *carrefours de droits* »¹.

Sur le contenu et l'architecture du site internet, il peut bénéficier de la protection du droit d'auteur dans sa présentation et ses divers éléments, c'est-à-dire une page-écran, un graphisme, une animation présente un caractère d'originalité suffisant pour prétendre à cette protection des œuvres de l'esprit. Il faut noter que si la reproduction de certains éléments d'un site internet est constitutive d'un acte de contrefaçon, la copie de certains autres est en revanche licite dans la mesure où, pris séparément, ils ne répondent pas aux conditions posées par le droit d'auteur. En effet, il est exclu les éléments techniques du champ de protection du droit d'auteur.

Par ailleurs, le simple concept d'un site web n'est pas protégé par le droit d'auteur. Les idées sont de libre parcours et ne sauraient de quelque manière que ce soit faire l'objet d'une appropriation². Les œuvres de l'esprit sont protégées, comme on le sait, à condition qu'elles soient originales. Cette originalité est définie comme étant l'expression de la capacité créative de l'auteur effectuant des choix libres et créatifs. Donc si un site se limite au remplissage de rubriques (par exemple un profil Facebook), le manque d'originalité interdit de lui accorder cette protection.

Les droits d'auteurs sont composés, comme on le sait, de deux séries de prérogatives : morales, tout d'abord, et patrimoniales, ensuite. Nos développements concerneront avant tout les droits moraux. Observons toutefois que le droit moral, et plus particulièrement de droit au respect de l'œuvre, peut être malmené sur les réseaux. De nombreuses techniques sont en effet susceptibles d'altérer l'œuvre sur l'internet. Nous songeons au *morphing* (qui permet certaines déformations), au *framing* (c'est-à-dire l'incrustation de l'image collectée sur un autre site), à certains modes de diffusion en *streaming* des films sur des plateformes d'échanges de vidéos. Le droit d'auteur comporte, aux cotés des droits moraux, comme

¹Michel VIVANT et Jean-Michel BRUGIERE, Droit d'auteur et droits voisins, Dalloz, 2^{ème} éd., Paris, 2012, p. 115.

²Fabrice MATTATIA, *Op. cit.*, p. 43.

le précise l'article 10 de la loi 2-00 des attributs d'ordre patrimoniaux. Ces prérogatives patrimoniales vont permettre à l'auteur de pouvoir contrôler la circulation de son site internet, le céder, le louer, le mettre en gage, la démembrer, etc., autant d'opérations juridiques qui sont destinées à tirer profit de la création et qui peuvent être mises en cause sur internet¹.

Paragraphe 3 : Le régime juridique de l'œuvre numérique créée par des salariés.

Les personnes protégées par la loi peuvent être des créateurs indépendants. Dans ce cas le concepteur indépendant sera titulaire de la propriété littéraire et artistique. Il convient de rappeler que tel n'est pas toujours le cas dans le domaine informatique. Le plus souvent les programmes ou logiciels sont l'œuvre d'auteurs multiples. Dans ce cas, le programme est une œuvre de collaboration ou une œuvre collective ou une œuvre composite selon que la participation de chaque auteur peut être déterminée ou non. Chaque auteur bénéficiera d'un droit distinct sur l'ensemble réalisé². Dans la plupart des cas, les droits sur l'ensemble sont exercés par une personne morale (normalement une société de service) cessionnaire de ces droits.

C'est le cas du site web, ce dernier peut être qualifié d'œuvre composite. En effet un site web est potentiellement constitué d'œuvres protégées préexistantes telles que des photographies, de la musique, des textes, un logiciel, etc. L'exploitation du site doit donc solliciter l'autorisation des titulaires des droits des œuvres premières afin de pouvoir licitement réutiliser ces dernières. C'est fréquemment le cas des graphistes qui conçoivent et réalisent le graphisme d'un site internet. Toute reproduction d'une œuvre préexistante sans autorisation pourrait être qualifiée de contrefaçon³.

Par ailleurs, le site internet peut parfaitement être réalisé dans les conditions de l'œuvre collective. Cette dernière permet, à titre exceptionnel, d'investir une personne morale

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 272.

²Lorsque plusieurs personnes ont concouru à la création de l'œuvre, il sera nécessaire de préciser l'apport de chacun en cas de litige sur la répartition des droits. La cour d'appel de Paris a débouté une personne qui revendiquait la qualité de co-auteur sur un logiciel, développé par une société qu'elle avait créée avec des associés, mais qu'elle avait quittée. La cour a noté que c'est un de ses collègues qui, depuis l'origine, étant désigné publiquement comme l'auteur du logiciel, et qui était cité comme tel dans tous les documents. Ce collègue bénéficiait dès lors d'une présomption de qualité d'auteur, que seules des preuves indiscutables auraient permis de renverser. Or, le plaignant ne disposait pas de telles preuves permettant d'évaluer l'importance de sa participation à l'élaboration du logiciel. Il est donc indispensable si l'on souhaite pouvoir revendiquer des droits sur l'élaboration d'un logiciel, de constituer des preuves de sa participation, au besoin par voie d'huissier.

C. Appel, 1^{ère} cham., 27 février 2013, David D. contre Thomas M. et Pascal F., Paris.

³ Voir infra p. 282.

des droits d'auteur, compte tenu du rôle prépondérant joué par celle-ci dans la création de l'œuvre. En effet, l'œuvre collective est créée à l'initiative d'une personne physique ou morale, qui l'édite, la publie ou la divulgue sous sa direction et son nom¹. Dans ce cas de l'œuvre collective, les contributions de chacun des participants fusionnent dans l'ensemble. L'œuvre collective est, sauf preuve contraire, la propriété de la personne physique ou morale sous le nom de laquelle elle est divulguée². Enfin, un site internet peut être également qualifié d'œuvre de collaboration selon les conditions de la création. Ces dernières sont des œuvres à la création desquelles ont concouru plusieurs personnes physiques, l'empreinte de la personnalité de chacun des auteurs pouvant y être décelée.

Mais la question qui se pose c'est lorsqu'on est en présence d'une situation de dépendance. L'auteur dont le site internet va être exploité peut se trouver dans une situation de dépendance juridique. C'est le cas des créations des salariés, point sur lequel nous nous concentrerons exclusivement, et se pose alors l'interrogation : A qui doit revenir l'œuvre, site web, réalisé dans le cadre du contrat de travail ? Il s'agit d'une question particulièrement délicate en matière de création ou développement protégeable par le droit d'auteur en général et d'internet en particulier.

Selon l'article 35 de la loi 2-00 relative aux droits d'auteur et droits voisins. Lorsqu'une œuvre est créée par un auteur pour le compte d'une personne physique ou morale, autrement dit l'employeur dans le cadre d'un contrat de travail et de son emploi, sauf disposition contraire du contrat, le premier titulaire des droits moraux et patrimoniaux est l'auteur, mais les droits patrimoniaux sur cette œuvre sont considérés comme transférés à l'employeur dans la mesure justifiée par les activités habituelles de l'employeur au moment de la création de l'œuvre. De ce fait, la gestion contractuelle en amont de la question se configure comme essentielle.

Pour les œuvres créées par les stagiaires ou intérimaires n'appartiennent pas sauf accord contraire, à l'organisme d'accueil-maitre de stage, mais en général, soit à l'institution de

¹Jean-Daniel BOUHENIC, « L'entreprise et la titularité des droits de propriété intellectuelle. L'œuvre collective » in in L'entreprise et la titularité des droits de propriété intellectuelle, Ouvrage collectif sous la direction Jean-Michel BRUGUIERE, Dalloz, Paris, 2015, p. 48.

² Il a été jugé qu'une ancienne salariée d'une maison d'édition ne pouvait pas prétendre à se voir déclarer auteur ou coauteur d'un dictionnaire divulgué sous le nom de cette dernière, alors que « la contribution de l'intéressé (...) se fondait dans l'ensemble de l'activité des nombreux auteurs ou collaborateurs réunis au sein de l'équipe animée par elle, sans qu'elle soit possible d'attribuer à chacun un droit distinct sur la création réalisée » C. Cass. 1^{ère} ch. Civile, décision n° 00-12.932, 3 Avril 2002, Mme X contre la Société Editions Larousse.

formation d'origine, soit au stagiaire lui-même. Il en est de même pour les intérimaires, dont les œuvres protégeables reviennent en général, contractuellement, à l'organisme d'intérim. Aussi il est important de songer, avant de procéder à l'accueil du stagiaire, à la formalisation d'une convention de cession de droits en bonne et dure forme, liant, pour plus de sécurité, l'ensemble des parties intéressées¹.

Plusieurs propositions sont envisagées pour assurer une sécurité juridique aux exploitants d'œuvre numérique. D'abord, l'une des solutions envisageables, afin de sécuriser le régime juridique applicable aux œuvres numériques, pourrait consister dans l'application distributive. Autrement dit, l'application des régimes juridiques propres à chacun de ses composants. Une société développant une œuvre numérique appliquerait le régime du logiciel à ceux de ses salariés ayant la qualité de programmeurs et étant à l'origine des composantes logicielles de l'œuvre numérique réalisée. Elle appliquerait, en corollaire, à ses salariés à l'origine de créations graphiques, textuelles ou encore musicales, les régimes de droit commun s'appliquant à ces matières. Il s'agira dès lors pour l'employeur d'identifier chacun des auteurs ayant participé à la création de l'œuvre numérique considérée et de qualifier les créations des différents auteurs afin de leur appliquer le régime juridique correspondant².

Toutefois, une intervention législative venant consacrer les assouplissements ainsi envisagés serait l'une des pistes à envisager pour faciliter la mise en œuvre par l'employeur d'une politique accessible de gestion des droits de propriété intellectuelle de ses salariés. Dans la pratique, il est en effet, fréquent de constater que de nombreuses entreprises ne procèdent pas de sorte et qu'elles s'exposent, à une insécurité juridique indéniable susceptible non seulement de leur faire courir des risques contentieux, mais également de les affaiblir dans un contexte international.

En outre, certaines voix s'élèvent pour demander la définition et la création d'un statut juridique ad hoc pour les œuvres numériques. Cependant, différents obstacles se dressent pourtant d'ores et déjà sur la route d'une telle création spécifique. Parmi eux figure, principalement, la difficulté d'élaborer une définition univoque de l'œuvre numérique qui bénéficierait du régime spécifique ainsi créé. Rares sont d'ailleurs les Etats à avoir opté pour un tel choix. A titre d'exemple, les Etats les plus actifs dans le domaine des jeux vidéo (tel

¹ Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, *Op.cit.*, p. 268.

² Viviane GELLES et Blandine POIDEVIN, *Op.cit.*, p. 117.

que les Etats-Unis, le Japon) ont choisi, le plus souvent le rattachement de ce type d'œuvre numérique au régime juridique en vigueur pour les catégories d'œuvres déjà existantes.

Néanmoins, au niveau de la Commission européenne, une directive relative au droit d'auteur dans le marché unique numérique a été adoptée en 2019. Cette nouvelle directive se fonde sur les textes antérieurs relatifs à la propriété littéraire et artistique ou au commerce électronique. Les autorités européennes ont estimé que l'évolution rapide des technologies devait être prise en considération afin de maintenir le haut niveau de protection mise en place tout en s'attachant à sécuriser les utilisations frontalières sans entraver l'évolution des technologies¹.

Sous-section 2 : Enjeux et défis de la *blockchain* en propriété intellectuelle.

La *blockchain* peut changer le monde, cette technologie décentralisée dans le monde entier, en dehors de tout cadre général et de toute institution publique, suscite donc l'intérêt du juriste. Nous nous limiterons à la question de savoir si la *blockchain* peut changer le monde de la propriété intellectuelle. Pour y répondre, il faut savoir ce dont on parle. Le procédé est complexe et fait appel à un vocabulaire savant et non juridique (Paragraphe 1) ce procédé connaît un engouement réel dans le domaine de la propriété intellectuelle, car cette technologie pourrait faciliter la preuve de l'antériorité des droits, permettrait de prouver les droits sur les créations et assurer une traçabilité (Paragraphe 2). Néanmoins, des risques et incertitudes persistent (Paragraphe 3).

Paragraphe 1 : Les étapes d'inscription d'une transaction dans la *blockchain*.

On peut expliquer concrètement et brièvement la *blockchain* utilisée en propriété intellectuelle par les étapes suivantes. D'abord, un document numérique sous forme de dessin ou modèle est transformé en empreinte numérique appelée le hash ; c'est une suite alphanumérique. Ensuite, une personne (auteur du document numérique, société tierce...) inscrit le numéro d'empreinte dans une transaction sur la *blockchain* ; on parle de l'ancrage de l'empreinte. L'utilisateur a besoin, pour inscrire une transaction, d'une clé publique² et d'une

¹P. SIRINELLI, « Première vues sur la directive droit d'auteur dans le marché unique numérique », in IP/IT, N° 5, Mai 2019, Dalloz, p. 279.

²Il s'agit de blockchain ouvert à tous. Tout acteur peut devenir un nœud du réseau c'est-à-dire y inscrire des nouveaux blocs, effectuer des transactions sur la blockchain et accéder à l'historique des transactions.

clé privée¹ (associée à la clé publique, personnelle et secrète), qui sert à authentifier la transaction. Ce qui est enregistré sur la *blockchain*, ce n'est ni une donnée ni un document original mais une empreinte numérique « hashée » qui décrit l'œuvre. Cette empreinte comporte une partie de l'empreinte numérique du bloc précédent. C'est pourquoi on parle de « bloc de chaines » (*blockchain*) car l'ensemble des transactions « hashées » s'inscrivent en blocs qui sont liés les uns aux autres.

Il faut garder à l'esprit les principales caractéristiques de cette empreinte numérique. D'une part, elle est unique c'est-à-dire qu'elle ne peut exister deux documents ayant la même empreinte cryptographique (si on change une virgule l'empreinte sera différente). D'autre part, le hachage ne fonctionne que dans un sens : on passe du document numérique au hash, c'est-à-dire une fonction impossible à inverser. Concrètement, cela signifie que même si tout le monde peut avoir accès à une *blockchain* publique, il est quasi impossible de reconstituer le document qui a été hashé et mis sur la *blockchain* ce qui garantit le secret des informations inscrites sur la *blockchain*.

Enfin, la transaction est ensuite partagée entre les nœuds du réseau² pour être validée par des mineurs³. Pour valider, les mineurs doivent résoudre sur des ordinateurs des opérations mathématiques avec des algorithmes. Ce travail de résolution est qualifié *de proof of work*. Le premier qui a réussi la résolution du problème mathématique est rémunéré en cryptomonnaie et propose la validation aux autres. Pour être inscrite dans la *blockchain*, la transaction doit être validée par 51% des mineurs⁴.

Les caractéristiques principales de la *blockchain* peuvent être synthétisées comme suit. En effet, elle est décentralisée c'est-à-dire il n'y a pas besoin d'autorité centrale chargée de valider et stocker l'information. Elle est dupliquée ; il existe de nombreuses copies

¹Appelée aussi blockchain de permission. Il s'agit d'une blockchain dont les nœuds du réseau sont contrôlés par un consortium avec des règles définies pour vérifier et autoriser l'apparition de nouveaux nœuds. Ce consortium contrôle donc également l'accès à l'historique des transactions, la possibilité d'y inscrire de nouveaux blocs ainsi que l'autorisation d'effectuer des transactions sur la blockchain. Les règles pour rejoindre le consortium peuvent être plus ou moins ouvertes et plus ou moins complexes.

²Les nœuds du réseau sont les ordinateurs du réseau de la blockchain.

³Un mineur est un individu vérifiant les transactions et opérations effectuées par les utilisateurs sur le réseau. Le mineur reçoit en temps réel toutes les transactions émises par les utilisateurs sur le réseau. Il vérifie si la signature électronique apposée par l'émetteur de la transaction est valide si l'adresse de l'expéditeur est bien en possession des fonds qu'elle prétend vouloir transférer sur une autre adresse. Puis il rassemble toutes les transactions validées dans un bloc et les inscrit sur la blockchain.

⁴S. LEGRAND, « Enjeux de la blockchain du point de vue du praticien », in IP/IT, N° 2, Février 2019, Dalloz, p. 86.

synchronisées de l'information assurant sa résilience. La *blockchain* est irréversible-toute inscription est sans possibilité de modification ou de suppression- et authentifiée puisque chaque information est de façon unique et véritable à un utilisateur unique qui peut choisir de rester anonyme.

La *blockchain* a trois fonctions principales. Elle assure le transfert d'actifs, constitue un registre numérique et facilite l'exécution automatique de contrats (*smart contract*). Seuls les deux derniers aspects intéressent principalement la propriété intellectuelle. A ce jour, nous voyons apparaître plusieurs cas d'usage en développement dans la propriété intellectuelle. En effet, il existe des systèmes de datations de créations liés au droit d'auteur, des systèmes de gestion de la rémunération d'ayant droit avec des smart contrats. Aussi, des registres de titres de propriété intellectuelle, des registres privés internes aux entreprises (cahier de laboratoire ou de créations numériques). De plus, il existe des projets d'amélioration de la lutte contre la contrefaçon en utilisant la *blockchain* pour améliorer la preuve et la traçabilité des produits.

Paragraphe 2 : L'admission de la *blockchain* comme moyen de preuve en matière de propriété intellectuelle.

La preuve est au centre du procès civil en contrefaçon. En effet, celui qui engage une action en contrefaçon doit successivement démontrer l'existence de droits de propriété intellectuelle¹, la titularité de ces droits et que ces droits ont été contrefaits et pour déterminer de quelle manière la preuve par *blockchain* pourrait être reçues par le juge et dans quelle mesure elle serait susceptible de concurrencer, voire de supplanter les moyens de preuves jusqu'à présent employés, il y a lieu d'opérer une distinction selon les droits en cause.

Les brevets d'invention, les marques et les dessins et modèles sont des titres de propriété industrielle, délivrés à la suite d'une procédure administrative et qui confèrent à leur titulaire un monopole d'exploitation. Pour prouver l'existence des droits dont il se prévaut, le demandeur doit produire un titre et, le cas échéant, justifier que celui-ci est toujours en vigueur. En réalité rien n'empêche le titulaire de ce titre de propriété industrielle de le convertir en une empreinte numérique et d'ancrer ensuite cette empreinte dans une *blockchain*. Mais devant le juge, seul le titre fait foi et celui-ci peut être obtenu qu'après

¹V. MAGNIER, *Op.cit.*, p. 76.

qu'ont été accomplies les formalités prévues par les textes auprès de l'office compétent pour le délivrer. Il s'ensuit qu'à ce stade, le recours à la *blockchain* ne présente pas ou peu d'intérêt.

La situation va autrement en matière de droits d'auteur. En effet, selon la loi 2-00 relative aux droits d'auteur et droits voisins, l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ainsi la protection au titre du droit d'auteur n'est subordonnée à l'accomplissement d'aucune formalité. En l'absence de titre, celui qui revendique des droits d'une œuvre doit rapporter la preuve, d'une part, de la date de la création, d'autre part du contenu de sa création.

Or, la *blockchain* permet de prouver qu'à la date où les mineurs ont validé la transaction, un document y a été ancré. La *blockchain* jouera un rôle dans l'horodatage de la création. Le demandeur de l'action en contrefaçon pourra en effet produire en justice un certificat numérique, attestant de la date d'ancrage de l'empreinte de l'œuvre. Aussi, l'inscription sur la *blockchain* prouve le contenu de la création, grâce au rapprochement entre le document, la décrivant et son empreinte. Par exemple, l'auteur pourra produire en justice l'original de sa création et le hash inscrit sur la *blockchain* et le comparer avec l'empreinte hashée sur la *blockchain*.

La preuve étant libre le juge n'a aucune raison d'écarter a priori un tel certificat ; il doit, au contraire, l'examiner. Mais, en l'état du droit positif, ce moyen de preuve n'a pas de force probante supérieure aux autres éléments qui lui sont soumis ; des éléments de preuve contraires pourront donc être produits par la partie adverse et seront pareillement pris en considération par le juge. Surtout, la question se pose de savoir dans quelles conditions la correspondance entre l'œuvre revendiquée et l'empreinte numérique enregistrée sur la *blockchain* sera établie ? Cette opération nécessite la traduction d'un langage intelligible en un langage crypté. Il se peut que les tribunaux exigent que le demandeur ait recours à un expert ou à un huissier de justice pour effectuer cette traduction ou en constater les conditions matérielles afin, d'en assurer la parfaite fiabilité¹.

Il faut aussi souligner qu'il ne suffit pas d'établir la date et le contenu d'une création pour bénéficier de la protection au titre du droit d'auteur ; il faut encore que cette création soit

¹S. LEGRAND, *Op.cit.*, p. 85.

originale. Or la *blockchain* ne permet évidemment pas de rapporter la preuve de l'originalité de l'œuvre. Le demandeur de l'action en contrefaçon doit par ailleurs démontrer et prouver la titularité. S'agissant, des brevets, marques et dessins et modèles enregistrés, la preuve de la titularité résulte par application des dispositions légales et réglementaires en vigueur, des mentions portées sur le titre de propriété industrielle et des éventuelles inscriptions aux registres des actes affectant la propriété ou la jouissance du dépôt concerné. Ce sont donc ces éléments et ceux-là seulement, que le juge va examiner. Là encore rien n'oppose à ce que, par exemple, un acte de cession fasse l'objet d'un ancrage dans la *blockchain* ; mais son opposabilité à l'égard des tiers est conditionnée à son inscription au registre.

En matière de droits d'auteur, et malgré l'absence de titre, le recours à la *blockchain* ne semble pas non plus être de nature à faciliter la preuve de la titularité. L'ancrage du document décrivant l'œuvre prétendument contrefaite est réalisé grâce à des clés, l'une publique, l'autre privée ; l'identité de celui qui procède à cet ancrage- qui, au demeurant, n'est pas nécessairement l'auteur de l'œuvre- n'est donc pas mentionnée. Le nom d'auteur pourra certes être indiqué dans le document initial, mais seule son empreinte cryptographique est ancrée sur la *blockchain*. Or, comme il a été dit plus haut, cette empreinte ne saurait constituer une divulgation de l'œuvre ; la mention du nom de l'auteur est donc purement déclarative et aucun effet de droit ne peut lui être attaché¹.

L'apport de la *blockchain* au stade de la preuve de la titularité des droits, semble ainsi être extrêmement réduit. Mais il pourrait s'avérer utile dans deux hypothèses spécifiques. D'une part, en présence d'une œuvre plurale et, plus particulièrement, d'une œuvre de collaboration ou d'une œuvre collective, la *blockchain* permet de protéger toutes les étapes de la création au fil de l'eau ce qui permettra en cas de litige, de déterminer plus aisément la part contributive de chacun. D'autre part, le défendeur pourrait lui-même avoir recours à la *blockchain* pour justifier de ses propres droits et ainsi tenter de renverser la présomption de titularité, qui est une présomption simple, susceptible de preuve contraire.

Par ailleurs, la *blockchain* permet d'assurer la traçabilité d'un produit, et partant de vérifier son authenticité. Elle pourrait donc constituer un outil extrêmement utile pour démontrer qu'un produit mis sur le marché par un tiers est une contrefaçon, quel que soit le droit de propriété intellectuelle en cause. Une telle preuve paraît parfaitement, admissible,

¹S. CANAS, « Blockchain et preuve le point de vue du magistrat », in IP/IT, N° 2, Février 2019, Dalloz, p. 82.

dès lors que la contrefaçon peut être prouvée par tous moyens. Pour justifier de l'atteinte portée à ses droits de propriété intellectuelle, et sous réserve des contraintes techniques déjà évoquées. Le demandeur à l'action en contrefaçon pourra donc verser aux débats la preuve qu'il sera ménagé en ancrant sur la *blockchain* chacune des étapes de la vie du produit objet de ces droits : conception, fabrication, transport, distribution, commercialisation.

Néanmoins, il ne s'agit pas d'une preuve parfaite pour plusieurs raisons. D'abord, il ne suffit pas de rapporter la preuve que le produit argué de contrefaçon ne peut être rattaché à la chaîne de blocs constituée par le titulaire des droits pour que la contrefaçon soit, à coup sûr, constituée. Le juge s'appuiera à vraisemblablement sur d'autres éléments de preuve pour retenir qu'une marque, un modèle ou une œuvre ont été illicitement reproduits ou limités. Surtout, il sera amené à examiner les autres éléments nécessaires à la caractérisation de la contrefaçon. Ensuite, la preuve par *blockchain* n'a pas une force probante supérieure à celle des autres éléments de preuve et le juge en appréciera donc souverainement la valeur et la portée. Enfin, la *blockchain* doit s'accorder avec le principe de loyauté dans l'administration de la preuve. On peut donc s'interroger sur les conditions dans lesquelles les informations stockées sur la *blockchain* devront être recueillies et analysées pour être considérées comme des preuves admissibles.

Paragraphe 3 : Les risques et les incertitudes entravant la preuve par *blockchain*.

Les risques et les incertitudes de la technologie sont encore très importants à l'heure actuelle. Quelques risques technologiques sont susceptibles, même, de mettre en cause l'utilisation de la *blockchain* pour constituer une preuve¹. En effet, comme cité plus haut, la *blockchain* serait une sorte de passeport numérique garantissant l'authenticité et la traçabilité du bien. Cependant, il ya toujours le risque qu'une transaction ne soit pas inscrite dans la *blockchain*, pour une raison ou une autre. Ainsi, pour que la *blockchain* soit efficace, il faut maîtriser tout le circuit de commercialisation. Or, un spécialiste du droit de la distribution, sait combien il est difficile d'assurer l'étanchéité d'un réseau de distribution, afin de lutter contre les reventes hors réseau. Cette difficulté va se retrouver avec la *blockchain*. La tête de réseau devra maîtriser tout son réseau pour que la *blockchain* puisse retracer toutes les transactions et garantir l'authenticité du produit jusqu'à l'achat par le client.

¹L. JOLY, « La Blockchain est-elle une révolution pour la propriété intellectuelle ? », in IP/IT, N° 10, Octobre 2018, Dalloz, p. 537.

Par ailleurs, la *blockchain* est présentée comme un outil qui démocratiserait le droit de la propriété intellectuelle, car le coût d'inscription sur la *blockchain* serait modique. Cela est vrai, le montant de la rémunération des mineurs est faible pour l'instant. Mais cette rémunération est en fonction de l'offre et la demande et le cours de la cryptomonnaies est extrêmement variable. On peut aussi envisager qu'à court, moyen ou long terme, les mineurs n'acceptent de miner rapidement que les transactions bien rémunérées et miner les transactions peu rémunérées avec beaucoup de retard. Il n'est donc pas certain que le coût reste toujours modique.

En outre, chacun sait qu'aucune technique n'est 100% fiable, il existe en effet deux risques, à savoir le risque de piratage et le risque d'altération des données. La *blockchain* publique est réputée infalsifiable, car pour y être inscrite, la transaction doit être validée par 51 % des mineurs comme cité plus haut. En conséquence, il est quasi impossible de modifier le contenu d'une *blockchain* publique, car il faut détenir 51% de la puissance de calcul du minage. Cependant, les mineurs qui valident et conservent les transactions sont censés être animés de bonnes intentions. On la question qui se pose est donc sur le risque de collusion entre mineurs pour modifier le contenu de la *blockchain*. Certes, pour effacer ou modifier une partie des données, il faut revenir sur les autres données antérieures puisque les blocs sont liés entre eux. Une telle opération est très lourde, d'autant plus lourde que la chaîne de blocs est longue.

Ajoutons à cela que la *blockchain* est une technologie. Or, tout change et tout passe. On peut donc légitimement se demander si la *blockchain* sera pérenne, car cette technologie repose sur la confiance que les opérateurs ont dans ce système. La confiance est fragile surtout si des failles informatiques surviennent. Aussi, la *blockchain* est très énergivore car l'opération de minage suppose des ordinateurs très puissants. En effet, des scientifiques réfléchissent à des nouveaux mécanismes et des juristes se demandent si la *blockchain* n'est pas déjà dépassée. Or, les droits de la propriété intellectuelle par exemple le droit d'auteur, s'inscrivent dans la durée de 70 ans pour le droit d'auteur¹. Même, si la certitude n'est pas absolue, on peut donc penser que la *blockchain* sera pérenne².

¹V. art. 59 de la loi 2-00.

²M. MARAURIE-VIGNAL, « Enjeux et défis de la Blockchain dans ses relations avec la propriété intellectuelle », in IP/IT, N° 10, Octobre 2018, Dalloz, p. 533.

Enfin, la caractéristique de toute innovation est d'être en constante évolution. On ne doute pas qu'avec le temps, la technologie *blockchain* évoluera pour faire face aux défis évoqués notamment le défi juridique. Se pose alors la question de la mise en conformité avec la réglementation sur la protection des données à caractère personnel. La *blockchain* est souvent présentée comme une preuve parfaite, car des milliers de mineurs sont, en effet, en concurrence pour valider les transactions. En plus, la *blockchain* repose non sur des personnes de confiance (pas toujours reconnues par tous les Etats), mais sur une technologie soumise à une cryptographie, le hash, qui est universel. Pour autant, il faudra débattre et savoir si cette preuve est supérieure aux autres modes de preuve jusqu'alors utilisées.

Conclusion du Titre II

Nous pouvons conclure que les concepts juridiques fondamentaux permettent d'appréhender les instruments digitaux utiles à la transformation numérique des entreprises. Ainsi, une transaction via internet n'était en principe jamais qu'un contrat à distance, qu'une signature électronique équivalait, à une signature au sens du DOC, que le téléchargement d'un logiciel équivaut à une reproduction d'une œuvre au sens classique du droit d'auteurs, etc. Les exemples ne manquent pas et on peut déduire qu'il n'y a donc pas de vide juridique, même lorsqu'il s'agit de réprimer les abus commis via le numérique.

Cependant, la dimension révolutionnaire du phénomène du numérique se concrétise dans la substitution à un espace physique d'un espace virtuel susceptible de s'étendre aux dimensions du monde et où la localisation des acteurs a perdu toute stabilité. En d'autres termes, la dimension internationale du réseau et la difficulté de localiser l'accès et l'utilisation suscitent un malaise lorsque le droit souhaite prendre le relais d'un contrôle social considéré comme défaillant.

Pour cela, il fallait renforcer le cadre législatif et mettre en place les structures organisationnelles appropriées, ce qui a été entrepris au fil des années touchant à la fois le droit des contrats, la protection du consommateur, la protection des noms de domaines, mais aussi la protection des données personnelles. Certes, comme nous venons de voir, ce qui a été réalisé instaure indéniablement un climat de sécurité dans le secteur du numérique au Maroc promouvant ainsi l'utilité et l'utilisation de celui-ci dans la vie des entreprises. Néanmoins, le législateur marocain a pris du retard concernant la réglementation du numérique et devrait ainsi emboîter le pas à ses homologues européens, afin de poser la pierre angulaire, d'une nouvelle phase économique et juridique celle de la digitalisation des entreprises.

Conclusion de la première partie

Internet a été construit sur un réseau technique : le web. Il a engendré un espace : le numérique. Sur ce nouvel espace des entreprises ont développé des services, des prestations et des biens. Cela a engendré une nouvelle ère. Dans cette ère numérique, les règles font souvent défaut, mais le vide et la liberté font bon ménage¹. Souvent décrit comme un désert juridique, le numérique apparaît comme une sorte de fatras de l'insécurité juridique. En réaction une sécurité juridique de fait et de droit est entrain de s'établir. Ainsi, le développement numérique a un impact sur la sécurité juridique des entreprises. L'entrée des juristes au club du numérique, les a sans doute un peu bouleversés. Difficile pour eux, à première vue, de retrouver leurs balises. Pourtant très vite l'impression de se retrouver en terrain connu.

Ces deux dernières décennies, de nombreuses entreprises nationales et multinationales ont adopté des stratégies de transformation numérique en vue de s'adapter aux contraintes contemporaines. Or un tel processus pourrait constituer un danger pour l'entreprise et son environnement interne : la vie privée de ses dirigeants, ses collaborateurs et ses consommateurs. Aussi, l'absence d'un cadre légal efficace constitue un frein pour les entreprises en phase de transformation digitale, mais surtout un facteur d'insécurité, et par ricochet, de perte de confiance dans le monde virtuel.

Les controverses autour de la digitalisation des entreprises révèlent les interactions entre la régulation juridique et la régulation technique, et d'une manière générale les rapports entre le droit et la technique. La technique et le droit doivent impérativement se reconfigurer pour intégrer la transformation digitale et accompagner les modèles émergents : le droit fondé sur la propriété exclusive et sa transmission ne doit pas rester figé, il peut intégrer les notions et les méthodes qui sont issues de la technique et de ses usagers².

L'avènement de l'internet intensifie d'avantage le sentiment d'insécurité juridique et par conséquent, altère le sentiment de confiance, d'ailleurs l'internet pose des problématiques juridiques aux regards des relations économiques. Certes comme on vient de le voir le législateur tient son rôle dans l'élaboration du droit mais ce qui est plus original c'est

¹Marie-Anne FRISON ROCHE, Internet, Espace d'Interrégulation, Dalloz, Paris, 2016, p.7.

²Mélanie DULONG DE ROSNAY, Les Golems du numérique, Droit d'auteur et Lex Electronica, Presses des Mines, Paris, 2016, p. 235.

la contractualisation du droit à laquelle on assiste dans ce secteur. L'enjeu est donc de mesurer si les secteurs régulés de l'économie engendrent des besoins de réglementation spécifiques lorsqu'ils sont ainsi prolongés ou transposés dans le numérique.

Partie II

La transformation digitale des entreprises et ses mesures de sécurité juridique externes

Le numérique offre aujourd'hui à l'entreprise des outils lui permettant de viser l'excellence opérationnelle : mobiliser ses collaborateurs, se rapprocher de son écosystème, dynamiser l'innovation, autant d'enjeux auxquels il est désormais possible de répondre. En effet, le digital transforme non seulement le monde de l'entreprise mais également ses rapports avec son environnement externe. Ainsi, croire à la transformation digitale en entreprise, c'est s'ouvrir au monde, c'est améliorer les relations avec l'administration, les concurrents et les partenaires. Le numérique est un formidable outil de développement mais il est également porteur de dérives et de menaces¹. Ainsi, l'espionnage industriel est omniprésent. L'interception ou l'appropriation, par le biais des connexions aux réseaux, de données à valeurs économiques constitue un risque qui peut induire à la rupture d'activité².

Par ailleurs, en l'absence d'un contrôle efficace de la part des fournisseurs des services et des autorités publiques compétentes, les internautes se trouvent libres d'accéder via des programmes et logiciels aux systèmes d'information et des bases de données des entreprises dont l'activité fondamentale s'enregistre en ce système³. Le risque numérique ne prend plus aujourd'hui la forme d'attaques visant uniquement les actifs numériques des cibles (système d'information, données), il peut également se matérialiser à travers des actions visant la réputation ou l'image des sociétés, ou encore être le résultat d'atteintes externes mettant en cause le patrimoine de l'entreprise⁴.

L'avènement du cyberspace, notamment en ce qu'il n'a pas de frontière, contraint de repenser les réponses juridiques et le traitement des procédures, et en particulier lors de la phase de responsabilité et de résolution de litiges nés dans l'environnement numérique. Les chefs d'entreprises numériques considèrent l'insécurité juridique comme l'une des principales menaces pesant sur l'activité de l'entreprise. Cette insécurité juridique naît de la nécessité de faire prévaloir des valeurs incarnées dans le droit sur un droit purement formel et désincarné.

Cependant, malgré le fait qu'une époque à l'autre, la recherche de sécurité juridique a connu un certain affaiblissement. La dernière décennie a connu un regain en force. Le succès actuel de la sécurité juridique se manifeste par la fréquence à laquelle revient l'expression

¹S. HOULIERE et D. DE BLOTEAU, « Faire du digital un levier », in Questions de management, N° 7, Septembre 2014, EMS Editions, p. 166.

²J.B. THOMAS-SERTILLANGES, *Op.cit.*, p. 18.

³M. GRANGE, « Internet rattrapé par le droit », in Politique étrangère, N° 4, 2019, Ifri, p. 64.

⁴B. GRUSELLE, *Op.cit.*, p. 62.

même dans le vocabulaire des juristes et des autorités publiques et même des acteurs privés. En effet, le rôle des acteurs privés à coté de l'Etat dans la garantie d'une sécurité juridique est primordial. On assiste de plus en plus à l'accroissement de la régulation non législative. Ainsi, il existe plusieurs mécanismes intervenant dans la régulation, à savoir : les coutumes, les règles mises en place par les réseaux, la cyberjustice ou l'arbitrage et la médiation en ligne, etc. En plus, on trouve des instances de normalisation qui jouent un rôle important dans la définition de la normativité telle que la CNUDCI¹.

C'est dans cette optique que l'entreprise souhaitant bâtir sa transformation digitale est tenue de mettre des mesures de sécurité juridiques visant sa relation avec son environnement externe quelle que soit la nature de la relation administrative, concurrentielle ou encore en cas de litiges. Ainsi il sera utile de se focaliser d'abord sur l'impact de la transformation digitale sur l'environnement externe de l'entreprise (Titre I), avant de s'attarder sur l'engagement de la responsabilité et la résolution des litiges au numérique (Titre II).

¹C. EL OUFIR et A. DIK, « La complémentarité du droit et de la sécurité en matière informatique », in Revue Marocaine de Droit Commercial et des Affaires, N° 3, 2015, p. 37.

Titre I

L'impact de la transformation digitale sur l'environnement externe de l'entreprise

La transformation digitale de l'entreprise impact sa relation avec son environnement externe que ce soit avec l'administration ou les autres entreprises. Parmi les administrations les plus concernées par la digitalisation des entreprises se trouve l'administration fiscale. En effet, à côté de la question fondamentale touchant à l'un des principaux attributs de la souveraineté nationale qu'est la collecte de l'impôt, la digitalisation et la numérisation de l'économie se traduisent également par un remaniement des cartes entre les contribuables et les administrations fiscales¹.

Il est vrai que la loi fiscale est complexe, et ce n'est pas seulement à cause de sa technicité. L'usage de notions aux contours imprécis et vague est une des causes qui affectent la clarté de la norme fiscale notamment en matière de numérique. Il convient d'examiner le degré de pénétration dans le système fiscal de l'impératif de sécurité juridique en matière de numérique. L'engouement pour cette notion exprimée par la doctrine ou par les entreprises est peu de choses par rapport à la place dont elle occupe dans l'ordre juridique². Pour déterminer le niveau de sécurité fiscale en matière numérique, il faut se référer à l'insécurité juridique qui s'y dégage.

Par ailleurs, l'environnement externe de l'entreprise comprend également ses concurrents et toutes personnes souhaitant porter atteinte à l'entreprise autrement dit les cyberattaquers. L'entreprise se trouve donc obliger à veiller au respect de la réglementation concurrentielle de l'économie numérique et se protéger contre toute cyberattaque². L'aspiration à une sécurité croissante nourrit perpétuellement le progrès technique, mais, inversement, chaque nouvelle innovation technologique significative engendre ses propres insécurités et peut fournir des moyens nouveaux pour déjouer des dispositifs de sécurité existants.

¹A-V. ATTIAS ASSOULINE et G. GLON, « Fiscalité du digital, digitalisation de la fiscalité », in *Revue d'économie financière*, N° 131, Mars 2018, p. 127.

²M. NEGGAOUI, « La sécurité juridique en droit fiscal lecture comparative », in *Revue scientifique arbitrale semestrielle des études juridiques juridictionnelles et jurisprudentielles*, N° 4, 2018, p. 42.

Ainsi, il convient de se pencher plus en avant sur l'imposition des entreprises numériques (Chapitre I) devra être abordé par la suite l'entreprise numérique entre concurrence et cybersécurité (Chapitre II).

Chapitre I

L'imposition des entreprises numériques

Du fait de l'évolution des modèles économiques en général, et de l'expansion de l'économie numérique en particulier, la manière dont les entreprises non résidentes opèrent aujourd'hui dans le pays où se situe le marché diffère totalement de ce qui prévalait lorsque les règles fiscales nationales et internationales ont été définies. Les nouvelles pratiques commerciales, conjuguées aux progrès du numérique et à la libéralisation des échanges, ont permis aux entreprises de centraliser la gestion de nombreuses fonctions qui appelaient auparavant une présence locale et physique, rendant ainsi obsolète le modèle commercial traditionnellement appliqué dans le pays du marché. Le fait que les modèles économiques de référence ne reposent désormais plus autant sur la présence physique soulève donc des défis en matière de fiscalité nationale et internationale¹.

En effet, de nombreuses caractéristiques essentielles de l'économie numérique, surtout celles qui ont trait à la mobilité, soulèvent des questions d'érosion de la base d'imposition et de transfert de bénéfices en lien avec la fiscalité directe et indirecte. Par exemple, l'importance des actifs incorporels dans le contexte de l'économie numérique, ajoutée à la mobilité de ces actifs aux fins de l'impôt dans le cadre des règles fiscales existantes, offrent de larges possibilités d'érosion de la base d'imposition et de transfert de bénéfices pour ce qui concerne les impôts directs. De plus, la possibilité de centraliser les infrastructures à distance d'un marché et d'exercer de loin des activités substantielles de vente de biens et de services sur ce marché, ouvrent également des possibilités d'érosion de la base d'imposition et de transfert de bénéfices au moyen d'une fragmentation des activités physiques ayant pour but d'éviter l'imposition.

La réalité est que l'économie numérique est en mutation permanente et il est nécessaire d'en suivre les évolutions futures possibles afin d'évaluer l'impact de celles-ci sur les systèmes fiscaux. Ces évolutions nous conduisent à s'interroger sur les défis posés pour la localisation de l'assiette fiscale des entreprises du secteur du numérique (Section 1), et sur

¹OCDE, « Relever les défis fiscaux posés par l'économie numérique », Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, éd. OCDE, 2014.

la façon dont la taxe sur la valeur ajoutée (TVA) peut être rattachée à l'économie numérique (Section 2).

Section 1 : Localisation de l'assiette fiscale des entreprises du secteur du numérique.

Le champ d'application territorial de l'impôt sur les sociétés est délimité par le Code général des impôts. Celui-ci précise que l'impôt s'applique obligatoirement aux sociétés dont le siège social est au Maroc¹. Néanmoins, il peut s'appliquer à des sociétés qui n'ont pas leurs sièges au Maroc ; si une société possède un établissement dit stable par exemple, exerce une activité sous forme de succursale² ; ou lorsqu'une société exerce une activité lucrative au Maroc dont l'imposition est accordée au Maroc en vertu d'une convention de non double imposition³.

L'existence d'un ou plusieurs éléments d'extranéité peut ainsi conduire à faire échapper les bénéfices réalisés par une entreprise à l'impôt sur les sociétés au Maroc. En présence d'un élément d'extranéité, il convient de déterminer si le droit d'imposer les bénéfices revient au Maroc ou à l'Etat auquel cet élément est rattaché. C'est la raison pour laquelle, le droit interne et la plupart des conventions fiscales font référence à la notion d'établissement stable. La notion d'établissement stable c'est presque entendue de la même façon en droit fiscal interne qu'en droit fiscal international. Néanmoins, elle ne se reflète pas de la même façon au niveau international, du fait que le critère d'établissement stable n'est pas le seul critère de rattachement en droit interne des bénéfices au Maroc alors qu'il est en droit fiscal international.

Les travaux de la Société des Nations Unies menés durant l'entre-deux-guerres sont à l'origine de la détermination du droit d'imposer les bénéfices des entreprises entre les Etats. L'objectif est de trouver un équilibre entre les intérêts des Etats et ceux des entreprises. Il était alors difficilement concevable qu'une entreprise intervienne sur un marché sans présence physique. La notion d'établissement stable a donc été retenue comme critère de localisation des bénéfices des entreprises. Néanmoins, l'économie du XXème siècle n'est plus celle du

¹Les sociétés marocaines (Une société est dite « marocaine » quand elle a son siège social au Maroc ; c'est une société qui est résidente au Maroc) sont imposables au Maroc sur l'ensemble de leurs bénéfices, produits et revenus, qu'ils soient de « source marocaine » ou de « source étrangère » ; à l'exception de certains bénéfices précis et qui sont réalisés à l'étranger.

²V. art. 5 du Code général des impôts.

³« L'impôt sur les sociétés au Maroc (I.S) », consulté le 09-04-2022 à 15h sur <https://www.upsilon-consulting.com>

XXIème siècle. Les échanges dématérialisés l'ont en partie renouvelée. Bien que le droit fiscal soit un droit de superposition ayant vocation à s'appliquer à des situations déjà régies par d'autres branches de droit¹, le Code général des impôts et les conventions fiscales internationales n'ont pas été modernisés, notamment la notion d'« établissement stable ». Cette absence de dépoussiérage fait que beaucoup d'acteurs du numérique – notamment les géants du web, désignés par les acronymes GAFAM² et BATX³ - ne sont pas imposables au Maroc faute d'y avoir un tel établissement.

De ce fait, il est important de préciser les règles de localisation des bénéfices au Maroc et de s'intéresser aux modalités d'imposition des sociétés étrangères disposant de bénéfices de source marocaine. En effet, les bénéfices passibles de l'impôt sur les sociétés sont déterminés en tenant compte des bénéfices dont l'imposition est attribuée au Maroc par une convention internationale relative aux doubles impositions. Le réseau conventionnel marocain est actuellement constitué d'une cinquantaine de conventions fiscales signées et en vigueur ; ce réseau qui s'enrichit chaque année d'une ou de deux nouvelles conventions.

Les conventions fiscales internationales sont rédigées sur la base du modèle de convention fiscale de l'OCDE. Pour éviter qu'une entreprise ne soit imposée à raison des mêmes bénéfices dans deux Etats différents, chaque convention fiscale internationale s'articule successivement autour de trois axes. Il s'agit, tout d'abord, de son champ d'application, ensuite de la détermination du droit d'imposer les bénéfices entre les Etats contractants (Sous-section1) et, enfin, de l'élimination des doubles impositions (Sous-section2).

Sous-section 1 : Détermination du droit d'imposer les bénéfices entre les Etats contractants : Le plan BEPS de l'OCDE.

S'agissant de la détermination du droit d'imposer les bénéfices entre les Etats contractants, les conventions fiscales établies sur la base du modèle de l'OCDE posent un principe aussitôt tempéré par une exception. En se basant sur l'article 7⁴ de ledit modèle, le

¹F. DOUET, « Fiscalité des initial coin offerings (ICOs) », in IP/IT, N° 4, Avril 2019, Dalloz, p. 237.

²Google, Apple, Facebook, Amazon et Microsoft.

³Baidu (Google chinois), Alibaba (équivalent partiel d'Amazon), Tencent (Similaire à Facebook avec notamment Wechat) et Xiaomi (constructeur équivalent d'Apple).

⁴Article 7 du modèle de l'OCDE : « les bénéfices d'une entreprise d'un Etat contractant ne sont imposables que dans cet Etat, à moins que l'entreprise n'exerce son activité dans l'autre Etat contractant par l'intermédiaire d'un établissement stable qui y est situé ».

droit d'imposer les bénéfices d'une entreprise est en principe accordé à l'Etat de résidence de cette entreprise, et, par exception, à l'Etat sur le territoire duquel cette entreprise a un établissement stable. Cette règle a été adoptée afin de localiser les opérations physiques.

La notion d'établissement stable est au cœur des conventions fiscales internationales. Dès lors, il convient de s'attarder sur cette notion telle qu'elle est définie par l'article 5 du modèle de convention fiscale de l'OCDE (Paragraphe1). Son actualisation permettrait l'imposition au Maroc des bénéfices qui y sont générés par les GAFAM (Paragraphe2). Toutefois, cette actualisation soulève des difficultés (Paragraphe 3). En effet, la notion d'établissement stable a été pensée à une époque antérieure à celle de l'économie du numérique d'où les tentatives mondiale de taxation de cette économie (Paragraphe 4).

Paragraphe 1 : Notion de l'établissement stable au sens du modèle de convention fiscale de l'OCDE.

L'article 5 du modèle de convention fiscale de l'OCDE dispose : « Au sens de la présente Convention, l'expression établissement stable désigne une installation fixe d'affaires par l'intermédiaire de laquelle l'entreprise exerce tout ou une partie de son activité ». De ce fait, la reconnaissance d'un établissement stable dans un Etat est subordonnée à l'existence soit d'une installation fixe d'affaires par l'intermédiaire de laquelle l'entreprise exerce tout ou partie de son activité (I), soit d'un agent ne jouissant pas d'un statut indépendant (II). En revanche, le fait qu'une société résidente d'un Etat contractant ait une filiale dans un Etat contractant ne permet pas, à lui seul, de caractériser l'existence d'un établissement stable dans cet autre Etat (III).

I- Installation fixe d'affaires.

En guise d'exemples d'établissement stables, l'article 5 du modèle de convention fiscale de l'OCDE cite notamment un siège de direction, une succursale, un bureau, une usine, un atelier, une mine, un puits de pétrole ou de gaz, etc. L'article 5 de ce modèle précise que la durée d'un chantier de construction ou de montage doit dépasser douze mois pour que ce chantier constitue un établissement stable. Dans ces conditions, la reconnaissance d'une

installation fixe d'affaires implique qu'il ait une présence physique et que cette présence soit durable¹.

Ainsi, de la lecture des exemples cités dans l'article 5, il apparaît que la reconnaissance de l'existence d'une installation fixe d'affaires dans un Etat est indissociable de l'existence d'une présence physique dans cet Etat et a défaut d'établissement stable dans un pays, une entreprise peut donc échapper à l'impôt en dépit du fait qu'elle y a des clients. Cela pose donc la question de savoir si l'utilisation de matériel informatique situé dans un pays peut caractériser l'existence d'un établissement stable dans ce pays².

De plus, la reconnaissance d'une installation fixe d'affaires suppose une présence physique qui soit durable de l'entreprise dans l'Etat d'accueil. La réalisation d'opérations ponctuelles est donc insuffisante pour parvenir à cette reconnaissance. Cependant, il faut souligner que la fonction de l'installation fixe d'affaires est de déterminer l'Etat compétent pour imposer les produits d'exploitation de l'entreprise, c'est-à-dire les produits générés par l'activité qui constitue son principal métier.

A cet égard, l'article 7 du modèle de convention fiscale de l'OCDE relatif aux bénéfices des entreprises – prévoit que « lorsque les bénéfices comprennent des éléments de revenu traités séparément dans d'autres articles de la présente Convention, les dispositions de ces articles ne sont pas affectées par les dispositions du présent article ». Les bénéfices dits passifs - soit les intérêts et les dividendes – ne sont donc pas concernés par le critère de l'installation fixe d'affaires.

En vertu de l'article 11 du modèle de convention fiscale de l'OCDE³, les intérêts perçus par une entreprise peuvent être imposés dans l'Etat de leur source même si cette entreprise n'y possède pas d'établissement stable. Enfin, l'article 5 (4) du modèle de convention fiscale de l'OCDE indique que la qualification d'établissement stable est exclue dans la mesure où les activités visées sont présumées être simplement préparatoire ou auxiliaires. Cela permet d'induire que tout ou une partie de l'activité de l'installation fixe d'affaires doit être productive.

¹Mohammed BELKHEIRI, La fiscalisation des sociétés étrangères : le cas des établissements stables au Maroc, Thèse de Doctorat d'Etat en Sciences Economiques, Université Hassan II, Casablanca, 2006, p. 120.

²Frédéric DOUET, Fiscalité 2.0 Fiscalité du numérique, LexisNexis, 3^{ème} éd., Paris, 2020, p. 283.

³« Articles du Modèle de Convention Fiscale concernant le Revenu et la Fortune, tel qu'il se lisait le 21 Novembre 2017 » consulté le 15-04-2022 à 10h sur <https://www.oecd.org/fr/ctp/conventions/articles-modele-de-convention-fiscale-2017.pdf>

II- Agent sans statut indépendant.

De la lecture de l'article 5 du modèle de convention fiscale de l'OCDE¹, il résulte qu'une entreprise est en principe considérée comme ayant un établissement stable dans un Etat à partir du moment où elle y dispose d'un agent sans statut indépendant. Mais cet article précise que la présence dans un Etat d'un agent sans statut indépendant d'une entreprise ne permet pas de caractériser l'existence d'un établissement stable dans cet Etat lorsque les activités de cet agent sont limitées à des activités préparatoires ou auxiliaires.

En principe, une entreprise est considérée comme ayant un établissement stable dans un Etat pour toutes les activités qu'un agent sans statut indépendant y exerce pour le compte de cette entreprise. La reconnaissance d'un tel agent est subordonnée au respect de deux conditions cumulatives. D'une part, il doit s'agir d'un agent dépendant d'une entreprise étrangère. En effet, les commentaires de l'article 5 (5) du modèle de convention fiscale de l'OCDE indiquent que ce critère du lien de dépendance doit s'effectuer sur la base des circonstances à la fois juridiques et économiques, donc il se subdivise en deux sous-critères cumulatifs à savoir la dépendance juridique et la dépendance économique. D'autre part, l'agent doit avoir le pouvoir de conclure à titre habituel des contrats au nom de l'entreprise étrangère. Ce second critère soulève des difficultés d'interprétation. En délaissant l'interprétation littérale de l'article 5 (5), les commentaires du comité d'affaires fiscales de l'OCDE retiennent que l'appréciation du pouvoir de conclure des contrats au nom d'une entreprise étrangère doit s'effectuer au regard des circonstances de droit et de fait².

III- Insuffisance de la seule existence d'une filiale.

De la lecture de l'article 5 du modèle de convention fiscale de l'OCDE, il résulte que le fait qu'une société résidente d'un Etat contractant contrôle ou soit contrôlée par une société résidente d'un autre Etat contractant ou qui exerce son activité (par l'intermédiaire d'un établissement stable ou non) ne suffit pas, à faire de l'une quelconque de ces sociétés un établissement stable de l'autre. « *Dans ces conditions, le fait qu'une société dispose d'une filiale dans un autre Etat contractant ne permet pas, à lui seul, d'en déduire que cette société*

¹Modèle de la Convention fiscale concernant le revenu et la fortune : Commentaires sur l'article 5, Version abrégée 2017, consulté le 09-04-2022 à 16h sur https://read.oecd-ilibrary.org/taxation/modele-de-convention-fiscale-concernant-le-revenu-et-la-fortune-version-abregee-2017/commentaires-sur-l-article-5_mtc_cond-2017-8-fr#page1 .

²Ibid., p. 5.

a un établissement stable dans cet autre Etat. Dans ce cas de figure, la reconnaissance d'un établissement stable suppose donc le respect des conditions qui permettent de caractériser un tel établissement »¹.

Paragraphe 2 : Actualisation des règles de localisation des bénéfices au Maroc.

Le modèle de convention fiscale de l'OCDE n'était en réalité adapté qu'à des opérations localisables physiquement. Il ne permettait pas d'appréhender les profits de l'économie du numérique. En effet, certains géants du numérique arrivent à réduire de façon importante leur taux global d'imposition. Le caractère immatériel d'une partie importante de leurs activités peut compliquer leur rattachement à un territoire précis aux fins d'imposition à l'impôt sur les sociétés. C'est dans ce contexte qu'en Septembre 2013, les dirigeants du G20² ont approuvé le plan d'action BEPS³ développé par le comité des affaires fiscales de l'OCDE. L'ensemble final BEPS de l'OCDE/G20 a été publié en Octobre 2015 et approuvé par le Conseil de l'OCDE et les dirigeants du G20 en Novembre 2015.

Cet ensemble de recommandations proposé par l'OCDE pour une approche internationale coordonnée de la lutte contre l'évasion fiscale de la part des entreprises multinationales, vise à définir un ensemble unique de règles fiscales internationales pour mettre fin à l'érosion des bases d'imposition et au transfert artificiel de bénéfices vers certains pays ou territoires dans le but de se soustraire de l'impôt⁴. Le plan BEPS dénombre treize rapports finaux et quinze actions destinées à lutter de façon globale et coordonnée contre l'érosion de la base d'imposition et le transfert des bénéfices notamment l'action 1 et l'action 7.

La première action intitulée « Relever les défis fiscaux posés par l'économie numérique ». Cette action identifie les principales difficultés posées par l'économie numérique pour l'application des règles fiscales internationales existantes et élabore des solutions détaillées pour les résoudre, en adoptant une démarche globale et en tenant compte à

¹Frédéric DOUET, *Op.cit.*, p. 284.

²Le Groupe des 20 (ou G20) est un groupe de 19 pays plus l'Union européenne dont les ministres, les chefs des banques centrales et les chefs d'États se réunissent régulièrement. Il a été créé en 1999, après la succession de crises financières dans les années 1990. Il vise à favoriser la concertation internationale, en intégrant le principe d'un dialogue élargi tenant compte du poids économique croissant pris par un certain nombre de pays. Le G20 représente 85 % du commerce mondial, les deux tiers de la population mondiale et plus de 90 % du produit mondial brut (somme des PIB de tous les pays du monde).

³Base Erosion and Profit Shifting ou érosion de la base d'imposition et transfert des bénéfices.

⁴Christiane FERRELL-SCHUHL, *Op.cit.*, p. 620.

la fois de la fiscalité directe et indirecte. La septième action intitulée « Empêcher les mesures visant à éviter artificiellement le statut d'établissement stable ». Cette action appelle à une révision de la définition d'établissement stable, afin d'empêcher le recours à certaines stratégies d'évasion fiscale utilisées pour contourner la définition existante. Cette nouvelle définition est destinée à permettre à un Etat où réside un commissionnaire de considérer que les activités déployées par celui-ci s'analysent en un établissement stable. Ainsi, constituerait un établissement stable toute personne agissant dans l'Etat contractant qui, pour le compte de toute entreprise quelle qu'elle soit, conclut habituellement des contrats ou joue le rôle principal menant à la conclusion d'un contrat dans l'Etat contractant sans que la société située dans l'autre Etat contractant n'ait besoin d'apporter de modification importante audit contrat.

Par ailleurs, une convention multilatérale¹ portée par l'OCDE a été adoptée pour la mise en œuvre des mesures visant à lutter contre l'érosion de la base d'imposition et le transfert des bénéfices et prévoit de modifier les conventions fiscales bilatérales existantes sans renégociation. L'actualisation des règles de localisation des bénéfices au Maroc va conduire à l'élargissement de la notion d'établissement stable. En effet, au sens de l'article 5 du modèle de convention fiscale de l'OCDE, la reconnaissance d'un établissement stable dans un Etat est subordonnée à la présence dans cet Etat d'une installation fixe d'affaires². Il est possible de soutenir qu'un serveur qui héberge des sites web est une installation fixe d'affaires. La difficulté est alors de déterminer l'Etat de situation du serveur. En effet les ressources peuvent être stockées sur de nombreux ordinateurs en réseau, ordinateurs qui peuvent être situés dans des Etats différents. En supposant, que cette difficulté puisse être résolue, cette solution permettrait de reconnaître l'existence d'un établissement stable dans l'Etat sur le territoire duquel est situé un serveur hébergeant des sites web.

Cependant, l'article 5 du modèle de convention fiscale de l'OCDE exclut la présence d'un établissement stable lorsqu'il est fait usage d'installations aux seules fins de stockages. Un serveur qui héberge des sites web est une installation aux seules fins de stockage et, pour cette raison, entre dans le périmètre des exceptions prévues par cet article. Afin d'éviter cette situation, l'OCDE préconise d'élargir la notion d'établissement stable en modifiant l'article 5 du modèle de convention fiscale de l'OCDE. La préconisation consiste à retenir qu'il n'y a pas

¹Convention adoptée le 24 Novembre 2016 et signée à Paris le 7 Juin 2017. Le texte de cette convention est disponible via le lien <https://www.oecd.org/fr/fiscalite/conventions/convention-multilaterale-pour-la-mise-en-oeuvre-des-mesures-relatives-aux-conventions-fiscales-pour-prevenir-le-BEPS.pdf>.

²Voir supra p. 226.

établissement stable uniquement lorsque les activités visées par cette disposition revêtent un caractère préparatoire ou auxiliaire.

La difficulté est alors de déterminer à partir de quel stade une ou des activités cessent d'être préparatoires ou auxiliaires. Selon l'OCDE, « *le critère décisif consiste à rechercher si les activités de l'installation fixe d'affaires constituent en elles-mêmes une part essentielle et notable des activités de l'ensemble de l'entreprise* »¹. Cela conduit à apprécier le caractère préparatoire ou auxiliaire d'une activité au regard de l'activité globale de l'entreprise. En guise d'illustration, il est possible d'imaginer une entreprise basée à l'étranger qui posséderait au Maroc un entrepôt de très grande taille ou travailleraient de nombreux salariés, entrepôt dont le but principal serait d'entreposer et de livrer des marchandises que cette entreprise vendrait en ligne à des clients marocain. Suivant, le raisonnement de l'OCDE, l'entrepôt n'entrera pas dans le champ d'application de l'exception prévue par l'article 5 du modèle de convention fiscale de l'OCDE dans la mesure où les activités qui y sont effectuées constituent une partie essentielle des activités de vente et de distribution de l'entreprise et, pour cette raison, n'ont pas un caractère préparatoire ou auxiliaire. Ainsi, l'usage d'installations aux seules fins de stockage, d'exposition ou de livraison pourrait constituer un établissement stable. Un serveur hébergeant des sites web pourrait être qualifié d'installation fixe d'affaires puisqu'il permet à l'entreprise à laquelle il appartient d'accomplir une part essentielle et notable de ses activités.

Paragraphe 3 : Les obstacles relatifs à l'actualisation des règles de localisation des bénéfices au Maroc.

L'actualisation des règles de localisation des bénéfices au Maroc soulève trois grandes difficultés relatives aux modalités d'application de la convention multilatérale BEPS, à l'optimisation fiscale agressive et à enfin à l'économie numérique. D'abord, les difficultés relatives aux modalités d'application de la convention multilatérale BEPS. En effet, Une grande liberté est accordée aux Etat signataires s'agissant du choix des dispositions de la convention multilatérale BEPS applicables dans leurs conventions bilatérales. A l'exception

¹OCDE, « Empêcher les mesures visant à éviter artificiellement le statut d'établissement stable, Action 7 », Rapport final, éd. OCDE, Paris, 2016, p. 29.

de quatre articles de la convention qui constitue le standard minimum¹, les Etats ont d'une part la possibilité d'émettre des réserves à l'égard des autres articles d'une part, et d'autre part, ils doivent choisir entre plusieurs options offertes au titre de certains d'entre eux.

La convention multilatérale BEPS ne peut s'appliquer qu'entre Etats ayant signé une convention fiscale bilatérale, déposé leur instrument de ratification, formulé les mêmes réserves et adopté les mêmes options. Ces différentes conditions sont de nature à relativiser fortement la portée de cette convention. En Juin 2019, le Maroc a signé la Convention multilatérale pour la mise en œuvre des mesures relatives aux conventions fiscales pour prévenir l'érosion de la base d'imposition et le transfert de bénéfices, devenant la 89ème juridiction à adhérer à la Convention qui couvre maintenant presque 1530 conventions fiscales. Six mois plus tard ; le BEPS a été institué par la loi de Finance de 2020 pour les exercices ouverts à compter du 1^{er} Janvier 2020.

Ensuite, les difficultés relatives à l'optimisation fiscale agressive. Les entreprises du numérique se livrent à une optimisation fiscale agressive. En supposant que la notion d'établissement stable vienne à être effectivement élargie, il est alors probable que ces entreprises mettront en œuvre des stratégies de contournement, notamment en délocalisant leurs serveurs et leurs entrepôts ou en apportant systématiquement des modifications substantielle aux contrats.

Enfin, on soulève des difficultés relatives à l'économie du numérique. Un éventuel élargissement de la notion d'établissement stable se fera au détriment des GAFAM et par conséquent indirectement des Etats-Unis². Sur ce sujet, Hubert Fuchs- représentant du Conseil européen au G20 – a rappelé que l' « *un des grands défis est que la fiscalité de l'économie numérique est avant tout une imposition des entreprises américaine car elles sont les acteurs clés du monde. Les Etats-Unis³ estimant alors qu'il s'agit d'une attaque contre leur économie numérique* »¹.

¹Les quatre actions concernent : la lutte contre les pratiques fiscales dommageables, la lutte contre l'utilisation abusive des conventions, la documentation de prix des transferts et une meilleure efficacité des mécanismes de règlement des différends.

²Frédéric DOUET, *Op.cit.*, p. 289.

³Néanmoins, il faut noter que les États-Unis eux-mêmes font en matière de taxation unilatérale de l'économie numérique. Bien qu'elle ait condamné les pays qui ont mis en place des taxes sur les services numériques au motif que celles-ci taxent les revenus bruts plutôt que les revenus nets, au moins trois États américains, le Maryland, le Nebraska et New York, ont mis en place des législations qui cherchent à faire exactement la même chose et à taxer les revenus bruts des entreprises numériques. En outre, d'autres États américains et au moins une

Paragraphe 4 : Les tentatives de taxation de l'économie numérique.

Suite aux différents obstacles aérant à la taxation de l'économie numérique, différents projets ont tenté de répondre au défi de cette taxation. D'abord, le projet d'assiette commune consolidée pour l'impôt des sociétés, plus communément appelé projet ACCIS. Il a été relancé en 2016 par la Commission européenne². Ce projet vise au renforcement du marché commun par une meilleure intégration des économies européennes et à lutter contre l'évasion fiscale. Bien que bénéficiant d'un fort soutien du Parlement européen et d'un soutien ferme de la France et de l'Allemagne³, le projet ACCIS est enlisé au niveau du Conseil de l'Union européenne. Cet enlèvement est dû au fait que l'unanimité est requise dans la mesure où il s'agit de fiscalité directe. De nombreux Etats sont opposés à la mise en œuvre de l'ACCIS, notamment Malte ou l'Irlande.

Ensuite, le projet d'établissement stable virtuel a commencé à prendre place. L'établissement stable virtuel ou numérique est considéré comme une parade au montage consistant pour une entreprise à s'implanter dans un Etat dans lequel elle sera faiblement imposée tout en réalisant des profits dans des Etats dans lesquels elle ne dispose que d'entrepôts⁴. Grâce à la notion d'établissement stable virtuel, le droit d'imposer les bénéfices qu'une entreprise réalise dans un Etat est attribué à cet Etat en dépit du fait que l'entreprise n'y dispose pas de présence physique. Toutefois, cela est subordonné à la condition que la présence numérique de l'entreprise soit significative.

En France, le concept d'établissement stable virtuel a été proposé en 2013 par la mission d'expertise sur la fiscalité de l'économie numérique. La présence numérique

administration locale, comme l'Oregon¹⁹ et San Francisco²⁰, ont présenté des propositions visant à taxer les revenus bruts de toutes les entreprises, et pas seulement les numériques. Par ailleurs, En juin 2018, la Cour suprême des États-Unis a statué sur l'affaire Dakota du Sud contre Wayfair, Inc. en déclarant que « une entreprise n'a pas besoin d'être physiquement présente dans un État pour satisfaire aux exigences d'une procédure régulière qui nécessitent un lien précis, un lien minimum, entre un État et la personne, les biens ou les transactions qu'elle cherche à taxer ».

¹⁹O. FAMIEN, « Taxation des GAFA : l'UE défend ce projet lors de la réunion du G20 » consulté le 10-04-2022 à 10h sur <https://www.developpez.com/actu/216234/Taxation-des-GAFA-l-UE-defend-ce-projet-lors-de-la-reunion-du-G20-et-souligne-qu-il-ne-s-agit-pas-d-une-attaque-contre-les-entreprises-americaines/>

²⁰Cette idée est ancienne. Elle remonte au « Rapport Neumark » de 1962, suivi du « Comité Ruding » en 1992, de la première esquisse d'une assiette unique est consolidée faite par la Commission européenne en 2001 et d'une proposition de directive du 16 Mars 2011 qui se heurte aux divergences des Etats membres.

³Proposition commune de la France et de l'Allemagne sur la directive ACIS, 19 Juin 2018, p.1.

⁴Les activités de stockage et de livraison constituent dans la plupart des conventions fiscales des exceptions à la qualification d'établissement stable.

significative a été introduite en Israël en 2016 et en Inde en 2019. En Israël et en Inde, l'établissement stable virtuel ne s'applique qu'à défaut de convention fiscale internationale. Au sein de l'Union européenne, la Slovaquie a étendu en 2017 à certaines plateformes la qualité d'installation fixe d'affaires prévue dans la définition de l'établissement stable. Et le 21 Mars 2018, l'établissement stable virtuel a fait l'objet d'une proposition de directive de la Commission européenne¹.

La notion d'établissement stable virtuel a vocation à s'appliquer entre Etats membres indépendamment des stipulations conventionnelles régissant leurs relations mutuelles. Cependant, la proposition de directive de la Commission européenne risque de se heurter à l'absence de consensus sur la question de l'imposition de l'économie numérique. L'unanimité des Etats est requise. De plus, la notion d'établissement stable virtuel ne semble pas avoir les faveurs de l'OCDE, probablement à cause de l'absence de consensus entre les Etats.

En outre, le 21 Mars 2018, la Commission européenne a présenté un projet de taxe sur les services numériques. Cette taxe est fixée à 3% sur les revenus tirés de certains services numériques, taxe appelée Taxe sur les Services Numériques ou TSN. Cette taxe se situe dans le prolongement d'un certain nombre d'initiatives nationales. Plusieurs Etats ont institué des prélèvements assis sur les revus de l'économie numérique. Tel est le cas de l'Italie avec un prélèvement sur les transactions numériques, de l'Inde avec un prélèvement de 6% assis sur le chiffre d'affaires retiré de la fourniture de publicités en ligne par des non –résidents. Dans la mesure où la taxe sur les services numériques s'applique à des activités et non à des entreprises, elle peut concerner des entreprises purement numériques et des entreprises plus classiques en cours de transition vers le numérique.

Les revenus soumis à la taxe sur les services numériques sont réputés localisés dans un Etat membre où les utilisateurs se trouvent. C'est donc l'Etat de destination du service qui est pris en compte et non celui où est située la résidence de l'entreprise qui fournit le service. La localisation est appréciée à partir de celle de l'appareil utilisé pour accéder aux services². L'adresse IP de l'appareil est utilisée pour déterminer sa localisation. La taxe sur les services

¹CE, « Proposition de directive du conseil établissant les règles d'imposition des sociétés ayant une présence numérique significative », 21 Mars 2018.

²Par exemple l'imputation de l'impôt sur les sociétés acquitté sur la taxe sur les services numériques due.

numériques devrait être exigible dans un Etat donné sur la part des revenus imposables considérée comme générée dans un Etat.

Cependant, la taxe sur les services numériques soulève plusieurs séries de difficultés à savoir les entreprises acquittant la taxe sur les services numériques risquent de la répercuter sur leur clients. Aussi, certaines entreprises soumises à l'impôt des sociétés sans chercher à y échapper pourraient également être redevables de la taxe sur les services numériques. Il conviendrait donc de trouver un mécanisme destiné à éviter ce phénomène de double imposition. De plus, la taxe sur les services numériques a été présentée comme une taxe anti-GAFA. En réalité seule Google et Facebook devraient être concernés à travers la vente de publicités ciblées à partir de l'exploitation de données. Pour l'essentiel *Apple* et *Amazon* ne devraient pas être impactés¹.

Enfin, dernièrement la communauté internationale a conclu un accord fiscal sans précédent adapté à l'ère du numérique. La réforme majeure du système fiscal international finalisée le 8 Octobre 2021 à l'OCDE permettra de garantir l'application d'un taux d'imposition minimum de 15 % aux entreprises multinationales (EMN) à compter de 2023². L'accord historique, approuvé par 136 pays dont le Maroc et juridictions représentant plus de 90 % du PIB mondial, permettra également de réattribuer à des pays du monde entier des bénéfices d'environ 100 entreprises multinationales parmi les plus grandes et les plus rentables au monde, de sorte que ces entreprises acquittent leur juste part de l'impôt quelles que soient les juridictions où elles exercent leurs activités et réalisent des bénéfices.

Après des années d'intenses négociations dans le but d'adapter les règles fiscales internationales aux réalités du XXI^e siècle, 136 juridictions (sur les 140 membres que compte le Cadre inclusif OCDE/G20 sur le BEPS³) ont adhéré à la Déclaration sur la Solution reposant sur deux piliers⁴ pour résoudre les défis fiscaux soulevés par la numérisation

¹Pour l'essentiel, l'activité d'Apple consiste à vendre des produits multimédias et l'activité d'Amazon à travers le e-commerce est la vente de contenus culturels. Ces activités sont hors champ.

²« La communauté internationale conclut un accord fiscal sans précédent adapté à l'ère du numérique », consulté le 10-04-2022 à 14h sur <https://www.oecd.org/fr/ctp/beps/la-communaute-internationale-conclut-un-accord-fiscal-sans-precedent-adapte-a-l-ere-du-numerique.htm>

³Quatre pays : le Kenya, le Nigéria, le Pakistan et le Sri Lanka n'ont pas encore adhéré à la Déclaration.

⁴Le Pilier Un garantira une répartition plus équitable entre les pays des bénéfices et des droits d'imposition concernant les entreprises multinationales les plus grandes et les plus rentables. Il permettra de réattribuer une partie des droits d'imposition sur les EMN de leurs pays d'origine aux marchés dans lesquels elles exercent des activités commerciales et réalisent des bénéfices, qu'elles y aient ou non une présence physique. Plus précisément, les entreprises multinationales dont le chiffre d'affaires mondial dépasse 20 milliards EUR et dont

de l'économie¹. L'accord sur l'impôt mondial minimum n'a pas pour objectif de mettre fin à la concurrence fiscale, mais d'y poser des limites convenues multilatéralement. Il faut noter que l'*African Tax Administration Forum (ATAF)* a été très fortement impliqué dans la finalisation de cet accord en mettant en exergue les spécificités de pays africains.

Sous-section 2 : Elimination des doubles impositions.

La problématique de la fiscalisation des bénéfices réalisés à l'étranger se trouve au premier plan des préoccupations des investisseurs engagés dans les affaires à l'international. En effet, le niveau de rendement de telles affaires dépend largement des régimes fiscaux qui leurs sont appliqués au niveau des Etats où les dits bénéfices ont été réalisés, mais aussi au niveau des Etats où les personnes concernées sont installées. La problématique de la double imposition internationale s'impose alors comme le souci majeur desdits investisseurs. D'une façon générale, on parle de double imposition internationale à chaque fois qu'un même bénéfice ou revenu est soumis à l'impôt dans plus d'un Etat. Dans la pratique, on distingue entre deux types de double imposition internationale : la double imposition juridique et la double imposition économique.

Selon l'OCDE, la double imposition juridique internationale peut être définie d'une manière générale comme l'application d'impôts comparables dans deux ou plusieurs Etats au même contribuable, pour le même fait générateur et pour des périodes identiques². La double imposition économique est définie par le comité des affaires fiscales de l'OCDE comme la situation dans laquelle deux personnes différentes sont imposées au titre d'un même revenu ou d'une même fortune. L'exemple classique de la double imposition économique est celui où une société qui est résidente d'un Etat donné subit un redressement d'imposition en matière

la rentabilité est supérieure à 10 % - qui peuvent être considérées comme les grandes gagnantes de la mondialisation - seront couvertes par les nouvelles règles, et 25 % des bénéfices au-delà du seuil de 10 % seront réattribués aux juridictions du marché.

Tandis que le Pilier Deux introduit un impôt mondial minimum sur les sociétés, dont le taux a été fixé à 15 %. Ce nouveau taux d'imposition minimum s'appliquera aux entreprises qui réalisent un chiffre d'affaires d'au moins 750 millions EUR et devrait générer chaque année environ 150 milliards USD de recettes fiscales supplémentaires à l'échelle mondiale. D'autres avantages découleront de la stabilisation du système fiscal international et de l'amélioration de la sécurité juridique en matière fiscale pour les contribuables comme pour les administrations fiscales.

¹Déclaration disponible sur le site suivant : <https://www.oecd.org/fr/fiscalite/beps/declaration-sur-une-solution-reposant-sur-deux-piliers-pour-resoudre-les-defis-fiscaux-souleves-par-la-numerisation-de-l-economie-octobre-2021.pdf>

²OCDE, « Commentaires du modèle de convention fiscale concernant le revenu et la fortune », 2008.

de prix de transfert pour un bénéfice qui a été soumis à l'impôt entre les mains d'une autre société basée dans un autre Etat.

Distinguer entre la double imposition juridique et la double imposition économique est d'un intérêt majeur, car c'est la première qui est principalement visée par les mesures de l'élimination de la double imposition internationale. Une raison logique à cela en est que la double imposition juridique est plus préjudiciable pour les contribuables que la double imposition économique. En effet, dans le cas de la double imposition juridique, c'est une même personne qui doit supporter doublement l'impôt sur le même bénéfice qu'elle aura réalisé, alors que dans la double imposition économique, il s'agit de deux impôts qui sont supportés par deux personnes différentes ; le poids de la double imposition étant moins lourd dans ce dernier cas.

Depuis très longtemps, les Etats ont pris conscience du fait qu'il est de leur intérêt de faire des efforts pour résoudre le problème de la double imposition internationale. En effet, en agissant d'une telle manière, les Etats peuvent, d'un côté, inciter les investissements étrangers à venir s'installer chez eux, et de l'autre côté, encourager les sociétés locales à conquérir des marchés extérieurs¹. En vue d'éliminer la double imposition internationale, un Etat peut mettre en place des mesures dites unilatérales. Il s'agit ici de règles de droit interne qui prennent la forme d'exonérations, de crédits d'impôts étrangers ou même de régimes spéciaux d'imposition. Ces mesures qui sont faciles à mettre en place, du fait qu'ils ne dépendent de la volonté de l'Etat en question, s'avèrent par contre très coûteuses étant donné que le sacrifice fiscal est entièrement pris en charge par l'Etat concerné. Dans la pratique, les Etats préfèrent le plus souvent se lier entre eux par des conventions fiscales internationales afin de contribuer ensemble dans l'effort de l'élimination des doubles impositions ; le sacrifice fiscal est alors partagé.

Il est question, dans ce qui suit, d'étudier les mesures de droit interne marocain pour l'élimination de la double imposition internationale (Paragraphe 1) pour examiner ensuite les méthodes l'élimination de la double imposition internationale et les conventions conclues par le Maroc (Paragraphe 2).

¹J. AIT OUKRIM, « Les techniques d'élimination des doubles impositions Internationales dans la réglementation fiscale marocaine », Université Hassan 1er – Settat, p. 65.

Paragraphe 1 : Les mesures de droit interne marocain pour l'élimination de la double imposition internationale.

Nous pouvons classer les mesures de droit interne marocain qui visent l'élimination de la double imposition internationale en trois catégories. D'abord, les exonérations de l'impôt. Le droit interne marocain prévoit des exonérations qui permettent à certains contribuables de se dispenser du paiement de l'impôt dans des situations spécifiques. Le code général des impôts dans son article 6 prévoit bon nombre d'exonérations qui s'appliquent dans le cas des sociétés engagées dans les affaires à l'international¹.

Concernant les sociétés résidentes, le Code général des impôts prévoit une seule et unique exonération qui bénéficie aux sociétés marocaines réalisant des bénéfices à l'étranger. Il s'agit de l'exonération des dividendes et autres produits de participation similaires de source étrangère. Cette exonération est prévue par l'article 6-I-C-1° du Code général des impôts², elle a été introduite en 2008. A l'opposé du cas des sociétés marocaines, les sociétés étrangères qui réalisent des bénéfices au Maroc peuvent bénéficier d'un grand nombre d'exonérations. Une liste d'exonérations est établie sur la base des dispositions fiscales applicables à partir du 1er janvier 2019 et qui n'est pas exhaustive.

Ensuite, les crédits d'impôt étrangers. En effet, une grande nouveauté introduite par la loi de finances pour l'année budgétaire de 2019 consiste en l'institution de crédit d'impôt étranger profitant aux sociétés marocaines qui réalisent des bénéfices à l'étranger³. Cette nouvelle disposition constitue certainement une grande avancée en matière de l'élimination des doubles impositions au Maroc. Enfin, à côté des exonérations et de la possibilité d'imputation de l'impôt étranger, le dispositif fiscal marocain prévoit également des régimes spéciaux favorables qui servent à alléger la charge fiscale de certaines sociétés qui réalisent des affaires à l'international. Donc, si la double imposition n'est pas éliminée,

¹Mohammed NMILI, Les impôts au Maroc Techniques et Procédures, 5^{ème} éd., 2015, p.

²Dahir n° 1-06-232 du 10 Hija 1427 (31 décembre 2006) portant promulgation de la loi n° 43-06 relative au Code général des impôts.

³Article 19-bis du Code général des impôts : « Lorsque les produits, bénéfices et revenus prévus aux articles 4 et 8 ci-dessus de source étrangère ont été soumis à un impôt sur les sociétés dans le pays de la source avec lequel le Maroc a conclu une convention tendant à éviter la double imposition en matière d'impôt sur les sociétés, l'impôt étranger, dont le paiement est justifié par la société, est imputable sur l'impôt sur les sociétés dû au Maroc, dans la limite de la fraction dudit impôt correspondant aux produits, bénéfices et revenus étrangers. Si les produits, bénéfices et revenus précités ont bénéficié d'une exonération dans le pays de la source avec lequel le Maroc a conclu une convention tendant à éviter la double imposition prévoyant d'accorder un crédit d'impôt au titre de l'impôt qui aurait été dû en l'absence d'exonération, celle-ci vaut paiement... ».

son effet est néanmoins atténué. En effet, plusieurs régimes dérogatoires sont prévus par le code général des impôts. Ces régimes profitent soit à des sociétés résidentes qui réalisent des bénéfices à l'étranger, ou bien à des sociétés non résidentes qui font des affaires au Maroc c'est le cas par exemple du régime des sociétés installées dans les zones franches d'exportation.

Paragraphe 2 : Les méthodes d'élimination des doubles impositions dans les conventions internationales.

Malgré l'intérêt indéniable des mesures de droit interne, il n'en demeure pas moins que les conventions fiscales internationales sont le principal outil en matière de l'élimination des doubles impositions internationales. Ces conventions expriment la volonté des Etats contractants à développer les courants de leurs échanges bilatéraux en concédant une partie de leurs attributions d'imposition respectives. En vue d'éliminer les doubles impositions, les conventions fiscales opèrent globalement de la même façon. Ainsi, et dans un premier temps, une catégorie de revenus se voit exclusivement soumise à l'impôt par l'un ou l'autre des deux Etats contractants. Ensuite, pour les autres revenus, il est prévu des méthodes alternatives d'élimination des doubles impositions au cas où les dits revenus sont imposables dans les deux Etats simultanément.

Dans certains cas, le pouvoir d'imposition d'un revenu donné est attribué à titre exclusif soit à l'Etat de la résidence¹, soit à l'Etat de la source². La double imposition du même revenu est par conséquent évitée, puisqu'un Etat seulement est autorisé à soumettre ledit revenu à l'impôt. Lorsque dans une convention, il est employé l'expression « Ne sont imposables que », celle-ci signifie qu'il y a exclusivité. A titre d'exemple, l'article 7 de la convention Maroc-Canadienne dispose que « Les bénéfices d'une entreprise d'un Etat contractant ne sont imposables que dans cet Etat, à moins que l'entreprise n'exerce ou n'ait exercé son activité dans l'autre Etat contractant par l'intermédiaire d'un établissement stable qui y est situé.... ». A l'inverse du cas précédent, lorsque la convention dispose que des

¹L'expression « Etat de la résidence » désigne l'Etat où une personne est considérée comme « résidente » au sens de la loi fiscale dudit Etat. Dans le cas des personnes morales, l'Etat de la résidence est généralement l'Etat où la personne en question dispose du lieu de son siège social. Mais, il peut également s'agir de l'Etat où une société dispose de son siège de direction effective.

²L'expression « Etat de la source » désigne l'Etat dans lequel un revenu donné prend naissance soit parce que l'activité génératrice du revenu y est exercée ; soit parce que le bien qui produit le revenu en question y est situé ; soit parce que le débiteur du revenu y est domicilié ; soit, enfin, parce qu'un établissement stable y est constitué.

revenus donnés « sont imposables » dans un Etat, cela signifie que les dits revenus peuvent être imposés dans cet Etat si la législation de cet Etat le permet. Mais, dans ce cas, rien n'empêche l'autre Etat d'appliquer l'impôt aux mêmes revenus, puisque la convention n'accorde pas l'exclusivité d'imposition au premier Etat¹.

Ceci étant dit, la convention doit prévoir une disposition parallèle pour l'élimination de la double imposition éventuelle qui apparaîtrait dans le cas où l'autre Etat venait à imposer les mêmes revenus. Généralement, et pour traiter cette situation, les conventions fiscales prévoient deux grandes méthodes de l'élimination des doubles impositions : la méthode de l'exonération et la méthode de l'imputation. Et chacune de ces méthodes contient elle-même des sous-variantes. Notons à ce niveau que ces méthodes d'élimination des doubles impositions se différencient non seulement par la technique de leur mise en œuvre, mais également par le degré de leur efficacité dans l'effacement de la double imposition. On distingue deux méthodes.

D'une part, la méthode de l'exonération, c'est lorsque le résultat de l'entreprise est soumis à l'impôt sur le revenu, la méthode de l'exonération réduit l'assiette de l'impôt marocain et, par conséquent, limite les effets de la progressivité du barème de l'impôt sur le revenu. Dans ce cas de figure, la méthode de l'exonération s'accompagne de la méthode dit du taux effectif. Celle-ci consiste à déterminer le taux de l'impôt en prenant compte les revenus exonérés au Maroc : Sur la base de l'ensemble des produits perçu par l'entreprise au Maroc et à 'étranger, il est tout d'abord nécessaire de calculer le montant de l'impôt qui serait dû par cette entreprise en l'absence de convention de double imposition. Le montant de l'impôt ainsi obtenu est ensuite réduit proportionnellement au rapport existant entre, d'une part, les produits effectivement imposables au Maroc et, d'autre part, les produits qui seraient imposables au Maroc en l'absence de convention de double imposition.

D'autre part, la méthode de l'imputation, cette méthode permet à l'Etat de résidence de l'entreprise d'imposer l'ensemble des produits perçus par cette entreprise. En contrepartie, l'Etat de résidence accorde à l'entreprise un crédit d'impôt égal au montant de l'impôt supporté dans l'autre Etat. Ce crédit d'impôt présente deux particularités. D'une part, il doit être compris parmi les produits imposables dans l'Etat de résidence. D'autre part, il est déductible de l'impôt brut dans l'Etat de résidence qu'à concurrence d'une limite

¹Jalal AIT OUAKRIM, Etude et appréciation critique du système d'imposition des affaires internationales au Maroc, Thèse de doctorat en Sciences Economiques, Université Hassan II, Casablanca, 2010, p. 70.

d'imputation. Cette limite est égale à la fraction de l'impôt calculé dans l'Etat de résidence correspondant au montant des produits nets de l'Etat de la source majoré du montant des crédits d'impôt attachés à ceux-ci.

La règle générale veut que les conventions fiscales ne visent que l'élimination des doubles impositions juridiques, mais il existe un cas de double imposition économique qui est également traité dans les conventions fiscales. En effet, il est des fois inséré dans les conventions fiscales la technique dite de l'ajustement corrélatif qui vise l'élimination de la double imposition dans le cas des redressements en matière des prix de transfert. On retrouve cette technique dans le dernier paragraphe de l'article 9¹ des modèles de conventions fiscales internationales. Le réseau conventionnel marocain est actuellement constitué d'une cinquantaine de conventions fiscales signées et en vigueur ; ce réseau qui s'enrichit chaque année d'une ou de deux nouvelles conventions.

Section 2 : TVA et économie du numérique.

Comme son nom l'indique, la taxe sur la valeur ajoutée frappe la valeur ajoutée dégagée à chaque stade de la production ou de la commercialisation d'un produit. C'est un impôt général sur la consommation perçu au profit de l'Etat. Le montant de la TVA est proportionnel au prix des biens vendus ou des services rendus. En effet, à chaque stade de production ou de distribution, le redevable calcule et facture à son client une taxe correspondant au prix de vente qu'il pratique. Mais lors du règlement au percepteur, l'intéressé impute sur cet impôt le montant de la taxe qui a grevé les éléments de son prix de revient et ne verse que la différence entre la taxe facturée et la taxe déductible.

Dans le commerce intérieur, la neutralité de la TVA pour les assujettis est assurée par le mécanisme du droit à déduction de la TVA. Ce mécanisme autorise, en principe, un assujetti à déduire la TVA sur ses intrants ; l'entreprise joue le rôle d'intermédiaire entre le consommateur et le percepteur. Dans le commerce international, la TVA doit également être

¹Selon le dernier paragraphe de l'article 9 du Model de convention fiscal de l'OCDE : « Lorsqu'un État contractant inclut dans les bénéfices d'une entreprise de cet État — et impose en conséquence — des bénéfices sur lesquels une entreprise de l'autre État contractant a été imposée dans cet autre État, et que les bénéfices ainsi inclus sont des bénéfices qui auraient été réalisés par l'entreprise du premier État si les conditions convenues entre les deux entreprises avaient été celles qui auraient été convenues entre des entreprises indépendantes, l'autre État procède à un ajustement approprié du montant de l'impôt qui y a été perçu sur ces bénéfices. Pour déterminer cet ajustement, il est tenu compte des autres dispositions de la présente Convention et, si c'est nécessaire, les autorités compétentes des États contractants se consultent. »

neutre dans la mesure où elle ne doit pas affecter la compétitivité des entreprises exportatrices et ne doit pas traiter différemment les produits importés et les produits locaux. Cette neutralité est en principe assurée par le principe de destination¹.

Selon le principe de destination, les exportations sont normalement exonérées de TVA avec droit à déduction c'est-à-dire imposées à un taux zéro et les importations sont normalement soumises à la TVA dans le pays de destination. La TVA est donc perçue sur la consommation finale qui a lieu dans la juridiction d'imposition. Au niveau national, la TVA frappe les opérations de nature industrielle, commerciale, artisanale ou relevant de l'exercice d'une profession libérale, accomplies au Maroc. Elle s'applique aussi aux opérations d'importation. Au niveau international, la TVA est régie par la règle de la taxation dans le pays de destination. En vertu de cette règle, la TVA doit être prélevée dans le pays où les biens et les services sont consommés.

L'expansion de l'économie numérique présente de nombreux avantages, Néanmoins, elle pose également un certain nombre de défis auxquels doivent faire face les pouvoirs publics. En effet, plusieurs défis fiscaux sont soulevés par l'économie numérique en matière d'imposition de la consommation, ces défis concernent les systèmes de taxe sur la valeur ajoutée (TVA), notamment lorsque les biens, services et produits incorporels sont achetés par des consommateurs privés auprès de vendeurs à l'étranger et par le biais d'internet². Sur cette base, il sera alors possible d'exposer tout d'abord les modes de recouvrement de la TVA sur les ventes en ligne (Sous-section 1), ensuite il convient de s'interroger sur le sort en matière de TVA de la marchandisation des données personnelles (Sous-section 2).

Sous-section 1 : Le recouvrement de la TVA sur les ventes en ligne.

Les échanges internationaux de biens, services et produits incorporels (qui incluent les téléchargements de produits numériques aux fins de la TVA) soulèvent des défis pour les systèmes de TVA, en particulier lorsque des consommateurs privés achètent des produits auprès de vendeurs situés à l'étranger. Ces difficultés sont renforcées dans le contexte de l'économie numérique, car les avancées technologiques ont considérablement accru les possibilités d'acheter en ligne pour les consommateurs privés et, respectivement, de vendre en

¹A. CHARLET et S. BUYDENS, « Les principes directeurs de l'OCDE pour la TVA/TPS- Présentation et perspectives », in *Revue Européenne et Internationale de Droit Fiscal*, N° 3, 2015, p. 411.

²OCDE, « Relever les défis fiscaux posés par l'économie numérique », *Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices*, éd. OCDE, 2014.

ligne pour les entreprises sans être présentes, physiquement ou par d'autres moyens, dans le pays du consommateur.

Ainsi, La tendance à la numérisation de l'économie¹ a transformé la nature des circuits de vente aux particuliers des biens, des services et des biens incorporels (B2C). Aujourd'hui, le premier réflexe des consommateurs est souvent de consulter le site Internet d'un magasin, ou, pour des biens incorporels, celui d'un fournisseur en ligne, celui d'un vendeur situé dans un autre pays, ou encore, de plus en plus fréquemment, une plateforme numérique par l'intermédiaire de laquelle une multitude de vendeurs réalise des ventes.

La croissance des ventes en ligne des entreprises aux consommateurs situés à l'étranger, tant en volume qu'en nombre de participants, compromet le plus gravement le recouvrement de la TVA. La TVA sur les ventes transfrontalières de services et biens incorporels entre entreprises (B2B), qui est aussi en expansion, est généralement collectée au moyen d'un mécanisme d'auto-liquidation ou d'auto-évaluation tel qu'il est recommandé par l'OCDE dans ses Principes directeurs internationaux pour la TVA². Ces mécanismes d'auto-liquidation fonctionnent généralement bien dans les transactions entre entreprises (B2B), mais ils sont largement inopérants en ce qui concerne les ventes des entreprises aux consommateurs finals (B2C), ce qui est de plus en plus préoccupant au vu de l'explosion des transactions B2C en ligne.

Au vu de l'augmentation ininterrompue du volume des ventes en ligne et du fait que, en principe, la majeure partie de celles-ci devrait être soumise à la TVA, le montant des recettes de TVA en cause est considérable. Comme cela avait été indiqué dans le rapport établi au titre

¹L'expansion de l'économie numérique et les conséquences qui en découlent pour les décideurs politiques, notamment dans le domaine fiscal, sont l'objet d'un grand projet interdisciplinaire de l'OCDE. Des informations supplémentaires sur le projet « Vers le numérique » sont disponibles à l'adresse <http://www.oecd.org/going-digital/>

²Les Principes directeurs internationaux pour la TVA/TPS préconisent un mécanisme d'auto-liquidation (parfois appelé TVA acquittée pour compte ou auto-imposition) dans les cas où cela est compatible avec la conception générale du système national de TVA/TPS. Selon cette procédure, le client est donc en principe tenu de déclarer le montant de la TVA/TPS due sur les services et biens incorporels reçus du fournisseur étranger dans la déclaration de TVA/TPS appropriée en tant que taxe collectée. Le taux applicable est celui en vigueur dans la juridiction du client. Le client dispose ensuite du droit à déduction de la taxe dans les limites autorisées par les règles en vigueur dans sa juridiction. Si le client peut prétendre au bénéfice de la déduction de l'intégralité de la taxe acquittée en amont sur l'opération concernée, il se peut que la législation locale en matière de TVA/TPS n'impose pas la déclaration de la taxe en aval en application du mécanisme de l'auto-liquidation. Dans beaucoup de systèmes de TVA/TPS fonctionnant selon la méthode soustractive indirecte, la TVA/TPS sur les échanges internationaux de services et de biens incorporels B2B est perçue selon le mécanisme de l'auto-liquidation. Néanmoins, le mécanisme de l'auto-liquidation ne s'applique pas dans toutes les juridictions et, là où il est en vigueur, les règles peuvent varier d'un pays à l'autre.

de l'action 1 du projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices (BEPS), intitulé « Relever les défis fiscaux posés par l'économie numérique », les échanges transnationaux de biens, de services et de biens incorporels mettent les systèmes de collecte de la TVA à l'épreuve, en particulier lorsque ces produits sont achetés par des particuliers à des fournisseurs situés à l'étranger. L'économie numérique amplifie ces menaces car l'évolution de la technologie a multiplié les possibilités pour les particuliers de réaliser des achats en ligne et, pour les entreprises, de vendre dans le monde entier sans avoir besoin d'avoir une présence, physique ou sous une autre forme, dans le pays du consommateur. De ce fait, il est opportun d'étudier le recouvrement de la TVA sur la vente en ligne de service (Paragraphe 1) avant d'exposer le rôle des plateformes en ligne dans le recouvrement de la TVA (Paragraphe 2).

Paragraphe 1 : Le recouvrement de la TVA sur les ventes en ligne de service.

Le défi relatif au recouvrement de la TVA résulte de l'essor important des prestations internationales de services et de biens incorporels aux consommateurs finaux réalisées en ligne. L'économie numérique facilite toujours davantage la vente en ligne de tels produits auprès de consommateurs situés dans le monde entier sans présence physique, directe ou indirecte, du vendeur dans le pays où se trouvent les clients¹. Les ventes en ligne de services et de biens incorporels soulèvent des défis pour les systèmes de TVA. Prenons l'exemple d'une entreprise qui propose la diffusion en flux de contenus numériques tels que des films et des programmes télévisés. Les ventes sont réalisées avant tout auprès de consommateurs qui ont accès au contenu numérique au moyen d'ordinateurs, d'équipements mobiles ou de télévisions connectés à l'Internet. Si le vendeur est résident du pays où se trouvent ses clients, il est tenu de collecter et de payer la TVA sur ses ventes dans la juridiction considérée. En revanche, des difficultés peuvent apparaître si le vendeur est non-résident dans la juridiction où se trouvent les consommateurs. En effet, les pays suivent dans l'ensemble deux approches pour recouvrer la TVA sur ces ventes internationales de services et de biens incorporels.

La première approche attribue les droits d'imposition au pays dont le vendeur est résident, selon l'exemple précédent, cette approche conduit à appliquer la TVA dans la

¹M. BOUVARD, T. CARCENAC, J. CHIRON, P. DALLIER, J. GENEST, B. LALANDE et A. de MONTGOLFIER, « Le e-commerce : propositions pour une TVA payée à la source », Rapport d'information, 17 Septembre 2015.

juridiction du vendeur, au taux local en vigueur. Si le pays dont le vendeur est résident n'a pas de TVA ou a fixé un taux plus faible que celui en vigueur dans le pays du consommateur, le montant de l'impôt collecté sera nul ou faible et aucune recette de TVA ne sera perçue par le pays où a lieu la consommation finale.

La seconde approche, attribue les droits d'imposition au pays dont le client est résident, dans ce cas elle devrait conduire, en principe, à une imposition dans la juridiction où a lieu la consommation. Cependant, dans cette situation, les pays rencontrent des difficultés à recouvrer efficacement la TVA sur les services et biens incorporels achetés à l'étranger par les consommateurs. La solution consiste à exiger du consommateur qu'il verse la TVA, ou procède à l'auto-liquidation de la TVA, dans son pays, au taux local en vigueur. Néanmoins, l'inefficacité du mécanisme d'auto-liquidation a été constatée et la probabilité que le consommateur n'acquitte aucune TVA dans ce scénario est très élevée. Pour cette raison, les principes directeurs de l'OCDE dans le contexte du commerce électronique¹ recommandent que les vendeurs non résidents soient tenus de s'enregistrer à la TVA, de la collecter et de la payer dans le pays dont le consommateur est résident, conformément aux règles en vigueur localement. De cette manière, le montant approprié de TVA est acquitté dans le pays où a lieu la consommation. Prenons l'exemple d'une entreprise française développant un site web d'information scientifique et souhaitant élargir son activité d'édition de contenus numériques au Maroc. Cette activité s'analyse juridiquement comme une prestation de service.

Or en vertu de l'article 259 du Code général des impôts, le territoire de rattachement fiscal d'une telle activité est celui du pays dans lequel le bénéficiaire de la prestation a son établissement stable ou sa résidence habituelle. Par conséquent, la clientèle visée étant celle du Maroc, le régime de TVA applicable sera celui inhérent au droit marocain. Ce dernier confirme d'ailleurs dans une note circulaire 717 relative à l'article 88 du Code général des impôts marocain que « pour les prestations de services, le principe fondamental qui détermine leur imposabilité est constitué par le lieu d'utilisation et d'exploitation du service ». Son activité sera taxée au taux marocain de droit commun. Et s'agissant des formalités, les opérations relèveront en vertu du droit marocain, d'une procédure d'auto-liquidation de la TVA. Cela veut dire en pratique que la taxe sera payée au Trésor public marocain par chaque client de l'entreprise via des procédures électroniques dédiées. Et côté entreprise français, les

¹OCDE, « Principes directeurs de l'OCDE du commerce électronique », 2003.

formalités seront donc relativement simples puisqu'il suffira d'établir des factures hors taxe pour chaque transaction¹.

Cependant, l'efficacité de cette approche dépend du respect par les vendeurs non résidents de l'obligation de s'enregistrer à la TVA, de la collecter et de la payer. En d'autres termes, si les droits d'imposition sont attribués à la juridiction dont le consommateur est résident mais qu'aucun dispositif approprié de recouvrement n'est mis en place, aucune TVA ne sera payée. Cet exemple illustre les pressions concurrentielles que les vendeurs nationaux de services concurrents pourraient subir de la part de vendeurs non résidents. Les vendeurs nationaux sont tenus de collecter et de payer la TVA sur leurs ventes de services et des biens incorporels auprès de clients nationaux, tandis que les vendeurs non résidents, selon le scénario retenu, pourraient organiser leurs activités de manière à collecter et payer un montant de TVA nul ou faible. L'exemple montre aussi comment les vendeurs nationaux pourraient être incités à réorganiser leurs activités pour réaliser leurs ventes de services et de biens incorporels depuis un site à l'étranger, afin de n'acquitter qu'un montant faible ou nul de TVA. Cette incitation pourrait résulter de la concurrence émanant des vendeurs non résidents, en mesure de payer des montants de TVA nuls ou faibles, ou s'inscrire dans une stratégie visant à acquérir un avantage concurrentiel sur d'autres vendeurs nationaux qui facturent la TVA. Ces relocalisations conduites par des entreprises nationales peuvent avoir des effets négatifs sur l'emploi et les recettes fiscales directes dans la juridiction considérée.

Dans ce contexte, les pays recherchent de plus en plus les moyens de garantir le recouvrement de la TVA sur les services et les biens incorporels achetés par des consommateurs résidents auprès de vendeurs à l'étranger conformément au principe de destination, en s'appuyant pour l'essentiel sur l'obligation pour les vendeurs non résidents de s'enregistrer à la TVA, de la collecter et de la payer. Le respect de cette obligation repose principalement sur une mise en conformité volontaire de la part des entreprises, les pays disposant de moyens limités pour la faire respecter par les vendeurs non résidents dépourvus d'établissement stable. Dans les pays qui ont adopté cette approche, il semble qu'un nombre important de vendeurs s'acquittent de cette obligation, soit en s'enregistrant à la TVA dans la

¹« Elargir votre e-commerce au Maroc : quelles règles fiscales », consulté le 13-04-2022 à 10h sur <https://compta-e-commerce.com>

juridiction concernée, qu'ils collectent et payent localement, soit en établissant une présence physique dans ce pays et en devenant, de fait, un vendeur national¹.

Toutefois, il est difficile d'obtenir les données relatives aux ventes de services numériques auprès des consommateurs et donc d'évaluer le niveau de respect de cette obligation. Selon certains auteurs, il est impossible à ce jour d'identifier les ventes réalisées par des vendeurs non résidents auprès de consommateurs privés qui devraient être assujetties à la TVA au moyen d'un système de collecte par le vendeur dans le pays où se trouvent les consommateurs. En conséquence, il est estimé que nombre de vendeurs non résidents pourraient manquer à l'obligation de s'enregistrer à la TVA et de la payer dans le pays du consommateur, sans que l'administration fiscale concernée ne puisse exercer des contrôles ou des sanctions à leur encontre. Cela se traduit par une perte de recettes de TVA pour les juridictions concernées et par un risque de pressions concurrentielles inévitables pour les vendeurs nationaux de ces pays.

Il convient en outre de noter que certains systèmes de TVA qui attribuent les droits d'imposition à la juridiction dont le consommateur est résident ou dans laquelle il se trouve réellement ne disposent pas de mécanisme de collecte de la TVA sur les services achetés par des consommateurs privés auprès de vendeurs non résidents. Le plus souvent, les pays concernés ont estimé qu'un tel mécanisme induirait une charge administrative excessive. En conséquence, aucune TVA n'est acquittée sur les fournitures numériques importées dans ces pays par des consommateurs privés. Cette approche pourrait cependant se révéler de moins en moins viable compte tenu de l'essor continu de l'économie numérique, en particulier de l'importance croissante des ventes de produits numériques destinées à des consommateurs finaux.

Paragraphe 2 : Le rôle des plateformes numériques dans la collecte de la TVA.

Les plateformes numériques permettent aux entreprises, en particulier les petites, de toucher aisément des millions de clients sur un marché à l'échelle de la planète. En effet, il ressort d'études récentes que 57 % des ventes transfrontalières de marchandises sont effectuées par l'entremise des trois plus grandes plateformes numériques², une multitude d'autres plateformes opérant à l'échelle d'un pays ou d'un ensemble géographique.

¹OCDE, « Relever les défis fiscaux posés par l'économie numérique », Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, éd. OCDE, 2014.

²International Post Corporation, « Cross-border E-Commerce Shopper Survey », 2017.

C'est pourquoi on estime que près des deux tiers des ventes de marchandises par voie électronique sont conclues par l'intermédiaire de plateformes numériques, le tiers restant étant le fait de ventes directes¹.

Lorsqu'ils conçoivent et appliquent les démarches qui y sont préconisées dans les Principes directeurs et le Rapport final établi en 2015 au titre de l'action 1 du projet BEPS, les pays prennent de plus en plus fréquemment en compte le rôle que les plateformes numériques peuvent jouer dans la collecte de la TVA. Plusieurs juridictions ²ont d'ores et déjà adopté, ou annoncé qu'elles appliqueraient, des mesures impliquant les plateformes numériques dans la collecte de la TVA sur les ventes en ligne de services numériques effectuées par leur intermédiaire. Cette approche est sous tendue par le raisonnement selon lequel une plateforme est considérée comme jouant le rôle d'un magasin dont l'offre englobe la fourniture numérique de films, de musique, de livres, de jeux et applications logicielles et, dans de nombreux cas, elle est le seul point de contact avec le consommateur final d'une prestation de service. On notera en outre qu'elle est considérée comme un moyen efficace et efficient de percevoir la TVA qui, à ce jour, a produit des résultats très positifs.

En outre, certains pays ont prévu le partage d'informations avec les administrations fiscales et ont instauré une responsabilité conjointe et solidaire pour inciter au respect des obligations fiscales. En effet, l'une de leurs principales motivations est le souci de dégager des moyens pour que les douanes puissent redonner aux autres fonctions critiques l'importance qu'elles méritent. En outre les juridictions qui ont adopté les mesures ci-dessus ont déclaré qu'elles étaient en grande partie motivées non seulement par la nécessité de protéger leurs recettes fiscales, mais aussi, dans certains cas, leurs entreprises, et en particulier les magasins physiques, contre une concurrence déloyale .

¹Cette étude couvre plusieurs marchés dans diverses zones du globe, notamment des pays d'Amérique du Nord et latine, d'Europe et de la zone Asie-Pacifique. Bien que le champ de l'étude inclue les ventes des entreprises aux consommateurs aux États-Unis, on notera que la TVA n'existe pas dans ce pays, de sorte que ces ventes n'y sont pas soumises, même si elles peuvent être passibles d'une taxe sur les ventes à l'échelon infranational. Pour des indications plus détaillées, voir le rapport d'enquête à l'adresse <https://www.ipc.be/services/markets-and-regulations/cross-border-shopper-survey>

²L'Australie et l'UE, ont déjà adopté des dispositions législatives pour rendre les plateformes responsables du recouvrement de la TVA/TPS sur les marchandises même si, dans un cas comme dans l'autre, ces règles ne s'appliquent qu'aux importations de biens dont la valeur est inférieure au seuil à partir duquel les droits de douane sont exigibles. Les réformes engagées par l'Australie ont pris effet au 1er juillet 2018. La législation de l'UE est entrée en vigueur en 2021.

De ce fait Le Groupe de travail n° 9 de l'OCDE sur les impôts sur la consommation (GT9), qui est formé par des fonctionnaires des pays membres de l'OCDE et des pays Partenaires, a souligné en 2017 la nécessité pressante d'œuvrer à des solutions cohérentes sur le rôle des plateformes numériques dans la collecte de la TVA sur les ventes en ligne. D'où la naissance d'un rapport¹ de l'OCDE édictant un certains nombre de mesures permettant de rendre les places de marché du commerce électronique redevables de la TVA sur les ventes effectuées au travers elles par les commerçants en ligne².

Les travaux de ce rapport s'inscrivent dans le Programme d'action du G20 sur la sécurité juridique en matière fiscale³. Ce dernier a pour finalité d'assurer une plus grande sécurité juridique aux contribuables afin de favoriser le développement des échanges et des investissements ainsi que la croissance économique, qui est devenue une priorité pour les États comme pour les entreprises. Ce travail part du constat que les plateformes numériques assument un large éventail de fonctions par lesquelles elles pourraient participer à la collecte de la TVA.

On peut ainsi soumettre les plateformes numériques à une obligation de calculer, collecter et reverser l'impôt, leur offrir la possibilité d'assurer volontairement la collecte de la TVA dans le cadre du régime de responsabilité intégrale. Dans ce cas la plateforme numérique est considérée par la loi comme le fournisseur aux fins de l'application de la TVA. Dans ce régime, conformément à la législation du pays d'imposition à la TVA, la plateforme numérique assume la responsabilité totale et exclusive du calcul, de la collecte et du reversement à l'administration fiscale de ce pays de la TVA sur les ventes en ligne effectuées par son entremise. Ce régime de responsabilité est circonscrit aux obligations relatives à la TVA. En dehors de la TVA, il n'aborde aucun autre aspect de la responsabilité des plateformes numériques tel que, par exemple, la responsabilité du fait du produit.

¹OCDE, « Le rôle des plateformes numériques dans la collecte de la TVA/TPS sur les ventes en ligne », Paris, 2019.

²« La communauté fiscale internationale salue les nouvelles mesures pour l'implication des places de marché en ligne dans la collecte de la TVA/TPS dans le commerce électronique », consulté le 13-04-2022 à 16h sur <https://www.oecd.org/fr/ctp/la-communaute-fiscale-internationale-salue-les-nouvelles-mesures-dans-la-collecte-de-la-tva-tps-dans-le-commerce-electronique.htm>

³L'OCDE et le FMI mènent ces travaux, une priorité du G20, avec toute la célérité qui s'impose. Le rapport a été publié dans sa version initiale en 2017 (<http://www.oecd.org/tax-policy/tax-certainty-report-oecd-imf-report-g20-finance-ministers-march-2017.pdf>). Une mise à jour de ce rapport a été publiée en juillet 2018 (<http://www.oecd.org/ctp/tax-policy/tax-certainty-update-oecd-imf-report-g20-finance-ministers-july2018.pdf>)

Parallèlement au régime de responsabilité intégrale en matière de TVA applicable aux plateformes numériques d'autres fonctions peuvent leur être confiées pour contribuer à un recouvrement efficient et efficace de la TVA sur les ventes en ligne. Les pays peuvent adopter des dispositions législatives imposant à ces plateformes l'obligation de communication et de partage informations avec les autorités fiscales. Les administrations fiscales peuvent aussi les utiliser pour atteindre les fournisseurs sous-jacents et proposer même la conclusion d'accords formels entre les autorités fiscales et les plateformes.

Pour ces fonctions, les autorités fiscales doivent veiller tout particulièrement à évaluer la logique sous-tendant ces mesures en étant conscientes qu'elles devront consacrer des moyens humains, financiers et technologiques à l'application et l'administration de ces mesures et, de manière générale, de la nécessité que toutes mesures imposées aux plateformes et aux entreprises soient proportionnées. Les autorités fiscales sont invitées à évaluer l'intégration éventuelle de ces mesures dans une stratégie globale de recouvrement effectif de la TVA sur les ventes en ligne, qui pourraient être combinées avec d'autres mesures.

Enfin, les administrations fiscales peuvent adopter plusieurs mesures pour assurer, entre autres, une meilleure discipline fiscale comme, par exemple, une communication et un dialogue efficaces avec les plateformes numériques, l'utilisation de moyens de contrainte tels qu'un régime de responsabilité conjointe et solidaire¹, sans oublier le renforcement de la coopération administrative et de l'échange de renseignements, tant à l'intérieur des juridictions qu'à l'échelon international².

Sous-section 2 : La TVA et les données à caractère personnel collectées.

Les technologies numériques permettent de collecter, de stocker et d'utiliser des données, ainsi que de rassembler les données de manière distante. Les entreprises recourent à diverses méthodes de collecte de données. Elles peuvent être proactives, en demandant ou en exigeant que les utilisateurs fournissent les données et en conduisant une analyse de celles-ci,

¹En France, la loi de lutte contre la fraude du 23 Octobre 2018 a instauré à l'encontre de certaines plateformes en ligne un dispositif de responsabilité solidaire pour le paiement de la TVA due par les opérateurs qui effectuent, par leur intermédiaire, des livraisons de biens ou des prestations de services taxables en France à destination ou au profit de personnes non assujetties à la TVA ou des importations taxables en France.

²OCDE, « Le rôle des plateformes numériques dans la collecte de la TVA/TPS sur les ventes en ligne », OCDE, Paris, 2019.

ou avant tout réactives, le volume et la nature des données obtenues dépendant en grande partie des utilisateurs, comme dans le cas des réseaux sociaux et de l'informatique en nuage¹.

La plupart des sites internet collectent et utilisent les données personnelles de leurs utilisateurs et sont en mesure de connaître leurs habitudes. Les utilisateurs doivent accepter cette collecte et ce suivi afin de pouvoir visiter le site et utiliser ses services. Une distinction doit être effectuée entre les services numériques qui ne font pas ou peu appel à ces données et ceux au contraire qui reposent sur les données et leurs utilisateurs. Google par exemple, donne accès gratuit à son moteur de recherche, à *Gmail*, *Google Map* et *Google docs*. Malgré l'apparente gratuité, il collecte cependant nombre de données lui permettant, par exemple, d'offrir de la publicité ciblée. De la même façon, *Facebook* ou *LinkedIn* offrent un accès gratuit à leur plateforme de médias sociaux, mais recueillent et vendent les données des utilisateurs.

Dans le contexte de l'économie numérique, la mise à profit des données peut créer de la valeur de différentes manières pour les entreprises, y compris en leur permettant de segmenter les clients potentiels pour proposer des offres sur mesure, de parfaire la mise au point de leurs produits et services, de mieux comprendre les variations de leurs résultats ou d'améliorer leur prise de décision. Les utilisateurs des sites internet et des réseaux sociaux participent à la création de valeur en concourant au fonctionnement d'un modèle économique qui repose sur la fourniture et l'utilisation de leurs données personnelles. La collecte des informations personnelles permet au site d'engranger des recettes en les vendant à un courtier de données (*data broker*), en vendant des bannières publicitaires ciblées et en orientant ses utilisateurs vers d'autres sites.

Suivant ce raisonnement, de nombreux contrats de fourniture de service de réseautage social prévoient des clauses affirmant que les services proposés sont gratuits c'est-à-dire sans contrepartie, alors que si toute contrepartie monétaire est exclue, les données, informations et contenus qu'il dépose, consciemment ou non lors de l'utilisation du réseau social, constituent une contrepartie qui s'analyse en une rémunération ou un prix. Par exemple, la chaîne

¹OCDE, « Relever les défis fiscaux posés par l'économie numérique », Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, éd. OCDE, 2014.

Japonaise *Shiru* Café propose à ses clients de payer leurs boissons en cédant leurs données personnelles à des entreprises qui effectuent ensuite du ciblage marketing¹.

Les prestations de services effectuées à titre onéreux par un assujetti agissant en tel que tel sont soumises à la TVA. Certains commentateurs caractérisent cette pratique comme une nouvelle forme de troc. La question est de savoir si d'un point de vue TVA, elle peut être qualifiée en tant que telle (transaction de troc), ou comme une prestation de service classique dans laquelle la rémunération prend la forme non pas d'argent, mais de données personnelles². Le rôle croissant joué par les données soulève plusieurs questions concernant la pertinence des règles actuelles en matière de lien, l'opportunité d'imposer les bénéfices obtenus par une entreprise grâce à une collecte de données, ainsi que la question de la pertinence de la qualification et de la valorisation des données aux fins fiscales.

A partir du moment où un site internet subordonne son utilisation à la condition que les internautes acceptent de lui transmettre des données personnelles à des fins mercantiles, reste alors à savoir si les services fiscaux peuvent ou non réclamer de la TVA à ce site à raison de cette opération. Cette question sous-tend plusieurs d'autres qui s'articulent autour du champ d'application de la TVA en matière de données personnelles d'une part (Paragraphe 1) et d'autre part de l'assiette, du fait générateur et de l'exigibilité de cette TVA (Paragraphe 2).

Paragraphe 1 : Le champ d'application de la TVA en matière de données personnelles.

Seules relèvent de la TVA les prestations de services intégrées dans un marché, même réglementé, ouvert à la concurrence. En d'autres termes, une activité située hors circuit économique normal échappe à la TVA dans la mesure où elle ne crée pas de risque de distorsion de concurrence avec les activités économiques³. La fourniture de prestation de services par un site Internet en contrepartie de données personnelles ayant une valeur marchande intègre un circuit économique normal. Retenir une solution contraire entraînerait une distorsion de concurrence avec les sites dont l'accès est subordonné au paiement d'une somme d'argent.

¹« Dans ce café, la clientèle paie avec ses données personnelles », consulté le 14-02-2022 à 10h sur <https://www.slate.fr/story/167921/cafe-clientele-donnees-personnelles>

²E. BERNSTEIN et Th. J. LEE . « Where the Consumer is the Commodity: The Difficulty with the Current Definition of Commercial Speech », 2013, p. 82.

³Par exemple un trafiquant de fausse monnaie ne peut être soumis à la TVA dans la mesure où son activité se situe hors du circuit économique normal et qu'il n'existe aucun risque de concurrence avec les activités économiques.

Par ailleurs, seules les opérations effectuées à titre onéreux entrent dans le champ d'application de la TVA. Une contrepartie est nécessaire mais sa nature (somme d'argent, échanges de biens, service rendu...) et son montant sont indifférents. La fourniture de leurs données personnelles par les utilisateurs d'un site internet en contrepartie de l'accès à ce site s'analyse donc en une contrepartie au sens de la TVA. Les utilisateurs et le site ont des obligations réciproques. Déjà en 2015, le Forum économique mondial avait posé la question de savoir si les données étaient la nouvelle monnaie ¹ et des chercheurs ont reconnu que la pratique consistant à fournir des données représente une forme de contrepartie dans le cadre d'un nouveau type d'échange. Il semble incontestable que les plateformes obtiennent une contrepartie en échange de leurs données.

S'agissant du montant de la contrepartie, la TVA ne frappe pas un résultat mais un chiffre d'affaires. La recette afférente à une opération est donc imposable même en cas d'opération effectuée à perte. Peu importe donc que la valeur des données personnelles des internautes soit ou non équivalente à celle de la prestation de services par les sites internet. En outre, pour qu'une opération entre dans le champ d'application de la TVA, il doit exister un lien direct entre le service rendu et sa contrepartie. Cette solution se situe dans le prolongement de la jurisprudence de la Cour de Justice des Communautés européennes qui a jugé que « *la notion de prestation de services effectuée à titre onéreux... suppose l'existence d'un lien direct entre le service rendu et la contre-valeur reçue* »². Concrètement, l'opération doit procurer un avantage au client et la contrepartie remise par celui-ci doit être en relation avec cet avantage étant précisé que cette seconde condition n'implique pas un rapport d'équivalence.

L'utilisation des services d'un site internet est subordonnée à l'acceptation par l'internaute de ses conditions générales d'utilisation, notamment à l'acceptation que ce site utilise les données personnelles de l'internaute. D'une part, l'opération procure à l'internaute le droit d'utiliser les services d'un site internet et, d'autre part, le fait de consentir que ses données personnelles soient utilisées est en relation avec cet avantage car à défaut il ne pourrait pas y accéder. Il faut donc que les parties agissent dans le cadre d'une relation juridique qui les oblige. Toutefois, il se peut que les clients ne se sentent pas engagés à partager des données afin d'obtenir l'accès à une plateforme à titre de contrepartie. Il peut

¹N. CHANDRASEKARAN, « Is Data the new Currency? », 14 August, 2015,

²CJCE, 6ème ch., arrêt n° 102/86, 8 Mars 1988, Apple and Pear Development Council contre Commissioners of Customs and Excise.

également être soutenu qu'il ne peut y avoir de lien direct entre la fourniture de données et la réception de services électroniques. En revanche, dans ce cas les plateformes peuvent bloquer ou entraver l'accès des consommateurs en cas de refus de partage de données personnelles¹.

Il semble donc qu'un lien direct puisse être reconnu entre le droit d'utiliser les services d'un site internet et les données personnelles de l'internaute qui accède à ce site. Peu importe le degré d'utilisation effective de ces services par l'internaute. Lorsqu'un contrat porte sur le droit d'accéder à un service, l'importance de l'utilisation effective de ce service est en effet indifférente en matière de la TVA. La doctrine souligne que l'existence d'un lien direct est compatible avec le fait que le service rendu ne soit pas mesurable avec précision.

Paragraphe 2 : L'assiette, le fait générateur et l'exigibilité de la TVA en matière de données personnelles.

Parmi les prestataires de services immatériels figurent les prestataires de services électroniques. Pour l'application de la TVA, ces prestataires soulèvent des difficultés liées à leur localisation et leurs modalités d'imposition. D'une part, pour les prestataires de services, l'assiette de la TVA est constituée par toutes les sommes, valeurs, biens ou services reçus ou à recevoir du preneur par le prestataire en contrepartie ces prestations. La TVA doit donc être assise sur la valeur des données personnelles que l'internaute autorise le site Internet à utiliser en contrepartie de l'utilisation des services de celui-ci. La détermination de cette valeur peut sans doute donner lieu à d'innombrables discussions, mais l'exercice semble loin d'être impossible. Il suffit de se référer au prix moyen auquel un courtier de données (data broker) revendrait à des fins publicitaires les données d'un utilisateur d'un site internet donné.

Nous pouvons envisager deux hypothèses, la première, très peu probable en pratique, est celle dans laquelle un site Internet s'acquitterait spontanément de la TVA afférente à la valeur des données personnelles des internautes qui, pour accéder à ce site, ont autorisé celui-ci à les utiliser. Les services fiscaux ont alors la possibilité de contester cette valeur dans le cadre d'une procédure contradictoire. La seconde, plus vraisemblable, est celle dans laquelle l'administration fiscale taxerait d'office un site Internet pour défaut de déclaration de TVA.

¹M. LAMENSH et E. TRAVERSA, « Plateformes numériques : développement récents en matière fiscale », in Revue International de droit économique, 3^{ème} trimestre, 2019, p. 342.

Il incomberait alors à ce site de démontrer le caractère excessif de l'évaluation faite par les services fiscaux¹.

D'autre part, le fait générateur et l'exigibilité de la TVA afférente aux prestations de services ne coïncident pas. En effet, le fait générateur est fixé à la date de l'exécution de la prestation alors que l'exigibilité est fixée à la date d'encaissement des acomptes, du prix ou de la rémunération. La date d'exigibilité de la TVA est la plus importante en pratique car il s'agit de la date à laquelle l'administration fiscale a le droit d'en réclamer le paiement. Le droit d'utiliser les services d'un site internet se situe au moment où l'internaute accepte que ce site utilise ses données personnelles. Dans la mesure où celles-ci constituent la contrepartie remise par l'internaute au site Internet en contrepartie du droit d'y accéder, il est donc possible de considérer que la TVA afférente à cette prestation de services est exigible lors de la première connexion à ce site. A défaut de dispositions spécifiques contenues dans le Code général des impôts, il convient de s'interroger sur le cas de figure dans lequel le volume des données personnelles de l'internaute détenue par le site Internet augmente avec le temps. Une difficulté majeure réside dans le fait que l'événement imposable doit se produire à un moment déterminé dans le temps, alors que la fourniture de données se déroule sur une base continue.

En théorie, le supplément de données pourrait être regardé comme un complément de contrepartie rendant la TVA exigible. Mais, en pratique, cette solution n'irait pas sans soulever de nombreuses difficultés relatives notamment à l'évaluation du supplément de données et à la détermination de l'exigibilité de la TVA. Cela devrait conduire le législateur à fixer des règles précises en rendant la TVA exigible soit une seule fois lorsque l'internaute accorde au site Internet le droit d'utiliser ses données personnelles, soit plusieurs fois en fonction de l'augmentation du pourcentage de ces données détenues par le site. Enfin, alors même que l'idée d'une application de la TVA sur les services offerts gratuitement par les plateformes en échange de données personnelles peut sembler séduisante, de nombreux obstacles techniques et pratiques semblent s'y opposer. Une taxation alternative pourrait être la solution. Une telle solution doit cependant faire l'objet d'une analyse critique afin de ne pas créer de nouvelles formes de discrimination².

¹Frédéric DOUET, *Op.cit.*, p. 362.

²Ibid., p. 362.

Chapitre II

L'entreprise digitale entre concurrence et cybersécurité

Le droit devra être peu adhérent aux techniques, harmonisé et ouvert aux initiatives des entreprises numériques. Le droit applicable au numérique est une matière vivante dont la mission est d'accompagner au bon rythme l'évolution des sociétés, en évitant les décalages susceptibles de déconnecter les approches juridiques des réalités techniques ou vécues par les utilisateurs et notamment les entreprises¹. En effet, les entreprises sont confrontées lors de leurs transformations digitales non seulement à une concurrence accrue sur le marché numérique mais également à des risques de cyberattaques.

L'analyse de la concurrence joue un rôle central dans l'ensemble de la théorie économique. En effet, le fonctionnement d'un marché n'est pas le même selon qu'il y a ou non une concurrence. La concurrence doit se définir, comme la liberté d'entrer sur un marché. Un marché, pour sa part, est le lieu sur lequel se pratiquent les échanges qu'il soit réel ou virtuel. On peut donc dire que la concurrence implique la liberté pour deux partenaires d'entrer dans une relation d'échange². Chacun est libre de proposer ses services ou ses biens, chacun est libre de les accepter ou de les refuser.

Par ailleurs, les cyberattaques ont vu leur nombre se multiplier ces dernières années. Elles se sont amplifiées depuis 2020 avec la crise sanitaire. Les cyberattaques participent à un phénomène criminel sans précédent. Elles sont répandues et liées à une cybercriminalité maintenant organisée en service et en marcher sur le *darknet*. Les victimes sont quotidiennes, les cibles sont diverses et ouvertes, et les attaquants ont recours à des techniques innovantes pour réaliser leurs activités malveillantes³.

C'est ainsi qu'il sera utile de se focaliser d'abord sur la régulation concurrentielle de l'économie numérique (Section 1), avant de s'attarder sur la cybermenace et la cybersécurité des entreprises numériques (Section 2).

¹G. POUPART, « Le droit au service de la cybersécurité », in IP/IT, N° 3 Mars, 2018, Dalloz, p. 160.

²Pascale SALIN, La concurrence, Presse Universitaire de France, 1^{ère} éd. Paris, 1995, p. 107.

³D. GUINIER, « Modèle de représentation des cyberattaques, mesures génériques et prospective », in IP/IT, N° 3, Mars 2018, Dalloz, p. 163.

Section 1 : La régulation concurrentielle de l'économie numérique.

L'information représente aujourd'hui le nouveau pétrole et la principale matière première de l'économie, et un instrument de compétition et de pouvoir de marché. Son utilisation et sa maîtrise sont devenus faciles du fait, de l'émergence du numérique. Aussi, on assiste à une naissance des pratiques qui se proposent de rechercher la bonne information, de vérifier les bonnes sources, de la diffuser afin de créer de la valeur ajoutée au sein des entreprises. Il s'agit de la veille stratégique ou de l'intelligence économique. L'intelligence économique est basée sur la collecte des informations et sur l'analyse quasi-automatique des données. Elle débouche sur une intelligence cognitive dont le but est de prendre une décision finale basée sur l'anticipation des comportements des concurrents et de leurs stratégies.

La concurrence désormais porte aussi sur les connaissances (des technologies, des *process*). De ce fait, l'analyse de l'intelligence économique ne se limite pas à une logique de sécurité et de protection mais aussi à un outil de management qui nécessite recherche, innovation et traitement au sens large des connaissances afin de préserver et d'accroître la compétitivité. C'est dans cette optique qu'il serait opportun de mettre la lumière sur la détention de la donnée comme facteur de pouvoir du marché (Sous-section 1), ce qui permettrait par la suite de comprendre l'intelligence économique à l'ère du numérique (Sous-section 2). Enfin, le monde du numérique fait naître des contentieux liés à la concurrence et la propriété intellectuelle de l'entreprise (Sous-section 3).

Sous-section 1 : La détention de la donnée comme facteur de pouvoir du marché.

Le pouvoir de marché d'une entreprise définit sa latitude à fixer les prix de vente sur un marché donné au-dessus de ses coûts de production sans tenir compte de ses concurrents. Transposée, au secteur de la donnée, cette analyse couvre également l'existence de facteurs spécifiques, tel que l'accès à un large volume de données ou à une importante variété de données qui peut constituer un véritable facteur de compétitivité sur le marché¹. Par principe, les données sont partout et substituables. Exceptionnellement, elles deviennent indisponibles si des entreprises ayant accès à des données très spécifiques ou à une grande quantité de

¹N. LANERET, R. KNITTEL et A. BAUDEQUIN, « Protection des données personnelles : quand le droit de la concurrence s'en mêle », in IP/IT, N° 12, Décembre 2017, Dalloz, p. 619.

données se montrent réticentes à en faire profiter leurs concurrents ou les utilisent à leur rencontre¹.

Ainsi, les ressources à mettre en œuvre pour collecter ces données peuvent constituer une barrière à l'entrée aux nouveaux entrants s'ils ne sont pas en mesure de collecter ou d'acheter le même type de données, en termes de volume et/ou de variété que les entreprises déjà en place. Et même si chaque entreprise peut en théorie acquérir des données et rattraper l'avantage des entreprises déjà établies, en pratique cela s'avère impossible au regard de la quantité et de la qualité des données détenues par ces entreprises déjà en place, lorsqu'elles disposent d'une base clientèle et d'informations tellement large que la question se pose de savoir si un nouvel acteur est en mesure de reproduire le même volume et la même qualité de données. Cette situation est courante pour les entreprises ayant une partie de leurs activités en situation de monopole et qui souhaitent développer des activités concurrentielles.

De ce fait, l'accumulation de données et leur exploitation algorithmique ne sont pas en soit condamnables par le droit de la concurrence². Ce qui l'est, en revanche, c'est le pouvoir de marché qu'elles peuvent conférer à des entreprises, qui en abuseraient et leur permettraient de dominer le marché du numérique (Paragraphe 1). Ce marché où les données massives constituent un actif ou un intrant important pour le succès commercial, il pourrait se poser le problème que l'accumulation massive d'informations personnelles et le recours intensif à l'analyse de données puisse accroître le pouvoir de marché, verrouiller le marché et créer des barrières à l'entrée. Une telle situation pourrait inciter les entreprises à adopter d'une part des pratiques anticoncurrentielles algorithmiques (Paragraphe 2). Et d'autre part, supprimer l'interopérabilité dans le marché numérique pour préserver leur position dominante (Paragraphe 3).

Paragraphe 1 : Le marché numérique dominé par les « *Big tech* ».

A l'heure actuelle, *Google* et *Facebook* forment un duopole dont la force repose sur sa complémentarité : l'un sait ce que vous cherchez et l'autre sait ce que vous aimez.

¹Amélie FAVREAU, « Remarque sur le droit de la concurrence et nouvelles technologies : perturbateurs des systèmes en place » in L'articulation des droits de propriété intellectuelle et du droit de la concurrence, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020, p. 56.

²Wladimir SOLTSMANN, « L'encouragement à l'innovation par la concurrence, malgré les contraintes du droit de la concurrence » in L'articulation des droits de propriété intellectuelle et du droit de la concurrence, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020, p. 126.

Mais, *Amazon*, second plus grosse valeur boursière après *Apple* est le challenger le plus sérieux avec sa plateforme de vente en ligne et désormais son enceinte *Bluetooth intelligente Echo*, qui lui permettent l'accès de nombreuses données. Or, il s'agit d'un autre *big tech* faisant partie des GAFAM. En effet, les *big tech* ne se concurrencent pas, ils cohabitent dans la domination et finalement convergent dans une stratégie qui consiste à capter les ressources et occuper le terrain. Deux facteurs semblent être à l'origine de la domination des *big tech* : l'accaparement des leviers de croissance par les plus forts, permis par une insuffisance d'encadrement¹.

Google et Facebook bénéficient de plusieurs avantages concurrentiels qui sont autant de leviers de croissance. D'abord, leurs effets sur le réseau, selon la loi *Metclaff*, du nom de son inventeur l'ingénieur américain *Robert Metclaff*, plus il y a d'utilisateurs dans un réseau, plus ce réseau attire d'autres utilisateurs jusqu'à enregistrer un emballement. *Google* et *Facebook* multiplient les interfaces qui profitent de cet effet de réseau, lequel constitue donc une barrière à l'entrée pour les challengers².

Ensuite, *Google* et *Facebook* ont aussi diversifié leurs services selon un modèle d'intégration verticale. Ainsi, en plus d'offrir des services aux internautes et des services publicitaires, ils sont présents également en tant qu'intermédiaires techniques³. *Google* représente 80% du marché de l'intermédiation. Les annonceurs deviennent donc dépendants des écosystèmes de *Google* et *Facebook* : en termes d'audience, leurs interfaces sont incontournables et leurs outils, compatibles entre eux, en font un véritable écosystème fermé⁴.

Enfin, avec leurs nombreuses interfaces, *Google* et *Facebook* ont un accès privilégié aux données de masse (*big data*)⁵ qui constituent, en matière de publicité digitale le nerf de la guerre. C'est ce qui explique la gratuité des services ; l'utilisateur est le produit. Les données personnelles sont qualifiées de nouvel or noir du XXI^{ème} siècle et y avoir accès représente un véritable enjeu. Les *big tech* redoublent d'efforts pour allonger le temps passé par l'internaute sur le réseau afin d'optimiser l'audience et d'améliorer la qualité et la précision des données de différentes natures permettant autant de formes de ciblage.

¹S. CHOLET, « La publicité digitale encouragée » in L'articulation des droits de propriété intellectuelle et du droit de la concurrence, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020, p. 151.

²Facebook a démarré avec un réseau social très populaire et a acheté Instagram et WhatsApp et Google a créé Google et a acheté Youtube.

³Achat par Google de DoubleClick en 2008 et d'AdMob en 2009

⁴Google Ads, AdSense, Google Ad manager

⁵Voir supra p. 174.

*Google*¹ et *Facebook* ont pu accaparer tous ces leviers de croissance car ils ont bénéficié d'un cadre juridique favorable. Ainsi, la loi 09-08 relative à la protection des données à caractère personnel n'impacte que peu *Google* et *Facebook* qui continuent de valoriser au maximum les données ; ils obtiennent le consentement des internautes à l'utilisation des cookies lors de leur entrée dans le réseau et, une fois le consentement obtenu sur l'usage de la technologie, il est très difficile de contrôler l'exploitation des données.

C'est vrai que *Google* a élaboré de nombreux produits innovants qui ont changé le cours de nos vies. Cependant, ceci ne lui permet pas pour autant le droit de priver les autres entreprises de la possibilité de la concurrence et d'innover. Dans ce sens, et plus récemment en 2019, *Google* a été condamnée par la Commission européenne à une amende de 1,4 milliard d'euros et lui a été enjoint de mettre fin à ses pratiques illégales et de s'abstenir de toute mesure ayant un objet ou un effet anticoncurrentiel. Dans cette affaire, *Google* est poursuivie pour des pratiques visant à exclure des régies publicitaires concurrentes, via sa plateforme *AdSense for search*, qui permet de placer de la publicité contextuelle sur les sites de ses partenaires, en fonction des recherches effectuées par l'internaute sur ces sites².

La Commission a dénoncé les pratiques suivantes. Premièrement, une exclusivité c'est-à-dire que les tiers ne peuvent afficher de publicités contextuelles émanant de concurrents de *Google* notamment *Microsoft* et *Yahoo*. Deuxièmement, *Google* se réserve des meilleurs emplacements de publicité autrement dit, les tiers doivent accepter un nombre minimum de publicités contextuelles de *Google* et leur réserver les meilleures places sur leurs pages de résultats de recherche. Troisièmement, *Google* se donne le droit d'autoriser des publicités concurrentes, ainsi les tiers doivent obtenir l'autorisation de *Google* avant de modifier l'affichage des publicités contextuelles concurrentes³.

La Commission européenne craint que ces pratiques réduisent les possibilités des concurrents de *Google* et donc la capacité des sites web tiers à investir dans la fourniture de choix et de services innovants aux consommateurs. Les lourdes sanctions prononcées par la Commission européenne contre *Google* font débats. Deux écoles s'affrontent ; certains considèrent que la domination des *big tech* ne peut plus prospérer sans aucun contrôle au prix

¹Google Chrome, Google Search, Google Play, Google Shopping, Gmail, Google Maps, Youtube, Google Video Search, Android.

²CE, décision n° C/369/6, Affaire AT.40411, 20 Mars 2019, Google Search (AdSense) et Alphabet Inc. (société mère de Google).

³S. CHOLET, *Op.cit.*, p. 157.

d'étouffer toute concurrence potentielle. D'autres, critiquent les GAFA et prônent le retour à l'utilisation rigoureuse des concepts juridiques et économiques et non pas du seul concept de ce qui est juste. La répression est un moyen parmi d'autres, mais ce qui est sûr c'est que le cadre se doit être suffisamment souple pour s'adapter sans cesse aux évolutions du secteur numérique.

Les plaintes et enquêtes à l'encontre des GAFA se sont multipliées. Aux côtés de celles mises en œuvre au niveau européen, s'ajoutent d'autres enquêtes au niveau de différents Etats¹. Raison pour laquelle, Le 15 décembre 2020, la Commission européenne a dévoilé les nouvelles règles s'appliquant à l'espace numérique. Il s'agit du *Digital Services Act (DSA)* et du *Digital Markets Act (DMA)*. Dans leur dimension économique et concurrentielle ces deux règlements ont pour objectif de garantir que les marchés numériques innoveront, restent ouverts à la concurrence, et que les relations commerciales entre les grands acteurs et leurs partenaires commerciaux demeurent équilibrées et loyales. Ils visent à contrôler le marché numérique en réduisant le risque d'abus par les grandes entreprises de la *tech*².

Le *DMA*, ou *Digital Market Act*, est un règlement permettant de cibler les acteurs majeurs de l'univers de la *tech*. Le système de régulation se base sur un mécanisme d'obligations graduelles. Le *DMA* concerne principalement les plateformes massives des réseaux sociaux, moteurs de recherche et publicité digitale. C'est le cas des GAFAM avec en tête de lice *Google*, *Amazon* ou *Facebook*. Les plus grands acteurs de l'univers de la *tech* devront ainsi se plier à des exigences supplémentaires³. Le *DSA*, ou *Digital Services Act* ou Règlement sur les services numériques, sert à désigner un règlement important pour la régulation des géants du digital. Son intérêt principal est de responsabiliser les plateformes numériques par rapport aux enjeux pour leurs utilisateurs, en ce qui concerne la production de

¹La société Apple a été sanctionnée par l'Autorité de la concurrence française à hauteur de 1,1 milliards d'euros en mars 2020. Elle fait également l'objet d'une enquête aux Etats-Unis, ainsi qu'au niveau de la Commission européenne, sur les conditions de son Apple Play, les règles de son App Store et les restrictions de concurrence mises en œuvre à l'encontre de ses concurrents.

²H. GOULARD, « Régulation des GAFA : le DSA et le DMA en 4 questions », in les Echos, 25 juin 2021 consulté le 24-04-2022 à 10h sur <https://www.lesechos.fr/tech-medias/hightech/regulation-des-gafa-le-dsa-et-le-dma-en-4-questions-1326964>

³« Digital Services Act (DSA) et Digital Market Act (DMA) : à quoi faut-il s'attendre », consulté le 24-04-2022 à 11h sur <https://www.dilitrust.com/blog/digital-services-act-dsa-et-digital-market-act-dma-a-quoi-faut-il-sattendre/>

contenus dangereux et de commercialisation de produits illicites et contrefaits¹. Le *DMA*, qui a fait l'objet d'un accord le 24 mars 2022, s'appliquera en Octobre 2022. Tandis que le *DSA*, après plusieurs mois de négociations, un accord a été trouvé, le 23 avril 2022, il s'appliquera en Octobre 2022 sur les grandes plateformes et 2023 sur les petites plateformes².

Paragraphe 2 : Les pratiques anticoncurrentielles algorithmiques.

Un algorithme est un ensemble cohérent d'instructions séquentielles appliquées à un intrant désigné afin d'obtenir un résultat clairement défini. Autrement dit l'algorithme est une procédure constitué d'une suite d'instructions et sa traduction dans un langage de programmation permet une exécution automatisée des opérations qui le composent³. Un algorithme peut être représenté au moyen du langage ordinaire, de diagrammes, de codes informatiques ou d'autres langages. Compte tenu de la puissance de calcul qu'ils mobilisent et de la quantité de données qu'ils peuvent exploiter, les algorithmes sont sources d'importants gains d'efficacité pour les entreprises, ces dernières se servent d'algorithmes pour améliorer leurs fonctions d'analyse prévisionnelle et optimiser leurs processus de multiples façons. En dépit de ces gains d'efficacité, les algorithmes peuvent, dans certains cas, susciter des préoccupations en termes de concurrence. En effet, l'usage des algorithmes suscite des inquiétudes car elle pourrait ouvrir la voie à des comportements anticoncurrentiels, ces outils facilitent l'établissement et le maintien d'ententes sans qu'un accord formel ou une interaction humaine soit nécessaire.

L'entente est généralement définie comme une pratique par laquelle des opérateurs vont être à l'origine d'une collusion au détriment d'un tiers. L'entente est ou bien explicite, c'est-à-dire maintenue au moyen d'un accord explicite, ou bien tacite, les concurrents parvenant à coordonner leurs stratégies sans avoir à communiquer entre eux, en reconnaissant simplement leur dépendance mutuelle⁴. Les algorithmes favorisent les ententes sur certains marchés en modifiant des caractéristiques structurelles comme la transparence et la fréquence

¹« Régulation de l'espace numérique européen : les projets de Digital Services Act et Digital Market Act », consulté le 24-04-2022 à 15h sur <https://derriennic.com/regulation-de-lespace-numerique-europeen-les-projets-de-digital-services-act-et-digital-market-act/>

²L. CHEMLA, « Accord historique : ce qu'il faut savoir sur la nouvelle législation de l'UE contre les dérives d'internet », 23 avril 2022, consulté le 25-04-2022 à 16h sur <https://www.franceinter.fr/societe/accord-historique-ce-qu-il-faut-savoir-sur-la-nouvelle-legislation-de-l-ue-contre-les-derives-d-internet>

³S. CHASSAGNARD-PINET, « Les usages des algorithmes en droit : prédire ou dire le droit », in IP/IT, N° 10, Octobre 2017, Dalloz, p. 495.

⁴Sanae EL HAJOUI, Le nouveau droit de la concurrence au Maroc, Remald, Casablanca, 2016, p. 137.

des interactions entre les entreprises et permettent de remplacer l'entente explicite par une entente tacite en supprimant le besoin de communication directe entre concurrents.

Le droit de la concurrence est aujourd'hui adéquat pour traiter les situations où des algorithmes sont utilisés comme moyen de mettre en œuvre de façon plus efficiente un accord explicite. Même lorsque la présence de technologies avancées rend l'analyse plus complexe, les autorités de la concurrence peuvent s'appuyer sur les normes en vigueur pour établir une infraction. C'est ce qu'ont fait avec succès le Département de la Justice des États-Unis et l'Autorité de la concurrence et des marchés du Royaume-Uni lorsqu'ils ont engagé des poursuites contre des vendeurs en ligne sur Amazon qui avaient programmé des algorithmes de fixation dynamique des prix de manière à obtenir des résultats conformes à l'accord explicite conclu entre eux¹.

Ainsi, dans le cas des pratiques de discrimination par les prix les entreprises utilisent les données pour déterminer la disposition à payer des clients en fonction de leur pouvoir d'achat ou de leurs habitudes de consommation. C'est le cas d'Amazon, qui utilise des algorithmes pour ajuster ses prix². Bien que l'on ignore encore pour l'essentiel l'étendue du phénomène, un nombre croissant d'entreprises se servent d'algorithmes informatiques pour améliorer leurs modèles de fixation des prix, adapter ou personnaliser leurs services et prévoir l'évolution du marché.

D'autres pratiques anticoncurrentielles utilisant l'algorithme des données sont présents dans le monde du numérique. C'est le cas par exemple des pratiques d'éviction. Les pratiques d'éviction consistent en un refus de donner accès à des données indispensables, un refus discriminatoire aux données, la conclusion de contrats exclusifs avec les utilisateurs, ou encore les ventes liées et une utilisation croisée d'ensembles de données. Dans ce cadre, la Commission européenne a prononcé des amendes exemplaires contre *Google* pour sanctionner des pratiques d'éviction abusives. Il s'agit de la décision du 27 Juin 2017 dite *Google Shopping*³.

En l'espèce, Google dispose d'un service de comparaison des prix qui permet aux utilisateurs de comparer les offres des produits qu'ils ont recherché sur Google. Google a accordé une position de premier plan à son service de comparaison des prix, jouant sur

¹OCDE, « Algorithmes et entente », Synthèse de la table ronde, Direction des Affaires Financière et des Entreprises Comité de la Concurrence, 17 octobre 2018.

²Amélie FAVREAU, *Op.cit.*, p. 57.

³CE, décision n° C 9/08, Affaire AT.39740, 27 Juin 2017, Moteur de recherche Google (Shopping).

l'algorithme pour le faire apparaître de manière très visible et préférentielle. Alors, que les services de comparaison des prix des concurrents sont soumis à des algorithmes de classement générique, qui les placent dans des résultats de recherche pour les consommateurs peu accessibles, ce qui favorise, mathématiquement, les services de *Google*. En agissant sur l'algorithme, *Google* est sanctionné pour avoir abusé de sa position dominante sur le marché en conférant un avantage illégal à son propre service de comparaison de prix et ne pas avoir garanti l'égalité des chances entre les différents opérateurs économiques. Or une telle forme de comportement constitue une forme d'abus bien établie, indépendante, qui sort du cadre d'une concurrence par les mérites. La sanction pécuniaire-2,42 milliards d'euros- était accompagnée d'une injonction de cesser les pratiques illégales dans un délai de 90 jours de s'abstenir de toute mesure ayant un objet ou un effet équivalent.

Cette décision illustre à quel point les données massives et les outils technologiques de pointe tels que les algorithmes affectent ou peuvent affecter le paysage concurrentiel. Raison pour laquelle l'autorité de la concurrence allemande a ouvert une procédure d'enquête à l'encontre de Facebook visant à déterminer si les conditions générales d'utilisation des données qu'elle impose aux utilisateurs de son site sont susceptibles de constituer un abus de son éventuelle position dominante sur le marché des réseaux sociaux.

Compte tenu de ces préoccupations, si une intervention réglementaire apparaît nécessaire, les décideurs devront opter pour une réglementation intelligente délimitant le champ de l'activité algorithmique sans nuire à la concurrence de marché¹. Une autre option permettant d'éviter la réglementation effective des algorithmes serait de faire l'audit des données. Cette méthode, outre que son application serait beaucoup moins coûteuse, permettrait au régulateur de déterminer si les entreprises se servent, pour fixer leurs prix, de données personnelles sensibles recueillies à des fins anticoncurrentielles.

Paragraphe 3 : L'interopérabilité dans le marché numérique.

L'interopérabilité dans le numérique constitue le fondement de la concurrence, l'interopérabilité est absolument essentielle. Il faut en effet que des matériels et logiciels différents puissent interopérer pour qu'il y ait une réelle concurrence sur le marché du numérique. De par cette importance l'interopérabilité fait l'objet d'une attention particulière. Elle concerne ainsi des acteurs tels que les fabricants de matériels informatique et les éditeurs

¹Amélie FAVREAU, *Op.cit.*, p. 56.

de logiciels ou de contenus numériques car, sans interopérabilité, les produits et services qu'ils proposent ne peuvent techniquement fonctionner avec ceux de leurs concurrents¹. De ce fait ces industriels ont tout intérêt à la garantie de l'interopérabilité, gage du développement de leur activité². A contrario, l'acteur majeur d'un marché peut être incité à ne pas assurer l'interopérabilité de ses propres biens et services, afin de préserver sa position dominante sur le marché en question.

Ainsi, pour bloquer ou se préparer à l'entrée de concurrents sur le marché, les écosystèmes dominants pourraient volontairement empêcher toute interopérabilité avec les innovations des entreprises rivales. Concrètement, une plateforme dominante pourrait façonner un écosystème de telle façon que seuls ses produits puissent se connecter les uns les autres. C'est l'exemple de l'assistant personnel intelligent *Siri d'Apple*, lequel est présent dans les *iPhones*, ne pourrait pas activer la musique sur une enceinte d'une autre marque que celle à la pomme, communiqué avec une télévision ou un véhicule.

Par ailleurs, certaines entreprises sont prisonnières de la norme retenue pour permettre l'interopérabilité dans un écosystème. Toutefois, de nombreuses affaires ont montré que les normes peuvent être instrumentalisées à des fins anticoncurrentielles. Certains titulaires de brevets peuvent agir pour extraire des redevances déraisonnables et affaiblir leurs concurrents potentiels ou actuels. Ce cas a été mis en lumière avec l'affaire de Samsung³. En l'espèce, la société Samsung possède des brevets essentiels liés à plusieurs normes de télécommunications mobiles et elle a pris l'engagement, auprès du *European Telecommunication Standard Institute*, ou Institut européen des normes de télécommunications, de les concéder sous licences FRAND⁴ à tout intéressé. En 2011, la société Samsung a introduit une action de cessation contre la société Apple sur la base de ces brevets -précisément la norme industrielle essentielle 3G- sachant qu'elle lui a concédée une licence FRAND.

¹C. Caron, « L'interopérabilité au service de la libre concurrence », in *Revue de Commerce Electronique*, Janvier 2012.

²CNN, « Ambition numérique. Pour une politique française et européenne de la transition numérique », Rapport remis au Premier ministre, Paris, 2015.

³CE, décision n° C 350/08, Affaire AT.39939, 29 Avril 2014, Société Samsung.

⁴Les engagements FRAND visent à garantir que la technologie essentiellement protégée par des DPI [droits de propriété intellectuelle] incorporée dans une norme soit accessible aux utilisateurs de cette norme à des conditions équitables, raisonnables et non discriminatoires. En particulier, les engagements FRAND peuvent empêcher les titulaires de DPI de rendre la mise en œuvre d'une norme difficile en refusant d'octroyer une licence ou en exigeant des redevances déloyales ou déraisonnables (en d'autres termes, des redevances excessives) une fois le secteur dépendant de la norme ou en imposant des redevances discriminatoires.

Il est vrai que l'introduction d'une action en cessation constitue généralement un recours légitime pour les titulaires de brevets en cas de violation de ceux-ci. Mais tel n'est pas le cas, selon la Commission européenne, elle peut constituer un abus de position dominante si le titulaire des brevets s'est volontairement engagé à accorder des licences à des conditions FRAND, et si l'entreprise contre laquelle est engagée l'action est disposée à conclure un accord de licence à ces mêmes conditions¹. En décembre 2012, la Commission a donc communiqué à Samsung son avis préliminaire reprenant ces principes : *Apple* étant un demandeur de licence à des conditions FRAND pour les brevets essentiels de Samsung, l'introduction par celui-ci de ces actions en cessation dans plusieurs Etats membres de l'UE pourrait constituer un abus de position dominante. Pour répondre aux préoccupations de la Commission, Samsung s'est donc engagée pour une période de 5 ans à n'introduire, contre les entreprises adhérant à un cadre spécifique pour la concession de licences, aucune action en cessation fondée sur des brevets essentiels, actuels ou futurs, concernant des technologies présentes dans les téléphones multifonctions et les tablettes. Cet engagement a été Accepté par la Commission le 29 avril 2014, et est devenu contraignants pour *Samsung*².

En revanche, la société Motorola qui, elle aussi, avait introduit une action en cessation contre Apple pour méconnaissance de ses brevets essentiels a fait l'objet d'une décision d'interdiction, la Commission lui enjoignant de mettre un terme à cette pratique considérée comme abusive, faute de justification objective³. Elle ne lui a toutefois infligé aucune sanction, compte tenu de l'absence de jurisprudence européenne sur le sujet. *Motorola* a finalement donné son accord pour l'exploitation de ses brevets essentiels selon les conditions énoncées dans le cadre FRAND.

En effet, une plateforme dominante qui participe au processus de normalisation pourrait bien cacher un brevet essentiel et par la suite l'opposer aux entreprises ayant adopté la norme pour empêcher toute interopérabilité avec ses produits. Une telle pratique pourrait réduire le bien-être du consommateur dans la mesure où ce dernier ne pourrait pas utiliser toutes les potentialités du produit acheté en raison d'absence d'interopérabilité. Néanmoins, il pourrait se détourner des produits des entreprises dont l'interopérabilité a été entravée. Dans

¹C. GRYNFOGEL, « Une illustration de la confrontation entre concurrence et propriété intellectuelle : les licences FRAND », in RJDA, N° 5, 2016, Francis Lefebvre, p. 343.

² http://publications.ut-capitole.fr/23923/1/Grynfofel_23923.pdf consulté le 24-04-2022 à 10h.

³La société Apple, en cours de procédure, a soumis à Motorola 6 offres successives de contrat de licence, puis une offre de contrat de licence FRAND, toutes refusées.

ce cas, la stratégie visée pourrait être qualifiée de refus de contracter dans l'hypothèse où la plateforme refuserait de concéder des licences de brevet à une entreprise. Enfin, les entreprises dominantes qui souhaiteraient bloquer leur écosystème aux concurrents devront donc être méfiantes. La licéité de cette pratique paraît douteuse lorsqu'elles détiennent un pouvoir de marché. La Commission européenne a clairement indiqué que ce type de comportement, lorsqu'il s'inscrit dans un contexte de standardisation peut dégénérer un abus¹.

Sous-section 2 : L'intelligence économique à l'ère du numérique.

L'économie actuelle se caractérise par sa nature fortement concurrentielle. Ainsi, la mondialisation des échanges et la concurrence accrue des marchés tracent les contours d'une économie qui se complexifie. De ce fait, pour survivre et se développer les entreprises doivent innover dans leur mode de fonctionnement, comme dans leur organisation et ceci dans une perspective de maîtrise de l'information. En effet, dans cette nouvelle économie, la compétitivité des entreprises dépend de leur capacité à générer, traiter et analyser rapidement et efficacement l'information pour prendre des décisions pertinente. Pour ce faire, l'entreprise a besoin de se doter d'un outil managérial performant de production d'informations : financières, actionnariales, technologiques, juridiques, etc. afin d'assurer en toutes circonstances sa pérennité et non sa simple survie. Cet outil qui existe depuis la nuit des temps sous des appellations diverses n'est autres que l'intelligence économique.

De plus en plus pratiquée à travers le monde, l'intelligence économique est une arme dont beaucoup se sont dotés dans le but de dégager un avantage compétitif ou encore de résister face à la concurrence². Toute activité d'intelligence économique repose sur la disponibilité d'informations et de renseignements pertinents et abondants, qui ont été élaborés, utilisés et transmis par différentes sources. Les entreprises doivent, donc se confronter a une pression accrue pour obtenir rapidement des informations utiles et pertinentes et le numérique a apporté un profond changement dans la manière de sélectionner et utiliser les informations pertinentes.

¹Walid CHAIEHLOUJ, « Innovation et préparation du marché à l'entrée de concurrents » in L'articulation des droits de propriété intellectuelle et du droit de la concurrence, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020, p. 99.

²I. BOUZIAR, « Les défis de l'intelligence économique au Maroc » le 6 Novembre 2020, consulté le 26-04-2022 à 14h sur <https://www.archimag.com/veille-documentation/2020/11/06/defis-intelligence-economique-maroc>

Ainsi, à l'ère du numérique et des grands basculements mondiaux, dans un monde en pleine récession, l'intelligence économique est l'arme de la nouvelle compétitivité. Le monde numérique est aujourd'hui au cœur des enjeux de l'intelligence économique. En effet, l'ère du numérique est sans conteste source de nouvelles opportunités permettant aux entreprises d'être plus compétitifs et plus efficace face à la concurrence¹. La digitalisation est un choix décisif et une prise de risque pour l'entreprise. D'où la contrainte pour cette dernière de disposer d'un système économique pour l'aider dans les prises de décision. A cette fin, nous présenterons d'abord un tour d'horizon de l'intelligence économique (Paragraphe 1) avant de s'étaler sur l'importance du numérique et des technologies nouvelles et leurs applications dans le soutien des activités du cycle d'intelligence économique (Paragraphe 2).

Paragraphe 1 : L'intégration de l'intelligence économique au sein de l'entreprise.

Depuis sa création plusieurs définitions de l'intelligence économique ont émergé. Nous allons retenir la définition de Christian Harbulot² « *L'intelligence économique se définit comme la recherche et l'interprétation systématique de l'information accessible à tous, afin de décrypter les intentions des acteurs et de connaître leurs capacités. Elle comprend toutes les opérations de surveillance de l'environnement concurrentiel (protection, veille, influence) et se différencie du renseignement traditionnel par : la nature de son champ d'application, puisque qu'elle concerne le domaine des informations ouvertes, et exige donc le respect d'une déontologie crédible ; L'identité de ses acteurs, dans la mesure où l'ensemble des personnels et de l'encadrement – et non plus seulement les experts – participent à la construction d'une culture collective de l'information ; ses spécificités culturelles, car chaque économie nationale produit un modèle original d'intelligence économique dont l'impact sur les stratégies commerciales et industrielles varie selon les pays* »³.

Autrement dit, l'intelligence économique est l'ensemble des activités coordonnées de collecte, de traitement et de diffusion de l'information utiles aux acteurs économiques, en vue de son exploitation. Elle fait référence à la façon dont on utilise l'information pour gouverner

¹C-R. JOLY, « Le numérique au cœur des enjeux de l'intelligence économique », 31 Janvier 2016 consulté le 26-04-2022 à 10h sur <https://www.droit-technologie.org/actualites/le-numerique-au-coeur-des-enjeux-de-lintelligence-economique/>

²Christian Harbulot est un stratège français qui a inventé le principe d'intelligence économique en France.

³Christian HURBULOT, Manuel d'intelligence économique, Presses Universitaires de France, coll. Major, Paris, 2012, p. 50.

et créer de la valeur dans une entreprise c'est-à-dire la manière de gérer stratégiquement l'information dans le but d'améliorer la compétitivité. Au lendemain de la deuxième guerre mondiale, les Etats-Unis sont les premiers à développer le concept d'intelligence économique, avec la création de *War Room*¹ à la fin des années 50. Il s'agissait d'une intrusion de l'intelligence économique du domaine militaire à celui des affaires, c'est au niveau des marchés, donc, que se déploie aujourd'hui la bataille concurrentielle².

Au Maroc, l'intelligence économique a fait son apparition dans les années 90, après une prise de conscience de l'importance de l'intelligence économique comme une démarche de maîtrise de l'information. L'importance de l'intelligence non seulement en tant que pratique qui permet d'anticiper les opportunités d'affaires mais aussi en tant que démarche qui empêche des pertes et réduit les risques et les menaces provenant de l'environnement³. L'introduction de l'intelligence économique au Maroc s'est traduite par la mise en place de plusieurs institutions et centres tels que l'IMIST⁴, le CNRST⁵, L'ANPME⁶, l'AMIE⁷ et bien d'autres. Il faut noter que le Maroc était parmi les pays les plus conscients des avantages de l'intelligence économique, c'est pourquoi en 2011, il a été le premier pays africain qui a mis en place une plateforme d'*Open-Data* pour faciliter l'accès aux données⁸.

L'intelligence économique a deux objectifs principaux, le premier est de comprendre l'environnement externe ou interne, le second est de faciliter la prise de décision stratégique. C'est donc un outil qui aide le dirigeant à prévenir les risques, à saisir les opportunités et anticiper les menaces, quelle que soit la taille de son entreprise⁹. La notion d'intelligence est centrée sur l'information, et étant donné que l'information constitue un des éléments majeurs

¹War room, créé par J. Howard Westing de l'université du Wisconsin, est un lieu où des personnes, bénéficiant d'un soutien matériel et logiciel, se basent sur une méthodologie commune afin de définir puis de mettre en œuvre une stratégie.

²J-L. MONINO et S. SEDKAOUI, « Les TIC un outil indispensable pour une démarche d'intelligence économique », in *Marché et Organisations*, N° 18, 2013, L'Harmattan, p. 175.

³I. BOUZEKAR, « Les défis de l'intelligence économique au Maroc » le 6 Novembre 2020, consulté le 26-04-2022 à 14h sur <https://www.archimag.com/veille-documentation/2020/11/06/defis-intelligence-economique-maroc>

⁴L'Institut Marocain de l'Information Scientifique et Technique.

⁵Le Centre National de la Recherche Scientifique et Technique.

⁶L'Agence nationale pour la promotion des PME.

⁷L'Association Marocain d'Intelligence Economique.

⁸H. ELAKKANI, « L'intelligence économique: Quels défis pour le Maroc ? », 2 Janvier 2021, consulté le 26-04-2022 à 10h sur <https://www.mapnews.ma/fr/actualites/economie/lintelligence-%C3%A9conomique-quels-d%C3%A9fis-pour-le-maroc>

⁹L. QUONIAM et A. LUCIEN, « L'Intelligence Economique 2.0 », in *Les Cahiers du numérique*, N° 4, 2009, Lavoisier, p. 14.

du patrimoine de l'entreprise, ses utilisations, sa protection et sa sécurité doivent être parfaitement maîtrisées et encadrée. La dimension juridique doit s'inscrire dans le domaine de l'intelligence économique et stratégique qui porte sur la gestion de l'information.

En effet, les trois axes au tour desquels doit se bâtir l'intelligence économique sont la connaissance pour l'anticipation, l'organisation en vue de la préparation et enfin l'action qui peut être préventive ou offensive. Chaque axe doit être assorti d'une stratégie de sécurité juridique, de la sorte que la stratégie globale de la sécurité de l'entreprise s'en trouve renforcée et son patrimoine et sa valeur économique et financière s'en trouve consolidée et valorisé. L'intelligence économique est un processus découlant d'un cycle de renseignement divisé en quatre étapes. D'abord la direction, dans cette phase, l'entreprise détermine ses besoins d'information stratégiques et dans quels aspects de l'environnement les données devraient être collectées. Ensuite la collecte des données ; l'entreprise détermine les sources qui peuvent être utilisé pour la collecte des données. Puis l'étape d'analyse, les données seront analysées afin de déterminer si elles sont utiles à des fins stratégiques. Enfin, la phase de diffusion, l'information produit dans la phase précédente sera transmise aux décideurs et utilisés pour formuler leurs plans stratégiques¹.

Tout au long de ce processus, la dimension juridique doit être intégrée lors des différentes phases de cycle de vie des informations de la direction jusqu'à la diffusion en passant par la collecte et l'analyse. Ainsi, le droit protège les biens, les personnes et il garantit des droits. Les systèmes d'information constituent l'épine dorsale de la collecte, de la création, du traitement et de l'exploitation de l'information des entreprises. Le droit a bien évidemment une incidence sur la protection des données des systèmes informatiques ; cela se traduit par la mise en place de stratégies de protection interne (charte informatique, politique de vie privée, règlement intérieur) et externe (conditions générales de sécurité), qui porte sur les propriétés intellectuelles et industrielles, sur la gestion de la confidentialité et sur la sécurité en général². Cependant, le développement exponentiel des échanges numérique et du volume des données et d'information numérique pose aujourd'hui des enjeux numériques dont la maîtrise devient vitale.

¹J-L. MONINO et S. SEDKAOU, *Op.cit.*, p. 183.

²E. A. CAPRIOLI, « Droit et Intelligence Economique dans l'Economie Numérique », 17 Octobre 2013, consulté le 27-04-2022 à 15h sur <https://www.caprioli-avocats.com/fr/informations/droit-et-intelligence-economique-dans-leconomie-numerique-elements-de-reflexion-sur-21-30-0.html>

Paragraphe 2 : Les enjeux numériques de l'intelligence économique.

Le numérique est un choix décisif et une prise de risque. Elle tient, de nos jours, une place prépondérante dans la stratégie d'entreprise et l'intelligence économique pourrait être un outil pertinent d'aide à la décision de la transition numérique et comment l'intégration du digital au sein de l'entreprise permet de renforcer ses capacités, se protéger des concurrents et assurer une avance essentielle de compétitivité¹. Les entreprises numériques doivent avoir les informations sur leurs environnements qui sont caractérisés par une concurrence plus rude, ce qui entraîne la nécessité de se tenir au courant des mouvements des concurrents, des caractéristiques des fournisseurs et de l'évolution des technologies.

L'entreprise numérique a besoin d'un système d'information efficace pour bien connaître les contraintes de son environnement : son personnel, ses clients, ses concurrents. Autrement dit, elle doit s'informer pour analyser, prévoir, organiser, décider, établir des projets, des stratégies et lancer des actions². Pour atteindre ces objectifs, l'entreprise doit d'abord mener une surveillance rigoureuse des technologies, des concurrents et des tendances du marché et ensuite établir un système d'intelligence économique efficace.

De ce fait, les pratiques de l'intelligence économique s'appuient fortement sur l'utilisation de l'internet qui est parfois considéré comme la source d'information la plus importante pour la veille concurrentielle. Le numérique a apporté un profond changement dans la manière de sélectionner et d'utiliser les informations pertinentes. Il impact le business model des entreprises et amène les dirigeants à impliquer toute leur organisation dans ce changement de culture. Grace au numérique la circulation de l'information est toujours plus rapide.

Comme le numérique se situe aux cœurs de l'information et des systèmes d'information, il a un rôle central en intelligence économique, car le numérique est le vecteur des informations produites, échangées et conservées. Outre la veille concurrentielle, la veille technologique est le moyen permettant à l'entreprise de suivre les évolutions susceptibles

¹N. EL HAOUD, « L'intelligence économique au service de l'entreprise innovante », in Revue internationale d'intelligence économique, N° 2, 2011, Lavoisier, p. 178.

²A. HAOUDI et M. BENNAGEM TOUATI, « Les TIC en intelligence économique : quels développements en Afrique ? », in Dossiers de Recherche en Economie et Gestion, N° 1, Juin 2020, Dossier 9, p. 148.

d'influer sur son propre avenir. La veille technologique nous permet de mesurer le volume et la quantité des travaux de recherche, des brevets, des résultats technologiques, etc¹.

Le numérique autorise des représentations simplifiées de l'information facilitant la prise de décision. Il peut être utilisé de nombreuses façons en faveur de l'intelligence économique : la recherche d'informations à l'aide de moteur de recherche, l'obtention de connaissances sur les clients par le biais des sites web, le suivi des concurrents et partenaire en visitant leurs *sites web*, etc. Ainsi, avec la digitalisation de l'économie, les PME ont pu se doter des moyens d'acquisition, de traitement et de diffusion de l'information qui étaient réservés aux grandes entreprises². Elles ont pu accéder plus facilement aux bases de données professionnelles, surveiller leur environnement et étendre leur influence par des moyens de technologie et de communication³.

Nous constatons, que les trois volets de l'intelligence économique : veille, sécurité et influence ont pu bénéficier de la numérisation de l'économie. De plus, le numérique rend l'information plus manipulable c'est-à-dire appropriée aux multiples traitements nécessaires aux pratiques de l'intelligence économique et ceci pour un coût réduit. Aussi, la numérisation permet de s'affranchir de la distance et d'utiliser des canaux d'information internationaux. Le monde numérique est un univers de communication, d'influence et de leadership. L'intelligence économique se doit d'ancrer ses pratiques dans la culture numérique. L'intelligence économique existe depuis bien longtemps mais le développement du numérique vient interroger sa conception et sa mise en œuvre⁴.

Par ailleurs, l'information représente aujourd'hui le nouveau pétrole et la principale matière première de l'économie, et un instrument de compétition. Son utilisation et sa maîtrise sont devenus faciles du fait, du numérique. Néanmoins, à la lumière de l'évolution générale du contexte concurrentiel ; on peut dire que l'entreprise est confrontée à un environnement instable et dynamique tant au niveau de la technologie que le marché. Dans ce cas, elle doit connaître les possibilités qu'offrent ces technologies pour fournir des données internes et

¹N. EL HAOUD, *Op.cit.*, p. 175.

²M. SQALLI HOUSSAINI, « Pratiques de sécurité informationnelle des PME exportatrices : le volet défensif de l'intelligence économique », in *Revue internationale d'intelligence économique*, N° 1 Janvier, 2020, Vol. 12, VA Presse Editions, p. 6.

³B. MAILL, « De l'intelligence numérique à l'intelligence économique », consulté le 26-04-2022 à 10h sur <https://portail-ie.fr/analysis/1433/de-lintelligence-numerique-a-lintelligence-economique>

⁴F. GUERINI, « L'intelligence économique d'entreprise face au défi du numérique », in *Revue du chercheur en sciences mathématiques et sociales*, N° 6, Université d'Alger, p. 450.

externes. De plus, toutes ces opportunités d'accès aux données ne sauraient masquer les risques inhérents à cette prépondérance de données¹. A la lumière des déclarations de lanceurs d'alerte ou des révélations des intrusions de hackers, l'entreprise se découvre vulnérable aux menaces du numérique et doit s'en prémunir.

Sous-section 3 : L'impact de la concurrence numérique sur la propriété intellectuelle de l'entreprise.

Avec le développement d'internet dans le grand public, ainsi que la montée en puissance du nombre des entreprises numériques, le nom de domaine, qui servait initialement de simple adresse d'un site internet, est devenu progressivement un élément en tant que tel au même titre que l'enseigne, à laquelle il est souvent comparé, le nom commercial ou la marque. Le nom de domaine permet aux utilisateurs du web, particuliers, professionnels ou consommateurs, d'identifier une personne physique ou morale et d'accéder aisément à son activité et à ses services. Ces avantages que procurent les noms de domaines les opposent à certains défis et contentieux concurrentiels (Paragraphe 1).

Par ailleurs, le défi majeur en matière des créations numériques des entreprises est de conjuguer harmonieusement le monde réel et le monde numérique pour conserver les créations des entreprises au cœur du système de protection juridique. Cependant, les règles telles qu'elles existent aujourd'hui peuvent paradoxalement être source d'inefficience économique et d'insécurité juridique dans l'économie numérique ce qui peut entraîner une violation des créations numérique de l'entreprise (Paragraphe 2).

Paragraphe 1 : Les contentieux de concurrence liés au nom de domaine.

La règle du « premier arrivé, premier servi », qui prévaut en matière d'attribution des noms de domaines, a contribué à la multiplication des agissements parasitaires (I) et a créé des situations de conflit entre les titulaires de noms et les propriétaires d'autres signes distinctifs. Ces conflits étaient d'autant plus délicats à gérer à l'origine, ce qui posait problème notamment au regard du droit des marques (II).

¹Ch. CHAMBET-FALQUET, « L'intelligence économique de l'entreprise à l'heure du numérique », in I2D : Information, données & documents, N° 4, 2015, Vol. 52, p. 11.

I- Les agissements parasites.

L'agissement parasite désigne l'attitude d'une entreprise qui, bien qu'elle exerce une activité dans un domaine différent, usurpe la notoriété ou les techniques qu'emploie d'une entreprise de renom¹. Parmi les agissements parasites, il y a le *cybersquat*. Cette pratique de *cybersquatting*², consiste à réserver des noms de domaines reprenant un nom de domaine ou une marque, au préjudice du titulaire légitime du nom ou de la marque concernée. Cette pratique a pu se développer à raison des situations créées par la coexistence des différentes procédures d'enregistrement de noms de domaines. Autrement dit, le *cybersquat* est défini comme une technique consistant à acheter des noms de domaines de manière abusive en ce qu'ils correspondent à un droit antérieur comme une marque pour détourner une partie du trafic attaché à cette marque afin de générer des recettes publicitaires ou de procéder au vol de données personnelles.

Le système d'attribution à l'échelle internationale se résumant à la règle du premier arrivé, premier servi, le premier à demander l'enregistrement d'un nom de domaine en bénéficie si ce dernier n'est pas déjà attribué, sans que ne soit prise en compte l'antériorité des éventuels dépôts de marques. Ainsi, de nombreux noms de domaines correspondant à des marques, des dénominations sociales, des sigles, des enseignes, ont été enregistrés au détriment ou à l'insu de leurs titulaires, occasionnant de ce fait un lourd contentieux. Certaines entreprises se sont même vues refuser l'emploi de leur propre marque à titre de nom de domaine pour leur propre site.

La pratique du *cybersquat* s'est encore intensifiée après l'annonce, le 26 février 2001, de l'introduction des noms de domaines accentués. En leur qualité de titulaires des enregistrements, les cyber-squatteurs mettent souvent les noms de domaines aux enchères ou les offrent à la vente directement à l'entreprise ou à la personne concernée, à des prix nettement supérieurs au coût de l'enregistrement. Véritable opération de chantage, elle oblige les titulaires de marques à acquérir les noms de domaines déjà enregistrés correspondant à leurs propres marques à des prix parfois exorbitants par exemple la cession du nom de

¹« Parasitisme », consulté le 02-04-2022 à 11h sur <https://www.juritravail.com/informations-pratiques/lexique/Parasitisme>

²La Commission générale de terminologie et de néologie, dans un avis publié au JO le 17 avr. 2008 a adapté le terme anglais « cybersquatting » à la langue française. Il convient dorénavant de dire « cybersquat » et « cybersquatteur ».

domaine « .business.com » qui a été revendu à 7,5 millions de dollars¹. Les auteurs de ce type d'agissement parasitaire poursuivent plusieurs but ; soit à revendre ou marchander le nom de domaine auprès de la marque ou de la société légitime, au prix le plus élevé possible, soit bloquer l'accès au nom à la marque ou à la société légitime, soit nuire à l'image de la marque ou de la société légitime en associant par exemple au nom de domaine à un site web dangereux, soit enfin profiter de la notoriété pour drainer un trafic sur le site web utilisant le nom de domaine.

Il existe d'autres formes d'agissements parasites, tel que le *typosquat*. Cette pratique est définie comme consistant à usurper volontairement l'identité d'un internaute ou d'une société. Elle consiste à enregistrer des noms de domaines proches de ceux des concurrents pour profiter des éventuelles fautes de frappe ou d'inattention des internautes, par exemple en ajoutant ou supprimant un s ou en remplaçant un e par un z, lettre voisine sur le clavier. Plusieurs décisions ont sanctionné un tel comportement. Ainsi, l'exploitation des noms de domaine « rueducommerc.com » et « rueducommerce.com »² a été sanctionnée, le juge ayant constaté l'utilisation frauduleuse de la marque, « rue du commerce ». Aussi une société qui concurrençait celle exploitant le site pneus-online, non reconnu original et pas purement descriptif, en utilisant les noms de domaines pneuonline, pneusonline et pneu-online, a commis une faute et a été condamnée à verser des dommages au plaignant³. De plus, il y a la pratique parasitaire *framing* qui consiste à proposer des sites par liens hypertextes, qui, une fois choisis, apparaissent tout en conservant l'interface (*frame*) du site initial (*framing*). Les cadres d'origine, comprenant notamment les logos et autres informations du site, ont été masqués. Il existe d'autres techniques telles que *grabbing*⁴, le *sucks*⁵, les sites parking⁶, etc.

¹Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, *Op.cit.*, p. 27.

²TGI, 3^{ème} chambre, Jugement n° 05/16184, 27 Avril 2006, Sté Rue du Commerce contre Société Brainfire Group et Société Moniker Online, Paris.

³C. Appel, 3^{ème} ch. Civile, décision n° 06/05922, 31 Janvier 2008, Société PNEUS-ONLINE SUISSE et Société PNEUS-ONLINE SARL contre Société DELTICOM AG, Lyon.

⁴Cette pratique, proche du typosquatting consiste à enregistrer des noms de domaine qui correspondent à des marques de grande renommée, en vue de les revendre.

⁵Cette pratique consiste à enregistrer un nom de domaine correspondant à un nom connu en y ajoutant le suffixe « suck » (« ça craint » dans le langage familier anglais). Elle a une connotation péjorative car elle pour finalité de critiquer le titulaire de nom.

⁶Le site parking permet de tirer profit des noms de domaine. Il s'agit d'une forme de référencement publicitaire qui consiste à enregistrer un nom de domaine et de le rediriger vers une page contenant des liens publicitaires.

Plusieurs recommandations ont été formulées à l'attention de l'ICANN en vue de limiter le phénomène du *cybersquat*. Ainsi, dès 1999, l'OMPI préconisait une exception pour les marques notoirement connues ou célèbres, qui aurait pour effet d'interdire à une personne autre que le titulaire de cette marque de l'enregistrer comme nom de domaine¹. Cette règle transposerait en fait sur l'internet la protection spéciale accordée aux marques célèbres ou notoirement connues par la Convention d'Union de Paris². Cette recommandation a conduit à l'adoption des principes UDRP³.

Par ailleurs, plus de réservation et surveillance ont été entamées. En effet, les tiers lésés ont décidé de réagir pour recouvrer leurs droits et pour mettre fin à ces procédés, en enregistrant massivement tous les noms de domaines se rapprochant, visuellement ou phonétiquement, des noms, dénominations sociales ou marques à protéger et dont ils détiennent légitimement les droits. Cette solution peut cependant s'avérer onéreuse, parfois même abusive. Aussi, la surveillance de noms de domaine, limitée à quelques noms de domaines peut s'avérer plus efficace. Il existe à cet effet des services de surveillance pour avertir le titulaire au cas où un nom de domaine, sélectionné au préalable sur «*.com*», «*.net*», «*.org*», devient disponible.

Il convient également de signaler l'ouverture, depuis le 26 Mars 2013, de la base de données mondiale dénommée *Trade Mark Clearing House (TMCH)* créée par l'ICANN pour permettre la mise en œuvre effective des services de réclamations⁴. Cette base de données centralise, authentifie et diffuse les informations relatives aux droits des titulaires de marques aux différents registres des nouvelles extensions. En enregistrant leur marque dans cette base, les détenteurs peuvent se prémunir contre le *cybersquat*. Ainsi il bénéficie d'un service d'alerte en cas d'enregistrement abusif d'un nom de domaine à l'identique de celle-ci. Même si ce système d'alerte ne bloque pas la demande d'enregistrement en cours, l'information lui permet de réagir.

Par ailleurs, les règles UDRP ont été modifiées pour limiter le transfert abusif du nom de domaine auquel le titulaire procède à réception de la mise en demeure du titulaire de la

¹OMPI, Rapport final concernant le premier processus de consultations de l'OMPI sur les noms de domaines de l'internet, Genève, 30 avril 1999.

²Convention de Paris pour la protection de la propriété industrielle, 1883.

³Voir infra p. 369.

⁴« Base de données mondiale des noms de domaine » consulté 03-04-2022 à 11h sur <https://www.nameshield.com/noms-de-domaine/nameshield-registry/tmch/>

marque ou en cours de procédure UDRP. Ces règles sont entrées en vigueur le 31 Juillet 2015. Elles visent pour l'essentiel à faire bloquer le nom de domaine litigieux par le bureau d'enregistrement concerné avant la notification de la procédure au défendeur. Le bureau d'enregistrement dispose d'un délai de 48 heures pour verrouiller le nom de domaine litigieux et doit prendre des mesures pour le maintenir bloqué jusqu'à la fin de la procédure. Il convient aussi de souligner que depuis la création de l'ICANN, les *registrars* sont tenus de procéder au transfert d'un nom de domaine lorsqu'une juridiction compétente, d'un pays quelconque, leur en fait injonction.

Par ailleurs, les conflits en cette matière donnent le plus souvent lieu à une action en contrefaçon, notamment en présence d'une marque, ou encore à une action en concurrence déloyale ou parasitaire lorsque les parties sont concurrentes, l'acte déloyal étant alors constitué par le risque de confusion ou encore le détournement de clientèle. L'action en contrefaçon vise à faire constater l'infraction, cesser le trouble et obtenir réparation du préjudice subi du fait de l'atteinte à l'image de marque et de l'indisponibilité du nom de domaine. Ce préjudice peut s'analyser comme une perte de chance de contacter des clients sur l'internet et donc, comme une perte financière subie. En effet, la présence sur l'internet est aujourd'hui considérée comme un vecteur de développement et de communication et la marque peut se trouver dévalorisée par les agissements de contrefacteurs.

La contrefaçon peut s'accompagner d'actes de concurrence déloyale. Pour qu'il y ait concurrence déloyale, il faut qu'il existe entre les parties une situation de concurrence effective. La Haute juridiction française a également considéré, dans un arrêt du 2 Février 2016¹, que le fait, pour une société de réparation d'instruments à vent, de racheter le nom de domaine d'une société concurrente, exerçant la même activité dans la même ville, constituait un acte de concurrence déloyale. La Cour a relevé que le nom de domaine « lesventsdu nord.fr » était inséré comme lien hypertexte dans d'autres sites internet, tels ceux d'une association partenaire et d'un fournisseur de la société concurrente, de sorte que le rachat de ce nom de domaine par la société a eu pour effet de diriger automatiquement l'internaute cliquant sur ces liens vers le site de celle-ci. Elle a ainsi confirmé l'arrêt d'appel en ce qu'il avait retenu l'acte de concurrence déloyale jugeant que cette situation était de nature à faire naître une confusion dans l'esprit du public entre les deux sociétés afin de capter

¹C. Cass, Civile, ch. Com., décision n° 14-20.486, 2 Février 2016, la société Les Vents du Nord contre la société Cuivres et bois.

la clientèle que la société concurrente. Sur la concurrence parasitaire, les actes de parasitisme sont constitués par l'usurpation de la notoriété d'une marque, de la dénomination sociale d'une entreprise, ou encore le détournement de clientèle.

Un jugement du tribunal de commerce de Belfort du 17 Octobre 2017 a également sanctionné des actes de concurrence déloyale par parasitisme constitués par la mise en place de liens de retours sur un moteur de recherche, permettant de détourner une partie du trafic de la demanderesse vers son propre site. Les juges ont estimé que de « *telles pratiques étaient constitutives d'une faute de par la nature même du système frauduleux mise en place fausse ainsi le jeu normal du marché* »¹.

II- Conflit entre nom de domaine et droit des marques.

Dans de nombreux cas, le nom de domaine déposé par une entreprise correspond à une marque. Or, le droit des marques fait partie de la propriété industrielle, différente de la propriété littéraire et artistique. Il fait l'objet des articles 133 et suivants de la loi n° 23-13 modifiant et complétant la loi 17-97 relative à la protection de la propriété industrielle². Selon l'article 133 de ladite loi « la marque de fabrique, de commerce ou de service est un signe susceptible de représentation graphique servant à distinguer les produits ou services d'une personne physique ou morale. » et pour être valable, une marque doit être distinctive³. Par ailleurs, et contrairement au droit d'auteur, qui s'acquiert par le simple fait de la création, la propriété de la marque s'acquiert par l'enregistrement auprès de l'OMPIC⁴. En cas de conflits entre marque et nom de domaine, on dispose de deux types d'action judiciaire pour défendre ses droits contre les actes des tiers pour lesquels il n'aurait pas donné son accord : l'action en contrefaçon et l'action en concurrence déloyale.

Le droit des marques est régi par le principe dit de spécialité, selon lequel le dépôt d'une marque n'ouvre des droits que les catégories de biens et de services visés lors de l'enregistrement. Il est donc logique qu'il ne puisse y avoir contrefaçon d'une marque par un nom de domaine que si les produits et services offerts sur ce site sont soit identiques, soit similaires à ceux visés dans l'enregistrement de la marque et de nature à entraîner un risque

¹Tribunal de commerce, jugement du 17 Octobre 2017, la société Autoconfiance 25 contre la société IES, Belfort.

²Dahir n° 1-14-188 du 27 Muharam 1436 (21 Novembre 2014) portant promulgation la loi n° 23-13 modifiant et complétant la loi n° 17-97 relative à la protection de la propriété industrielle.

³V. art. 134 de la loi 23-13.

⁴Article 140 de la loi 23-13 : « La propriété de la marque s'acquiert par l'enregistrement. La marque peut être acquise en copropriété. ».

de confusion dans l'esprit du public¹. Pour une application classique de ce principe, un arrêt de la Cour de Cassation marocaine du 23 Janvier 2019 a jugé que la ressemblance entre deux marques en termes d'écriture, de forme et de prononciation entraîne une confusion chez le public et constitue une contrefaçon surtout que les deux entreprises ont le même type d'activité à savoir la vente de produits de peinture².

De ce fait, en adaptant ce principe au *cyberspace*, ce dernier est naturellement appliqué par les tribunaux pour déterminer si l'enregistrement et l'exploitation d'un nom de domaine doit être considéré comme la contrefaçon d'une marque existante. Le seul dépôt d'une marque est ainsi insuffisant pour soutenir qu'un nom de domaine identique à une telle marque serait automatiquement contrefaisant. Les juges raisonnent ainsi en deux temps : en premier lieu, ils procèdent à une analyse du contenu du site exploité sous le nom de domaine litigieux et, en second lieu, ils comparent ce contenu avec les services et produits pour lesquels la marque a été enregistrée³. Ainsi la Cour d'appel française a jugé que l'utilisation du nom de domaine *reflexauto.fr* par une société de courtage automobile ne constituait pas une imitation de la marque déposée et du nom de domaine *autoreflex.com*. En l'espèce, la Cour d'appel française a souligné que « *visuellement, la similitude tient à la reprise, quoique inversés, de deux termes lesquels s'avèrent peu distinctifs, le mot « Reflex » renvoyant à l'évidence au réflexe, banalement incitatif, et le mot « Auto » étant générique pour désigner les automobiles ; que l'inversion des termes permet au plan phonétique de distinguer les expressions en cause à raison de sonorités d'attaque très différentes* »⁴.

Par ailleurs, le principe de spécialité est tempéré pour les marques bénéficiant d'une renommée. Cela est aussi valable dans le cas d'une contrefaçon par un nom de domaine, si cette imitation est de nature à porter préjudice au propriétaire de la marque. C'est l'exemple de la personne ayant déposé le nom de domaine *redbull.re* qui a été condamnée à verser une indemnité à la société *Red Bull* et à lui transférer le nom de domaine, car « *l'enregistrement du nom de domaine www.redbull.re constitue en effet une atteinte à la marque communautaire verbale renommée* » de la société et « *le nom de domaine en cause se trouve de fait indisponible pour celle-ci qui se trouve dès lors empêchée d'exploiter un nom de*

¹V. art. 225 et 226 de la loi 17-97.

²C. Cass., ch. Com., 23 Janvier 2020.

³Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 241.

⁴C. Appel, 18 Décembre 2013, la Société Autorefle.com contre David P., Paris.

domaine pourtant construit identiquement à d'autres sites qu'elle exploite, notamment www.redbull.fr »¹.

Selon l'article 184 de la loi n° 23-13 modifiant et complétant la loi 17-97 relative à la protection de la propriété industrielle : « Constitue un acte de concurrence déloyale, tout acte de concurrence contraire aux usages honnêtes en matière industrielle ou commerciale. Sont notamment interdits : tous faits quelconques de nature à créer une confusion par n'importe quel moyen avec l'établissement, les produits ou l'activité industrielle ou commerciale d'un concurrent, les allégations fausses dans l'exercice du commerce de nature à discréditer l'établissement, les produits ou l'activité industrielle ou commerciale d'un concurrent ; et les indications ou allégations dont l'usage dans l'exercice du commerce est susceptible d'induire le public en erreur sur la nature, le mode de fabrication, les caractéristiques, l'aptitude à l'emploi ou la quantité des marchandises ». La concurrence déloyale doit être appréciée au regard du principe de la liberté du commerce qui implique qu'un produit qui ne fait pas l'objet de droits de propriété intellectuelle puisse être librement reproduit sous certaines conditions, tenant à l'absence de faute par la création d'un risque de confusion dans l'esprit de la clientèle sur l'origine des produits, circonstance attentatoire à l'exercice paisible et loyal du commerce².

De ce fait pour être protégé par le droit de la propriété intellectuelle, un nom de domaine doit revêtir un caractère distinctif et original : il ne doit pas se borner à décrire l'activité de son titulaire. Ainsi, ont été déboutés les propriétaires du domaine mariagesencorse.com, qui se plaignent de la concurrence déloyale du site concurrent mariageencorse.com. Le nom « mariagesencorse » a été considéré par les juges comme trop générique et trop descriptif pour pouvoir revendiquer une protection, même en présence d'un risque de confusion³.

En revanche, un nom de domaine peu original peut être protégé par l'action de concurrence déloyale. Selon la Cour de cassation française, « *l'action en concurrence déloyale étant ouverte à celui qui ne peut se prévaloir d'un droit privatif, le caractère*

¹TGI, 3^{ème} ch., 23 Mai 2014, la société Red Bull contre M. Mohamed B., Paris.

²Jacques LAURRIEU, « Les territoires disputés de la concurrence déloyale et de la propriété intellectuelle » in La propriété intellectuelle dans les droits du marché et de la rivalité concurrentielle, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2016, p. 102.

³C. Appel, ch. Civile, décision n° 12/00023, 20 Mars 2013, M. B. et la société Iris Media contre Mme Angela A., Bastia.

*original ou distinctif des éléments dont la reprise est incriminée n'est pas une condition de son bien fondé, mais un facteur susceptible d'être pertinent pour l'examen d'un risque de confusion »*¹. Par ailleurs, même si le nom de domaine ne présente pas de caractère distinctif et ne présente aucune originalité, il y a lieu de rechercher si les faits n'ont pas été commis dans le but de profiter de la notoriété ou des investissements de la société imitée.

Aussi, le fait de profiter de l'expiration du nom de domaine d'un concurrent pour le racheter et le diriger vers son propre site, alors que ce nom de domaine, identique au nom commercial du concurrent, était utilisé par ce dernier, constitue une concurrence déloyale qui porte atteinte à l'attractivité et à l'image du concurrent, crée de la confusion dans l'esprit du public et justifie le versement de dommages et intérêts. Des conflits peuvent aussi surgir entre le déposant d'un nom de domaine et le titulaire d'une enseigne, d'un nom commercial, d'une dénomination sociale ou d'un nom patronymique ; le cas par exemple des personnes qui tentent d'exploiter la célébrité de certains acteurs, politiciens, sportifs, etc. dont l'antériorité est certaine. Le déposant le cas échéant condamnée pour concurrence déloyale en présence d'un risque de confusion. La meilleure solution, en cas de risque de conflit entre un signe antérieur et un nom de domaine consiste pour le déposant du nom de domaine à tenter d'obtenir l'autorisation du titulaire du signe antérieur².

Paragraphe 2: La violation des créations numériques de l'entreprise.

L'entreprise en transition digitale doit en effet se cuirasser contre la pression concurrentielle d'acteurs émergeant susceptibles de violer ses créations numériques. En effet certains annonceurs profitent de la réputation de la marque à travers l'usage de la technique des mots-clés proposée par les moteurs de recherche (I). De plus, les créations numériques de l'entreprise font l'objet de plusieurs actes illégaux tels que la piraterie ou la contrefaçon. Ces actes constituent un phénomène en augmentation constante, amplifié par la mondialisation et par la vente sur internet. Aucun secteur de l'activité économique, n'est aujourd'hui épargné et la gamme des produits contrefaits ou piraté ne cesse de se diversifier (II).

¹C. Cass., Civile, ch. Com., décision n° 15-18.470, 6 Décembre 2016, la Société Pressimmo on ligne contre la Société La Cote immobilière.

²Philippe LE TOURNEAU, *Op.cit.*, p. 592.

I- Le droit des marques face à la contrefaçon sur Internet.

La majorité des problématiques sur internet relative au droit des marques est liée au service de publicité par mot-clé à savoir les *AdWords*. Tout le monde connaît le fonctionnement d'*AdWords*, le système de publicité sous forme de résultats de recherche dits sponsorisés ou payants déclenchés par les mots-clés tapés par les internautes et préalablement réservés par les annonceurs¹. De nombreux conflits de droits sont apparus liés à l'usage par les annonceurs de mots-clés correspondant à des marques appartenant à des tiers. Ce conflit entre *Google* et certains propriétaires de marques a été tranché par la Cour de justice de l'Union européenne en 2010².

En effet, les titulaires de marques souhaitent empêcher la sélection de tels mots-clés par les annonceurs. Ils veulent également empêcher que les exploitants de moteurs de recherche n'affichent des annonces en réponse à ces mots-clés, dans la mesure où cela peut conduire l'internaute vers des sites de produits ou de services concurrents³, voire des sites proposant des contrefaçon à côté des résultats naturels correspondant à leurs propres sites. La nouvelle économie issue de l'internet soulève ainsi la question de savoir si la mise à disposition, l'aide à la sélection ainsi que la réservation de ces mots-clés, constituent ou non des actes de contrefaçon de marque⁴.

Ainsi pour qu'il ait contrefaçon, en l'absence d'autorisation du titulaire, trois conditions cumulatives doivent donc être réunies. La première condition ; il faut que l'usage du signe dans la vie des affaires soit caractérisé. Donc la question qui se pose est de savoir si le moteur de recherche fait un usage dans la vie des affaires de la marque lorsqu'il propose, par l'intermédiaire d'un outil générateur de mots-clés un signe protégé. Rappelons que pour qu'il ait atteint la marque, il convient de faire la distinction entre usage privé et usage dans une activité commerciale visant un avantage économique. Cette condition est remplie car en proposant des listes de mots-clés aux annonceurs, les moteurs de recherche font bien un usage

¹Benjamin AMAUDRIC DU CHAFFAUT, « « Web 2.0 » et titularité des droits : une complexité renforcée » in *L'entreprise et la titularité des droits de propriété intellectuelle*, Ouvrage collectif sous la direction Jean-Michel BRUGUIERE, Dalloz, Paris, 2015, p. 60.

²CJUE, Grande ch., arrêt n° C-236/08, 23 Mars 2010, la société Google contre la société Louis Vuitton.

³Dans un jugement du Tribunal de grande instance de Lyon, la société décathlon a été condamnée pour contrefaçon de la marque « inuka » en la reproduisant à trois reprises, dans la balise titre, dans la balise description puis sur son site internet.

⁴Pascale TREFIGNY, « Les liens commerciaux et le droit des marques » in *L'entreprise à l'épreuve du droit de l'Internet*, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014, p. 93.

de ces mots-clés à des fins commerciales puisque ceux-ci sont destinés à être réservés et à générer l'affichage des annonces qui procurera un revenu au moteur si l'internaute clique sur le lien.

La deuxième condition ; il faut que l'usage de la marque soit en lien avec des biens ou services. Plusieurs auteurs estiment que l'usage consistant à permettre aux annonceurs de sélectionner dans *AdWords* des mots-clés qui correspondent à des marques ne constitue pas une atteinte à la marque. Ils estiment qu'il serait artificiel de qualifier toutes les activités déployées par *Google* ou autres moteurs de recherche dans *AdWords* d'usage dans la publicité. Car l'usage de la publicité qu'il faut retenir et celui fait par les tiers soit l'annonceur et non le moteur de recherche. Ce qui importe c'est la notion d'usage pour des produits ou services et que le lien soit établi entre la marque et le produit ou service vendu. Or, il n'y a pas de produits ou services vendus au public dans l'activité générateurs de mots-clés¹.

Troisième et dernière condition, oblige que l'usage doit porter atteinte à l'une quelconque des fonctions reconnue à la marque et notamment sa fonction première qui est d'identifier et d'individualiser un produit ou un service, en raison d'un risque de confusion de la part du public. La jurisprudence, notamment française, considère majoritairement que la mise à disposition des annonceurs de mots-clés suggérés par les moteurs de recherche génère un risque de confusion et en conséquence affecte la fonction essentielle de la marque qui est de créer un lien entre un produit ou un service et celle-ci. Ainsi, le fait de contrefaçon ne réside pas dans le choix par les annonceurs d'un signe déposé à titre de marque mais dans le choix par le moteur de recherche de reproduire, en réponse à une sollicitation d'un annonceur, un ou des signes déposés à titre de marque, ce qui constitue une captation du pouvoir attractif de ceux-ci dans le champ des produits pour la désignation desquels ils ont été enregistrés².

La réservation de mots-clés, qui n'est pas un achat, repose sur un système extrêmement subtil et complexe. En effet, pour que l'annonce de l'annonceur s'affiche à l'écran deux conditions doivent être remplies. La première tient au fait qu'un autre annonceur n'ait pas proposé un prix supérieur pour le même mot-clé : dans le cas contraire la réservation du premier annonceur ne produira pas d'effet car la réservation du second l'emportera, sans que le premier n'en soit informé. La seconde condition tient à la condition que le mot-clé soit

¹A. BENSAMOUN, « Droit souple et lutte contre la contrefaçon en ligne », in IP/IT, N° 4, Avril 2016, Dalloz, p. 183.

²Philippe LE TOURNEAU, *Op.cit.*, p. 557.

activé par un internaute¹. Or, contrairement à ce que l'on peut croire, bon nombre de mot-clé réservés ne vont pas générer de requête et ne déclencheront donc pas l'affichage de la publicité. Autant dire qu'au stade de la réservation de mots-clés correspondant à une marque appartenant à un tiers, il n'est pas possible de caractériser un usage de cette marque puisqu'aussi bien l'usage sera inexistant. En outre et quand bien même on retiendra l'existence d'un usage, celui-ci ne serait pas susceptible de porter atteinte à la marque compte tenu du caractère hypothétique de l'affichage de l'annonce.

II- Les actes illégaux relatifs aux œuvres numériques de l'entreprise.

Plusieurs actes illégaux sont susceptibles de porter atteinte aux créations numériques de l'entreprise. Nous allons nous limiter à la contrefaçon et à la piraterie. La contrefaçon est habituellement définie comme l'imitation frauduleuse ou la fabrication d'une chose au préjudice de celui qui avait seul le droit de fabriquer ou de la reproduire². Plus particulièrement, en matière de propriété intellectuelle, la contrefaçon a été définie comme toute atteinte portée à un droit de propriété littéraire, artistique ou industrielle (reproduction, imitation, vente, mise en vente...).

En effet l'article 201 alinéa 1er de la loi n°17-97 telle que modifiée et complétée par la loi n° 23-13 relative à la protection de la propriété industrielle dispose que toute atteinte portée aux droits du propriétaire d'un brevet d'invention, d'un schéma de configuration (topographie) de circuits intégrés, d'un dessin ou modèle industriel enregistré, d'une marque de fabrique, de commerce ou de service enregistrée ou d'une indication géographique ou d'une appellation d'origine enregistrée constitue une contrefaçon.

De nombreuses illustrations existent d'ores et déjà dans la jurisprudence concernant la contrefaçon d'éléments protégés par la propriété intellectuelle sur internet : reprise de chartes graphiques de sites web, reproduction d'éléments graphiques appartenant à un tiers, utilisation abusive des liens hypertextes. En atteste, l'exemple suivant, le cas des dirigeants d'une entreprise qui avait plagié le site internet d'une société de diffusion d'annonces immobilières, reproduisant « *notamment son logo avec des étoiles et la totalité des rubriques (...), l'exact libellé de ses annonces publicitaires dans certains journaux gratuits et également des*

¹F. CORONE, « Liens commerciaux sur internet et contrefaçon de marque », in LEGICOM N° 44, 2010, Victoires, p. 124.

²N. AZDDOU, « Le droit marocain des marques », in Revue Marocaine Droit, Economie et Gestion, N° 57, 2018, p. 14.

documents commerciaux : plaquette de présentation, brochure mode d'emploi, contrat de diffusion, dossier descriptif du bien, et aussi le livre commercial en tous points identiques »¹, ont été condamnés pour contrefaçon des droits d'auteurs sur le site et sur les documents, ainsi que pour contrefaçon de marque, à des peines et des dommages et intérêts. En revanche le site web qui assigne un concurrent pour contrefaçon doit démontrer l'originalité de son site sous peine d'être débouté².

L'entrée en vigueur, de la loi n° 2-00 relative aux droits d'auteur et droits voisins et de la loi n° 23-13 modifiant et complétant la loi 17-97 relative à la protection de la propriété industrielle, offre un dispositif au juge pour assurer une protection, et ce, à l'instar du droit comparé et conformément aux recommandations des instances internationales, y compris, pour la première fois les œuvres ayant un caractère informatique ou disponible sur le réseau. Ce qui nous intéresse surtout dans ces lois, ce sont les textes relatifs aux sanctions civiles et pénales et liés à la criminalité numérique.

D'une part, la loi 17-97 relative à la protection de la propriété industrielle, de sa lecture, on déduit que les effets de l'action en contrefaçon diffèrent selon qu'il s'agisse de l'action civile ou de l'action pénale en contrefaçon. En cas de contrefaçon en matière de marques, l'action pénale donne lieu à un emprisonnement de 3 mois à un an et d'une amende de 100.000 DH à 1.000.000 DH ou l'une de ces deux peines seulement³. En atteste, l'affaire entre la société *Al arabia lilaawlama* et la société *Ecart Service Morocco* représentante de Jumia.ma. Dans l'espèce *Al arabia lilaawlama* spécialisée dans la commercialisation de sa marque des outils de *smartphone* connu sous le nom *AirPLUS* accuse le site Jumia.ma de commercialiser des produits contrefaites qui porte le nom de sa marque à savoir *AirPLUS*. Après constatations du fait de contrefaçon et suite aux preuves présentées, le Tribunal de commerce de Casablanca en date du 27 Septembre 2021 a condamné Jumia.ma a arrêté la vente des produits contrefaites de la marque *AirPLUS* sous peine d'une amende de 5000,00

¹C. Appel, 3^{ème} ch. Correct., 13 Avril 2016, J. B., C.L., le Ministère public contre Le Partenaire Européen, Montpellier.

²Selon un jugement du TGI de Paris du 12 janvier 2017 : Le contenu d'un site internet est susceptible de bénéficier de la protection du droit d'auteur si son créateur démontre que la forme et la présentation et/ou le contenu de son site procèdent d'un apport personnel qui relève l'empreinte de sa personnalité. Par ailleurs, le fait que le site contienne des éléments, dont l'originalité n'a pas été retenue précédemment, n'empêche pas la société de revendiquer la protection du droit d'auteur, dès lors qu'elle justifie en quoi le choix de combiner l'ensemble ces éléments constituent une démarche originale. A défaut de prouver le caractère original des éléments revendiqués et du contenu du site web la société sera déclarée irrecevable dans sa demande en contrefaçon de droit d'auteur.

³V. art. 225 de la loi n° 23-13.

Dirhams et l'a condamné à payé des dommages et intérêt d'une valeur de 50.000,00 Dirhams au profit de *Al arabia lilaawlama*¹.

Par ailleurs, en cas d'imitation, l'action pénale donne lieu à un emprisonnement de deux mois à six mois et d'une amende de 50.000 dirhams à 500.000 dirhams ou l'une de ces deux peines seulement². Il existe une peine complémentaire à l'action pénale en contrefaçon, à savoir la destruction des objets reconnus contrefaits appartenant au contrefacteur ainsi que celle des dispositifs ou moyens destinés à la réalisation de la contrefaçon³. L'action civile quant à elle permet au demandeur la récupération de son droit exclusif sur sa marque et la réparation du préjudice subi. En présence de contrefaçon, l'entreprise peut choisir l'action en concurrence déloyale pour suppléer l'action spéciale en contrefaçon et avoir la faculté de n'invoquer en justice que le risque de confusion dont elle souffre comme élément de concurrence déloyale.

D'autre part, les sanctions civiles et pénales prévues par la loi 2-00 relative aux droits d'auteur et droits voisins sont très multiples, mais généralement la piraterie reste la plus répandue. Les sanctions sont traitées dans la loi 2-00, à partir de l'article 61 jusqu'à 65 de la dite loi. Concernant les sanctions pénales outre l'élément matériel exigé pour cette infraction qui se concrétise dans la piraterie. Il faut aussi l'existence de la mauvaise intention chez l'auteur de l'infraction et cela est laissé à l'appréciation souveraine des juridictions. Le législateur exige qu'il ait un dol général ou spécial. L'article 64 de la loi 2-00 « punit d'une peine d'emprisonnement de deux à six mois, et d'une amende de 10.000 à 100.000 dirhams ou l'une de ces peines seulement, quiconque a commis d'une manière illicite et par quelque moyen que ce soit, à des fins d'exploitation commerciale, une violation délibérée :des droits d'auteur mentionnés aux articles 9et 10 ou des droits des artistes interprètes ou exécutant à l'article 50 ou des droits des producteurs de phonogrammes mentionnés à l'article 51 ou des droits des organismes de radiodiffusion mentionnés à l'article 52 ». Cependant, en cas d'infraction d'habitude, lesdites peines sont portées au double. La juridiction compétente pour ces infractions peut ordonner, en outre, des mesures de sureté et des peines accessoires.

¹Tribunal de commerce, jugement n° 8350, 27 Septembre 2021, *Al arabia lilawlama* contre Ecart Service Morocco, Casablanca.

²V. art. 226 de la loi n° 23-13.

³V. art. 228 de la loi n° 23-13.

Quant aux sanctions civiles, la commission de l'infraction de piraterie donne la possibilité à la victime de se constituer partie civile, outre l'action publique, au procès afin de réclamer la réparation du dommage subi. Le montant des dommages est fixé par rapport au préjudice matériel qu'a subi le titulaire du droit, ainsi que l'importance des gains que l'auteur de la violation a retiré de celle-ci. Dans le cas où l'auteur ne le savait pas ou n'avait pas des raisons valables de se livrer à une telle activité, les autorités judiciaires pourront limiter les dommages et intérêt par rapport à ses gains sur le programme objet du piratage. Lorsque des exemplaires de ces logiciels piratés existent, les autorités judiciaires peuvent ordonner qu'ils soient détruits, ou qu'ils soient mis hors des circuits commerciaux de manière à ne pas causer des préjudices au réel titulaire de cette prérogative. Toutefois le titulaire légale d'une copie piratée ne peut voir son bien lui être retiré sous motif qu'il n'est pas original¹.

Il est vrai que le droit positif marocain offre un arsenal juridique consistant, relativement, pour combattre la criminalité numérique liée à la propriété littéraire et artistique et à la propriété industrielle. Toutefois, l'efficacité de cet arsenal reste suspendue à cause des spécificités des systèmes informatiques. De plus le Maroc occupe une place prépondérante, à l'échelon international, dans la violation des droits d'auteurs, dans la contrefaçon et dans le phénomène de la piraterie des logiciels et des applications. Plusieurs cas sont disponibles dans la jurisprudence marocaine relative à la piraterie des logiciels, à la conception des virus, l'exemple de l'affaire du virus Zotob².

Section 2 : La cybermenace et la protection des entreprises numériques.

La transition numérique est porteuse d'innovation et de croissance, néanmoins, elle crée une immense surface d'attaque qui profite aux cybercriminels. Ainsi, si le numérique offre tant d'opportunités de développement économique et de bonne gouvernance, il est aussi porteur de risques et de menaces³. Une cybermenace est définie comme étant « *une action qui*

¹Khalid ENNASHI, *Op.cit.*, p. 86.

²Un Marocain de 19 ans, Farid Essebbbar, considéré comme le concepteur du virus "Zotob" qui s'est attaqué notamment au système d'exploitation Windows 2000, a été condamné à deux ans de prison par la justice marocaine. Le virus Zotob aurait exploité des brèches dans la sécurité des plates-formes Windows 95, 98, ME, NT, 2000 et XP. Les chaînes de télévision CNN et ABC News, le journal New York Times, la filiale Disney, et l'aéroport de San Francisco figuraient parmi les victimes du virus Zotob.

³أيوب رابح، الحماية الجنائية من القرصنة الإلكترونية في ظل جائحة كورونا مجلة منازعات الأعمال، ع. 52، يونيو 2020، ص. 163.

visée à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système de l'information qu'il contient »¹.

Il n'en demeure pas moins que sur son versant relatif à la sécurité du numérique, tous les acteurs du droit sont concernés par la lutte contre les cybermenaces. Le temps n'est plus à l'attente mais à la compréhension de ces cybermenaces, aussi bien dans leurs diversités que dans leurs aspects techniques. *Botnet*, *rançongiciel*, vol de données, etc. sont autant de termes et de pratiques qu'il appartient désormais aux juristes de comprendre et d'appréhender. Cette section envisage les réponses préventives et répressives apportées par l'Etat, mais englobe également des solutions opérationnelles mises en place par les entreprises au cours de leurs transformations numériques. De ce fait, si les menaces numériques sont toujours plus nombreuses et sophistiquées à mesure que les systèmes et objets se connectent davantage (Sous-section 1). Des actions de cybersécurité doivent être menées pour en lutter contre. (Sous-section 2).

Sous-section 1 : Les menaces numériques.

En janvier 2021, ils étaient 27 millions Marocains à utiliser internet et 22 millions sur les réseaux sociaux d'après l'Agence Nationale de Réglementation des Télécommunications. L'explosion du numérique, la simplification de l'accès à l'informatique et la démocratisation des réseaux sociaux contribuent au développement des cyberattaques. Pas une semaine ne s'écoule sans qu'un grand groupe ne soit victime d'une faille majeure. Les agressions sont de plus en plus insidieuses car elles s'accompagnent de signaux faibles et laissent peu de traces². La cybercriminalité, désigne « *l'ensemble des actes contrevenant à la législation nationale ou aux traités internationaux ratifiés par le Royaume du Maroc, utilisant les réseaux ou les systèmes d'information comme moyens de la commission d'un délit ou d'un crime ou les ayant pour cible* »³.

Pour l'Organisation de Coopération et de Développement Economiques, la cybercriminalité renvoie à tout comportement illégal ou contraire à l'éthique ou non autorisé qui concerne un traitement automatique de données et/ou de transmission de données, et pour l'Organisation des Nations Unies, elle a trait à tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des

¹Article 2 de la loi 05-20.

²Christiane FERAL-SCHUHL, *Op.cit.*, p. 1075.

³Article 2 de la loi 05-02.

données qu'ils traitent. Elle cible différents dispositifs informatique : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à un internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les *smartphones* ou les tablettes¹. Il s'agit d'une menace croissante, irradiante, difficile à maîtriser et aux conséquences très importantes pour les entreprises victimes.

Cet accroissement s'explique d'abord par l'explosion du télétravail, puis par le niveau de vigilance face à cette cybercriminalité encore bien en dessous des standards minimums. Une grande disparité s'observe entre les mesures de protection mises en place sur les postes de travail professionnels et personnels. La Covid-19 a rapidement révélé aux entreprises leurs failles en matière de sécurité informatique et les a exposées au risque cyber. Les attaques prennent différentes formes (Paragraphe1), et les attaques qui ont touché de grandes entreprises ont démontré que l'intérêt principal des pirates est de dérober des informations ayant une valeur économique stratégique à savoir les données (Paragraphe 2).

Paragraphe 1 : Les modes opératoires des cyberattaques.

Des logiciels malveillants, aux *botnets*, en passant par les rançongiciels, le *cryptojacking* et bien d'autres, les modes opératoires des cyberattaques sont nombreux et les cybercriminels ne cessent d'innover pour perpétrer leurs méfaits dans un anonymat total². Nous allons se limiter sur deux menaces majeures les plus courantes à savoir les logiciels d'infiltration fonctionnant en réseau dénommés *botnets* d'une part, et d'autre part les rançongiciels.

Les *botnet* ou robots net ou encore réseau de robots³ sont très utilisés par les cybercriminels et constituent une réelle menace de cybersécurité car bien souvent les victimes ne savent pas que leur équipement est contaminé. Ces *botnets* posent de réelles difficultés de sécurité puisqu'ils ont la faculté de s'introduire dans tous les appareils, y compris dans les objets connectés. Une fois injectés dans le système d'information de la victime, ils servent au

¹D. GUINIER, *Op.cit.*, p. 164.

²Gilbert Blaise BEKALE NGUEMA, « La concurrence déloyale et le numérique : le détournement de la clientèle par l'utilisation du dévoiement (pharming) » in L'entreprise face aux défis du numérique, Ouvrage collectif sous la direction d'Alexandre RIERA et Sylvain CHATRY, MARE & MARTIN, Paris 2018, p. 197.

³Il s'agit d'un ensemble d'appareils connectés à internet et contrôlés par un même logiciel malveillant. Lorsqu'ils s'infiltreront dans les machines via une pièce jointe ou un site corrompu, ces logiciels fonctionnent à l'insu de l'utilisateur pour scanner ses données, copier les informations bancaires, économiques ou stratégiques d'entreprises, ou encore miner de la cryptomonnaie, scanner les failles de sécurité ou envoyer automatiquement des spams.

déclenchement de cyberattaques¹ d'envergure par déni de service² ou l'injection de virus de type cheval de Troie³.

Les rançongiciels⁴, eux, ont démontré leurs capacités destructrices, soit par le nombre de victimes touchées, soit par la sensibilité de leurs cibles. La grande majorité des attaques par rançongiciels se révèlent opportunistes et profitent du faible niveau de maturité en sécurité numérique de leurs victimes. Cependant, depuis 2018, on observe une croissance de ces attaques menées par des groupes cybercriminels qui, après avoir ciblé des particuliers, s'en prennent désormais à des organisations dont les moyens financiers sont importants et les activités sensibles⁵. Cette tendance fait entrer les rançongiciels dans la catégorie dites *Big Game Hunting*⁶.

Ainsi, en 2021 une vague mondiale de cyberattaques a été enregistrée suite à la découverte de plusieurs exploits de type *zero-day* dans des serveurs de messagerie *Microsoft Exchange*. *Microsoft* a certes publié des mises à jour afin de corriger les failles, mais cela n'a pas permis d'éviter les dommages enregistrés ou de supprimer les portes dérobées installées par les attaquants. Par la suite, une nouvelle famille de rançongiciels a été déployée sur les serveurs initialement infectés, chiffrant tous les fichiers, rendant le serveur inopérant et exigeant un paiement pour réparer les dommages⁷. En effet, selon le rapport sur les cybermenaces 2021 de *SonicWall*, les attaques de rançongiciels ont enregistré une augmentation de 62% depuis 2019.

¹Le travail de la sous-direction de lutte contre la cybercriminalité en France dans le cadre d'une opération policière coordonnée par Europol a permis de faire tomber le réseau botnets Emotet en Janvier 2021 et de démanteler une structure-support d'un écosystème cybercriminel basé sur une offre de sous-traitance. Cette opération a permis de mettre hors service les serveurs de contrôle. Le travail d'investigation des polices européennes consistait à remonter les adresses IP des machines infectées jusqu'aux serveurs de distribution, puis à cartographier les réseaux de machines compromises. Le principal mis en cause a été interpellé en Ukraine. Cette opération a permis la saisie de 32 serveurs en France.

²Attaque informatique dont l'objectif est de rendre indisponible un service et d'empêcher les utilisateurs légitimes d'un service à s'en servir.

³Logiciel malveillant en apparence légitime qui contient une fonctionnalité malicieuse : ouverture de portes dérobées, prise de contrôle de l'appareil affecté, exfiltration des données de la victime, etc.

⁴Logiciel malveillant qui permet aux hackers de pénétrer dans un système informatique et de bloquer l'accès à des systèmes ou à des données en échange du versement de rançon.

⁵Les activités de rançongiciels auraient généré en 2020, plus de 350 millions Dollars US d'après Chainalysis.

⁶Pratique visant à cibler des entreprises et institutions particulières capables de payer des rançons importantes avec préparation en amont des opérations d'extorsion.

⁷EL. M. RABII, « La DGSSI : Rempart contre les cyberattaques et garant de la cybersécurité des systèmes d'information vitaux de notre pays », in *Revue de police*, N° 42, Décembre 2021, p. 12.

Au Maroc, durant la crise pandémique la DGSSI¹ a été saisi d'une affaire de rançongiciel relative à une application développée par un ingénieur informaticien marocain baptisée *CovidLock*. Cette application, paraissait à première vue anodine pour tout le monde, et donnait une vue globale sur l'état de la pandémie dans le monde et proposait même des conseils sur la conduite à tenir face à la Covid-19. Mais, en réalité, il s'agissait d'un malware, qui une fois téléchargé, bloque l'accès via un mot de passe généré automatiquement pour mettre la main sur le contenu de l'appareil. Pour le débloquent, les victimes devaient payer une rançon en cryptomonnaie².

Ce type d'attaque génère souvent une rupture ou une dégradation d'activité chez la victime. Le rançongiciel s'inscrit donc comme une menace sérieuse et durable pour les organisations comme pour les particuliers en offrant une modèle économique très rentable aux cybercriminels. Dès lors, payer les rançons ne fait qu'entretenir cette activité criminelle. Le dépôt de plainte est un indicateur pertinent pour évaluer cette menace. Or, les entreprises victimes, essentiellement les TPE et PME, sont encore réticentes de faire un dépôt de plainte, une partie de ces victimes préférant payer la rançon afin de récupérer la clé de déchiffrement et pouvoir, le cas échéant, relancer rapidement la production. Le paiement de cette rançon présente pourtant des conséquences importantes. Cela incite les cybercriminels à lancer de nouvelles attaques. L'entreprise devient également la cible d'autres attaques qui cherchent à leur tour à lui soutirer de l'argent. Sans compter que l'argent injecté dans ce système permet de financer ces réseaux criminels qui ne cessent de s'améliorer.

L'amélioration de cette criminalité est due aussi au *darkweb*. Ce dernier représente la face obscure d'internet, où agissent de nombreux réseaux criminels et où se perpétuent des activités malveillantes. Les cyberpirateries³ mènent leurs activités illicites dans les profondeurs du web, les *darknets* qui permettent le développement d'activités clandestines lucratives. Tous ces *darknets* forment ce que l'on nomme le *deepweb* ou *darkweb*, espace

¹Direction Générale de la Sécurité des Systèmes d'Information.

²M. SASSI, « La lutte contre la cybersécurité », in Revue de police, N° 42, Décembre 2021, p. 56.

³La piraterie est une notion intemporelle qui vise classiquement l'espace maritime mais, aussi, désormais, l'espace numérique dénommé cyberspace tout en gardant des modes opératoires empruntant le langage maritime comme la pêche ou phishing, la navigation sur le web ou le surfing. La piraterie est, en effet, une délinquance non seulement maritime mais également numérique dans un nouvel espace qui est aussi un terrain de conflits sans frontière, à savoir le cyberspace. Il présente comme, l'univers marin, des profondeurs abyssales et sombres que l'on nomme le Darkweb.

abstrait, décomposé, présent à la fois par tout et nulle part, sans être rattaché à aucune juridiction territoriale en particulier et garantissant l'anonymat à ses utilisateurs¹.

Les délinquants agissent dans le *darkweb* avec un sentiment d'impunité, protégés par leur anonymat et l'absence de traçabilité de leurs échanges. L'évolution des outils, le jeune âge des pirates, leur motivation, la mise à disposition de programmes sur le web, l'automatisation des systèmes employés pour détecter les failles dans les entreprises et lancer des attaques, l'utilisation des réseaux sociaux, des technologies mobiles et des accès à distance, le recours au *Cloud computing*, sont autant de facteurs de phénomènes facilitant la cybercriminalité².

Paragraphe 2 : La donnée : une cible principale des cyberattaques visant l'entreprise.

Une technologie, à l'instar de toutes les inventions humaines, est d'abord ce que nous en faisons. La révolution industrielle et sociétale en cours fait des données une richesse importante. Le carburant de l'économie, disent même certains. Le *big data* est généralement présenté comme une révolution positive. Grâce au *big data* la vie des entreprises ne pourrait qu'être améliorée. Ainsi, des millions de données sont collectées chaque jour par des entreprises, lorsque nous surfons sur internet, nous envoyons des courriels, nous effectuons des achats en ligne. Les données se multiplient, le phénomène sera encore en pleine croissance avec les objets connectés. Les entreprises analysent ces données en ayant pour objectif de mieux cibler leur clientèle et développer de nouveaux marchés. Les données sont devenues le nouvel or noir de l'économie.

Le *big data* se définit comme une méga base de données qui ne cesse de se développer avec le temps. La règle des 5V permet de mieux comprendre le concept. Il s'agit de *big data* dès lors que l'on est en présence d'un grand Volume de données, d'une Variété de données et d'un flux continu de données c'est-à-dire une Vitesse des données. Ajoutons deux autres V, un pour Valeur et pour Validité c'est-à-dire la conformité des données. L'exploitation de cette manne financière que sont les données profite principalement aux entreprises privées qui ont les moyens techniques et financiers de collecter, traiter, analyser les données transmises par leurs clients. Ces données attirent les convoitises et les entreprises sont de plus en plus touchées par des attaques de plus en plus sophistiquées visant à violer des données

¹M. QUEMENER, « Enquêtes dans le Darkweb », in IP/IT, N° 2, Février 2017, Dalloz, p. 84.

²Certains groupes qui font du chantage aux entreprises ont leur vitrine sur le Darweb comme par exemple celle du groupe Rex Mundi qui a fait du chantage à l'entreprise Domino's Pizza.

stratégiques, parfois en très grande quantité. En outre, en matière de *big data*, les entreprises ont leurs propres serveurs, mais peuvent aussi avoir recours au *Cloud computing* pour héberger leurs données. Ainsi, les cyberattaques peuvent avoir lieu aussi bien sur les serveurs internes de l'entreprise que sur les serveurs externes de leurs prestataires en *Cloud*. Le *big data* ne différencie pas les types de données qu'il englobe, mais il peut s'agir de données à caractère personnel. Dès lors, cela crée une problématique supplémentaire pour les entreprises, compte tenu des obligations de sécurité de ces données que requiert la CNDP.

En effet, nous constatons un côté obscur du *big data*. Il s'agit des escroqueries telles que le *phishing*¹, le *skimming*², la fraude au président³, le vol de données⁴, etc. Le droit en vigueur au Maroc ne prévoit pas d'incrimination d'actes de *phishing*. D'ailleurs, un arrêt de la Cour d'appel de Rabat en 2006 en témoigne⁵. En effet, un groupe de délinquants escroquaient les gens via internet se faisant passer pour plusieurs banques. Ils avaient à cet effet envoyé un formulaire aux clients de certaines banques leur demandant de saisir des données concernant leur compte. Ces données sont ensuite utilisées pour alimenter des cartes de paiement. La Cour les avait poursuivis en vertu des articles 293, 294, 657, 509 et 540 du Code pénal⁶, et condamnés ensuite sur la base de l'article 510⁷.

Concernant le vol de données, défini pour caractériser le fait d'accéder à une information ou d'en prendre connaissance indument, le vol des données appelé aussi vol d'information ou espionnage de données est considéré comme le fait d'obtenir des données protégées « *sans motif ou justification légitime, ou en se prévalent à tort d'un motif ou d'une justification légitime* »⁸. Au Maroc, l'infraction de vol est définie par le code pénal⁹ comme

¹Dans ce cas le pirate se fait passer pour une banque et veut connaître les coordonnées bancaires de la personne afin de prélever de l'argent sur son compte en banque. Les données personnelles de la personne sont dérobées et utilisées frauduleusement ou revendues sur le marché noir des données personnelles.

²C'est l'utilisation frauduleuse de numéros de cartes bancaires sur internet.

³Elle consiste à convaincre le collaborateur d'une entreprise d'effectuer en urgence un virement important à un tiers (le fraudeur) pour obéir à un prétendu ordre du dirigeant.

⁴Le pirate s'introduit dans un système d'information pour voler des données stockées, les modifier, les détruire ou prendre le contrôle du système.

⁵C. Appel, décision n° 23-2005-50, 7 Avril 2006, Rabat.

⁶Les articles 293-294 du C.P : Association de malfaiteurs.

Les articles 357 et 359 du C.P : Faux écritures de commerce ou de banque.

L'article 540 du C.P : Escroquerie.

⁷L'article 510 du C.P : Vol avec circonstances.

⁸Amina DIK, La Fraude informatique au Maroc, Librairie Dar Essalam, 1^{ère} éd., Rabat, 2017, p. 53.

⁹Dahir n° 1-59-413 du 28 jourmada II 1382 (26 novembre 1962) portant approbation du texte du Code pénal.

« la soustraction frauduleuse de la chose d'autrui »¹. Il peut être commis par un employé à l'intérieur de l'entreprise ou par un cybercriminel extérieur à l'entreprise et il peut concerner des données à caractère personnel ou d'autres données (savoir-faire de l'entreprise, données commerciales...). La difficulté rencontrée ici est que les éléments constitutifs de l'infraction ne sont pas réunis.

En effet, le Code pénal parle de chose, donc un bien matériel. Cependant, la donnée est un bien immatériel. Par ailleurs, pour que le vol soit constitué, il faut qu'il y ait soustraction. Or, nul n'est propriétaire de ses données personnelles. Les critères du droit de propriété ne sont pas conciliables avec la notion de donnée. Ainsi, on a seulement un droit d'usage sur ces données. En revanche, il ne peut pas y avoir de soustraction de données, alors même qu'il est toujours possible d'utiliser ces données personnelles après un vol². L'article 607-3 du code pénal³ pallie cette difficulté, il dispose que « le fait d'accéder, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un mois à trois mois d'emprisonnement et de 2000 à 10 000 dirhams d'amende ou de l'une de ces deux peines seulement ». Ainsi, on peut assimiler le fait d'extraire frauduleusement des données d'un système de traitement automatisé à un vol et cette infraction est sanctionnée, le législateur a facilité la caractérisation de cette infraction complexe. Aussi, la notion d'accès n'a pas été définie légalement par le législateur, suivant en cela la convention du Budapest sur la cybercriminalité et d'autres législateurs. La formulation de l'article incrimine l'accès sans énumérer les procédures d'accès, reflétant la volonté du législateur à avoir une loi évolutive non liée à des techniques précises⁴.

Dans ce contexte, le tribunal de première instance de Marrakech a condamné en 2013 un salarié de deux mois de prison ferme et d'une amende de 10.000 Dirhams par applications des articles 549, 607-3, 607-5 et 607-6 du Code pénal. Dans cette affaire la société PF a accusé un de ses salariés pour le maintien ou l'accès illégale au système de traitement automatisé de données et le changement de certaines informations et la suppression des données ce qui a produit un désordre dans le fonctionnement de ce STAD⁵.

¹Article 505 du Code pénal.

²بخيت طريبيش المنصوري، الجرائم الإلكترونية الماسة بالأشخاص ، مجلة القانون المغربي، ع. 43، يناير 2020، ص. 27.

³Complété par la loi 07-03 qui concerne les infractions relatives aux systèmes de traitement automatisé des données.

⁴Amina DIK, *Op.cit.*, p. 31.

⁵TPI, décision n°2013/2103/5538, 12 Décembre 2013, Marrakech.

Les conséquences économiques des vols de données pour l'entreprise sont importantes. Il peut s'agir de pertes commerciales et l'entreprise peut subir des dommages collatéraux (atteinte à la réputation de l'entreprise, chute des actions en bourse). A titre d'exemple, la cyberattaque de l'entreprise Sony en 2011, qui a exposé les données à caractère personnel de 77 millions d'utilisateurs du *PlayStation Network* a entraîné une chute du cours de bourse immédiate de près de 5%. L'entreprise a aussi dû supporter le coût de la maintenance et de la sécurisation du réseau, ainsi qu'une sanction pécuniaire de 250000 de livres prononcée par l'équivalent britannique de la CNDP¹.

Enfin, l'exploitation à des fins malveillantes de l'intelligence artificielle par des cybercriminels représente un vrai danger, notamment avec l'usage de techniques de *machine learning*² dans les campagnes de *phishing* ou de la conception de *deepfake*. En particulier, le *machine learning* envoie massivement des messages piégés à partir de données en libre accès sur Internet. Ils ciblent ainsi des milliers de victimes potentielles en les renvoyant par exemple vers des sites corrompus pour leur voler leurs identifiants et des données personnelles monnayables³. Les hackers savent créer des virus dotés de fonctionnalités de *machine learning* capables d'analyser l'ensemble des correspondances et apprendre, afin de préparer des courriers électroniques d'hameçonnage trompeurs qui sont ensuite ouverts et consultés par leurs destinataires. Un exemple très récent est celui d'une entreprise allemande qui a été victime courant 2019 d'une fraude utilisant l'intelligence artificielle pour contrefaire la voix de son PDG. A l'heure où tout média peut être contrefait, ce cas inédit interroge sur les solutions pour faire face à ces nouvelles menaces⁴.

Les menaces sont donc très présentes et s'intensifient avec la numérisation de la société. Il est donc urgent de ne pas rester dans l'ignorance ou de ne plus adopter une attitude de déni, voire de fatalisme. Bien au contraire, il est indispensable d'intégrer les questions de sécurité dans tout usage ou développement numérique le plus tôt possible. Cette sécurité est la

¹ G. HASS, « La cybercriminalité à la fois coté obscur et face cachée du Big Data », in IP/IT, N° 1, Janvier 2016, Dalloz, p. 23.

² Le Machine Learning est une technologie d'intelligence artificielle permettant aux ordinateurs d'apprendre sans avoir été programmés explicitement à cet effet. Pour apprendre et se développer, les ordinateurs ont toutefois besoin de données à analyser et sur lesquelles s'entraîner. De fait, le Big Data est l'essence du Machine Learning, et c'est la technologie qui permet d'exploiter pleinement le potentiel du Big Data. Découvrez pourquoi cette technique et le Big Data sont interdépendants.

³ Publiée en Avril 2018, une enquête du Pnemon Institute-Service Now a révélé que 54% des entreprises françaises estiment que les pirates maîtrisent mieux qu'elles certaines technologies, telles que la machine learning.

⁴ Myriam QUEMENER, Frédérique DALLE et Clément WIERRE, *Op.cit.*, p. 31.

condition sine qua non de la confiance qui elle-même est la condition d'une transformation numérique réussie.

Sous-section 2 : Les moyens de lutte contre les cyberattaques.

L'entreprise, comme toute collectivité, doit faire face à de nombreux défis face à la transformation numérique. L'un de ces défis, est celui de la sécurité. On parle de cybersécurité ou de sécurité numérique pour désigner l'ensemble des processus de protection, de défense et de résilience dans ce nouvel espace dit cyber¹. Enjeu de défense et de sécurité, de croissance économique, et donc de souveraineté, la cybersécurité est désormais, partant dans le monde, une priorité au niveau le plus élevé.

Selon l'article 2 de la loi 05-20, la cybersécurité désigne : « l'ensemble de mesures, procédures, concepts de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques, et technologies permettant à un système d'information de résister à des événements issus du cyberspace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ce système offre ou qu'il rend accessible ». La cybersécurité est plus que jamais, placée au centre des préoccupations des pays du monde entier, qui cherchent à mettre en place des stratégies intégrées de prévention, de détection et de réponse aux cyberattaques, et à développer des solutions technologiques à la hauteur des défis de la menace cyber qui guette tout le monde.

Le Maroc s'est engagé depuis 2012 sur la voie du renforcement de ses capacités nationales de sécurités des systèmes d'information et de la consolidation de la confiance numérique, il a adopté une approche transversale en matière de cybersécurité. En effet, la sécurité informatique se voit érigée en priorité nationale vu le nombre de projets tant législatif qu'organisationnel dont elle, fait l'objet. On cite à cet égard l'exemple le projet de code numérique qui consacre tout le titre 6 à la sécurité et confiance numérique. Ce dernier oblige² l'autorité compétente, dans le cadre de l'administration électronique, à procéder à

¹R. ECHARD, « Cybersécurité en entreprise, comment protéger votre patrimoine intellectuel et industriel ? », in IP/IT, N° 12, Décembre 2019, Dalloz, p. 675.

²Article 4 du projet du Code Numérique : « Avant toute création d'un service de l'administration électronique, l'autorité compétente doit : 1- Identifier les risques en termes de sécurité du système et des données qu'il comporte et ce, conformément, s'il existe, au référentiel général de sécurité prévu à l'article 16 ci-dessous; 2-Fixer, au regard des risques identifiés, les objectifs de sécurité, notamment en terme de disponibilité, d'intégrité, de confidentialité et d'identification des usagers ; 3- En déduire les mesures et fonctions à déployer pour atteindre les objectifs de sécurité ainsi fixés et s'assurer de leur adéquation et leur proportionnalité. Les modalités de création d'un service de l'administration électronique sont fixées par voie réglementaire ».

l'identification des risques et les solutions ou mesures proposées pour gérer ces risques et assurer le fonctionnement des systèmes d'informations¹. En plus la loi 09.08 oblige le responsable du traitement à mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger et sécuriser les données à caractère personnel contre tout traitement illicite. Et enfin la loi 05-20 relative à la cybersécurité qui introduit également à l'égard des entités une obligation de signalement à l'Autorité nationale de cybersécurité des incidents de sécurité dont elles sont victimes à charge pour cette dernière d'aider ces entités à prévenir et solutionner ces vulnérabilités.

En quête d'une posture de cybersécurité efficace, les pays tentent aujourd'hui de réglementer le cyberspace. Au Maroc, la prise de conscience de l'importance de la cybersécurité a été matérialisée par la mise en place d'un arsenal organisationnel de lutte contre la cyberattaque (Paragraphe 1). Mais, le fait d'internet soit considéré comme un espace de liberté absolu pour certains pays et un espace qui doit être supervisé pour d'autres, rend difficile l'atteinte de cet objectif de cybersécurité qui nécessite de facto une coopération internationale intense (Paragraphe 2). Dans ce contexte international mitigé, chaque entreprise doit se doter de capacités pour protéger et sécuriser ses données (Paragraphe 3) et adopter de bonnes pratiques qui lui permettront de réduire considérablement les risques de ces cyberattaques. Surtout, la prise en compte de ces questions par les décideurs permet d'entreprendre des démarches et actions qui aboutiront à une véritable résilience de l'organisation concernée (Paragraphe 4).

Paragraphe 1 : L'arsenal organisationnel de lutte contre la cybermenace.

Pour se positionner parmi les pays émergents dynamiques dans les technologies numériques, le Maroc s'est doté d'une stratégie globale s'articulant autour de deux pôles : la réforme d'un cadre juridique, et le renforcement institutionnel par la création de nouvelles instances ou l'adaptation des services d'enquête et de veille stratégique en les dotant de nouvelles prérogatives. Ainsi, en 2011, le Maroc s'est doté de deux instances nationales de sécurité des systèmes d'information créées au sein de la direction de défense nationale, et qui sont : le Comité Stratégique de la Sécurité des Systèmes d'Information² et la Direction

¹Amina DIK, *Op.cit.*, p. 140.

²Le Comité Stratégique de la Sécurité des Systèmes d'Information a été créé par la loi 05-20 du 25 Juillet 2020.

Générale de la Sécurité des Systèmes d'Information¹. En outre, il a inauguré le 2 Novembre 2011 le Centre marocain de veille, de détection et de réactions aux attaques informatiques (maCERT)². Ces instances ont une coloration de prévention et de veille stratégique. En effet, le premier a pour rôle d'établir les orientations stratégiques dans le domaine de la sécurité des systèmes d'information. Le second se charge, d'une part, de coordonner entre les différents ministères pour élaborer une stratégie nationale de sécurité, et veiller à l'application des recommandations dudit comité.

Quant au centre national maCERT, il est l'une des directions de la DGSSI et a pour principales missions de coordonner, prévenir et répondre aux incidents liés à la sécurité des systèmes d'information, ainsi qu'analyser ou restaurer les vulnérabilités des systèmes infectés³. L'année 2021 a été marquée par de nombreuses cybermenaces et d'activités malveillantes détectées par le maCERT et rapidement prises en charge. Grâce à l'activité dynamique de veille, 784 bulletins d'alerte de sécurité ont été produits et diffusés. De plus, le maCERT a pu détecter au cours de la même année 342 cybermenaces et activités malveillantes.

En 2014, la DGSSI a élaboré la Directive Nationale de la Sécurité des Systèmes d'Information. L'objectif étant d'élever et d'homogénéiser le niveau de protection et de maturation de la sécurité de l'ensemble des systèmes d'information des administrations et organismes publics, ainsi que des infrastructures d'importance vitale⁴. La DNSSI s'appuie sur un ensemble de règles, procédures et bonnes pratiques reconnues au plan international, dont la norme ISO/CEI 270002 version 2009.

En 2020, le Comité Stratégique de la Sécurité des Systèmes d'Information a été remplacé par le Comité Stratégique de la cybersécurité suite à l'adoption de la loi 05-20 relative à la cybersécurité⁵. Ce comité est chargé d'élaborer les orientations stratégiques de

¹La Direction Générale de la Sécurité des Systèmes d'Information a été créée par Décret n° 2-11-509 du 21 Septembre 2011.

²Il a été mise en place grâce à une coopération entre le gouvernement marocain et l'agence coréenne de coopération internationale (KOICA).

³A noter que dans un premier temps, les services de ce centre étaient limités à protéger quelques sites seulement à savoir le site internet du ministère de l'Industrie et celui de l'Office marocain de propriété industrielle et commerciale avant que la protection couvre les sites internet de l'administration publique et les sites du secteur privé qualifiés comme sensibles.

⁴Décret n° 2-15-712 du 22 Mars 2016 qui a pour objet de fixer le dispositif de protection des Systèmes d'information sensibles (SIS) des Infrastructures d'importance vitale.

⁵Article 35 de la loi 15-20.

l'Etat en matière de cybersécurité et veiller sur la résilience des systèmes d'information des entités, des infrastructures d'importance vitale et des opérateurs. Il est responsable de l'évaluation annuelle du bilan d'activité de la DGSSI et des travaux du comité national de gestion des crises et événement cybernétiques majeurs. Par ailleurs, il arrête le périmètre des audits de la sécurité des systèmes d'information effectués par la DGSSI. Le comité soutient également l'instauration de programmes et d'actions de sensibilisation et de renforcement des capacités en cybersécurité au profit des entités et des infrastructures d'importance vitale. Enfin, il est chargé de donner son avis sur les projets de textes législatifs et réglementaires se rapportant au domaine de la cybersécurité.

Auprès de ce comité, à savoir le Comité Stratégique de la cybersécurité, il a été institué le comité de gestion des crises et événements cybernétiques majeurs chargé, d'assurer une intervention coordonnée en matière de prévention et de gestion de crise par suite d'incidents de cybersécurité. A cet effet, les fournisseurs d'accès à internet, les prestataires de services de cybersécurité et les prestataires de services numériques sont tenus, en cas de crises cybernétiques majeures, de répondre aux prescriptions et demandes de concours et d'assistance technique du comité de gestion des crises et événements cybernétiques majeurs.

En outre, la loi 05-20 relative à la cybersécurité a créé l'autorité nationale de la cybersécurité chargée en principe de mettre en œuvre la stratégie de l'Etat en matière de cybersécurité. L'article 38 et suivant de ladite loi énumère les missions dévolue à l'autorité nationale de la cybersécurité. Un décret d'application¹ a vu le jour en 2021 qui fixe la composition et les modalités de fonctionnement des organes de gouvernance de la cybersécurité, prévus par la loi n°05-20, à savoir l'autorité nationale de la cybersécurité, le comité stratégique de la cybersécurité et le comité de gestion des crises et événements cybernétiques majeurs. Ledit décret détaille les dépositions propres aux entités disposant de systèmes d'information sensibles, et aussi celles relatives aux opérateurs. Il détermine aussi les critères de qualification des prestataires de services d'audit² et de cybersécurité. Enfin, la traque de la cybercriminalité est du ressort également de la Brigade Nationale de la Police Judiciaire, cette dernière s'est dotée en 2018 d'un Office National Contre la Criminalité liée

¹Décret n° 2-21-406 du 15 juillet 2021 pris en application de la loi n° 05-20 relative à la cybercriminalité.

²L'audit de sécurité est un mécanisme de gouvernance qui permet de fournir une assurance raisonnable au commanditaire quant à la maîtrise des risques pouvant affecter la disponibilité du système d'information, l'intégrité des données ou leur disponibilité. Les principales activités d'audit portent sur ; la conformité à la réglementation, normes et directives en vigueur, l'évaluation des vulnérabilités des applications web et l'analyse des architectures et les audits des configurations.

aux Nouvelles Technologies. C'est une entité d'élite chargée de la lutte contre la criminalité transnationale sous toutes ses formes et manifestations et traitant les grandes affaires à ramifications nationales et internationales liées à la cybercriminalité¹.

Paragraphe 2 : La coopération internationale comme instrument de lutte.

Les populations du monde profitent largement des vertus d'internet, mais subissent aussi le fléau de la menace cybernétique. Une action malveillante à l'autre bout du monde peut rapidement avoir un impact planétaire. De ce fait, la protection est certes d'abord une question de souveraineté, elle est, en raison des interdépendances des réseaux et des systèmes, une affaire multilatérale. La menace est transnationale, la réponse devra être internationale. Dans ce contexte la coopération internationale s'impose comme un levier incontournable pour faire face à la menace cybernétique. Elle constitue un garant de la sécurité et la stabilité et un moyen d'échange et de partage de l'information et des bonnes pratiques entre les Etats.

La coopération internationale constitue également un moyen idoine de transfert de compétences permettant aux pays en développement de profiter de l'expertise des pays avancés pour développer leurs capacités dans le domaine de la cybersécurité. Au Maroc, la coopération est envisagée sur plusieurs axes ; l'harmonisation de la législation, le renforcement des unités judiciaires et l'assistance technique. En plus, elle repose principalement sur trois piliers à savoir la coopération internationale, la coopération à l'échelle régionale et la coopération bilatérale.

Au niveau international, la convention sur la cybercriminalité², communément dit Budapest, a été signée en 2001 à Budapest en Hongrie et est entrée en vigueur 2003. Il s'agit d'un traité international, dont l'objectif est d'assurer la protection des usagers du cyberspace contre la cybercriminalité, notamment par l'adoption d'une législation appropriée, le renforcement des cybercapacités et l'amélioration internationale³. 67 pays ont ratifié cette convention, dont le Maroc, qui a déposé les instruments d'adhésion à la convention et son Protocole additionnel en 2018. Cette convention a instauré dans ses articles 23 à 28 des principes généraux relatifs à la coopération internationale, et dans ses articles 29 à 35 des

¹Au cours de l'année 2021, les services de la Sûreté Nationale ont traité 5275 affaires et ont pu détecter sur la base d'un travail anticipatif de veille, 3533 publications de contenus illicites. En relation avec la sextorsion, 498 affaires ont été traitées, ayant mené à l'arrestation de 270 maitre-chanteurs et à l'identification de 508 victimes, dont 95 nationalités étrangères.

²Convention sur la cybercriminalité, Budapest, 23 Novembre 2001.

³Eric CAPRIOL, *Op.cit.*, p. 100.

dispositions spécifiques à cet égard. Parmi ces dispositions spécifiques, on trouve la mise en œuvre d'un réseau de coopération dit 24/7 conformément à l'article 35 de la convention. Il s'agit d'un mécanisme qui met à la disposition de l'organisation internationale Interpol¹, un point de contact joignable 24 heures sur 24, 7 jours sur 7, afin d'assurer une assistance immédiate pour des investigations ou des preuves concernant les infractions informatiques. Cette assistance englobe aussi bien l'apport de conseils techniques, la conservation des données, le recueil de preuves électroniques, l'apport d'informations à caractère juridique et la localisation des suspects².

En 2021, un présumé cybermalfaiteur très actif a été appréhendé au Maroc à la suite d'une enquête menée conjointement par Interpol, la police marocaine et Group-IB³. Agissant sous le pseudonyme de « *Dr Hex* », le suspect aurait, des années durant, ciblé des milliers de victimes sans méfiance en se livrant à l'hameçonnage, à la fraude et au piratage de cartes bancaires à l'échelle mondiale. Il est aussi accusé de s'être livré au défacement de nombreux sites web en modifiant la présentation et le contenu, et d'avoir ciblé des entreprises de télécommunications francophones, plusieurs banques et des multinationales en utilisant des logiciels malveillants. Ces logiciels étaient ensuite utilisés pour usurper l'identité de banques en ligne, ce qui a permis au suspect et à d'autres de voler des informations sensibles et d'escroquer des personnes sans méfiance à des fins de profit. Le préjudice causé aux particuliers et aux entreprises était ensuite publié sur internet, afin de faire la publicité de ces services malfaisants⁴.

En outre, la Direction Générale de la Sécurité des Systèmes d'Information a fait de la coopération internationale un axe majeur de sa stratégie de cybersécurité. Elle est ainsi un membre actif de nombreuses structures et organisations internationales, dont le Groupe

¹L'Interpol ou Organisation Internationale de Police Criminelle (OIPC), a été créée en 1929. Elle vise à améliorer la coopération policière grâce à des bureaux dans les 186 pays membres. Ces bureaux sont des services de police permanents composés de policiers agissant dans le cadre de leur législation nationale. Le rôle d'Interpol est de faciliter pour ses membres la lutte contre plusieurs crimes, Interpol dispose d'un système de communication informatique commun à tous les pays membres et de bases de données criminelles internationales.

²M. EL MADANI, « L'arsenal pénal et aspects de la protection juridique en matière de la criminalité informatique au Maroc », in *Revue Marocaine de Droit Pénal et de Sciences Criminelles*, N°6-7, 2019, p. 17.

³Group-IB est un fournisseur de solutions basé à Singapour visant à détecter et à prévenir les cyberattaques, la fraude en ligne, la protection de la propriété intellectuelle et les enquêtes sur les crimes de haute technologie. Le système Threat Intelligence de Group-IB a été nommé l'un des meilleurs de sa catégorie par Gartner, Forrester et IDC.

⁴INTERPOL, « Evaluation 2021 des Cybermenaces en Afrique », Rapport, Singapore, Octobre 2021.

d'Experts Gouvernementaux de la Cybersécurité créée par l'ONU, qui a pour mission principale l'élaboration de normes internationalement acceptées pour instaurer un comportement responsable des Etats dans le cyberspace. Aussi, le *Forum of Incident Response and Security Teams* qui est une organisation mondiale regroupant la majorité des CERTs publics et privés, dont l'adhésion permet, outre la veille sur les tendances en matière cybersécurité, la réponse efficace aux incidents de sécurité. Dans le même cadre international, le Maroc fait partie du *Global Forum on Cyber Expertise*, une communauté multipartite regroupant des gouvernements, des organisations internationales, des organisations non gouvernementales, la société civile, des entreprises privées, la communauté technique et le monde universitaire, qui vise à renforcer les capacités et l'expertise en matière de cybernétique au niveau mondiale.

Au niveau régional, l'union africaine a conduit à travers le projet HIPSSA¹, une réflexion en vue d'aboutir à la mise en place d'un cadre juridique de confiance pour la cybersécurité en Afrique à travers l'organisation du commerce électronique, la protection des données à caractère personnel et la lutte contre la cybercriminalité. Ce projet fait de la coopération un pivot de la lutte contre les crimes informatiques. Dans l'article III-14 du projet, les Etats membres sont interpellés à échanger des informations et partager des données réciproques sur une base bilatérale ou multilatérale.

Par ailleurs, les pays arabes ont élaboré une Convention arabe pour la lutte contre les crimes liés aux technologies de l'information et de la communication². Cette convention vise à renforcer la coopération entre les pays arabes en matière de lutte contre la cybercriminalité. En plus, elle offre aux autorités spécialisées des pays membres, la possibilité de procéder à des expertises pour poursuivre les cyber-délinquants.

Au niveau bilatéral, le Maroc a signé de nombreux accords bilatéraux liés à l'entraide judiciaire internationale. Les dispositions de ces accords sont applicables en premier lieu puisque la convention de Budapest sur la cybercriminalité respecte le principe de subsidiarité³. Elle affirme que les accords bilatéraux existants en matière pénale sont

¹Le titre de la convention a été modifié en 2012. Avant, elle portait sur l'adoption d'un cadre juridique propice de la cybersécurité en Afrique. Depuis 2012, elle porte sur la confiance et la sécurité dans le cyberspace.

²Dahir n°1-13-46 du 23 Joumada 1434 (4 Avril 2013) portant promulgation de la loi 75-12 portant approbation de la Convention arabe pour la lutte contre les crimes liés aux technologies de l'information et de la communication (TIC), faite au Caire le 21 décembre 2010.

³Le principe de subsidiarité est une maxime politique et sociale selon laquelle la responsabilité d'une action publique, lorsqu'elle est nécessaire, revient à l'entité compétente la plus proche de ceux qui sont directement

applicables aux infractions et procédures définies dans ladite Convention. En plus, le Maroc a une large régulation interne de la coopération judiciaire internationale via son C.P.P. ce dernier lui consacre tout le titre III intitulé « Des rapports judiciaires avec les autorités étrangères ».

Au même niveau-bilatéral- la DGSSI a tissé des relations de coopération avec les entités similaires des pays leaders dans le domaine de la cybersécurité notamment, la France, les Etats-Unis, l'Espagne, la Corée du Sud, l'Inde et la Malaisie. La DGSSI coopère également avec *Escal Institute of Advanced Technology*, une compagnie américaine spécialisée dans la sécurité de l'information et la formation sur la cybersécurité. Aussi, la DGSSI a entretenu courant 2020 des échanges avec le Royaume Uni pour la mise place d'un plan d'action de coopération en matière de cybersécurité entre la DGSSI et le *National Cyber Security Center*¹.

Paragraphe 3 : La protection des données, un enjeu cardinal de la cybersécurité.

Dans un écosystème numérique en expansion, la protection des données personnelles constitue un préalable stratégique et un prérequis fondamental, qui prenne en compte le respect de la vie privée. Dans un monde digitalisé où des données personnelles envahissent la toile, la donnée devient un actif stratégique et sa protection devient alors, gage de confiance, pour une transformation digitale réussie et responsable. Bien souvent, les attaques informatiques impliquent, d'une manière ou d'une autre une violation des données. Dans cette hypothèse, il sera nécessaire de veiller au respect de la réglementation en vigueur. L'entreprise qui souhaite bénéficier d'une sécurité maximale doit, tout à la fois, exiger de son prestataire le respect des plus hauts standards, s'assurer de l'existence de contrôles effectifs et d'une transparence adaptée et, dans le même temps, organiser sa gouvernance pour lutter contre la cybermenace.

L'entreprise doit, tout d'abord, s'assurer que ses données sont traitées dans un environnement hautement sécurisé. Cette garantie repose sur deux impératifs. Le premier

concernés par cette action. Lorsque des situations excèdent les compétences d'une entité donnée responsable de l'action publique, cette compétence est transmise à l'entité d'un échelon hiérarchique supérieur et ainsi de suite. Le principe de subsidiarité veille à ne pas déconnecter la prise de décision publique de ceux qui devront la respecter. C'est en somme la recherche de la sphère d'influence adéquate dans une organisation sociale par laquelle se déploie une action publique.

¹A. BOUTRIG, « Le contrôle, l'assistance et le renforcement des capacités nationales en matière de cybersécurité. D'autres fonctions de la DGSSI », in *Revue de police*, N° 42, Décembre 2021, p. 33.

consiste en l'utilisation d'infrastructures *Cloud* spécifiquement conçues pour assurer une sécurité maximale de données depuis le jour où celles-ci sont stockées jusqu'aux moments de leur consultation par les utilisateurs sur leurs appareils¹. On parle ici de sécurité physique et logique, intégrant notamment le chiffrement des données², que ce soit lors de l'accès au service, sur les supports de stockage ou encore dans les communications entre les centres de données. L'objectif est de protéger le client contre les fuites d'informations, le détournement du flux de leurs données, l'utilisation du contenu des disques des centres de données en cas de vol et les accès malveillants ou la perte des données en transit entre les utilisateurs.

Le second impératif impose à l'opérateur *Cloud* de justifier la mise en place d'une politique de sécurité conforme aux normes internationales en la matière, notamment ISO 27001 et ISO/IEC 27018³, premier standard applicable aux prestataires de *Cloud* pour la protection des données. Le Maroc dispose, à cet égard d'une réglementation relative à la protection des données à caractère personnel à savoir la loi 09-08. L'opérateur de *Cloud* doit pouvoir s'engager envers ses clients à respecter les dispositions relatives aux transferts de données personnelles hors du territoire marocain ainsi qu'à la durée de conservation des données⁴. Dans ce cadre, la loi 09-08 comporte des dispositions sur les flux transfrontaliers des données personnelles et confie à la CNDP la tâche d'établir la liste des pays à la législation adéquate pour les transferts de données à l'étranger⁵. Aussi, la commission a aussi un pouvoir de commandement qui se manifeste dans le pouvoir d'ordonner le verrouillage,

¹M. MOSSE, « Quand le Cloud rime avec la cybersécurité », in IP/IT, N° 1, Janvier 2016, Dalloz, p. 17.

²Le chiffrement des données, en particulier dans un contexte d'ouverture et de mondialisation des écosystèmes d'entreprises et de généralisation des outils de collaboration et de productivité, s'avère de plus en plus crucial. L'émergence de solutions permettant le chiffrement, l'envoi et le stockage des fichiers échangés par courriel, sans altérer ni la performance ni l'ergonomie des outils de messagerie devient nécessaire pour les entreprises.

³La norme ISO/CEI 27018:2014¹ concerne la protection des données à caractère personnel dans l'informatique en nuages. Elle a été publiée en août 2014 par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) sous le titre en français : « Technologies de l'information, Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII ». La norme ISO/CEI 27018:2014 permet d'établir les objectifs de contrôle, les contrôles et les lignes directrices communément acceptés pour la mise en œuvre de mesures de protection des informations personnelles (PII) conformément aux principes de respect de la vie privée de l'ISO/CEI 29100.

⁴Le projet du code numérique a introduit le principe de conservations des données dans son article 26 : « Les prestataires de services, dans le respect de la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires... ».

⁵Voir supra p. 133.

l'effacement et la destruction de données, ainsi que la possibilité d'interdire un traitement de donnée personnelles comme le stipule l'article 30 dans son alinéa 4.

Ensuite, et afin de renforcer d'avantage la sécurité de son *Cloud*, il importe de s'engager de manière proactive dans la lutte contre la cybercriminalité. De ce fait l'organisation interne doit être adaptée. Ainsi l'exemple de la création d'une unité spécialisée au sein de l'équipe juridique de *Microsoft* appelée *Digital Crimes Unit* et dont l'action vise à renforcer la sécurité des entreprises utilisatrices de *Cloud* agissant directement contre les cybercriminels. Certes, toutes les entreprises ne vont pas se doter d'un tel service. Il reste qu'en termes de gouvernance interne, il importe de créer les conditions d'une hygiène de la sécurité des données. En effet, connaître la nature des données collectées ou/et traitées est une nécessité pour avoir une approche efficace de la sécurité. Une segmentation fine permet de mieux connaître les risques potentiels et d'optimiser les garanties.

Enfin, il est impératif que l'entreprise garde l'entière maîtrise sur les données qu'elle confie à son prestataire de *Cloud*. Ce dernier doit notamment, être en mesure de lui fournir une information précise sur les conditions de traitement de ses données, lui laisser le choix de la zone géographique de stockage, permettre l'audit régulier de ses infrastructures et services *Cloud* par un tiers indépendant habilité ou encore lui mettre à disposition des fonctionnalités d'administration étendues.

La protection des données contre le cyber risque est une question globale et il paraît hasardeux de conclure définitivement sur un sujet en constante évolution. Il reste que des lignes forces se dégagent. D'une part, il apparaît plus que jamais nécessaire de définir un cadre juridique international harmonisé. D'autre part, il convient de plaider pour une innovation responsable alliée à des régulations innovantes propre à garantir les droits de chacun et favoriser une société numérique de croissance et de confiance.

Paragraphe 4 : Les bonnes pratiques pour faire face aux cyberattaques.

Les responsables de la sécurité des systèmes d'information s'accordent pour affirmer que la majorité des attaques n'auraient pas lieu si certaines bonnes pratiques étaient respectées. La très grande majorité de ces attaques n'aboutiraient cependant pas si des mesures simples d'hygiène informatique étaient mises en œuvre. Et la très grande majorité de ces mesures ne coutent rien, si ce n'est un peu d'énergie et de temps. Mettre en œuvre ces mesures de base est donc très rentable au vu des dégâts que peut engendrer une attaque

informatique. Parmi ces mesures, voici celles à mettre en œuvre très rapidement et qui vont permettre d'augmenter la résilience face aux virus.

D'abord, il est recommandé de se doter des anti-virus et de les mettre à jour régulièrement, l'évolution des versions étant liée à l'identification de failles de sécurité. Ainsi, il faut procéder aux mises à jour dès lors qu'elles vous sont proposées, sans les reporter. Ensuite, bien encadrer l'utilisation du *BYOD*¹ en mettant en place un réseau internet privé et un autre public ainsi qu'en filtrant les accès aux sites web accessibles depuis le réseau de l'entreprise. Les tests d'intrusion constituent également une mesure de précaution dans certains cas, l'identification de signes suspects n'étant ni évidente ni suffisante². En cas de déplacement, il faut protéger physiquement ces ressources informatiques et éviter les réseaux wifi publics. Au-delà des règles simples, il est nécessaire d'utiliser des logiciels de chiffrement de données mais aussi d'échanges sécurisés, que ce soit par le chiffrement pour protéger la confidentialité ou par signature électronique pour assurer l'intégrité et l'authentification³.

En outre, une attention particulière doit être portée aux mots de passes et plus largement à la gestion des accès. Ces restrictions d'accès, cette gestion de droits, le cloisonnement des usages sont, avec des mots de passe robustes, essentiels à la résilience numérique⁴. Par ailleurs, la sensibilisation de tous les collaborateurs joue un rôle important dans la sécurité de l'entreprise⁵. Il est possible de commencer par des publics plus sensibles, comme les managers, les financiers et les administrateurs systèmes. Mais les enjeux de sécurité numérique, au sein de l'organisation, concernent tous et toutes. La démarche de sensibilisation peut commencer par des choses très simples : apprendre à ne pas cliquer de manière irréfléchie sur toute pièce jointe ou n'importe quel lien, à reconnaître un mail frauduleux ou encore à ne pas mélanger les usagers professionnels et personnels. Il s'agit

¹Bring Your Own Device.

²Christiane FERAL-SCHUHL, *Op.cit.*, p. 1077.

³R. ECHARD, « Cybersécurité en entreprise, comment protéger votre patrimoine intellectuel et industriel ? », in IP/IT, N° 12, Décembre 2017, Dalloz, p. 677.

⁴Il serait illusoire de penser protéger vos biens si vous partagez vos clés avec tout le quartier ou laissez les portes ouvertes. Une stagiaire n'a pas à accéder à toutes les données de votre entreprise, et une clé USB personnelles, comme celle trouvée dans un parking, ne doit pas être branchée sur le réseau de l'entreprise.

⁵J-Y. LATOURNERIE, « Cybermenaces et protection des entreprises : une priorité de l'Etat », in IP/IT, N° 1, Janvier 2016, Dalloz, p. 11.

fondamentalement d'acculturer les acteurs, de prendre des bonnes habitudes, il faut fermer la session de son ordinateur lorsque l'on quitte le bureau.

Enfin, pour que la sécurité devienne l'affaire de tous, il est indispensable que cela devienne un sujet prioritaire pour les décideurs. La menace numérique relève désormais du niveau stratégique. Ces questions doivent sortir de leur domaine réservé et ne sont plus des affaires d'informaticien. La personne responsable de l'entreprise doit gérer le risque cyber comme elle gère le risque financier ou autre. Avant d'être une question technique, la cybersécurité est une affaire d'organisation. Par l'adoption d'une démarche itérative et agile, il est possible de se sécuriser progressivement, et avec efficacité, en fonction des priorités et des contraintes. Il appartient donc au chef d'entreprise d'anticiper pour ne pas subir.

Conclusion du Titre I

Le pouvoir de lever l'impôt relève de l'Etat. Mais dans un espace virtuel sans frontière, les modalités de taxation d'activités numériques devenues lucratives ne vont pas de soi. Certains Etats ont donc fait le choix d'instaurer, seule, une taxe pour imposer les sociétés numériques. Cependant, l'efficacité d'une loi isolée n'est pas évidente et la disparité normative inquiète¹. Par ailleurs, dans sa relation avec son environnement externe, l'entreprise en transformation digitale est confrontée à des situations qui sont source d'insécurité juridique que ce soit face à des concurrents ou des cyberattaques.

D'une part, à l'heure où la concentration industrielle dans des secteurs comme le numérique suscite des inquiétudes de l'opinion, la question de la régulation de la concurrence revient en force² et lorsqu'elles veulent intervenir sur les sujets numériques, les autorités de la concurrence sont confrontées à plusieurs défis pratiques qui nécessitent de disposer de compétences spécialisées pour détecter les pratiques anticoncurrentielles sources d'insécurité.

D'autre part, en guise d'épilogue, on déduit de ce qui précède que la cybercriminalité constitue un défi pour l'Etat marocain qui est invité à actualiser, à chaque fois, son arsenal juridique pour pouvoir incriminer les nouveaux actes criminels. Les cyberattaques ne sont pas figées, mais elles évoluent et ne cessent de changer leurs formes et cela en totale harmonie avec le développement du digital. Ce qui rend la tâche du législateur marocain plus dure, mais surtout plus compliquée.

¹ M. GRANGE, *Op.cit.*, p. 71.

² Emmanuel COMBE, *Economie et politique de la concurrence*, Dalloz, 2^{ème} éd., Paris, 2020, p. 505.

Titre II

L'engagement de la responsabilité et la résolution des litiges au numérique

En seulement quelques décennies, la transformation numérique est devenue une condition de plus en plus indispensable à la prospérité de nos économies modernes. Tous les secteurs d'activité sont concernés. Ainsi, le numérique est un levier de performance pour les organisations, une souplesse dans leur fonctionnement et un outil de réponse optimale aux attentes de leurs salariés et leurs consommateurs.

Cependant, comme tout outil, il fait peser des responsabilités sur les entreprises, tant sur les modalités de collecte, les algorithmes utilisés et la sécurité des données collectées, que ce soit sur leurs parties prenantes ou sur leurs données internes¹. Par ailleurs, souvent, en matière du numérique, plusieurs droits et libertés entrent en conflit, comme le droit d'auteur, le droit à la vie privée. Des violations de ces droits s'en suivent inévitables, violations auxquelles les tribunaux tentent de remédier en appliquant des principes de droit commun traditionnels, qui n'ont souvent, en fin de comptes, rien de novateur, contrairement aux technologies en causes.

En matière de transformation digitale des entreprises, ce sont les contrats et la responsabilité extracontractuelle et pénale qui doivent retenir notre attention. Les matières spécifiques, telles que le droit des incapacités ou encore le droit des sociétés, ne présentant pas de particularités propres à l'internet, celles-ci ne justifient donc pas d'être évoquées dans ces développements². Néanmoins une nouvelle notion commence à prendre place ces dernières années il s'agit de la responsabilité numérique.

En revanche, déterminer à l'avance le droit applicable au contrat à conclure ou la loi compétente pour sanctionner la pratique commerciale déloyale revêt la plus grande importance pour les professionnels et consommateurs internautes. Ces derniers gardent le choix de déterminer la loi applicable et le tribunal qui va trancher leurs litiges ou à défaut ils font appel à un arbitrage.

¹P. KERMARREC, « Numérique et responsabilité des organisations » consulté le 14-06-2022 à 17h sur <https://pascalkermarrec.com/2021/02/09/numerique-et-responsabilite-des-organisations/>

²Luc GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, *Op.cit.*, p. 980.

Avant de soulever la question de la compétence des litiges nés sur internet (Chapitre 2), nous entamerons une étude de la responsabilité à l'ère du numérique (Chapitre 1).

Chapitre I

La responsabilité à l'ère du numérique

Le numérique désigne cette réalité hyper-connectée dans laquelle nous évoluons quotidiennement à partir de nos ordinateurs, tablettes ou *smartphones*. L'univers virtuel qui est désormais le notre n'est plus celui de la réalité physique, façonnée par la nature, mais conçu par des acteurs bien particuliers. Dans cet environnement, les individus peuvent à la fois apparaître sous une autre identité et adopter des comportements inhabituels. Plus généralement, les nouvelles technologies affectent notre conception de nous-mêmes, nos relations avec autrui, notre conception de la réalité et nos interactions avec la réalité. Les mutations des modes de vie contemporains au contact du numérique et leur impact sur la condition humaine conduisent alors à repenser des concepts majeurs et essentiels comme la propriété, la vie privée et la responsabilité.

Le concept de responsabilité serait donc à refonder dès lors que notre environnement est fondamentalement différent de celui dans lequel les sociétés humaines ont évolué depuis l'origine. Cet univers se caractérise par un brouillage de la distinction entre réalité et virtuel, par une intrication entre l'humain, la machine et la nature, par le passage d'une pénurie d'informations à une abondance d'informations et celui de la primauté de choses, propriété et relations binaires isolées à la primauté des interactions, des processus et des réseaux.

Cette montée en charge significative du numérique a conduit les autorités à soulever non seulement la question du régime légale de la responsabilité des différents acteurs de l'internet (Section 1) mais également, l'apparition d'une notion plus récente et peu connue des juristes, à savoir, la responsabilité numérique (Section 2).

Section 1 : La responsabilité des acteurs d'Internet.

Avec le développement de l'activité économique sur internet de nombreux acteurs sont apparus et ont développé des modèles inédits de services. Cependant, le problème principal d'internet, réseau mondial, est celui de la responsabilité et plus précisément le responsable susceptible d'être identifié, trouvé ou atteint. Aussi, outre les responsabilités pouvant être encourues par l'éditeur du site internet sur la base des règles relatives à la protection de données personnelles et de la propriété intellectuelle, l'internet a donné lieu à une catégorie de

responsabilités particulière, celles des différents opérateurs qui interviennent en la matière, à savoir, les prestataires de service internet¹.

Le fonctionnement d'un réseau internet repose sur des professionnels qui mettent à disposition de leurs clients et des utilisateurs une infrastructure technique. En effet, ces personnes ont pu être reconnues comme étant responsables des contenus des sites qu'elles rendent accessibles sur le réseau internet, sur la base d'un devoir général de vigilance, de surveillance, de prudence, de diligence et d'information².

Le besoin s'est alors fait sentir de mettre en place un cadre juridique qui, détermine la responsabilité de ces prestataires de services internet des infractions commises sur le réseau internet (Sous-section1). Outre, les prestataires de service internet, d'autres acteurs sont susceptibles de voir leurs responsabilités engagées du fait de la transition digitale que connaît l'entreprise actuelle. (Sous-section 2).

Sous-section 1 : La responsabilité des prestataires de services Internet.

Les rapports d'échanges dans la société d'information ne peuvent se faire qu'en empruntant le réseau des réseaux. Or, un tel emprunt implique l'intervention de plusieurs opérateurs techniques appelés généralement prestataires des services Internet. En effet, personne ne peut diffuser ni accéder aux informations sur le réseau internet sans le concours de ces prestataires de services internet.

Selon l'article 65-3 de la loi 34-05 le prestataire des services internet est un prestataire ou un opérateur d'installations pour des services en ligne ou pour l'accès à des réseaux, y compris un prestataire de transmission, d'acheminement ou de connexion pour les communications numériques en ligne, sans modification du contenu, entre les points spécifiés par l'utilisateur de la matière, à son choix³. Les prestataires de services internet assurent donc à titre gratuit ou onéreux, le stockage direct et permanent pour mise à disposition du public de signaux, d'écrits, d'images de sens ou de messages de toute nature accessible par ces services. Cette définition, nous permet de rendre compte de la multiplicité des services fournis par les prestataires de service internet dont le rôle est essentiel pour le

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 377.

²Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, *Op.cit.*, p. 114.

³Article 65-3 de la loi 34-05.

fonctionnement de l'internet. Ces derniers se composent principalement des fournisseurs de services d'accès à internet et des fournisseurs de services d'hébergement.

Le fournisseur d'accès est un prestataire technique offrant à ses clients la possibilité de se connecter au réseau internet, en contrepartie d'un prix déterminé. Il n'assume aucune des fonctions qui sont celles d'un éditeur dans le domaine de la presse écrite, d'un producteur ou d'un diffuseur dans le domaine de la communication audiovisuelle. Les textes, les images, les informations circulent sur le réseau sans qu'il ait pris l'initiative de le publier ou de les programmer. L'émission des données et leur propagation lui sont étrangère ; en outre, le fournisseur d'accès n'entretient aucun rapport contractuel avec le fournisseur d'information¹.

Le fournisseur d'hébergement, lui, permet de mettre à la disposition des utilisateurs de l'internet un service leur permettant de publier des contenus sur le réseau. Plus précisément, l'hébergement consiste à conserver sur le disque dur du matériel informatique du prestataire des informations et à connecter les sites web à l'internet afin de les rendre accessibles aux internautes. Autrement dit, il met à la disposition des fournisseurs de contenus les moyens techniques leur permettant de les mettre à la disposition du public sur internet.

L'implication de ces prestataires suscite la question relative à la responsabilité de ces prestataires des services Internet lorsque, notamment, le contenu circulant sur le réseau auquel ils donnent accès comporte des éléments incriminés par la loi pénale ou occasionne un préjudice à autrui susceptible de donner lieu à réparation. Au Maroc, il n'existe pas un régime juridique général régissant la responsabilité de ces prestataires. Deux situations de responsabilité des prestataires des services Internet peuvent se présenter : la situation où le législateur marocain a prévu expressément, dans certains cas, un régime spécial de responsabilité réservé aux prestataires des services Internet (Paragraphe 1) et la situation où le droit marocain a préféré relever la responsabilité des prestataires des services Internet, en dehors des cas prévus par le régime spécial de responsabilité de ces prestataires, du régime général de responsabilité (Paragraphe 2).

Paragraphe 1 : Le régime spécial de la responsabilité des prestataires de services Internet.

En droit marocain, le seul texte particulier qui s'intéresse à la responsabilité des prestataires des services Internet demeure la loi n° 34-05 modifiant et complétant

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 379.

la loi n° 2-00 relative aux droits d'auteur et droits voisins. Mais cette loi n'a qu'une portée spéciale, dans la mesure où elle ne définit les conditions de la responsabilité des prestataires de services Internet qu'en matière de violation des droits d'auteur et des droits voisins. Elle institue un régime spécial de responsabilité des prestataires des services internet qui ne peut être étendu au-delà du champ des violations des droits d'auteur et des droits voisins qui lui est assigné, à défaut d'un texte de loi réalisant expressément cette extension¹.

Le prestataire de service n'est pas responsable du contenu des messages qui transitent par son intermédiaire. Il n'est responsable que de l'acheminement de l'information au client et non du contenu de celle-ci². Il engagerait sa responsabilité tant civile que pénale s'il a eu connaissance ou a eu des raisons valables d'être au courant de toute violation des droits d'auteur ou droits voisins commise par une autre personne qui aurait entraîné ou encouragé, causé ou contribué de manière substantielle à cette violation³.

Le prestataire des services internet peut bénéficier des limitations de responsabilité prévues par la loi n°34-05, sous certaines conditions, lesquelles, si elles sont toutes réunies, font obstacle à la mise en jeu de la responsabilité du prestataire⁴. Plusieurs conditions doivent être réunies pour éviter la responsabilité prévue par la loi n°34-05 en matière de violations des droits d'auteur ou droits voisins commises par l'entremise de systèmes ou de réseaux contrôlés ou exploités par un prestataire des services Internet ou en son nom⁵.

¹« A quel régime de responsabilité se trouvent soumis les prestataires des services internet ? », consulté le 13-05-2022 à 10h sur <https://bassamat-laraqui.com/a-quel-regime-de-responsabilite-se-trouvent-soumis-les-prestataires-des-services-internet/>

²Othman IHRAI, La propriété intellectuelle à l'ère de l'économie numérique, Thèse de doctorat en droit privé, Université Mohammed V- Souissi, Rabat, 2012, p. 273.

³Le prestataire de service sur Internet doit avoir commis en tant que prestataire de services Internet l'un des actes qui suivent :

-Entraîner, encourager, causer ou contribuer de manière substantielle à toute violation des droits d'auteur ou des droits voisins commise par une autre personne, après avoir été au courant ou avoir eu des raisons valables d'être au courant de cette violation. La responsabilité dans ce cas sera une responsabilité civile ;

-Entraîner, encourager, causer ou contribuer de manière substantielle et délibérée à toute violation des droits d'auteur ou droits voisins commise par une autre personne. La responsabilité sera, dans cette hypothèse, une responsabilité pénale.

-Avoir le droit de superviser ou de contrôler les violations des droits d'auteur ou droits voisins commises par une autre personne tout en détenant directement un intérêt financier dans l'activité illicite. La responsabilité sera une responsabilité civile.

-Superviser ou contrôler délibérément toute violation des droits d'auteur ou des droits voisins commise par une autre personne, et avoir directement un intérêt financier dans cette activité. La responsabilité sera, dans ce cas, une responsabilité pénale.

⁴ Article 65-10 de la loi 34-05.

⁵Le prestataire de services Internet ne doit avoir ni le contrôle, ni l'initiation, ni le pouvoir de direction des violations commises ;

-Il ne doit pas prendre l'initiative de la transmission de la matière et de la sélection de la matière ou de ses

En ce qui concerne les fournisseurs d'accès à l'internet, le législateur consacre le rôle purement technique de ces intervenants. Par conséquent, ils bénéficient d'un régime d'exonération de responsabilité du fait des contenus qui transitent par leur intermédiaire, à condition qu'ils ne soient pas à l'origine de la transmission et qu'ils ne modifient pas les informations faisant l'objet de la transmission. Comme pour les fournisseurs de services d'accès, les fournisseurs de services d'hébergement ne sont pas en principe responsables du contenu qu'ils hébergent et n'ont pas l'obligation de surveillance des contenus hébergés. La limitation de responsabilité dont ils bénéficient est toutefois moins large que celle des fournisseurs d'accès à internet¹.

Lorsque les limitations de la responsabilité bénéficient au prestataire, le tribunal pourra ordonner soit la résiliation des comptes précisés soit l'instauration des mesures raisonnables pour bloquer l'accès à un emplacement en ligne situé à l'étranger, lorsque le rôle du prestataire consiste uniquement dans la transmission ou l'acheminement de la matière ou la fourniture de connexions pour cette matière, sans modification de son contenu, ou dans le stockage intermédiaire et temporaire de ladite matière au cours de ces opérations. Soit ordonner l'enlèvement de la matière portant violation des droits d'auteur ou droits voisins ou la désactivation de son accès, la résiliation des comptes précisés, et toutes autres mesures que les tribunaux pourront estimer nécessaires, sous réserve que ces mesures soient les moins contraignantes pour le prestataire de services parmi les mesures présentant une efficacité analogue.

Toutes les mesures ordonnées par le tribunal doivent tenir compte de la contrainte relative imposée au prestataire de services et du dommage causé au titulaire des droits d'auteur ou des droits voisins, de la faisabilité technique et de l'efficacité de la mesure et envisager la disponibilité de méthodes d'exécution d'efficacité comparable mais moins lourdement contraignantes. Sauf pour les ordonnances assurant la conservation des preuves,

destinataires, sauf dans la mesure où le renvoi des utilisateurs ou l'établissement d'un lien à un emplacement en ligne au moyen d'outils de localisation d'information, y compris les liens hypertexte et les répertoires, comporte intrinsèquement une forme de sélection.

-Il doit prévoir et mettre en œuvre une procédure de résiliation, dans des conditions appropriées, des comptes des récidivistes en matière de violations des droits d'auteur ou droits voisins ;

-Il doit se conformer et s'abstenir d'interférer avec les mesures techniques standards de protection et d'identification de la matière protégée par le droit d'auteur ou les droits voisins, élaborées suite à un consensus entre les titulaires des droits d'auteur et des droits voisins et les prestataires de services. Ces mesures doivent être disponibles à des conditions raisonnables et non discriminatoires et ne doivent pas imposer des frais substantiels aux prestataires de services ou des contraintes substantielles pour leurs systèmes ou réseaux.

¹F. BENSEGHIR, « Responsabilité juridique des prestataires de services internet », consulté le 12-12-2021 à 9h sur <https://www.legavox.fr/blog/fouad-benseghir/responsabilite-juridique-prestataires-services-internet-22456.htm>.

ou celles qui n'ont pas d'effets négatifs majeurs sur l'exploitation du réseau de communications du prestataire des services, les mesures prévues ne sont disponibles que lorsque le prestataire des services aura été notifié dans les formes et conditions prévues par le code de procédure civile. Les limitations de la responsabilité des prestataires des services Internet consistent en leur exonération de toute responsabilité.

Paragraphe 2 : Le régime général de la responsabilité des prestataires de services Internet.

Lorsque la responsabilité d'un prestataire des services internet est évoquée, en dehors des cas de violation des droits d'auteur et des droits voisins, il n'y a pas lieu de faire application du régime spécial de la responsabilité des prestataires des services internet il y a lieu de se référer au régime général de responsabilité ; c'est-à-dire à ce qui est communément désigné le régime de responsabilité du droit commun, pour y puiser les solutions à appliquer. Ainsi, les prestataires des services internet sont obligés de par la loi d'intervenir pour empêcher l'accès aux contenus illicites ou préjudiciables. Sur cette base, si ayant été saisis par une autorité judiciaire les dits prestataires n'ont pas agi promptement pour empêcher l'accès à ce contenu, leur responsabilité sera évidemment engagée.

Cela signifie que les prestataires des services internet peuvent se trouver responsables civilement ou pénalement ou civilement et pénalement, même si leur rôle s'est limité à un rôle purement technique, si les différentes conditions des responsabilités civile et pénale sont remplies au sens du droit commun. Cependant, les prestataires aiment à qualifier leur prestation d'obligation de moyens. Ils revendiquent la nature technique de leur prestation et leur dépendance à l'égard de la technologie pour expliquer ce choix.

Il est vrai que la qualification d'obligation de résultat peut les inquiéter en cas de panne. Si cette dernière qualification est retenue seule l'exonération totale pour force majeure est possible, ou partielle pour faute du client. Toutefois, il n'est pas acquis qu'une prestation qui consiste à stocker des données et à les rendre accessibles sera qualifiée d'obligation de moyens. C'est une prestation technique, qui une fois la technologie à mettre en œuvre connue, ne devrait pas donner lieu à trop d'incertitudes. En effet, ce sont les prestations intellectuelles qui présentent un aléa qui sont généralement qualifiées d'obligation de moyens. Non seulement les prestataires qualifient leur obligation de moyens, mais encore ils la limitent très strictement. Réalisant une prestation technique, ils offrent un contrat d'adhésion qui laisse

peu de place à une éventuelle responsabilité du fait d'un manquement à leurs obligations. Ils vont souvent exiger de leur client qu'il prouve une faute à leur encontre¹.

C'est dire donc à quel point le régime général de responsabilité appliqué à la responsabilité des prestataires des services internet est sévère et inadapté. Sévérité et inadaptation ayant été, à l'origine de la conception au Maroc du régime spécial de responsabilité des prestataires des services internet en matière de violations des droits d'auteur et des droits voisins et de la mise en place à l'étranger d'un régime spécial de responsabilité dérogeant au régime de droit commun et dédié aux prestataires des services internet, quelles que soient l'origine et la nature de la cause de leur responsabilité en milieu cybernétique².

Sous-section 2 : La responsabilité des autres acteurs du numérique.

La transformation digitale de l'entreprise a permis l'intrusion de plusieurs acteurs dans l'utilisation de l'internet. En effet, au sein de l'entreprise, les salariés se trouvent obligés d'utiliser le numérique pour effectuer leur travail, ce qui pose le problème de la responsabilité en cas de dommage causés par ces-derniers. De plus, l'activité même de l'entreprise s'est digitalisée ce qui rend le professionnel cybercommerçant face à un défi de bonne exécution de ses obligations issues des contrats en ligne qu'il conclut. En outre, tout le système de digitalisation de l'entreprise ne peut se réaliser sans une protection efficace de ses données personnelles et celle des personnes dont elle est responsable. C'est pourquoi se pose la question de la responsabilité du responsable de traitement et du sous-traitant dans le cadre de l'exercice de leurs fonctions.

Nous allons procéder à l'étude de ces différentes responsabilités comme suit. D'abord, la responsabilité du professionnel commerçant en ligne (Paragraphe 1). Ensuite, la responsabilité de l'employeur du fait de l'usage d'internet par ses salariés (Paragraphe 2). Enfin, la responsabilité du responsable de traitement et du sous-traitant (Paragraphe 3).

¹J-A. BENARERAF, « Qualification et responsabilité des sites contributifs », in IP/IT, N° 4, Avril 2016, Dalloz, p. 174.

²« A quel régime de responsabilité se trouvent soumis les prestataires des services internet ? », consulté le 11-12-2021 à 12h sur <https://jurismaroc.vraiforum.com/t728-A-quel-regime-de-responsabilite-se-trouvent-soumis-les-prestataires-des-services-Internet.htm>

Paragraphe 1 : La responsabilité du professionnel commerçant en ligne.

Dès la conclusion du contrat conclu à distance, le fournisseur est tenu d'exécuter les obligations résultant de ce contrat. Ainsi pour éviter que sa responsabilité soit mise en cause, il doit respecter les obligations précitées, à défaut de sanctions¹. Il engage sa responsabilité même dans le cas où ces obligations sont effectuées par un prestataire de service. C'est ce qui est prévu par l'alinéa 2 de l'article 26 de la loi 31-08 qui prévoit une responsabilité de plein droit du cybercommerçant. Ainsi, le professionnel est responsable de plein droit à l'égard du consommateur de la bonne exécution des obligations, que ces obligations soient à exécuter par le professionnel lui-même ou par un tiers qu'il se substitue.

Le dernier alinéa de l'article 26 prévoit trois possibilités d'exonération de la responsabilité du cybercommerçant ; le cas notamment lorsque ce dernier arrive à apporter la preuve que l'inexécution ou la mauvaise exécution est imputable au consommateur, ou à un fait imprévisible et insurmontable d'un tiers au contrat, ou encore en cas de force majeure. Donc, l'exonération totale ou partielle pourrait venir d'un cas de force majeure, de la faute du consommateur ou du fait d'un tiers. Le professionnel ne peut donc pas écarter sa responsabilité en démontrant son absence de faute. Ces dispositions ont été adoptées afin de donner confiance au consommateur qui doit entièrement se fier au professionnel bien qu'il n'y ait pas de contact physique.

Le professionnel est responsable de l'ensemble de la chaîne contractuelle qui part de la conclusion du contrat jusqu'à la livraison du bien ou l'exécution du service. Seul le consommateur ayant conclu un contrat à distance peut bénéficier de cette disposition. Il n'y a pas lieu ici de s'interroger sur la nature du contrat conclu, il peut s'agir aussi bien d'une vente que d'un contrat d'entreprise. Le professionnel est celui qui propose ou offre ses biens ou services à distance dans les conditions définies par la loi 31-08². De surcroît, le tiers substitué au professionnel contractant direct du consommateur est celui qui exécute une partie de la prestation : manutentionnaire, transporteur, sous-traitant... le professionnel doit donc

¹ « Les obligations du cyber commerçant à la lumière des dispositions de la loi 31-08 édictant les mesures de protection des consommateurs », consulté le 11-05-2022 à 15h sur <https://bassamat-laraoui.com/les-obligations-du-cyber-commerçant-a-la-lumière-des-dispositions-de-la-loi-31-08-edictant-les-mesures-de-protection-des-consommateurs/>

² خليل زكرياء، المسؤولية المدنية للبائع المهني وتطبيقاتها على عقد البيع الإلكتروني، رسالة لنيل الدكتوراه في القانون الخاص، جامعة القاضي عياض، كلية العلوم القانونية والاقتصادية والاجتماعية، مراكش، السنة الجامعية 2012-2013، ص. 131.

répondre de tout tiers qui participe à l'exécution de la prestation ; il pèse sur lui une obligation de résultat.

La responsabilité de plein droit qui s'illustre par la responsabilité générale du fait des choses, ne permet à l'auteur du dommage de s'exonérer qu'en démontrant la force majeure¹ ou la faute de la victime. La responsabilité de plein droit instaurée par le législateur à la charge du professionnel exerçant son activité par voie électronique revient donc à faire peser du ce dernier une obligation de résultat. Le débiteur d'une obligation de résultat est placé dans la même situation que le gardien d'une chose², dès lors que le résultat prévu au contrat n'est pas atteint, il est responsable directement. Il n'est pas nécessaire pour le créancier de l'obligation de prouver une faute, il appartient au débiteur de prouver la force majeure ou la faute du cocontractant pour s'exonérer³. En effet, il appartient au vendeur de faire délivrer la chose convenue dans la quantité et qualité prévue et à la date précisée, sans qu'il puisse être soutenu que ce sont des obligations de moyens.

Il faut noter qu'il est prohibée d'insérer des clauses limitatives ou exonératoires de responsabilité dans le contrat conclus à distance. En effet, le professionnel qui exerce son activité par internet doit donc s'attendre à supporter une obligation de bonne fin dans l'exécution du contrat conclu avec le consommateur. Toutefois, cette obligation ne saurait s'étendre au-delà de la stricte exécution du contrat. En cas de produit présentant un défaut de sécurité, le consommateur victime dispose du choix entre le régime restrictif de la responsabilité du fait des produits défectueux ou du régime de la responsabilité pour faute. Le régime de la responsabilité de plein droit présente donc le mérite de concentrer sur le professionnel la responsabilité de l'exécution pleine et entière du contrat sans pour autant lui imposer une garantie du produit lui-même.

Paragraphe 2 : La responsabilité de l'employeur du fait de l'usage d'Internet par ses salariés.

L'entreprise peut voir sa responsabilité civile recherchée suite à une utilisation illicite ou fautive d'internet sur le lieu de travail. Civilement, l'employeur est responsable en tant que

¹Qui comprend le fait d'un tiers imprévisible, irrésistible et cause exclusive du dommage.

²Le gardien de la chose à l'origine du dommage ne peut s'exonérer qu'en démontrant la force majeure ou la faute de la victime.

³Luc GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, *Op.cit.*, p. 19.

commettant de ses salariés, des fautes commises par ceux-ci dans leur utilisation d'internet pendant le temps de travail. La responsabilité de l'employeur du fait de l'usage d'internet par ses salariés s'inscrit dans le cadre de la responsabilité délictuelle reconnue par le D.O.C à l'employeur. En effet, l'employeur se trouve être responsable des actes de ses employés.

En droit marocain, l'employeur est de plein droit responsable de l'activité de ses salariés. En effet, aux termes de l'article 85 du D.O.C : « on est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde » De plus, aux termes du même article : « les maîtres et les commettants ...sont responsables... du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ». Il s'agit là d'une responsabilité dite de plein droit, ce qui signifie qu'aucune faute personnelle de l'employeur n'est exigée pour que sa responsabilité soit engagée au regard de l'activité de ses salariés¹.

La solution pourrait paraître sévère pour l'employeur si ce dernier ne pouvait s'exonérer de sa responsabilité en invoquant l'abus de fonction de son employé. Ainsi, sa responsabilité est toutefois conditionnée et n'exclue pas la totale responsabilité du salarié. L'employeur ne peut être exonéré de ce genre de responsabilité qu'à trois conditions : que le salarié ait agi hors des fonctions pour lesquelles il était employé, que le salarié ait agi sans autorisation et enfin que le salarié ait agi à des fins étrangères à ses attributions. Dans ce cas précis, le salarié sera seul responsable de ses actes dommageables sans que son employeur n'ait alors à en assumer la responsabilité. Les deuxième et troisième conditions sont aisées à mettre en œuvre. La première condition est plus délicate à apprécier. Ainsi, par principe, l'employeur est responsable des faits fautifs de ses salariés et c'est seulement par exception, si les conditions précitées sont remplies, que l'employeur se verra exonéré de sa responsabilité².

La mise en cause d'un employeur par le biais des activités internet de ses salariés, même à des fins privées, est donc tout à fait envisageable³, comme le prouve un arrêt de

¹« La responsabilité de l'employeur de fait de l'usage des mails par ses salariés », consulté le 11-05-2022 à 10h sur https://www.murielle-cahen.com/publications/p_responsabilite2.asp

²V. SEDALLIAN, « La responsabilité de l'employeur en tant que fournisseur d'accès à internet », in LEGICOM, N° 27, Février 2002, p. 48.

³D. BOUGEROL, « L'utilisation d'internet par les salariés : quels risques pour les employeurs ? », 23 Avril 2013, consulté le 11-05-2022 à 10h sur <https://business.lesechos.fr/entrepreneurs/ressources-humaines/dossier/10028444/tpepme-00010028444-1-l-utilisation-d-internet-par-les-salaries-quels-risques->

la Cour d'appel d'Aix-en-Provence du 13 mars 2006¹. Dans cette affaire, l'employé d'une entreprise de nouvelles technologies avait élaboré et mis en ligne, depuis son lieu de travail, un site internet particulièrement virulent à l'égard d'une grande société d'autoroutes. De nombreuses expressions employées furent rapportées comme outrageantes à l'égard des employés et même des clients de ladite société, qui ne tarda donc pas à porter plainte. Ainsi donc, le salarié fût condamné sur différents fondements au regard de son activité délictuelle et dommageable (contrefaçon ...). Mais, fait d'une importance toute particulière, son employeur le fût également sur la base de l'article 1242 alinéa 1 du Code civil français. Pour la première fois, la responsabilité d'un employeur fût engagée du fait de l'activité de l'un de ses salariés sur internet.

Cette jurisprudence peut sembler très risquée pour l'employeur dont la responsabilité risque de se trouver fréquemment engagée du fait de l'activité de ses salariés sur internet. En effet, il est très facile aujourd'hui de publier au moyen des réseaux sociaux différentes photos ou textes sur n'importe quel sujet. Or, tous les pièges juridiques sont alors envisageables pour l'employé ; de la diffamation en passant par la contrefaçon, même parfois involontaire, jusqu'au viol manifeste de l'intimité de la vie privée. Les dérapages sont d'autant plus rapides et facilités que la mise à disposition au public internaute est instantanée et aujourd'hui techniquement aisée.

Il semble donc qu'il sera nécessaire pour les employeurs de se prémunir contre cet engagement de leur responsabilité et, si cette jurisprudence est maintenue dans d'autres cas d'espèce futurs, et ceci par exemple par un refus d'utilisation d'internet (inscrit au règlement intérieur) pour des utilisations autres que celles en rapport direct avec l'activité du salarié. Dans ce cas, en cas de dommage causé par l'employé lors de son utilisation d'internet, l'employeur se trouverait couvert, car l'agissement délictuel serait alors perpétré en l'absence totale de son autorisation et qui plus est en violation d'une obligation du règlement intérieur.

Néanmoins, Cette situation ne semble pourtant peut être pas souhaitable pour deux raisons principales. D'une part, l'esprit ayant présidé à l'élaboration de l'article 1242, alinéa 1 du Code civil français ainsi que l'article 88 du D.O.C est inscrit dans un souci de protection de la victime qui trouvera bien entendu une bien meilleure indemnisation dans les mains d'un

¹C. Appel, 2^{ème} ch. Civile, décision n° 03/15440, 13 Mars 2006, Aix-en-Provence.

employeur que dans les mains de son employé. L'ébauche de jurisprudence développée sur la responsabilité de l'employeur du fait de l'activité de ses salariés sur internet répond à une telle logique. Ce serait peut être fragilisé les victimes que de trop facilement déresponsabiliser l'employeur au regard de l'activité de ses salariés. D'autre part, il paraîtrait à l'époque actuelle particulièrement liberticide que d'empêcher un salarié de se connecter à internet lors d'une utilisation n'entravant en rien son travail et en accord avec les bonnes mœurs. Une telle mesure serait très difficile à faire accepter dans le monde de l'entreprise actuel. De plus, elle ne semble en tout état de cause pas nécessaire au regard du seul arrêt ayant été rendu à ce sujet.

Paragraphe 3 : La responsabilité civile du responsable du traitement et du sous-traitant.

La question de la responsabilité est loin d'être un effet secondaire de la réglementation. Néanmoins, la loi 09-08 ne déclare qu'implicitement la responsabilité pesant sur le responsable du traitement et du sous-traitant contrairement au RGPD. En effet, l'article 82 du RGPD définit le mécanisme de responsabilité du responsable du traitement comme suit : « Tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du présent règlement ».

Le régime prévu par le RGPD implique un préjudice résultant d'une violation du règlement et impose une obligation de dédommager la personne préjudiciée. Deux types de protagonistes peuvent être tenus de réparer ce dommage : le responsable du traitement et le sous-traitant. Pour le responsable du traitement, l'article 82 du RGPD impose à ce-dernier une obligation de pouvoir démontrer qu'il se conforme à la réglementation. Il demeure qu'en cas de manquement aux obligations, la responsabilité du responsable du traitement pourra être engagée. Il s'agit d'assumer les conséquences du non-respect de ces obligations¹.

Quant à la loi 09-08, elle prévoit dans son article 61 que tout responsable de traitement est responsable pénalement lorsque dans le cadre de l'exercice de ses fonctions cause ou facilite l'usage abusif ou frauduleux des données traitées ou reçues ou les communique à des tiers non habilités. Pour ce qui concerne un sous-traitant, celui-ci n'est tenu, vis-à-vis d'une personne préjudiciée, pour responsable du dommage causé par le traitement que s'il n'a pas respecté les obligations qui incombent spécifiquement aux sous-traitants en vertu de

¹Karen ROSIER et Antoine DELFORGE, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » in Le règlement général sur la protection des données Analyse approfondie, Ouvrage collectif sous la direction de Cécile de TERWANGNE et Karen ROSIER, Larcier, Paris, 2018, p. 665.

la loi 09-08 ou qu'il a agi en dehors des instructions licites du responsable du traitement ou contrairement à celles. En effet, il découle de l'article 58 de la loi 09-08 qu'en cas de non-respect du sous-traitant des obligations souscrites dans le cadre du contrat qui le lie au responsable de traitement, sa responsabilité pourra être engagée pénalement. En outre, il pourra être tenu responsable envers une entreprise des dommages qui seraient causés par suite d'un manquement aux obligations résultant du présent contrat, ainsi qu'au versement de réparations du préjudice subi¹.

Par ailleurs, le RGPD a institué un principe de responsabilité solidaire entre les responsables de traitements et les sous-traitants intervenant dans le même traitement². Si les conditions sont réunies pour considérer qu'il y a responsabilité de plusieurs responsables de traitement ou sous-traitants qui participent à un même traitement, chacun peut être tenu, vis-à-vis de la personne préjudiciée, de réparer le tout, à charge pour lui de récupérer les sommes versées auprès des autres intervenants. Le plus exposé est donc le plus solvable et non celui qui a pris la plus grande part dans le traitement³. Quant aux conditions de cette solidarité, elle naît entre les personnes dont la responsabilité peut être chacun engagée sans qu'une cause d'exonération ne puisse être invoquée.

Si l'on prend le cas de plusieurs responsables de traitement, le texte du RGPD induit une responsabilité solidaire dès lors que plusieurs responsables participent au même traitement. De ce fait, chaque responsable a une obligation à la dette pour la totalité du dommage. Pour ce qui est de la répartition entre eux, le RGPD prévoit que « lorsqu'un responsable du traitement ou un sous-traitant a [...] réparé totalement le dommage subi, il est en droit de réclamer auprès des autres responsables du traitement ou sous-traitants ayant participé au même traitement la part de la réparation correspondant à leur part de responsabilité dans le dommage, conformément aux conditions fixées au paragraphe 2 »⁴. Ce texte concerne les rapports entre le responsable du traitement et le sous-traitant,

¹« Exemple de clause d'obligation de sécurité », consulté le 12-05-2022 à 16h sur <https://www.cndp.ma/fr/responsabilites/mentions-types/sous-traitance.html>

²L'article 82, § 4, du RGPD prévoit que « Lorsque plusieurs responsables du traitement ou sous-traitants ou lorsque, à la fois, un responsable du traitement et un sous-traitant participent au même traitement et, lorsque, au titre des paragraphes 2 et 3, ils sont responsables d'un dommage causé par le traitement, chacun des responsables du traitement ou des sous-traitants est tenu responsable du dommage dans sa totalité afin de garantir à la personne concernée une réparation effective ».

³T. DOUVILLE, « Le contrat en matière de responsabilité conjointe de traitement de données », in IP/IT, N° 4, Avril 2021, Dalloz, pp. 188-189.

⁴V. Parag. 5 de l'art. 82 du RGPD.

en envisageant la possibilité d'une action récursoire. Le contrat conclu entre le responsable du traitement et le sous-traitant pourra aménager les conditions de cette action récursoire¹.

En outre, un responsable de traitement ou un sous-traitant peut s'exonérer de sa responsabilité, s'il prouve que le fait qui a provoqué le dommage ne lui ait nullement imputable. Ainsi, la responsabilité du responsable du traitement ou du sous-traitant nécessite l'imputabilité personnelle d'un fait ayant provoqué le dommage. Il suffit donc que le fait qui a provoqué le dommage ne leur soit pas imputable. De ce fait, il pèse sur chacun d'eux, responsable de traitement ou sous-traitant, une obligation de prouver l'absence d'imputabilité personnelle du fait ayant provoqué le dommage. D'où l'importance du contrat conclu entre le responsable du traitement et du sous-traitant.

Enfin, le régime de responsabilité sous l'angle de la responsabilité civile demeure un régime de responsabilité objective alors même que la plupart des obligations qui sont mises à la charge des responsables de traitement et des sous-traitants sont des obligations de moyens. Raison pour laquelle, Il est fait appel à renforcer le régime de la responsabilité de la loi 09-08 dans l'optique de permettre aux personnes qui subissent un préjudice du fait du non respect de la réglementation sur la protection des données personnelles d'obtenir réparation tout en encadrant sommairement la répartition du dédommagement en cas de pluralité de débiteurs.

Section 2 : La construction d'une responsabilité numérique.

Alors même que le développement exponentiel du numérique impacte substantiellement l'ensemble des activités humaines, la thématique de la responsabilité numérique constitue une problématique juridique majeurs. En effet, une responsabilité numérique est entrain d'émerger, et dont on voit de dessiner les contours, comme l'illustre l'apparition du concept de responsabilité numérique de l'entreprise, qui repose sur le postulat selon lequel les organisations à la pointe de la transition numérique ont la responsabilité de nous mener à un futur meilleurs. D'un point de vue juridique, la responsabilité numérique viserait à envisager la responsabilité du fait de comportements dommageables propres au monde numérique, tels les discours en ligne, la réparation de dommages d'un nouveau genre,

¹« La responsabilité du responsable de traitement et du sous-traitant », consulté le 12-05-2022 à 10h sur <https://www.lettredesreseaux.com/P-2559-454-A1-l-article-82-du-rgpd-relatif-a-la-responsabilite-du-responsable-de-traitement-et-du-sous-traitant.html>

comme la violation de données personnelles. L'on verrait, en outre, apparaître de nouveaux responsables, comme les grandes plateformes ou les robots¹.

Malgré toute l'attraction de la notion de responsabilité numérique, il reste cependant difficile d'identifier, à ce stade, une réelle unité dans les questions de responsabilité suscitées par la transition numérique. Si l'on pourrait supposer que ces questions se structurent autour des enjeux relatifs aux données, il apparaît toutefois, à l'examen, que les problématiques sont diverses. Elles impliquent des supports technologiques variés qui vont de la simple numérisation aux techniques d'apprentissage automatique, en passant par les *blockchains*. Elles concernent, en outre différents responsables, qu'il s'agisse des utilisateurs des réseaux sociaux, des opérateurs de plateformes ou des machines autonomes. Elles conduisent, enfin, à des fondements qui varient selon les technologies envisagées et l'activité des responsables potentiels².

Dès lors, le changement de paradigme de toutes les formes d'activités humaines, dans un délai extrêmement rapide, pose le défi de la construction d'une responsabilité numérique (Sous-section 1). Cependant, si l'on ne peut que convenir que la transition numérique conduit à des questions de responsabilité inédites, il paraît difficile de parler d'une seule responsabilité numérique plutôt que des responsabilités éclatées, propres à des situations spécifiques et donc l'émergence de nouvelles formes de responsabilités numériques. (Sous-section 2).

Sous-section 1 : Le défi de la responsabilité numérique du XXI^{ème} siècle.

Après le positivisme³ juridique et le jusnaturalisme⁴, il faut désormais compter avec le numérisme juridique. La société numérique et algorithmique du XXI^{ème} siècle est une société ultra libérale ou la froideur de la raison algorithmique l'emporte sur la sagesse de la raison humaine. L'algorithme n'est pas neutre il encourage la morale des forts. La gouvernance par les nombres domine notre société. La normalisation et la standardisation l'emporte. Le critère

¹Ch. BYK, « Présentation des enjeux de la responsabilité numérique », in IP/IT, N° 3, Mars 2020, Dalloz, p. 151.

²Ibid., p. 152.

³Le positivisme juridique est une certaine approche du droit selon laquelle le droit n'est pas lui-même une science, mais peut être l'objet d'une science qui se donne pour tâche de le connaître et de le décrire. Le positivisme juridique est alors une tentative pour construire une telle science.

⁴Doctrines qui défendent la notion de droit naturel. Selon le jusnaturalisme il y a des normes naturelles aux individus, et que ces normes sont au-dessus du droit en vigueur.

quantitatif domine tellement le monde qu'il devient un critère qualitatif. L'emprise des nouvelles technologies est un sujet très vaste.

Dans ce contexte, les fonctions du droit de la responsabilité mises à l'épreuve du numérisme juridique constitue un mouvement qui va entraîner une disparition des fonctions traditionnelles de la responsabilité civile pour laisser la place à une nouvelle responsabilité dite numérique. De ce fait, le défi d'une construction d'une responsabilité juridique numérique originale, conjuguée à la révolution des mathématiques, des technosciences, des biotechniques s'est vite déployée (Paragraphe 1). Cependant, par ses fonctions indemnitaire et normative, le droit de la responsabilité civile se veut humain, raison pour laquelle la responsabilité numérique risque de porter atteinte à la personne et présenter donc un risque de déshumanisation (Paragraphe 2).

Paragraphe 1 : La construction d'une responsabilité numérique originale.

A l'aube d'une ère de développement des robots, d'algorithmes et diverses formes ou divers stades d'intelligence artificielle, la question de l'encadrement juridique de ces nouvelles technologies fait l'objet de vifs débats¹. En effet, l'exploitation considérable des données de toutes natures, personnelles, entrepreneuriales, publiques, de masse, par l'émergence continue de techniques nouvelles, associées à l'intelligence artificielles, telle que la *machine learning*, le *deep learning*, la *blockchain*, l'ordinateurs quantique offre des potentialités inédites, multiples, variées et illimitées. La numérisation des données concerne tout ou presque tout ce que réalise la personne morale, qu'il s'agisse de son identification, de ses activités, de sa disparition. Tout devient donnée numérique, stockage numérique, exploitation numérique, responsabilité numérique.

Il n'est pas certains que les règles classiques puissent suffire pour répondre aux bouleversements engendrés par l'activité numérique contemporaine et ceci pour plusieurs raisons. La première tient à ce que les nouveaux acteurs, à l'origine de cette révolution sont incontournables. Les GAFAMI et les BATX disposent d'outils majeurs indispensables impactant l'ensemble des activités humaines. La seconde tient au déploiement d'une variété d'acteurs pour une même activité, ce qui renvoie à une cascade d'actions désormais enregistrées, tracées, identifiées directement à l'aide des techniques numériques, ce qui

¹B. BESSERMANN, « Les enjeux du développement de la responsabilité numérique pour les assureurs », in IP/IT, N° 3, Mars 2020, Dalloz, p. 170.

permet de déterminer l'intervention individuelle de chacun à l'image des géants du numériques enregistrant, analysant et contrôlant tout. Par exemple, les actions de chaque personne, physique ou morale, n'ont plus de secret pour *Google*, filiale de la société *Alphabet*, enregistrant une multitudes de données, d'actions, de décisions autant par le biais de son moteur de recherche *Google* que divers outils, logiciels, services¹ tels que *Google Map* permettant de localiser chacune des actions de la personne y recourant. La dernière raison tient à la présence de plus en plus importante des robots numérisés et d'applications associées se substituant à de nombreuses activités humaines, au risque d'une certaine déshumanisation.

De ce fait, toute l'originalité de la responsabilité numérique tient à ce que, progressivement, compte tenu des bouleversements générés par la technique du numérique, les règles classiques de la responsabilité, encore applicables pendant cette période intermédiaire de mise en place, risquent peu à peu d'être substituées par une responsabilité numérique originale. Incontestablement, les règles classiques de la responsabilité civile ont toujours pu répondre aux besoins évolutifs de la société. Toutefois, les bouleversements générés par le numérique dans les activités humaines sont tels qu'il n'est pas certains qu'elles restent opérationnelles. Elles pourraient progressivement être remises en cause, voire tomber en désuétude.

En effet, impactant l'ensemble des actions humaines, que ce soit en termes d'activités (robotique, télétravail, télé-expertise, justice prédictive), de communication (nouveaux moyens générés par la 5G, ordinateurs quantiques), de moyens de communications, de transports (voitures, avions autonomes) de fabrication (nanotechnologies, imprimantes 3D/4D), de cadre de vie (maisons connectées , domotique), le droit classique de la responsabilité est appelé progressivement à répondre, dans les années à venir, à ces différents changements. Il en est ainsi, par exemple dans les domaines de la protection de la propriété intellectuelle (logiciels, applications), de la perte ou de la destruction des données, des pannes informatiques paralysant les grandes entreprises, de la cybercriminalité, donnant lieu à différentes actions en matière de responsabilité civile, pénale, administrative compte tenu de l'accroissement sans précédent de dommages numériques de toutes natures².

¹Google Analytics récolte différents éléments statistiques sur l'utilisateur pour leur exploitation publicitaire. Aussi Google Play recense les achats de diverses applications, abonnements à des films, musiques, livres, appareils numériques, permettant de mieux connaître le consommateur.

²B. BEVIÈRE-BOYER, « Responsabilité numérique : le défi d'une responsabilité spécifique « humanisée » », in IP/IT, N° 3, Mars 2020, Dalloz, p. 159.

L'application même des règles classiques est susceptible d'évoluer. Par exemple en matière probatoire, les nouveaux moyens tel que la *blockchain* constitue une véritable révolution en ce qu'elles permettent d'opérer des traçabilités numériques de toutes les activités menées par les parties, ce qui bouleverse notablement la démonstration de la preuve, l'appréciation même de celles-ci par les juges, la répartition des responsabilités en cas d'activités interdépendantes menant à l'action dommageables, etc.

La transformation de la responsabilité générée par la révolution numérique a ainsi pour effet de répondre à de nouveaux besoins en construction ou de plus en plus d'activités humaines sont substituées par des machines numérisées, programmées, alimentées par les outils de l'intelligence artificielle. Toutefois, un tel changement de paradigme ne doit pas, par sa déshumanisation, porter atteinte à la personne en ce que la technicité, si objective et précise soit-elle, peut devenir inhumaine. Ceci mène au nouveau défi de l'humanisation de la responsabilité numérique.

Paragraphe 2 : Le risque de déshumanisation de la responsabilité numérique.

L'évolution de la responsabilité numérique, a pour effet de répondre aux besoins immédiats éminemment techniques au détriment d'une approche humaine. La responsabilité numérique, pour asseoir sa légitimité, doit indiscutablement s'humaniser. Le risque majeur qui se dessine lors de la mise en place contemporaine de la responsabilité numérique est sa déshumanisation. En effet, par essence, la responsabilité numérique est associée à l'utilisation de technique de plus en plus sophistiquées ne permettant pas de répondre à la finalité première de toute action juridique quelle qu'elle soit ; organiser les relations des humains.

Ce glissement s'explique par le fait que de nombreuses actions humaines sont remplacées par des machines, des robots, des applications, ce qui justifie certes l'évolution des règles de responsabilités, mais ne doit pas faire oublier qu'il convient toujours de mettre en avant l'intérêt de l'humain, finalité première et originelle de toute forme de responsabilité de quelque nature que ce soit.

La déshumanisation complète le phénomène de désindividualisation. Spécialement, certains éléments fondamentaux du droit de la responsabilité perdraient en coloration morale pour être réduits à des critères purement quantitatifs¹. Normalisation, standardisation,

¹M. MEKKI, « Les fonctions de la responsabilité civile à l'épreuve du numérique : l'exemple des logiciels prédictifs », in IP/IT, N° 12, Décembre 2022, Dalloz, p. 677.

quantification sont les maîtres mots d'un droit de la responsabilité civile algorithmique à l'excès. Par conséquent, tout recours à l'intelligence artificielle, et aux techniques qui y sont associées, doit être accompagné d'une garantie humaine¹. Cette garantie devrait s'étendre à l'ensemble des activités numériques. Outre l'indispensable respect du principe originel de garantie humaine, la responsabilité sociétale devrait aussi être mise en exergue au profit d'une responsabilité numérique humanisée. En effet, la digitalisation des activités numériques et, en parallèle, le développement d'une responsabilité numérique automatique déshumanisée posent d'importants questionnements éthiques qui ne cesseront de s'accroître au fil du développement des nouvelles techniques liées à l'intelligence artificielle².

Le numérique s'immisce dans l'ensemble des actions humaines, y compris les plus élémentaires. Le système judiciaire lui-même est fortement impacté par le numérique³, risquant de produire une justice implacable, inhumaine et potentiellement injuste, et ce, même si les statistiques, les études, avec l'aide des outils numériques, affirment offrir des résultats objectifs et précis. Le droit ne peut pas répondre de manière proactive à toutes les évolutions très rapides des technologies. Pour y parvenir face à ses nouveaux enjeux, l'une des solutions serait d'adopter une démarche éthique dans l'utilisation de ces technologies. En effet, il faut laisser place à l'innovation sans la contraindre par des règles juridiques. En revanche, il apparaît essentiel d'avoir une position éthique dans l'adoption de celles-ci.

Il convient, par conséquent, de réagir par une responsabilité sociétale élargie, en laissant une plus grande place à la réflexion éthique en aval des travaux parlementaires, mais aussi plus globale qui se fasse à différents niveaux : par des rencontres des citoyens et au sein des établissements scolaires et universitaires, au sein des entreprises notamment les *start up*, mais aussi dans les institutions publiques qu'elles soient judiciaires, fiscales, sociales, ou autres. Devraient aussi être institués divers comités d'éthiques au sein des entreprises, organismes, institutions afin d'inciter à une réflexion collective sur les enjeux et les finalités

¹Jean-Gabriel GANASCIA, *Intelligence artificielle vers une domination programmée ?*, Le Cavalier bleu, 2^{ème} éd., 2017, p. 199.

²G. SHI et T. ZHANG, « Comments on Chinese civil subject qualification of artificial intelligence », in *IP/IT*, N° 12, Décembre 2020, Dalloz, p. 658.

³La justice prédictive est une notion récente évoquée par une partie de la presse, et par une partie des professionnels du Droit qui partent de la constatation que toute décision judiciaire comporte sa part d'aléa. Le calcul portant sur la fréquence des décisions rendues par les tribunaux devrait permettre de dégager des algorithmes mesurant les risques courus dans l'engagement d'une procédure ou d'un arbitrage. Le fait de quantifier le risque juridique permettrait de désengorger les juridictions et un traitement de masse des dossiers libérant les professionnels de la réalisation de tâches bien trop souvent répétitives.

du numérique et, le cas échéant, sur les responsabilités numériques afférentes. La responsabilité sociétale des entreprises déjà, mise en place constitue une première étape.

La responsabilité sociétale invite à réfléchir et à agir à l'égard du développement durable en lien avec le numérique, à la responsabilité environnementale numérique en plein déploiement compte tenu notamment de la consommation d'énergie développée dans le cadre du numérique ou encore les déchets numériques qui ne vont, cesser de croître dans les années à venir, ce qui est là aussi un nouveau type de responsabilité numérique. Elle devrait donc être amenée à s'élargir à l'ensemble des acteurs de la société dans toutes les activités. Cette condition est majeure pour la légitimité de toutes les actions numériques en développement et les responsabilités juridiques numériques qui y sont associées.

Toute la question est de savoir s'il convient de s'en tenir aux outils juridiques classiques ou d'imaginer de nouvelles formes de responsabilités compte tenu de la révolution numérique qui bouleverse tous les champs de la société du XIX^{ème} siècle. Est envisagé le passage d'une responsabilité juridique classique à une responsabilité numérique spécifique, avec le développement progressif de nouvelles formes de responsabilités numériques. Le défi se trouve tout particulièrement dans celui d'une responsabilité spécifique humanisée tenant compte du principe de garantie humaine, assorti d'une responsabilité sociétale élargie.

Sous-section 2: Les nouvelles formes de responsabilité numérique.

Les transformations numériques sont telles qu'elles sont susceptibles d'impacter directement le droit classique de la responsabilité. Ainsi, il demeure indispensable, à moyenne et longue échéance de réfléchir sur de futurs mécanismes de responsabilité répondant aux nouvelles techniques du numérique. Nous assistons à un déploiement potentiel et exponentiel de la responsabilité numérique dans la plupart des activités menées par les Etats, les entreprises et les particuliers et ceci sous l'influence grandissante des GAFAMI.

Par ailleurs, dans le monde de l'intelligence artificielle, le développement rapide des machines intelligentes ne sera pas sans effet en matière de transformations des règles de responsabilités¹. Il en sera ainsi, tout d'abord, de la responsabilité des différents acteurs tels que les fabricants, contribuant à la conception, directement impactés par le numérique et

¹J. SENECHAL, « Responsabilité Ab initio, Régulation Ex ante et responsabilités A Posteriori : le cœur des débats européens sur les systèmes d'intelligence artificielle, hors et dans le secteur du commerce électronique », in IP/IT, N° 12, Décembre 2020, Dalloz, p. 668.

l'analyse direct des données par les différents outils de l'intelligence artificielle. Ce nouveau paradigme, qui tend à s'accélérer, sera susceptible de transformer, de bouleverser, voire même remettre en cause les règles classiques au profit d'autres règles plus adaptées. Certes, les responsabilités du fait des choses, du fait des produits défectueux pourront encore être invoquées, au moins pour une période transitoire, mais reste à savoir si elles permettront elles seules, sur le plus long terme, à assurer un équilibre juridique satisfaisant, ne serait que d'un point de vue probatoire ou la victime, de par sa qualité de demandeur, connaître des difficultés majeures d'accessibilité aux différentes techniques numériques en vue de démontrer leur causalité avec ses dommages.

L'hypothèse émergente d'une intelligence artificielle responsable ou encore de la responsabilité juridique des machines intelligente mérite une attention (Paragraphe 1). Cette attention devra se faire à l'échelle internationale et non plus aux niveaux national en raison de l'internationalisation des acteurs du numérique essentiellement les plateformes numériques (Paragraphe 2).

Paragraphe 1 : La responsabilité de l'intelligence artificielle.

Définir l'intelligence artificielle n'est pas simple. Peut-être parce qu'il s'agit d'une notion relativement nouvelle, aucune définition ne s'est encore imposée. Nous la définirons, pour les besoins de cette analyse, comme la faculté qu'ont certaines machines (appelées couramment des robots, mais ce terme est très imprécis) d'utiliser des processus cognitifs comparables à ceux des être humains, ce qui leur confère une aptitude à agir de façon autonome de telle sorte qu'elles sont capables d'accomplir des tâches qui jusqu'ici semblaient réservées aux êtres humains¹.

L'appréhension de l'intelligence artificielle par le droit soulève de nombreuses interrogations. Le droit a été pensé par et pour les être humains ; comment pourra-t-il s'appliquer à des machines imitant l'intelligence humaine ? Les difficultés concernent toutes les branches du droit et notamment le droit de la responsabilité civile, auquel il sera fait appel pour assurer la réparation des dommages provoqués par l'utilisation d'une intelligence artificielle. La perspective de voir apparaître dans le futur des machines de plus en plus intelligentes et susceptibles de causer des dommages par leur action autonome conduit à s'interroger sur les responsables potentiels. Ils sont nombreux ; il peut s'agir de l'utilisateur,

¹Stéphane RODER, Guide pratique de l'intelligence artificielle dans l'entreprise, Eyrolles, Paris, 2019, p. 5.

du propriétaire, du fabricant de la machine, du concepteur du logiciel intégré à la machine. Reste à savoir si les régimes existants peuvent leur être appliqués, le cas échéant en les adaptant, faute de quoi il faudrait concevoir un régime spécial de responsabilité pouvant appréhender cette situation inédite.

Avant toute éventuelle réforme, il convient d'évaluer les règles existantes. Il s'agit d'apprécier si les régimes de responsabilité actuellement en vigueur offrent des solutions satisfaisantes pour la réparation des dommages provoqués par l'intelligence artificielle¹. Cette évaluation permettra de déterminer s'il ya lieu de légiférer et dans l'affirmative comment le faire. Il faut en effet éviter d'encombrer le droit positif de statuts inutiles qui sont un facteur de complication et d'injustice. « *Les lois inutiles affaiblissent les lois nécessaires* » écrivait Montesquieu². C'est seulement si les dispositions existantes ne permettent pas de répondre aux besoins qu'il conviendra d'instaurer de nouvelles règles spécialement adaptées.

Le droit s'organise autour de la distinction fondamentale entre les personnes et les choses. Les personnes sont des sujets de droit, les choses des objets de droit. Une approche audacieuse consiste à appréhender l'intelligence artificielle comme une personne, ce qui conduit à raisonner en termes de responsabilité du fait personnel. Une approche classique consiste à considérer l'intelligence artificielle comme une chose ce qui conduit à raisonner en termes de responsabilité du fait des choses.

Une autre option, largement discutée consisterait tout simplement à retenir la responsabilité de la machine elle-même en lui conférant la personnalité juridique. Il a été suggéré d'examiner la possibilité de créer « *à terme, une responsabilité juridique spécifique aux robots, pour qu'au moins les robots autonomes les plus sophistiqués puissent être considérés comme des personnes électroniques responsables, tenues de réparer tout dommage causé à tiers* »³. Les machines intelligentes dotés d'une intelligence artificielle seraient dotées d'une personnalité électronique, qui leur permettrait de conclure des contrats et d'être dotées d'un patrimoine, donc de conclure des contrats d'assurance afin de faire face de faire peser sur eux la responsabilité des dommages qu'ils pourraient causer.

¹Ch. LACHIEZE, « Intelligence artificielle : quel modèle de responsabilité ? », in IP/IT, N° 12, Décembre 2020, Dalloz, p. 664.

²Charles-Louis de SECONDAT (Montesquieu), *De l'esprit des lois*, Paris, 1748, p. 40.

³Résolution du Parlement européen du 16 Février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique.

Cette proposition consistant à conférer la personnalité juridique à certains robots suscite les plus vives réserves. Elle est à la fois dangereuse et inutile. Elle est dangereuse car elle aurait pour conséquence de brouiller la distinction des personnes et des choses qui est le fondement de notre système juridique. A cet égard, il convient de souligner que la comparaison entre la notion de personne morale et celle de personne électronique est séduisante mais trompeuse. Parfois avancée comme un argument en faveur de la reconnaissance de la notion de personne électronique, la comparaison devrait au contraire inciter à la plus grande défiance. La personne morale est une abstraction ; simple personnification juridique d'un patrimoine, elle n'a aucune autonomie par rapport à ses dirigeants. La personne électronique au contraire ne serait pas une simple abstraction ; personnification juridique d'une intelligence artificielle, elle aurait la faculté d'évoluer de façon autonome en qualité de sujet de droit. Ainsi, selon le principe d'égalité le régime juridique des personnes morales a été quasiment aligné sur celui des personnes physiques jusqu'à leur reconnaître des droits fondamentaux. On pourra donc penser que la personne électronique connaîtrait une évolution identique.

Or, la reconnaissance de droits propres attachés à la personne électronique pourrait soulever des difficultés autrement plus redoutables que celles posée par les droits reconnus aux personnes morales. En effet, accorder la personnalité juridique aux robots ou à certains d'entre eux est une expérience aventureuse à laquelle la plus élémentaire prudence commande de renoncer. L'idée d'accorder aux robots la personnalité juridique est en outre inutile car elle ne permet pas vraiment de faciliter l'indemnisation des victimes. La personnalité juridique du robot n'aurait d'intérêt que si celui-ci était doté d'un patrimoine et couvert par une assurance de responsabilité. Il faudrait donc désigner une personne (le fabricant, le propriétaire ou l'utilisateur) chargée de représenter juridiquement ce robot (conclure les contrats en son nom...).

Dans ces conditions, il est plus simple de faire penser la responsabilité directement sur cette personne, plutôt que de faire un détour inutile par la responsabilité du robot. On en revient à l'idée que l'intelligence artificielle doit être considérée comme une chose dont une personne doit répondre¹. D'une part, sur le terrain de la responsabilité du fait des choses les conditions de garde et de fait de la chose paraissent remplies en cas de dommage causé par

¹S. DORMONT, « Quel régime de responsabilité pour l'intelligence artificielle ? », in Communication Commerce Electronique, N °11, 2018, p. 14.

une intelligence artificielle, que celle-ci soit matérialisée physiquement ou qu'il s'agisse d'un programme informatique.

Le principe général de responsabilité du fait des choses découlant de l'article 88 du D.O.C est suffisamment souple pour appréhender les dommages causés par l'intelligence artificielle. Le gardien d'une intelligence artificielle est responsable de plein droit des dommages causés à autrui par celle-ci. La machine ayant déclenché un transfert de fonds ou la vente de valeurs mobilières de manière préjudiciable serait considérée comme ayant produit un fait de chose anormal. Son utilisateur serait réputé gardien dès lors qu'il donne des ordres à la machine.

Cependant, l'application du principe de la responsabilité du fait des choses aux dommages causés par une intelligence artificielle suscite cependant un certain nombre de difficultés. On n'en relèvera deux. En premier lieu, la question qui se pose est si le principe de responsabilité du fait des choses est applicable aux choses incorporées. Cette question se pose car l'intelligence artificielle n'est pas nécessairement incorporée dans une chose matérielle. Cette question suscite un débat en doctrine. Cependant, la généralité du principe de responsabilité du fait des choses, qui n'opère aucune distinction entre les choses corporelles ou incorporelles devrait permettre de répondre par l'affirmative¹. En second lieu, il faut savoir le gardien de l'intelligence artificielle. Le gardien est la personne qui a l'usage, la direction et le contrôle de la chose. Cette conception de la garde prend en compte la maîtrise effective de la chose et non le pouvoir juridique sur la chose. Or, cette conception matérielle de la garde ne manquera pas de soulever des difficultés dès lors que les capacités de l'intelligence artificielle lui ouvrent une certaine autonomie d'action susceptible de la faire échapper à la maîtrise de l'utilisateur. La difficulté n'est cependant pas insurmontable.

On pourrait en effet, comme cela a été suggéré, faire appel à la distinction entre la garde de la structure et la garde du comportement : le fabricant resterait le gardien de la structure, tandis que l'utilisateur n'aurait que la garde du comportement. Mais certains régimes spéciaux de responsabilité sont également susceptibles d'être mis en œuvre pour réparer les dommages causés par une intelligence artificielle

¹Patrice JOURDAIN, Les principes de la responsabilité civile, Dalloz, 10^{ème} éd., Paris, 2021, p. 150.

D'autre part, le régime spécial de responsabilité du fait des produits défectueux issu de la loi 24-09¹ pourrait être appliqué aux dommages causés par une intelligence artificielle. Une caractéristique essentielle de ce régime est la canalisation de la responsabilité vers le producteur considéré comme le plus apte à s'assurer. Un logiciel provoquant un dommage pourrait être qualifié de produit défectueux car n'offrant pas la sécurité à laquelle on peut légitimement s'attendre. Le fabricant de la machine ou de ses composantes logicielles serait alors responsable. Cette responsabilité s'appliquerait même si le comportement de la machine ne pouvait être anticipé par ses concepteurs mais les fabricants et les programmeurs seraient sans doute incités, pour échapper à cette responsabilité très lourde, à multiplier les mises en garde des utilisateurs sur les risques éventuellement liés aux comportements de la machine.

Néanmoins, l'application de ce régime spécial aux dommages causés par une intelligence artificielle suscite cependant un certain nombre de difficultés. Tout d'abord, se pose la question de savoir si le régime spécial de responsabilité du fait des produits défectueux est applicable aux choses incorporelles. Une réponse affirmative apparaît s'imposer². Ensuite, l'appréciation de la condition du défaut du produit pose problème. La complexité du fonctionnement de l'intelligence artificielle pourra soulever des difficultés notamment sur le terrain de la preuve. Enfin, il est prévu une possibilité d'exonération pour le risque de développement. Cette exonération permet au producteur de s'exonérer de sa responsabilité en prouvant qu'il ignorait, au moment de la mise en circulation du produit, l'existence du défaut et que cette ignorance était inéluctable compte tenu de l'état des connaissances scientifiques et technique à cette date³. Appliquée à l'intelligence artificielle qui se caractérise par un fonctionnement complexe et par sa capacité à agir de façon autonome, cette cause d'exonération risque d'être trop largement admise. Une réforme serait sans doute souhaitable pour évincer cette cause d'exonération s'agissant des dommages causés par l'intelligence artificielle.

¹Dahir n° 1-11-140 du 16 ramadan 1432 (17 août 2011) portant promulgation de la loi n° 24-09 relative à la sécurité des produits et des services et complétant le dahir du 9 ramadan 1331 (12 août 1913) formant code des obligations et des contrats.

²Ch. LARROUMET, « La responsabilité du fait des produits défectueux après la loi du 19 mai 1998 », in Recueil Dalloz, N° 33, 1998, Dalloz, p. 311.

³Article 106-9 du D.O.C : « Le producteur n'est pas responsable en application du présent chapitre s'il prouve :... d - que le défaut est dû à la conformité du produit avec des règles obligatoires émanant des pouvoirs publics, ou e - que le défaut ne pouvait pas être décelé dans l'état des connaissances scientifiques et techniques au moment de la mise à disposition du produit sur le marché... ».

Dans l'ensemble, les régimes envisagés visent tous à faire peser le poids de l'indemnisation sur des concepteurs de machines si sophistiquées qu'ils ne peuvent eux-mêmes en anticiper le comportement et l'évolution. Indépendamment des éventuels effets qu'une responsabilité si lourde pourrait avoir sur l'innovation, il faut être conscient des limites du recours aux régimes existants en présence d'outils intelligents : la responsabilité du fait des produits suppose de montrer que le défaut invoqué existait lors de la mise en circulation du produit ; le fait que le comportement de la machine échappe à son utilisateur ou son concepteur conduit à évacuer toute idée de garde.

D'où, peut-être, la nécessité d'un régime spécial conçu pour tenir compte des spécificités de l'intelligence artificielle. L'inadaptation des régimes existants conduit à envisager la création d'un régime spécial de responsabilité du fait des machines dotées d'intelligence artificielle. A défaut de véritable contrôle de la machine, elle pourrait être fondée sur l'idée d'autorité de l'utilisateur sur la machine et s'inspirer de la responsabilité du fait des préposés, de la responsabilité du fait des enfants mineurs ou même de la responsabilité du fait des animaux. L'on pourrait aussi tout simplement estimer qu'il revient au propriétaire de la machine de supporter le risque que celle-ci représente avec, là encore, l'éventualité que le coût des assurances pesant sur les propriétaires de machines si sophistiquées devienne prohibitif. Ces questions renouvelées suscitées par le déploiement de l'intelligence artificielle n'épuisent toutefois pas la notion de responsabilité numérique, dès lors que d'autres difficultés se présentent, comme celles découlant de l'émergence des plateformes.

Paragraphe 2 : La responsabilité des plateformes numériques.

Comme pour les machines autonomes, la question de savoir si les plateformes constituent aujourd'hui des acteurs dotés de particularités telles qu'elles devraient faire l'objet d'un régime de responsabilité spécifique est aujourd'hui clairement posé. S'il est difficile de donner, à cette heure, une réponse définitive à cette interrogation, il est incontestable que l'ère numérique voit émerger la notion de plateforme comme une nouvelle catégorie appelant une responsabilité particulière qui n'est pas encore entièrement clarifiée.

La transition numérique a mise en exergue de nouveaux acteurs. A l'heure du *big data*, le responsable de traitement a désormais un rôle essentiel. Mais au-delà de la figure du responsable de traitement, ce sont surtout les plateformes elles-mêmes qui constituent des

acteurs d'un genre nouveau. Le développement exponentiel des plateformes et de leurs capacités hégémoniques constitue la nouvelle étape de la révolution numérique, faisant des grandes plateformes les nouveaux empires industriels de notre époque¹.

L'opérateur de plateforme en ligne est une personne physique ou morale qui, à titre professionnel, commercialise deux types de prestations. La première consiste en un service de communication au public en ligne qui a pour objet le référencement de contenus, de biens ou de services qui sont proposés ou mis en ligne par des tiers. La seconde consiste en la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service².

De nouvelles responsabilités semblent alors s'imposer aux plateformes numériques alors même que les qualifications qui leur sont applicables sont encore discutées. De fait, il était tentant à l'origine, d'utiliser à leur égard les qualifications traditionnelle et les règles du droit commun. Leur caractère multiforme permet, en effet, de douter de la pertinence d'une qualification commune et de la nécessité d'une régulation spécifique. Cependant, l'évolution, depuis une quinzaine d'années, de l'économie numérique, avec l'apparition de grandes plateformes collaboratives et un renforcement sans précédent de la puissance des GAFAM, a progressivement conduit à reconnaître l'opportunité de règles spéciales³.

Il a fallu, notamment, répondre aux difficultés suscitées par l'apparition de plateformes d'intermédiation, comme *Uber* ou *AirBnB*, qui invoquent généralement leur statut de simple intermédiaire pour faire peser l'essentiel des responsabilités liées à leur activités sur leurs utilisateurs. Ainsi, l'émergence des grandes plateformes comme *Uber*, *AirBnB* ou *Amazon*, conduit à des questions inédites résultant notamment du fait qu'elles se présentent, pour la plupart d'entre elles, comme se livrant à une simple activité d'intermédiation qui ne les rend pas directement responsables du fait des services ou des biens proposés en ligne. Or, le pouvoir dont elles disposent vis-à-vis tant des professionnels que des consommateurs utilisant la plateforme justifiaient pourtant que leur responsabilité soit plus importante que celle d'un simple courtier ou d'un hébergeur.

¹Christiane FERL-SCHUHL, *Op.cit.*, p. 1426.

²Lémy GODEFROY, « L'émergence de nouvelles responsabilités autour des plateformes » in *Quelles régulations pour l'économie collaborative*, Ouvrage collectif sous la direction d'Irina PARACHKEVOVA et Marina TELLER, Dalloz, Paris, 2017, p. 116.

³F. G'SELL, « Vers l'émergence d'une responsabilité numérique ? », in *IP/IT*, N° 3, Mars 2022, Dalloz, p. 157.

La question du statut des plateformes est importante puisqu'elle détermine le régime de la responsabilité applicable. En l'absence d'un statut légal spécifique pour les plateformes, la jurisprudence s'est chargée d'apporter des éléments de réponse. Selon une première analyse, les plateformes sont de simples intermédiaires techniques qui se limitent à mettre en relation des internautes par la fourniture d'un moyen technique d'hébergement et de communication. Une seconde analyse opère une distinction entre les différentes activités proposées par les plateformes, considérant que l'ensemble de celles-ci dépasse très largement le simple rôle d'intermédiaire. Dans ce cas la plateforme pourrait être responsable du fait de ses utilisateurs, notamment professionnels. Cette idée fait son chemin tant chez les juges que chez le législateur.

Il y a quelques années, la plateforme de vente aux enchères en ligne *eBay* a vu sa responsabilité engagée du fait de la vente, sur son site, de nombreux produits contrefaits¹. Aussi, des juges américains ont, dans un arrêt remarqué, décidé qu'*Amazon* pouvait être réputé vendeur, et donc responsable, des produits proposés par des vendeurs tiers sur sa place de marché, en se fondant sur l'important pouvoir dont dispose la plateforme, qui peut refuser un vendeur ou retirer discrétionnairement un produit de la vente².

Ainsi, une plateforme a nécessairement un rôle interactif puisqu'il détermine les contenus mis en ligne et exerce sur eux un contrôle : ils sont accessible aux internautes via son adresse web et donc sous son enseigne ou sa marque. De plus, soumise au droit commun, sa responsabilité peut être engagée du seul fait de l'existence d'un contenu illicite. Néanmoins, il est considéré que le droit commun ne permet pas de répondre pleinement aux enjeux posés par les grandes plateformes de l'économie numérique. Il conviendrait ainsi, à l'exemple des médias audiovisuels et de la presse pour lesquels existent des règles spécifiques, d'élaborer des règles particulières pour certains acteurs majeurs qui occupent un rôle clés dans l'accès aux informations³. D'où l'adoption du *DSA* et *DMA* par la l'Union européenne⁴.

Il apparaît donc, le besoin de faire évoluer le droit positif en présence d'une réalité nouvelle, difficile à saisir au moyen des catégories traditionnelles. L'évolution se fait

¹CJUE, Grande ch., décision n° C-324/09, 12 Juillet 2011, Société L'Oréal contre Société eBay International.

²C. Appel, 3ème circuit, décision n° 18-1041, 3 Juillet 2019, La société Obedorf contre la société Amazon, Etats-Unis.

³Christiane FERL-SCHUHL, *Op.cit.*, p. 1427.

⁴Voir supra p. 254.

toutefois à petits pas. Dans le cas des plateformes, comme dans celui de l'intelligence artificielle, il n'y a pas encore de consensus quant à la désignation de ceux qui doivent supporter les risques découlant de situations inédites et en pleine mutation. Dans l'ensemble, l'évolution de la technologie et l'avènement des plateformes posent des questions radicalement nouvelles sans que l'on puisse, toutefois, identifier une perspective, une logique permettant de saisir les évolutions en cours. C'est pourquoi la prudence commande sans doute, au moins pour l'instant, de parler plutôt de responsabilité numériques au pluriel, et de garder en tête que ces responsabilités sont encore en devenir.

Chapitre II

La compétence des litiges nés sur Internet

L'internet trouvant sa base et ses moyens d'expression dans les réseaux mondiaux, il n'est pas étonnant que la question se soit posée de savoir quelle est la juridiction compétente pour connaître des litiges le concernant, ou la loi applicable à ceux-ci. En effet, l'internet de par sa nature est susceptible de mettre en cause des entreprises se trouvant dans des pays différents. Quelle loi doit-on appliquer, celle du pays d'origine du message ou celle du pays de destination de ce dernier ? Quel tribunal est compétent pour connaître des litiges pouvant en découler, celui du pays d'émission ou celui du pays de réception ?

Les réponses à ces questions ont été apportées de manière éminemment unilatérale, au niveau de chacun des différents pays confrontés à cette problématique, utilisant les règles traditionnelles de conflit de lois internes et celles issues des conventions internationales. Cette myriade de solutions n'a pas manqué de générer une certaine insécurité juridique, dissuasive tant pour les consommateurs que pour les entreprises. La question du droit applicable et du tribunal compétent est accompagnée souvent, en matière d'internet, d'une difficulté supplémentaire, celle tenant à l'exécution dans un pays donné des jugements rendus dans un autre pays.

Afin de pallier ces difficultés et compte tenu de la spécificité de l'internet, outre les solutions traditionnelles applicables en la matière, des pratiques particulières se sont développées, par la création d'instances d'autorégulation et d'arbitrage¹. De plus, la pandémie de la Covid-19 a forcé les autorités marocaines, comme plusieurs gouvernements à procéder à la transformation numérique du système judiciaire. Ainsi, une mise en œuvre bien réfléchie de l'innovation technologique s'impose, soit pour repenser le fonctionnement judiciaire, soit pour en réformer ses moyens et ses méthodes, soit encore pour assurer les notifications et l'exécution des jugements. Pour mettre en œuvre cette e-justice, il faut assurer le dilemme de la sécurité juridique. Chose qui n'est pas facile vu la non-harmonisation entre les textes de loi et l'application de ce système développé.

¹Pierre-Alain GOURION et Maria RUANO-PHILIPPEAU, *Op.cit.*, p. 123.

De ce fait, le présent chapitre évoquera successivement les problématiques liées à la loi applicable à l'environnement numérique d'une part (Section 1) et d'autre part, les différents modes de résolution de litiges nés sur internet (Section 2).

Section 1 : La détermination de la loi applicable dans l'environnement numérique.

Pendant un temps relativement bref, d'aucuns ont considéré que l'internet n'était en lui-même soumis à aucune autorité : il devait être un espace virtuel de liberté. Or la réalité juridique est bien différente. Aujourd'hui, comme hier d'ailleurs, le droit s'applique à cet espace. Il n'y a pas de vide juridique. Cependant, se pose la question de savoir si le droit international privé peut appréhender un phénomène immatériel par essence, alors que sa technique repose sur la localisation des actes et des faits juridiques dans l'espace et dans le temps. S'interroger sur une telle aptitude conduit alors, en réalité, à confronter les règles de conflits de lois avec les problèmes contractuels ou délictuels en relation avec le monde virtuel.

En effet, déterminer la loi applicable est un élément essentiel dans le développement du commerce électronique international. A titre d'exemple, la difficulté de trouver les textes étrangers relatifs au droit applicable au contrat arrive en tête des obstacles aux transactions entre professionnels et consommateurs, et à la troisième place en ce qui concerne les transactions entre professionnels. Ainsi, de nombreux conflits peuvent naître à l'occasion de l'utilisation de réseaux numériques. Le média peut être soit le lieu, soit l'instrument d'une activité déterminée. Raison pour laquelle nous allons traiter la loi applicable en cas de conflit entre de contractant sur internet autrement dit le cas de responsabilité contractuelle (Sous-section 1) ainsi que la loi applicable en matière délictuelle que ce soit en cas de fautes civiles ou pénales (Sous-section 2).

Sous-section 1 : Les lois applicables aux contrats conclus sur Internet.

Même si les individus s'abstiennent de franchir physiquement les frontières étatiques, l'ubiquité de l'internet constitue un moteur essentiel de la multiplication des contrats internationaux. Le réseau offre la possibilité de se rencontrer en ligne et de tisser des relations contractuelles. Cette possibilité est maintenant ouverte aussi bien aux consommateurs qu'aux professionnels¹. La question de la loi applicable ne se pose que pour les contrats

¹Chiheb GHAZOUANI, Le contrat de commerce électronique international, Laatrache, 1^{ère} éd., Tunis, 2011, p. 221.

internationaux qui présentent un ou plusieurs éléments d'extranéité. Ce qui constitue une situation fréquente en matière de contrats conclus sur internet. La possibilité de déterminer le droit applicable au contrat est un élément essentiel dans le développement des relations contractuelles électroniques internationales.

On peut identifier une grande variété de situations contractuelles sur internet, c'est le cas par exemple de la réservation par un annonceur, d'un espace publicitaire sur un site web étranger dont l'audience est attractive, qui nécessite la conclusion d'un contrat d'achat d'espace publicitaire, ou encore l'utilisation de services de *Cloud computing* ou d'informatique en nuage proposés par une société étrangère¹. Dès lors, que ces situations ou autres présentent une dimension internationale, se pose la question de la loi applicable au contrat. En conséquence, dans un contrat électronique de droit international privé, caractérisé par un élément d'extranéité, la première question que l'on peut se poser est de savoir si les parties ont émis une volonté de choisir leur droit applicable.

Les solutions peuvent ainsi être radicalement différentes selon qu'il existe une volonté des parties quant au choix de la loi (Paragraphe 1) ou qu'aucune volonté n'est perceptible, ce qui entraînera le juge dans une recherche objective des critères rattachement du contrat (Paragraphe 2). C'est pourquoi il faut envisager tour à tour ces deux modes différents de rattachement. Enfin, il arrive des fois que les parties font appel à la *lex electronica* c'est-à-dire les usages en tant que loi du contrat électronique (Paragraphe 3).

Paragraphe 1 : Le rattachement subjectif.

Les actes juridiques étant par essence des manifestations de volonté en vue de la production d'effets juridiques, il paraît alors fondé de permettre aux parties à l'engagement contractuel de choisir leur propre *lex contratus*. Il est alors admis que les acteurs professionnels du marché électronique puissent contracter librement en choisissant les conditions contractuelles qui leur sont les plus favorables. La liberté des parties de choisir la loi qui va régir leur relation contractuelle est largement admise en droit international privé. En effet, « *un exercice réfléchi de l'autonomie de la volonté garantit une certaine sécurité juridique* »². L'application du principe d'autonomie résulte dans le droit marocain de

¹Voir supra p. 178.

²W.WENGLER, « L'évolution moderne du droit international privé et la prévisibilité du droit applicable », in Revue critique de droit international privé, 1990, p. 657. Cité dans Chiheb GHAZOUANI, Le contrat de commerce électronique international, Laatarche, 1^{ère} éd., Tunis, 2011, p. 241.

l'article 13 du D.O.C : « Les conditions de fond et les effets des contrats sont déterminés par la loi à laquelle les parties ont eu l'intention expresse ou tacite de se référer ».

Cette liberté peut s'exercer de deux manières : élire le droit applicable à la relation électronique d'une part, et prévoir d'autre part des solutions pouvant s'adapter à la relation contractuelle par l'incorporation de règles qui ne relèvent pas d'une loi étatique. Les sociétés qui contractent sur internet ont un intérêt évident à désigner en amont la loi nationale qui régira leurs relations avec les sociétés étrangères¹. Ce choix est souvent effectué par le prestataire, dans les contrats qu'il propose à ses utilisateurs et le choix d'une loi étrangère est bien évidemment source d'une grande insécurité juridique pour le bénéficiaire des services².

La convention de Rome de 19 Juin 1980, remplacée par le Règlement de Rome I³ en 2007, conclues entre les Etats membres de la communauté Européenne et relative à la loi applicable aux obligations contractuelles désigne expressément la loi d'autonomie pour régir le contrat. Dans son article 3 intitulé « liberté de choix » dispose en effet dans son paragraphe premier que « le contrat est régi par la loi choisie par les parties. Ce choix doit être exprès ou résulter de façon certaine des dispositions du contrôle des circonstances de la cause ». Il faut noter que le Règlement va dans le sens de l'assouplissement des règles de la Convention de Rome concernant le choix subjectif de la loi applicable. Il consacre ainsi le choix des parties comme loi applicable, des principes et règles de droit matériel des contrats, reconnus au niveau international. Cette attitude paraît plausible puisqu'elle permet aux contractants d'avoir d'avantage de liberté dans la rédaction de leurs conventions électroniques. L'existence d'une clause expresse d'élection du droit applicable au contrat dispense, en principe, le juge de recourir à d'autres éléments. Il doit s'en tenir au choix exprimé. Cependant, quelques problèmes peuvent surgir quant aux conséquences de la mise en œuvre de la loi désignée.

D'abord, il convient de s'intéresser à la validité des clauses d'élection de droit lorsqu'elles sont insérées dans un accord distinct du contrat principal. A titre d'exemple, la clause peut se trouver dans des conditions générales mises en ligne sur le site de commerce électronique. La problématique qui se pose est de savoir si la communication des conditions générales avant la conclusion du contrat peut être assurée par voie électronique ? Cette

¹Sous réserve que ce choix n'ait pas pour effet de priver l'une des parties d'une protection qui lui offerte par la loi, ou de contourner les lois de police d'un Etat.

²Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 46.

³Règlement (CE) n°593/2008 du Parlement Européen et du Conseil du 17 juin 2008 sur la loi applicable aux obligations contractuelles (Rome I).

question peut être rencontrée très souvent dans la pratique car les conditions générales sont très fréquentes puisqu'elles répondent à un souci de standardisation et de rapidité dans le domaine contractuel. En effet, le document électronique qui contient l'élection de droit est en principe accessible à l'internaute dans une rubrique différente du site internet mais à proprement parler, le document ne lui est pas remis au sens du droit. A vrai dire, seules les conditions générales contenues dans le contrat principal ou dans une annexe signée et acceptée par l'acheteur peuvent être prises en compte pour désigner la loi applicable.

Ensuite, se pose le problème de l'incorporation par référence. Cette dernière consiste dans le fait d'incorporer des clauses au contrat par la voie de liens hypertextes. Un lien hypertextes, ou hyperlien, est généralement représenté par un mot, un ensemble de mots, ou une image. Il permet par un simple clic d'accéder à une autre partie de la page web consultée, une autre page du même site ou un autre site. On retrouve une reconnaissance de l'utilité et de l'intérêt pratique des liens hypertextes dans la loi type de la CNUDCI à l'article 5 qui précise que « L'information n'est pas privée de ses effets juridiques au seul motif qu'elle est incorporée par référence dans un message de données »¹. Ainsi, partant du principe que la clause d'élection de la loi applicable n'est soumise à aucune condition de forme, il est souhaitable de prendre en compte l'intérêt pratique des liens hypertextes et de la facilité pour avoir accès aux clauses contractuelles.

Enfin, il est fréquent en pratique de voir des contrats électronique comporter des clauses d'élection du droit dans les conditions générales des sites internet sans que cette clause ait été sujette à une négociation préalable. Le consentement électronique à la clause d'élection de droit sonné sans aucune possibilité de négocier les détails et les conditions de la stipulation est largement critiqué par la doctrine. Sur le plan légal, en droit marocain la communication des conditions générales est requise avant la conclusion du contrat. La loi 53-05 relative à l'échange électronique des données numériques a intégré au Dahir formant Code des obligations et des contrats une nouvelle disposition dans son premier chapitre selon laquelle « Quiconque propose, à titre professionnel, par voie électronique, la fourniture de biens, la prestation de services ou la cession de fonds de commerce ou l'un de leurs éléments met à disposition du public les conditions contractuelles applicables d'une manière permettant leur conservation et leur reproduction »². Ainsi, l'intérêt de cette disposition est de montrer

¹Loi type de la CNUDCI sur le commerce électronique, 12 Juin 1996.

²Article 65-4 du chapitre premier bis du D.O.C.

que le législateur marocain reste réticent à l'encontre de l'incorporation par référence dans les contrats de consommation.

Paragraphe 2 : Le rattachement objectif.

En l'absence de choix de la loi applicable au contrat électronique par les parties, certaines clauses peuvent révéler au juge, indirectement, la volonté des parties de soumettre leur contrat à une loi donnée. Autrement dit, lorsque les parties n'ont pas stipulé expressément quelle serait la loi applicable à leur contrat, les juges doivent rechercher quelle était leur volonté présumée. En effet il arrive que les parties, sans avoir pensé à choisir expressément leur loi applicable, s'en soient manifestement inspirées pour rédiger leur contrat. C'est le cas lorsqu'elles ont recouru à un contrat-type en usage dans un domaine déterminé. Si le contrat ne suffit pas à lui-même et doit être complété par l'application d'une loi, ce ne peut être que de celle qui a servi de référence pour l'établissement du modèle. De même, lorsqu'un contrat d'adhésion est conclu- ce qui est pratique dans le commerce électronique- il est normalement établi conformément à la législation du pays qui sert de cadre aux activités de la partie qui l'impose. Ceci lui permet de traiter toutes ses affaires, conformément à une loi unique¹.

Par ailleurs, les parties peuvent insérer des clauses attributives de juridiction, à l'instar du choix de la loi applicable ces clauses sont une manifestation de l'autonomie de la volonté des parties. Ainsi les clauses attributives de juridictions peuvent constituer des indices contractuels de rattachement car on peut penser que si l'ordre juridictionnel d'un pays convient aux parties, son ordre juridique leur convient aussi, de plus l'application par un juge de sa propre loi est la solution la plus normale et la plus commode. Cette solution n'est cependant pas partagée par toute la doctrine. Entre ceux qui sont favorables au rattachement contractuel dont la source d'inspiration est une clause de choix du juge compétent, et d'autres qui n'estiment que l'insertion d'une clause attributive de juridiction en faveur d'un juge donné ne permet pas de caractériser, à lui seul, un choix certain de la loi du juge désigné, nous pourrions considérer que le simple fait qu'une seule des lois en présence valide une clause déterminée du contrat peut faire présumée que les parties ont entendu choisir cette loi, surtout

¹Pierre MAYER, Vincent HEUZE et Benjamin REMY, Droit international privé, LGDJ, 12^{ème} éd., Paris, 2019, p.718.

si les circonstances de la conclusion montrent qu'elles connaissent la teneur des diverses lois en présence¹.

En l'absence de choix des parties, la désignation de la loi applicable est singulièrement compliquée. Les règles de conflits de lois reposent sur la localisation du contrat. En effet, si la détermination des critères de localisation concernant un contrat dont l'exécution s'effectue hors ligne n'est pas aisée, elle l'est davantage si celle-ci se fait en ligne. Faute d'avoir exprimé leur liberté de choix, la loi applicable à leurs contrats va dépendre inévitablement du jeu des règles de conflits d'une part et de l'application des lois de police d'autre part.

Lorsque le choix est accordé à la loi désignée par les règles de conflit, le juge saisi d'un litige commercial international est bien évidemment tenu de puiser dans son système juridique national les normes qu'il va utiliser. C'est la *lex fori* qui lui indique les rattachements. En revanche, l'arbitre est évidemment un juge indépendant, qui n'est lié à aucun système juridique étatique et qui n'a donc pas de *lex foi*. Lorsqu'il est saisi d'un litige international, en cas de silence des parties sur la question de la loi applicable, il ne peut donc recourir à sa propre législation nationale pour y trouver un facteur de rattachement².

Par ailleurs, l'application des lois de police trouve son fondement dans les principes de justice contractuelle et d'ordre public. L'idée générale est de la suprématie de la collectivité sur les intérêts individuels. Il est admissible qu'un certain ordre public s'imposera au commerce électronique en ce qui concerne les activités interdites ou prohibées. On peut citer à titre d'exemple les loteries et les casinos dont la réglementation est très stricte en cas de mise en place de salle de jeu virtuels. De même, on doit s'inquiéter de la multiplicité des offres de produits ou de services gratuits sur l'internet. Cette gratuité peut être illicite si elle vient au soutien de pratiques anticoncurrentielles notamment d'abus de position dominante.

Paragraphe 3 : L'admissibilité de la *lex electronica* en tant que loi du contrat électronique.

La pratique du commerce international a favorisé l'accroissement en nombre des usages et l'activité normative internationale spécifique à la matière du commerce électronique

¹Chiheb GHAZOUANI, *Op.cit.*, p. 58.

²Sylvette GUILLEMARD, *Le droit international privé face au contrat de vente cyberspatial*, Thèse de Doctorat en droit privé, Université Laval Québec et Université Panthéon-Assas Paris II, Paris, 2002, p. 171.

reste limitée. Les organisations internationales non gouvernementales ont pris des initiatives très tôt en la matière. On a observé l'émergence d'une « *soft law* », une *lex electronica* et *leges electronica* ¹ qui ne s'impose que par l'adhésion des Etats ou par la volonté des parties respectueuses des usages du commerce électronique international.

Le commerce électronique s'est enrichi de l'émergence de normes souples et adaptées à la réalité du réseau. En exerçant leur autonomie de volonté pour déterminer l'étendue de leurs droits et obligations, les acteurs du commerce électronique international participent à la création d'une *lex electronica*. La raison du choix d'un usage en tant que loi du contrat électronique réside dans le fait qu'elle constitue également un instrument de pluralisme juridique qui permet d'adapter le droit aux conditions particulières de la vie locale ou professionnelle. La pratique joue en effet un rôle important dans les relations contractuelles et très souvent, les stipulations des contrats se conforment à des usages².

La *lex electronica* se compose de deux éléments : un élément matériel et un élément psychologique. L'élément matériel consiste dans la répétitions, la fréquence et la constance. Cet élément est souvent considéré comme étant la donnée la plus objective nécessaire à la réalisation de l'usage. L'importance de trouver une origine à la *lex electronica* et de démontrer qu'elle est suivie et répétée par un groupe ou par une communauté d'intervenants est capitale. Tandis que l'élément psychologique réside dans le fait que la *lex electronica* trouve sa source dans les pratiques des acteurs du commerce électronique formant eux-mêmes la communauté du cyberspace. Par conséquent, la *lex electronica* est une norme supplétive, par opposition au caractère impératif qui caractérise l'ordre public de protection de la partie faible du contrat, le plus souvent, des consommateurs.

A l'image de la *lex mercatoria*, la *lex electronica* inclut aussi bien des principes que des règles et des usages. On peut donc intégrer dans les sources de la *lex electronica* les techniques de réglementation telles que les principes³, les standards, les codes de conduite⁴,

¹Olivier CACHARD, La régulation internationale du marché électronique, LGDJ, Paris, 2002, p. 164.

²Chiheb GHAZOUANI, *Op.cit.*, p. 259.

³L'institut international pour l'unification du droit privé a publié en 1994 un recueil de principes destinés à être utilisés dans le monde entier pour régir les contrats de commerce international. La version de 1994 a été adaptée en 2004 en vue de répondre aux besoins de commerce électronique.

⁴Les codes de conduite procurent des normes de comportement qui, sans être revêtues de la force obligatoire qui appartient au traité ou à la loi, définissent la déontologie des relations économiques transfrontières en matière de codes de conduite disponible dans le monde numérique, on peut citer les règles de conduite proposées par la Chambre de commerce internationale CCI qui dès 1987, mi à la connaissance des utilisateurs de réseaux « The Uniform Rules of Conduct for Interchange of Trade Data by Teletransmission ».

les contrats types¹ des résolutions diverses et des décisions arbitrales. Les intérêts de la *lex electronica* peuvent être aussi bien théoriques que pratiques. Plusieurs arguments sont avancés pour démontrer l'intérêt théorique de la *lex electronica*.

D'abord, l'internationalité du réseau internet en ce sens que les réseaux électroniques ont, dans leur nature même, une portée internationale. Cette donnée exige par conséquent que la loi tienne compte de ce facteur international. Or eu égard aux difficultés d'élaboration de règles internationales, les traités n'étant le fruit que d'un processus fastidieux, les risques de divergences d'un pays à un autre, les inconvénients occasionnés par la doctrine des conflits de lois, il fallait donc une norme ayant la souplesse nécessaire pour s'exonérer de ces contingences de formation. Les normes informelles disposent en l'espèce d'une reconnaissance toute particulière en droit international du fait de la moindre concurrence des normes plus formelles. Ensuite, la lenteur attachée à l'élaboration d'une règle écrite s'accorde mal avec la vitesse d'évolution des nouvelles technologies d'information. Davantage maintenant que plus tard, les normes informelles seront donc une référence normative importante dans le commerce électronique.

De plus, le caractère technique du commerce électronique rend le développement des normes informelles encore plus propices. Aussi, la matière commerciale est propice à l'intégration de nouveautés juridiques. Les commerçants perçoivent la règle comme un support à leurs opérations de négoce. Pour ce faire, ils exigent une fonctionnalité et un pragmatisme que les normes informelles sont souvent prête à leur apporter. Enfin, le dernier argument qu'il évoque en faveur de la *lex electronica* se résume dans la place particulièrement importante qu'occupe la communauté commerçante. Les entreprises sont naturellement opposées à toute entrave étatique dans leur commerce et préfèrent appliquer leurs propres usages.

Les intérêts pratiques de la *lex electronica* peuvent être regardés à travers deux considérations. D'une part, on peut envisager la *lex electronica* comme un moyen de

¹La doctrine souligne le rôle, sans cesse croissant que jouent, au niveau national comme dans l'ordre international, les contrats-types et les usages du commerce. Ces contrats-types, en marge des conditions générales se sont développés pour faciliter les relations d'affaires. Ce constat a conduit les juges à leur reconnaître, dans le cadre de la profession dans laquelle ils s'exercent, la force d'un usage. En matière de *lex electronica* le contrat type électronique précise les obligations des contractants et peut mettre en place un système de communication sécurisé et organise les conditions de responsabilité et de preuve. Parmi les contrats-types dans le domaine des nouvelles technologies les contrats d'échange de données informatisées EDI.

régulation du marché électronique. Ainsi, en matière de commerce électronique, les règles régulant le marché électronique trouvent leur source dans les différentes lois promulguées afin d'adapter le droit positif aux évolutions technologiques et dans les contrats conclus par les usagers. Cependant, la loi et le contrat peuvent avoir des limites dans l'environnement numérique¹. C'est pourquoi les Etats devraient permettre aux acteurs professionnels du commerce électronique d'organiser leurs relations contractuelles en toute liberté tant que leurs agissements ne constituent pas des infractions pénales. En effet, le fait de s'obstiner à réguler le marché électronique par la création d'institution *ad hoc* pourrait constituer un frein au développement des activités électronique. Il serait ainsi préférable de laisser les acteurs du commerce électronique être les acteurs de leur propre régulation par la création de règles échappant au contrôle étatique préalable², en l'occurrence, la *lex electronica*. D'autre part, la *lex electronica* pourrait être envisagé comme un complément du droit positif du commerce électronique. L'autonomie de la volonté permet de trouver des solutions pratiques à bien de problèmes juridiques et d'outrepasser les vides juridiques et les incohérences de certaines lois et traités. Les acteurs du marché électronique se trouvent alors dans un environnement où le processus d'autoréglementation est largement consensuel.

Bien que la *lex electronica* ait trouvé un accueil favorable, il faut rester sceptique à son égard. En effet, contrairement à la *lex mercatoria*, qui est décrite comme la loi des marchands professionnels, la *lex electronica* regroupe une multitude d'utilisateurs des réseaux numériques qu'ils soient professionnels, consommateurs ou acheteurs sur les sites d'enchères en lignes. Ainsi, « l'absence d'uniformité et de cohésion entre les membres des marchés électroniques devrait freiner l'émergence des usages »³. De plus, l'assimilation de la *lex electronica* à la *lex mercatoria* appelle une nouvelle critique d'ordre moral. Alors que la substance de la loi des marchands a été inspirée par une pratique commerciale constante ou l'autonomie de la volonté trouve une place de choix, les relations contractuelles et les pratiques répétées sur le réseau internet sont souvent imposées par le contractant fort au détriment du faible. C'est vrai que la *lex electronica* est une norme dont l'usage ne peut être que limité, mais nous ne pouvons pas nier que le recours à la *lex electronica* présente néanmoins plusieurs intérêts.

¹Chiheb GHAZOUANI, *Op.cit.*, p. 291.

²Le contrôle étatique préalable serait celui du législateur en tant qu'entité créatrice de règles de droit, par opposition au contrôle a posteriori, celui exercé par le juge.

³Olivier CACHARD, *Op.cit.*, p. 31.

Sous-section 2 : Les lois applicables aux fautes civiles et pénales commises sur Internet.

Comme en matière contractuelle, il convient en matière délictuelle de déterminer la loi applicable aux fautes civiles commises sur internet ainsi que les fautes pénales. Il existe de nombreuses illustrations des fautes civiles (délits et quasi-délits) susceptibles de survenir sur le réseau. Outre le cas général d'acte de toute nature ayant des conséquences dommageables, des cas spéciaux comme l'atteinte aux droits de la personnalité, la contrefaçon ou la concurrence déloyale méritent une attention particulière en droit des activités numériques.

La diversité de ces situations peut expliquer la diversité des solutions retenues par les juridictions (Paragraphe 1). En matière pénale, la question du droit pénal international applicable aux infractions commises par internet est à la fois simple et extrêmement complexe. Les règles sont assez simples en ce qu'il y a unité de solutions entre la question du tribunal compétent et la loi applicable, mais la difficulté s'accroît lorsqu'il s'agit de lutter de manière coordonnée contre la cybercriminalité (Paragraphe 2).

Paragraphe 1 : La loi applicable en matière délictuelle.

Les délits commis via le réseau présentent souvent un caractère complexe, le lieu de l'événement qui a donné naissance au dommage (lieu du fait générateur) et le lieu où le dommage va être subi (lieu du dommage) se situant, le plus souvent, dans des pays distincts. La loi du fait générateur et la loi du pays dans le ressort duquel le dommage a été subi ne sont donc pas les mêmes et les juridictions ont du, lorsque les litiges leur étaient soumis, à déterminer la loi applicable. Traditionnellement, la compétence de la loi du lieu du délit était la solution de principe, même si les juridictions du fond tentaient de trouver des expédients pour justifier l'application de la loi du for, notamment en choisissant d'appliquer la loi du lieu dans lequel le dommage avait été subi¹.

L'application de ces règles de conflits transposées au réseau internet fait apparaître une difficulté spécifique, relative à la notion de lieu de l'acte générateur du dommage et à celle de lieu du préjudice. D'abord, où et comment situer le lieu de l'événement causal ou de l'acte dommageable ? La réponse relève principalement des définitions que l'on donne. Certains ont soutenu que cette question est un non-sens car elle invite à rechercher un lieu

¹Olivier CACHARD et Paul KLOTGEN, Droit international privé, Bruylant, 9^{ème} éd., coll. Paradigme, Paris, 2021, p. 327.

géographique de commission de l'acte dans un espace réel, alors que par hypothèse le délit se situe dans le cyberspace, monde virtuel. Une telle réponse ne correspond en aucune manière à la logique juridique, car l'internet n'est qu'un moyen de communication, c'est-à-dire l'instrument de réalisation ou de la commission du délit. L'appréhension de la réalité doit être plus banale dans la mesure où l'acte délictuel est commis en un point de l'espace qu'il convient de déterminer de façon idoine. En effet, cette localisation de l'acte lui-même est parfaitement possible.

C'est donc logiquement que s'agissant de fautes commises sur internet, les juridictions vont appliquer la loi du pays dans lequel l'information litigieuse a pu être consultée et a donc causé un dommage et non celle du pays dans lequel l'information a été mise en ligne. Donc le lieu du fait générateur est le lieu de chargement du message dommageable sur le réseau, c'est-à-dire le pays à partir duquel une page web est chargée sur un serveur, ou bien le lieu d'expédition d'un courrier électronique. Dès lors, en appliquant cette solution, la compétence serait attribuée en principe à la loi du pays de réception, laquelle coïncide le plus souvent avec le lieu de réalisation du dommage. Par exemple, les tribunaux marocains, saisis d'une action en dommages et intérêts par la victime d'un délit ou d'un quasi-délit commis en ligne, feront application de la loi marocaine pour juger de la demande en réparation si le message électronique délictuel, émis sur le réseau depuis un pays étranger, a pu être consulté au Maroc et y a causé un dommage. Ce triomphe de la loi du pays de réception sur celle du pays d'émission prête cependant le flanc à la critique¹. Il faut en effet prendre conscience que les lieux de réception sont potentiellement planétaires et ne pas perdre de vue que la compétence et ne pas perdre de vue que la compétence du tribunal est généralement limitée à la connaissance du seul préjudice local.

En conséquence, en l'état actuel du droit international privé, la transposition de la règle classique encourt un double reproche. D'une part, la victime sera contrainte de faire face à des frais importants de procédure diligentant des demandes en réparation dans les principaux pays où elle a subi un dommage, alors peut-être que sa législation nationale est peu protectrice de ses droits. A quoi s'ajoutent les probables difficultés d'exécution des condamnations obtenues dans les pays de réception, dont il faudra obtenir l'exequatur dans le pays d'émission où réside l'auteur du délit. D'autre part et surtout, l'application de la loi du

¹C de HASS, « L'omnipotence du juge français de la propriété intellectuelle face à l'internet ou l'histoire d'une incompétence largement ignorée », in LPA, N° 226, 13 Novembre 2001, p. 4.

pays de réception conduit théoriquement à obliger tout internaute émetteur d'informations à connaître et à se conformer à la législation de tous les pays, afin d'éviter toute poursuite en responsabilité. Or, une telle exigence est pratiquement impossible à satisfaire, sauf pour les sociétés multinationales.

Pour paner à cette critique, il a été proposé en doctrine de perfectionner la règle de conflit en l'assortissant d'une condition de nature en restreindre le champ d'application. Serait maintenu le critère de rattachement désignant la loi du pays de réception. Mais cette loi ne serait applicable que s'il s'agit d'un pays cible. Ce dernier doit être compris comme étant, selon la volonté de l'auteur responsable, le pays destinataire de la transmission de données délictueuses. L'un des critères à prendre en considération pourrait être la langue utilisée sur le site, permettant ainsi de présumer du public auquel le message ou la page web sont destinés. On objectera toutefois qu'il ne sera pas toujours facile de déterminer quel est le pays ou quels sont les pays cibles.

C'est pourquoi le règlement de Rome II¹ énonce une solution d'application plus simple à internet. Il dispose que serait applicable à la responsabilité délictuelle la loi du pays qui a les liens les plus étroits avec le fait dommageable, étant présumé que c'est la loi du pays de la résidence habituelle de la victime. Celle-ci serait applicable pour apprécier et réparer l'intégralité du dommage. Une part significative des délits commis sur le réseau consiste, en pratique, en des atteintes à des œuvres de l'esprit (logiciel, sites web...). Les circonstances de chaque espèce sont particulièrement importantes, pour comprendre les solutions dégagées.

En matière de propriété littéraire et artistique, le régime échappe dans une large mesure aux conflits de lois et obéit à des règles de droit matériel issues des conventions de Berne, de Genève et d'accords internationaux. Schématiquement, l'existence et la titularité du droit relèvent de la loi du pays de la première publication ou divulgation de l'œuvre. Par ailleurs, l'exercice et la sanction d'une atteinte au droit relèvent de la loi du pays où la sanction est demandée. Le règlement de Rome II soumet également les atteintes portées au

¹Règlement (CE) n° 864/2007 du Parlement Européen et du Conseil du 11 juillet 2007 sur la loi applicable aux obligations non contractuelles (Rome II). Le règlement traite la question de la loi applicable dans des conflits transfrontaliers résultant des engagements non contractuels est fortement importante dans le cadre de la mobilité en constante croissance au sein de l'UE, et peut probablement résulter dans des cas de responsabilités délictuelles. Afin d'augmenter la certitude légale, le règlement de Rome II définit la loi applicable en fournissant une liberté limitée de choix aux parties et en indiquant des règles générales, ainsi que spécifiques pour certains types de responsabilités délictuelles ou de délits.

droit de propriété intellectuelle à la loi du pays pour lequel la protection est revendiquée ce qui laisse penser qu'il s'agira le plus souvent de la loi du for¹.

Résoudre la question de la preuve, enfin, ne sera plus aisé². La victime devra prouver que le site web, objet du dommage, a été visualisé par de nombreux internautes, lui causant ainsi un grave préjudice. Elle devra s'adresser aux fournisseurs d'accès locaux dans chaque pays de réception afin d'obtenir des traces des connexions sur le serveur qui héberge le site litigieux. Elle pourra essayer d'obtenir ces traces de la part du serveur hébergeant l'éditeur fautif, mais cela sera encore moins aisé. Ainsi, il faudra parvenir à identifier correctement le ou les responsables du dommage, ce qui peut soulever quelques difficultés particulières compte tenu des nombreux intervenants à des titres très divers sur le réseau des réseaux numériques. Cependant, ce problème se pose aussi en des termes très voisins pour les infractions pénales et son examen peut donc être différé pour être abordé ci-dessous.

Paragraphe 2 : La loi applicable aux infractions de cybercriminalité.

Après la fin des investigations, se pose la question de la loi applicable. La règle essentielle de droit pénal international réside dans le fait que toute infraction qui présente à la fois un élément d'extranéité et un point de contact avec le Maroc peut relever des juridictions marocaines et de la loi marocaine. Sans point de contact particulier, bien que l'infraction soit intégralement commise à l'étranger, la loi marocaine peut encore s'appliquer quand un Marocain est impliqué.

L'article 10 du Code pénal marocain dispose que : « Sont soumis à la loi pénale marocaine, tous ceux qui, nationaux, étrangers ou apatrides, se trouvent sur les territoires du Royaume, sauf les exceptions établies par le droit public interne ou le droit international ». La règle signifie que la nationalité de celui qui commet l'infraction sur le territoire du Royaume importe peu, ce peut être un étranger ; il sera appréhender et jugé dès lors qu'il est soupçonné avoir commis cette infraction.

En outre, l'article 12 du code pénal dispose que : « la loi pénale marocaine s'applique aux infractions commises hors du Royaume lorsqu'elles relèvent de la compétence des juridictions répressives marocaines en vertu des dispositions des articles 751 à 756 du code de

¹Article 8 du règlement de Rome II : « La loi applicable à une obligation non contractuelle résultant d'une atteinte à un droit de propriété intellectuelle est celle du pays pour lequel la protection est revendiquée »

²Olivier CACHARD et Paul KLOTGEN, *Op.cit.*, p. 161.

procédure pénale ». Et d'après la lecture des articles 751¹ et 752² du Code de procédure pénale, il existe une compétence personnelle active et passive, par prise en considération de la nationalité marocaine de l'auteur de l'infraction. Cela va permettre de faire réprimer par la loi marocaine toute infraction dont l'auteur est de nationalité marocaine, selon des nuances tenant compte de la gravité de l'infraction.

La compétence personnelle active permet de juger un ressortissant marocain, alors même qu'il y a absence de localisation au Maroc d'un élément constitutif de l'infraction. Le CPP distingue selon que l'infraction commise à l'étranger par le ressortissant marocain est un crime (compétence de la loi et du tribunal marocain pour en juger, sans exigence de condition supplémentaire) ou un délit (une condition de double incrimination est exigée : les faits doivent également être punis par la législation du pays où ils ont été commis). La compétence personnelle passive, permet de juger de tout crime ou de tout délit d'emprisonnement, commis à l'étranger, et dont la victime est française au moment de l'infraction.

En définitive, le droit pénal marocain a un champ d'application extrêmement vaste et il peut appréhender l'ensemble des infractions en relation avec l'internet, pour peu que l'ordre juridique marocain s'estime concerné par les actes répréhensibles. Néanmoins, l'application du principe de territorialité ne suffit pas à régler toute la question des infractions commises sur les réseaux numériques. En effet, outre sa compétence territoriale générale, encore faut-il que la loi marocaine incrimine spécialement tel comportement pour qu'elle puisse réprimer infractions commises sur les réseaux numériques. En d'autres termes, il faut qu'il existe expressément un texte de loi, dont au surplus on doit rappeler qu'il est par nature d'interprétation stricte.

Or, les comportements délictueux pratiqués sur ou par l'internet sont parfois très nouveaux et leurs éléments constitutifs n'entrent pas toujours nécessairement dans la

¹Article 751 du CPP : « Tout fait qualifié crime par la loi marocaine et commis hors du royaume par un marocain peut être poursuivi et jugé au Maroc. Toutefois la poursuite ou le jugement ne peut avoir lieu que définitivement jugé à l'étranger et, en cas de condamnation, avoir subi ou prescrit sa peine ou obtenu sa grâce ».

²Article 752 du CPP : « Tout fait qualifié délit tant par la loi marocaine que par la législation du pays où il a été commis, peut être poursuivi et jugé au Maroc, lorsque son auteur est un Marocain. La poursuite ou le jugement ne peut avoir lieu que dans les conditions prévues au deuxième alinéa de l'article précédent » ;

définition légale des textes du Code pénal marocain. Il importe donc de confronter les incriminations prévues par la loi marocaine aux pratiques délictueuses constatées sur les réseaux numériques. Il va sans dire que les infractions spécifiques au numérique, introduite par la loi 07-03 qui concerne les infractions relatives aux systèmes de traitement automatisé des données, peuvent être réprimées par application de la loi marocaine, à condition que l'un de leurs éléments se rattache au territoire marocain, que l'auteur soit une personne physique ou morale. Ces infractions ne posent pas vraiment de problème spécifique au regard du droit pénal international.

Plus courants et préoccupants sont les comportements délictueux classiquement incriminés par des dispositions du Code pénal, et par lesquels l'internet apparaît comme étant soit le lieu de l'infraction par exemple l'attente aux données à caractère personnel prévue par la loi 09-08, soit l'instrument de l'infraction c'est le cas de détournement de fond par numérique ou encore abus de confiance. Parmi ces infractions traditionnelles, certaines soulèvent des difficultés particulières, de leur solution dépend en effet le régime de l'incrimination et de la répression. En outre, ces infractions concernent le secteur de la communication, donc de la diffusion d'informations, qui est de l'essence même des échanges électroniques. L'une de ces difficultés consiste dans le choix de la qualification appropriée du service proposé sur l'internet et qui est la source ou le support des agissements répréhensibles. Ainsi, ce problème est intrinsèque à la nature de l'internet, dont les divers services (Web, messagerie électronique, *Cloud*, réseaux sociaux) peuvent relever de régimes légaux distincts.

En effet, plusieurs régimes d'incrimination et de répression sont applicables en fonction de la qualification qui sera retenue, que se soit la loi 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel ou la loi 53-05 qui prévoit les infraction en matière d'échange électronique de données juridiques ou encore la loi 24-96 relative à la poste et aux télécommunication qui édicte elle aussi des infractions assorties de sanctions pénales. Il est donc essentiel de détecter la nature du message transmis sur internet pour retenir une qualification.

L'autre difficulté concerne la détermination des personnes responsables pouvant être poursuivies. Nombreux et disparates quant à leurs fonctions sont les intervenants susceptibles d'entrer dans une chaîne de responsabilité pénale. Depuis, l'internaute émettant ou utilisant de l'information hébergée sur un site et produite par un fournisseur de services en passant par un fournisseur d'accès, un hébergeur jusqu'au transporteur de l'information en qualité

d'opérateur des communications électroniques, chacune de ces personnes pourrait éventuellement être poursuivie en responsabilité comme auteur principal ou comme complice. La réponse dépend du rôle joué respectivement par ces acteurs, en relation avec la nature de l'infraction considérée.

Section 2 : Les modes de résolution de litiges nés du numérique.

Plusieurs litiges liés à des opérations en ligne, dont le nombre se multipliera à mesure de l'essor de la transformation digitale des entreprises. Ainsi, afin d'accompagner la résolution de tels litiges, on a vu fleurir diverses initiatives ou propositions pour leur règlement en ligne, lesquelles ont aussi vocation à traiter d'autres contentieux apparus hors des réseaux mais pour lesquels les intéressés s'en remettent à une procédure en ligne. Les mécanismes existants sont appelés selon les cas arbitrage, médiation, ou conciliation. Ils sont pour l'essentiel portés par des acteurs privés, et s'adressent à un objet particulier aux seuls professionnels, ou aux relations de ces derniers avec les consommateurs¹. Cependant, l'analyse juridique de la résolution des litiges considère que les parties ont le choix entre résoudre leur différend à l'amiable ou aller devant un juge. C'est pourquoi, nous allons déterminer les juridictions compétentes pour trancher les litiges sur internet (Sous-section 1).

Dans son sens le plus courant, mais aussi le plus étroit, la résolution des conflits en ligne réfère à la migration, vers internet, des modes alternatifs de règlement des conflits. Notre mémoire se concentre sur la transposition, en ligne, des seuls modes amiables de règlement des différends. Cependant, nous assistons aujourd'hui à la dématérialisation des procédures judiciaires aussi. En effet, dans un monde où le nombre supplante le mot, l'introduction du numérique dans un secteur éminemment régalien présente un enjeu démocratique évident qui pose la question de la dématérialisation des procédures de résolution des litiges nés du numérique (Sous-section 2).

Sous-section 1 : Les juridictions compétentes pour trancher les litiges sur Internet.

Depuis quelques années, le droit et la justice sont confrontés au développement croissant des technologies numériques notamment en cas de litiges nés du numérique. De plus,

¹ سلطان بن ناصر بن سالم البلوشي، التحكيم في المنازعات الإلكترونية، رسالة لنيل الدكتوراه في القانون الخاص، جامعة محمد الأول، كلية العلوم القانونية والاقتصادية والاجتماعية، وجدة، السنة الجامعية 2013 – 2014، ص. 35.

en l'absence de juridiction supranationale susceptible d'être saisie par toute entreprise ou citoyenne, se pose la question de la détermination du juge national compétent pour trancher les litiges civils et commerciaux, civils ou délictuels sur internet. Nous allons traiter successivement les juridictions compétentes pour trancher les litiges civils et commerciaux sur internet (Paragraphe 1). Puis, les juridictions compétentes pour trancher les infractions pénales sur internet. (Paragraphe 2).

Paragraphe 1 : Les juridictions compétentes pour trancher les litiges civils et commerciaux sur internet.

En l'absence de juridiction supranationale susceptible d'être saisie pour tout citoyen, se pose la question de la détermination du juge national compétent pour trancher les litiges civils et commerciaux sur internet.

En matière contractuelle, le tribunal compétent est par principe le lieu du siège du défendeur ou celui où l'obligation doit être exécutée. Entre professionnels, les dispositions du contrat, selon le choix des *Incoterms*¹, relatives au lieu de livraison, seront déterminantes des juridictions compétentes. Dès lors, qu'un contrat est conclu entre des professionnels, ces derniers ont la possibilité de convenir d'une clause d'élection de for. Pourtant, il est encore fréquent qu'en cas de litige et de faute d'avoir fait entrer dans le champ contractuel la désignation du juge compétent, qu'il soit nécessaire de trancher le conflit de juridictions au moyen des règles de compétence judiciaire en matière civile et commerciale².

Le développement des communications par internet rend plus difficile la détermination du lieu où sont accomplis les actes nécessaires à la conclusion du contrat, tout en argumentant la vulnérabilité du consommateur à l'égard des offres des commerçants. Ainsi les dispositions de l'article 28 du Code de procédure civile, laisse le choix au demandeur en matière commerciale de porter son action soit devant le tribunal du domicile du défendeur, soit devant celui dans le ressort duquel l'exécution devrait être effectuée. En matière de protection du consommateur, plusieurs règles visent à protéger le consommateur, afin de permettre que le contentieux résultant d'un manquement à un contrat se déroule dans le pays où il réside et qu'il ne soit pas privé des règles protectrices dont il bénéficie par l'application de la loi de son

¹International Commercial Terms sont des termes normalisés, qui permettent dans les relations commerciales de définir les grands principes du contrat (moment du transfert de propriété, lieu de livraison etc...).

²Eric CAPRIOL, *Op.cit.*, p. 12.

pays. Toutefois, la simple accessibilité d'un site étranger ne suffit pas à justifier la compétence des juridictions du lieu ou demeure le consommateur et il convient de déterminer si l'activité du professionnel est dirigée vers le pays dans lequel réside le consommateur. Dans ce cas, le consommateur pourra bénéficier des règles de compétence propres aux contrats conclus par les consommateurs.

En matière délictuelle, l'article 28 du Code de la procédure civile donne le droit au demandeur de saisir à son choix, en matière de réparations de dommages, de porter son action soit devant le tribunal du lieu où le fait dommageable s'est produit, soit devant celui du domicile du défendeur. S'agissant du réseau internet, les règles permettant de déterminer les juridictions territorialement compétentes ont évolué. L'application des règles de conflits transposées au réseau internet fait apparaître une difficulté spécifique, relative à la notion de lieu de l'acte générateur du dommage et à celle de lieu du préjudice. En outre l'adéquation des foras compétents, tels que désignés par les règles de conflits, peut prêter à discussion à propos des cyberdélinquances. Il faut d'abord pouvoir situer le lieu de l'événement causal ou de l'acte dommageable. Certains ont soutenu que cette question est un non-sens car elle invite à rechercher un lieu géographique de commission de l'acte dans un espace réel, alors que par hypothèse le délit se situe dans le cyberspace, monde virtuel. Cette réponse ne correspond pas à la logique juridique, car l'internet n'est qu'un moyen de communication, c'est-à-dire l'instrument de réalisation ou de la commission du délit¹.

A titre de droit comparé, en France les juridictions ont dans un premier temps considéré qu'elles étaient compétentes dès que le site était accessible en France². Toutefois, le critère de la seule accessibilité revenait à reconnaître systématiquement la compétence territoriale des juridictions françaises, pour des faits litigieux ayant pour support technique le réseau internet. C'est la raison pour laquelle le critère d'accessibilité a progressivement été complété par d'autres critères tels que ceux de la destination, de l'impact économique sur le public français, du caractère actif ou passif du site, ce qui permettrait d'établir l'existence d'un

¹Ibid., p. 29.

²Ce critère avait été dégagé dans l'affaire Yahoo. Les sociétés Yahoo France et Yahoo s'étaient vu imposer de prendre des mesures destinées à prévenir la consultation par des internautes français de pages proposant à la vente des objets nazis. La société Yahoo avait fait valoir qu'il n'existait pas de solution technique lui permettant de respecter la décision du tribunal et avait soulevé une exception d'incompétence, au motif que ses services s'adressaient essentiellement à des internautes situés sur le territoire des Etats-Unis d'Amérique, que ses serveurs étaient installés sur ce même territoire et enfin qu'une mesure coercitive à son encontre ne pourrait recevoir aucune application aux Etats-Unis puisqu'elle serait en contradiction avec le premier amendement de la Constitution des Etats-Unis qui garantit à tout citoyen la liberté d'opinion et d'expression. Le tribunal a rejeté cette argumentation et s'est déclaré compétent pour connaître de cette affaire.

lien suffisant, substantiel et significatif entre les informations accessibles sur le site internet et le dommage.

Au niveau européen, la Cour de justice de l'Union européenne a 'également confirmé l'insuffisance du seul critère de l'accessibilité et la nécessité de recherche d'autres éléments pour déterminer les juridictions compétentes. Ainsi dans une affaire de la société eBay contre la société l'Oréal, la Cour de justice saisie d'une question préjudicielle a eu à se prononcer sur la question de la compétence des juridictions des Etats membres, lorsque les produits offerts à la vente par internet sont entreposés dans un pays dans lequel le propriétaire de la marque ne bénéficie par d'un droit de marque¹. La Cour de justice de l'Union européenne a ajouté qu'il incombait aux juridictions nationales « *d'apprécier au cas par cas s'il existe des indices pertinents pour conclure qu'une offre à la vente ou une publicité affichée sur une place de marché en ligne accessible sur ledit territoire est destinée à des consommateurs situés sur celui-ci* »². La Cour de justice de l'Union européenne a par la suite répondu à une question préjudicielle qui semble élargir les critères permettant aux juridictions de retenir leur compétence. Elle a énoncé dans une affaire que « *la limitation territoriale de la protection d'une marque nationale n'est pas de nature à exclure la compétence internationale des juridictions autres que celles de l'Etat membre dans lequel ladite marque est enregistrée* »³.

Paragraphe 2 : Les juridictions compétentes pour trancher les infractions pénales sur Internet.

La compétence du juge marocain se détermine en fonction d'un principe très général de territorialité. Il n'existe pas, en matière pénale, de conflit de juridictions. En effet, seuls les juges répressifs marocains ont vocation à appliquer le droit pénal marocain pour les actes répréhensibles commis sur le territoire marocain. Les juridictions répressives marocaines sont toujours compétentes pour juger les auteurs des infractions commises sur le territoire marocain. Dans une telle hypothèse, la préservation de l'ordre public implique le recours systématique aux tribunaux de l'ordre juridictionnel marocain⁴. Les articles 704 à 711 du Code de procédure pénale prévoient une compétence exclusive des juridictions répressives marocaines avec certaines nuances. Toutefois, la preuve de ce que l'infraction a été commise

¹Vincent FAUCHOUX, Pierre DEPREZ et Jean-Michel BRUGUIERE, *Op.cit.*, p. 66.

²CJUE, ch. Comm., décision n° C-324/09, 12 Juillet 2011, la société l'Oréal contre la société eBay.

³CJUE, 1^{ère} ch., décision n°C-235/10, 19 Avril 2012, Wintersteiger AG contre Products 4U Sondermaschinenbau GmbH.

⁴V. art. 704 du CPP.

au Maroc est nécessaire. Lorsque l'infraction est commise hors du Maroc, les juridictions marocaines sont compétentes si la loi pénale marocaine se déclare ou si une convention internationale donne compétence à la loi marocaine pour connaître le motif de l'infraction¹.

Par ailleurs, lorsqu'il y a dissociation entre le lieu de la réalisation matérielle de l'infraction de celui où elle produit ses effets, ce ci donne aux tribunaux marocains une très large compétence. Mais la plupart des ordres juridiques « étrangers adopte une solution identique. Il s'ensuit qu'en matière internationale, on assiste à une multiplication des lois pénales applicables et des tribunaux compétents pour réprimer une même infraction commise par la voie de l'internet. En conséquence l'auteur coupable est passible d'une multiplication des condamnations, nonobstant le principe *non bis in dem*² : la triple identité matérielle, d'objet, de parties et de cause devrait interdire de nouvelles poursuites. En effet, l'exception de l'autorité de la chose jugée au pénal n'est pas reçue sur le plan international.

Cependant, au niveau de l'Union européenne le principe est plus largement admis. Selon l'article 4 du protocole n°7 de la Convention européenne de sauvegarde des droits de l'homme ainsi que l'article 50 de la Charte européenne des droits et libertés fondamentaux font état de l'application de la règle *non bis in idem*. Mais le texte de la Charte précise que des limitations aux droits garantis par elle peuvent être prévues par la loi nationale, dans certaines conditions de nécessité et de proportionnalité³. Sur l'internet, la détermination du lieu de l'infraction pénale, du lieu du dommage ou d'établissement de l'auteur de l'infraction, permettra de qualifier l'ordre juridique compétent pour juger l'auteur de l'infraction délictuelle, voir d'une infraction criminelle⁴.

Sous-section 2 : La dématérialisation des modes de résolution de litige.

L'immixtion des technologies de l'information et de la communication dans la sphère du droit amène des évolutions majeures dans le traitement des différends en raison de la dématérialisation que celles-ci permettent : alors que les sites proposant des services en ligne d'aide à l'exercice d'une action en justice se développent, les algorithmes probabilistes exploitant la masse des décisions de justice numérisées sont en cours de développement et la dématérialisation des procédures judiciaires se poursuit. (Paragraphe 1). Ce déploiement

¹V. art. 707 à 711 du CPP.

²Nul ne peut être poursuivi ou puni pénalement à raison des mêmes faits.

³V. art. 52 de la Charte européenne des droits et libertés fondamentaux.

⁴Eric CAPRIOL, *Op.cit.*, p. 13.

d'outils numériques d'aide au traitement des litiges entre en collusion avec la promotion des modes alternatifs de règlement des différends notamment l'arbitrage en ligne (Paragraphe 2).

Dans ce contexte, nous allons s'arrêter sur l'exemple des modes alternatifs de résolution de litiges en cas de conflits entre noms de domaines (Paragraphe 3). Plusieurs Etats se montrent, en effet, soucieux d'alléger la charge du contentieux pesant sur les juridictions et encourage, ce faisant, le recours à des modes extrajudiciaires de traitement des conflits. De plus, ils incitent, au développement des modes amiables en ligne, dans le but de renforcer la confiance des consommateurs et de favoriser le développement du commerce électronique. La jonction de ces deux idées crée un contexte favorable au développement des plateformes de règlement extrajudiciaire des différends, spécialement pour le traitement des litiges e-commerce (Paragraphe 4).

Paragraphe 1 : La dématérialisation des procédures judiciaires.

L'année 2020 marque l'amorce d'un virage numérique dans le domaine judiciaire. En effet, le contexte sanitaire¹ a provoqué la fermeture partielle des tribunaux et la suspension des activités judiciaires régulières. Cette situation a ainsi forcé l'accélération de la transition de la justice vers le numérique².

Au niveau national, Le ministère de la Justice a lancé, de nouveaux services numériques sur la plateforme d'échange électronique des avocats avec les tribunaux, dans le cadre de la promotion de la transformation numérique de la justice. Ces nouveaux services, comprennent le retrait des copies électroniques des jugements ainsi que l'enregistrement des demandes de notification et des demandes d'exécution. Il est à noter que la plateforme d'échange électronique des avocats avec les tribunaux permet à ses affiliés, après inscription et ouverture de compte, de signer des articles, pièces jointes et notes de service par voie électronique, mais aussi d'enregistrer des articles, requêtes et leurs pièces jointes, et de les envoyer électroniquement. La plateforme permet également aux avocats d'accéder par voie électronique à toutes les notifications liées au dossier judiciaire, et d'enregistrer toutes les

¹Au Maroc, durant la période de Covid-19, plus 37000 audiences ont eu lieu à distance ce qui a donné lieu à plus 256 466 décisions de justice.

²P-L. DEZIEL et M-P. JOLICOEURJ, « Vers une approche synergique de la dématérialisation des dossiers judiciaires : la protection de la vie privée des justiciables comme vecteur d'accès à la justice », in IP/IT, N° 5, Mai 2021, Dalloz, p. 257.

données dans une base de données sécurisée, qui pourra être exploitée et traitée par les greffiers ultérieurement, en complément du paiement électronique des frais de justice.

En outre, le ministère de la justice a finalisé le projet de loi n°27.21 réglementant la numérisation des procédures judiciaires dans les domaines civil. Composée de cinq volets, le projet définit les domaines qui seront concernés par cette dématérialisation. Il s'agit en l'occurrence des procédures et services judiciaires civils qui seront désormais digitalisés, la tenue des audiences, les jugements, et la prise de contact des tribunaux avec les parties concernés par les affaires¹. Le texte fournit également des détails sur les modalités de recours aux enquêtes ou encore les audiences tenues à distance. Le texte prévoit également l'adoption de comptes électroniques professionnels pour les avocats, les huissiers de justice et les experts, l'utilisation de la dématérialisation des procédures pour toutes les étapes du procès public, et le traitement informatique des procès-verbaux réalisés dans le cadre des procédures civiles en imposant la signature électronique, en plus d'autres procédures. Cette démarche vise à offrir aux personnes et aux entreprises des services plus rapides, accessibles et efficaces. Néanmoins, en parallèle avec cette transformation digitale un système juridique dématérialisé doit garantir une sécurité juridique aux entreprises en termes de transparence et de confidentialité.

Au niveau international, les évolutions numériques conduisent à s'interroger sur l'avenir de la justice face à l'irruption de l'intelligence artificielle dans le processus judiciaire. On parle désormais de justice prédictive. Une justice élaborée dans le but d'améliorer la sécurité juridique des entreprises et particuliers/ Cette justice se base sur l'intelligence artificielle. C'est une technique qui consiste à interpréter la masse d'informations composée par la jurisprudence en la structurant dans le filtre logique des algorithmes et des modèles mathématiques. Ce système repose en effet essentiellement sur l'identification de récurrences et l'identification de corrélations lexicales, entre les motifs de la décision et son dispositif. Autrement dit la justice prédictive consiste en un logiciel d'anticipation des décisions de justice sur la base de l'analyse d'une grande quantité de jurisprudence.

Le Conseil de l'Europe est, la première organisation à avoir élaboré et obtenu le consensus de 47 Etats membres pour un cadre non contraignant sur l'application de

¹Y. AMRANI, « Procédures judiciaires : le projet de loi sur la numérisation revient à la case départ », consulté le 25-05-2022 à 10h sur <https://lematin.ma/express/2022/usage-moyens-technologiques-procedures-judiciaires-projet-loi-revient-case-depart/371409.html>

l'intelligence artificielle dans la justice¹ : il s'agit de la Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires², adoptée par l'assemblée plénière de la Commission européenne pour l'efficacité de la justice³. La justice prédictive se base sur la quantité d'informations et de jurisprudence disponible. Ainsi, l'*open data* qui permet un accès ouvert aux décisions de justice est le préalable nécessaire à la justice algorithmique ; mais cette ouverture ne saurait méconnaître le droit à la protection des données personnelles.

En effet, les décisions de justice sont des documents singuliers à la fois en raison de leur source, puisqu'elles proviennent d'institutions juridictionnelles, et de leur objet, dans la mesure où elles portent sur les droits de justiciables. Elles comportent donc, outre des données de nature publique, des données à caractère personnel relatives à l'ensemble des personnes impliquées. La transformation du contexte technologique et l'accès aux décisions amplifieront donc le risque de conflit avec la protection des données personnelles des personnes visées, en ce que ces nouveaux modes de communication et de traitement pourrait aboutir à la constitution d'un gigantesque casier juridique des personnes sans qu'aucun contrôle ne puisse être exercé, voire un risque de mise en péril électronique en cas d'accès à des données portant condamnations pénales, ce qui pourra nuire à la réputation de certaines entreprises.

En outre, ce mouvement de justice prédictive est un vecteur de nombreux défis pratiques. Ainsi, la mise en place de ces outils opère indéniablement une rupture avec une justice traditionnellement personnalisée et conduit à repenser le rôle du juge. L'intelligence artificielle calcule une probabilité parmi l'ensemble des situations auxquelles la machine est confrontée. Les décisions fondées sur ce calcul algorithmique peuvent faire douter dans la mesure où la justice serait alors administrée par une machine⁴. La mise en place d'un tel outil aurait également pour conséquence d'amoindrir la force décisionnelle des juges et le rôle traditionnel des avocats, qui verraient leur implication reculer au profit de l'intelligence

¹Y. MENECEUR, « Justice et intelligence artificielle : la confiance naîtra d'une réglementation internationale », in IP/IT, N° 5, Mai 2021, Dalloz, p. 250.

²Ce document composé de cinq principes et d'annexes dont une étude approfondie technique et juridique, est certainement le premier texte mondial à s'être départi de l'effet de mode de l'IA dans la justice pour y apporter une analyse pluridisciplinaire et poser une claire ligne de démarcation.

³CEPEJ, « Charte éthique européenne d'utilisation de l'intelligence artificielle dans les systèmes judiciaires et leur environnement », Strasbourg, 2018.

⁴M. CHANG, M. FABIANO, O. APOLLINE et V. VACHON, « Le traitement des décisions de justice en droit français », in IP/IT, N° 5, Mai 2021, Dalloz, p. 255.

artificielle. Le traitement des décisions se ferait au détriment des victimes¹, qui verraient leur situation litigieuse réglée par un outil d'intelligence artificielle plutôt que par le juge, être humain doté de sens et de conscience faisant craindre à ce titre une robotisation de la justice.

Si la justice prédictive entretient une sorte de mythe scientifique fondé sur l'exactitude de calculs algorithmiques, cela ne se fait pas sans dénaturation : en remplissant sa fonction prédictive, la justice perd son essence, qui est de rendre des décisions équitables et personnalisées. Le juge est également marginalisé, ses décisions se trouvant infléchies par les résultats de l'intelligence artificielle. La justice prédictive modifie ainsi l'ADN d'une justice traditionnelle et humaine. Il est donc peu certain que les justiciables aient gagné en droit avec un tel mécanisme. L'avenir nous dira si un perfectionnement de ces outils d'intelligence artificielle permettra de rendre une justice prédictive, soucieuse d'une bonne administration judiciaire ou si ces principes sont irréconciliables.

Paragraphe 2 : La pratique de l'arbitrage en ligne.

L'arbitrage est l'institution reposant sur un accord de volontés qui investit un tiers de trancher un litige². C'est donc une justice privée, d'origine conventionnelle, à laquelle des litigants choisissent de recourir, et qui offre les garanties dues par toute justice, c'est-à-dire celles du procès équitable. L'arbitrage en ligne s'entend comme tout procédé numérique ou dématérialisé, lato sensu. Cela recouvre donc aussi bien le simple échange de documents par voie électronique dans une instance arbitrale qui reste essentiellement physique, que la dématérialisation partielle avec la constitution de *data rooms* ou la dématérialisation totale dans des procédures où les arbitres et les parties ne se rencontrent plus ni même ne se parlent entre eux, voire des procédures où les arbitres sont carrément remplacés par des algorithmes générés par l'intelligence artificielle³.

Il n'y a d'ailleurs aucune corrélation entre la source du litige et son mode de résolution. Le litige peut être né en ligne et être résolu par un mode classique ou, inversement,

¹Aux Etats-Unis, de nombreuses juridictions font appel à l'algorithme COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), outil d'IA utilisé par les juges afin d'évaluer le risque de récidive des personnes jugées et, in fine, de fixer le quantum de la peine. Or, il a été démontré que COMPAS comportait des biais discriminatoires, la probabilité calculée de récidive étant plus élevée pour une personne afro-américaine.

²Jean-Baptiste RACINE, Droit de l'arbitrage, PUF, 1^{ère} éd., Paris, 2016, p. 340.

³J. El AHDAB et M. MAKOU, « Arbitrage international versus intelligence artificielle », in Revue Droit et Affaires, 2018, p. 49.

être né hors ligne et résolu en ligne. La nature numérique de l'arbitrage n'est pas liée à l'origine du litige : seul le mode en ligne de résolution du litige importe ici. L'arbitrage en ligne présente des enjeux que nous résumons en deux catégories ; les enjeux juridiques et les enjeux économiques.

Les enjeux juridiques, premièrement, consistent à éprouver la robustesse des concepts pour savoir s'ils résistent à la vague numérique. A priori, si le concept d'arbitrage est robuste et résiste à la forme numérique qu'il peut emprunter, certains concepts dans l'arbitrage, eux, doivent s'adapter. Ainsi en est-il, par exemple, de l'exigence d'écrit pour la convention d'arbitrage interne. Cette condition doit être remplie, quand bien même l'écrit n'existerait que sous forme électronique. Sur ce point, le D.O.C admet d'ailleurs déjà l'écrit électronique au même titre de l'écrit papier, même quand il est exigé pour la validité de l'acte¹. Or, ces notions d'original et de copie sont inadaptées à l'arbitrage en ligne qui peut ne générer ni original ni copie dès lors que les documents n'existent que sous forme électronique. Il faut donc adapter les concepts, et même les règles, pour prendre en compte l'arbitrage en ligne. C'est d'ailleurs ce que prévoit la nouvelle loi 95-17 relative à l'arbitrage et la médiation conventionnelle.

Outre les aspects juridiques l'arbitrage en ligne emporte aussi, des enjeux économiques. L'appétence pour le numérique et la dématérialisation est telle que la quête d'un nouveau modèle économique pour la justice est lancée, dont l'un des mérites, et non des moindres, est aussi un progrès écologique : moins de déplacements, moins de papier, malgré, peut-être, plus de procès. L'arbitrage en ligne attire des acteurs économiques qui y voient une source de profits. Tout est donc réuni pour que l'arbitrage en ligne se développe de manière exponentielle².

Au niveau national, une nouvelle loi vient d'être adoptée en 2022, il s'agit de la loi 95-17 relative à l'arbitrage et la médiation conventionnelle. Le nouveau dispositif juridique vient modifier les dispositions applicables à l'arbitrage et la médiation conventionnelle. En effet, la loi 95-17 traite de l'arbitrage en ligne autrement dit, elle prend en compte les avancées technologiques pour permettre tant la conclusion de la convention d'arbitrage, que les échanges de requêtes et mémoires par voie électronique ou la possibilité

¹Arania Jعفر، فعالية التحكيم الإلكتروني في تسوية النزاعات الناشئة عن التجارة الإلكترونية، مجلة القانون والأعمال الدولية، ع. 29، أكتوبر 2020، ص. 331.

²Commission Ad hoc, « L'arbitrage en ligne », Rapport du Club des juristes, Paris, Avril 2019.

de rendre les sentences arbitrales par le même biais, ainsi que la tenue de réunions et audiences par visioconférence¹.

Au niveau international, le Maroc a ratifié la Convention de *New York* pour la reconnaissance et l'exécution des sentences arbitrales étrangères de 1958 qui trouve, pour l'arbitrage en ligne, un intérêt particulier. Sur diverses questions, notamment eu égard au consentement des parties à l'arbitrage ou au contrôle et de l'exécution de sentences arbitrales, cette convention est de nature à prévaloir sur le droit national en cas d'arbitrage international. Or, le caractère désormais électronique de la procédure d'arbitrage en ligne met à l'épreuve la compatibilité de ce texte avec les nouveaux enjeux techniques des procédures dématérialisées.

Plusieurs organismes internationaux promeuvent l'arbitrage international comme méthode privilégiée de résolution de conflits du commerce international². C'est le cas de la Commission des Nations unies pour le Droit Commercial International (CNUDCI), l'*International Council for Commercial Arbitration* (ICCA) et l'*International Bar Association* (IBA). Dans le cadre de cette promotion, ces organismes produisent des régulations de droit souple qui servent de lignes directrices pour les procédures arbitrales. La loi type de la CNUDCI sur l'arbitrage commercial international de 1985 et sa version amendée de 2006 peuvent ainsi servir de modèle à tout type de procédure arbitrale si les parties en font le choix. La CNUDCI a également publié une loi type de signature électronique en 2001 pouvant servir notamment de référence sur des questions liées à la dématérialisation de procédures, telle que le consentement de parties à l'arbitrage. Enfin, se trouvent les *IBA Rules on the Taking of Evidence in International Arbitration* de 2010, complétées par le *IBA Guide to Good Practice on the Use of Video-Links Under the Evidence Convention*³, qui ont vocation à englober l'arbitrage en ligne.

À l'heure actuelle, aucune autre source interne n'est de nature à réglementer directement l'arbitrage en ligne⁴. Au niveau international, il n'y a de même pas de convention

¹Z. NACIRI-BENNAN, « La loi marocain 95-17 sur l'arbitrage et la médiation conventionnelle », consulté le 06-08-2022 à 10h sur <https://www.village-justice.com/articles/loi-marocaine-sur-arbitrage-mediation-conventionnelle,43044.html>

²Lors d'une conférence du 1er décembre 2020, la CCI a annoncé qu'elle lançait une nouvelle plateforme de gestion des affaires en ligne et mettait en place un réseau d'échange pour chaque affaire, afin d'encourager le dépôt des mémoires et communications écrites ultérieures par voie électronique plutôt qu'en version papier.

³IBA Rules on the Taking of Evidence in International Arbitration, 17 Décembre 2020.

⁴Pour ce qui est du droit souple, diverses sources ont abordé la question, de manière éparse. La Chambre de commerce internationale de Paris a notamment constitué l'ICC Commission on Arbitration and ADR's Task Force on the Use of Information Technology in International Arbitration. Cette commission s'est occupée de la

ni de jurisprudence traitant directement de l'arbitrage en ligne. L'arbitrage en ligne, s'il n'est aujourd'hui pas prévu explicitement par les textes, existe en réalité d'ores et déjà, bien que cette réalité soit encore modeste. En effet, il n'est pas une réelle nouveauté. Il existe depuis de nombreuses années comme peuvent en témoigner quelques acteurs. Parmi ces acteurs, on retrouve l'Organisation Mondiale de la Propriété Intellectuelle (OMPI), l'une des pionnières de cette pratique, et la Chambre de Commerce Internationale (CCI).

Le Centre d'arbitrage et de médiation de l'OMPI a mis au point un système de règlement des litiges en ligne, utilisant l'Internet. On peut accéder à ce mécanisme de règlement en ligne et obtenir tous les renseignements utiles. Grâce aux outils de communication numériques, les parties pourront déposer leur demande en remplissant un formulaire électronique, et communiquer des pièces et échanger de la correspondance, en ligne, par des voies de communication sécurisées. Ainsi, les parties, les arbitres et le centre communiqueront par voie électronique, tout en gardant la possibilité d'utiliser les moyens de communication audio et vidéo existants. Le mécanisme de l'OMPI comportera un système de notification automatique, ainsi que des bases de données pour l'enregistrement et l'archivage des documents. Les transactions financières qui seront effectuées pendant le cours de la procédure, notamment le paiement en ligne par carte de crédit, utiliseront des bases de données financières spéciales¹.

L'OMPI met donc en œuvre une procédure mixte d'arbitrage en ligne, permettant également d'utiliser certains atouts de l'arbitrage en ligne, couplés avec des éléments de procédure arbitrale plus classique. Néanmoins, l'OMPI pousse la réflexion plus loin sur la place de la machine dans la prise de décision quant aux dossiers traités, travaillant à ce qu'un algorithme puisse répondre de manière autonome. L'OMPI n'est pas la seule institution à recourir aux procédés en ligne. C'est aussi le cas de la Chambre de commerce internationale. Pour sa part, après la suppression en 2002 de *Netcase*², sa plateforme d'arbitrage en ligne pour la résolution de petits litiges, la CCI aborde la question de l'arbitrage en ligne de façon très limitée.

question de la dématérialisation de l'arbitrage dans ce centre et a publié deux rapports en 2004 et 2017 sur l'utilisation de technologies de l'information dans l'arbitrage international.

¹« Arbitrage en ligne », consulté le 06-08-2022 à 14h <https://www.wipo.int/amc/fr/arbitration/online/index.html>

²La CCI a créé au début des années 2000 la plateforme d'arbitrage en ligne Netcase. L'expérience a cependant pris fin assez rapidement.

La CCI propose une offre mixte, comme dans certains cas pour l'OMPI. Elle va ainsi mêler la procédure traditionnelle de l'arbitrage avec les nouvelles technologies, tout en l'adaptant à ces nouvelles possibilités, mais de façon assez restreinte. En effet, il suffit de s'intéresser au règlement d'arbitrage applicable lors de tout arbitrage devant la CCI pour voir que la question n'y est traitée que très partiellement. Il n'y est même fait référence qu'une seule fois, dans l'appendice IV du règlement¹ abordant les techniques de gestion de la procédure².

Une autre catégorie d'acteur regroupe les nouveaux opérateurs constitués sous forme de start-up de la *Legaltech*³. Ces entreprises offrent des services d'arbitrage en ligne avec pour objectif la dématérialisation la plus complète possible des procédures, laquelle est censée entraîner une baisse des coûts et une célérité accrue. La part donnée à la machine et à l'intelligence artificielle par ces nouveaux acteurs est donc plus forte. Les outils numériques facilitent d'ores et déjà la rédaction de la sentence. Celle-ci doit mentionner des éléments tels que l'identification des parties, de leurs conseils et des arbitres, les faits, le déroulement de la procédure, les moyens et prétentions des parties. Il suffit désormais de puiser ces éléments dans les mémoires et les pièces échangées par voie numérique lors de la procédure. Plus innovants, des logiciels de reconnaissance vocale permettent de transcrire par écrit en un temps record les échanges oraux ayant lieu devant le tribunal. Les algorithmes savent également lire et classer les bases de données, notamment jurisprudentielles, et peuvent ainsi servir à sélectionner les précédents pertinents, avec toujours la limite tenant au faible nombre de sentences arbitrales publiées. Cependant, si l'intelligence artificielle peut, constituer une aide précieuse à la décision, elle doit rester sous contrôle. Laisser le soin à une intelligence non humaine de trancher les différends contribuerait à augmenter une méfiance. De plus, l'assistance de l'intelligence artificielle dans la prise de décision ne doit pas permettre au tribunal de se soustraire à son obligation de motivation.

L'arbitrage en ligne apparaît aujourd'hui comme une réalité modeste. S'il est important de promouvoir l'utilisation des outils numériques dans la conduite de l'arbitrage, il n'est pas souhaitable que l'intelligence artificielle puisse se substituer totalement à l'humain

¹Règlement d'arbitrage de la CCI, applicable au 1er mars 2017.

²Dans ce document, la CCI offre la possibilité aux parties et au tribunal arbitral, dans une optique de bonne administration des coûts de la procédure, de recourir aux technologies de l'information et d'échanger des communications en ligne, entre elles, avec le tribunal arbitral ou avec le Secrétariat.

³C'est l'exemple de FastArbitre ou eJust.

dès lors qu'il s'agit de rendre une décision contraignante. Les technologies numériques peuvent constituer une aide précieuse dans l'organisation de la procédure, mais elles ne devraient avoir qu'une incidence limitée pour ce qui est de l'élaboration de la sentence, tâche qui devrait relever à titre principal de l'intelligence humaine. En d'autres termes, il importe que l'arbitrage assisté par la machine ne dégénère pas en un arbitrage réalisé par la machine.

Paragraphe 3 : Les procédures alternatives de résolution des conflits en matière de nom de domaine.

Depuis plusieurs années maintenant, les décisions judiciaires relatives aux noms de domaine se font plus rares. Concomitamment, la plupart des conflits entre noms de domaine et marques sont le plus souvent réglés en ayant recours aux méthodes alternatives de résolution des conflits. Il s'agit de procédures autres qu'étatiques qui permettent de trancher les conflits. Ces procédures présentent l'avantage d'être transnationaux, rapides, peu coûteuses, et peuvent se dérouler entièrement en ligne. On évoquera ici trois mécanismes ; la procédure *UDRP* à savoir l'*Uniform Dispute Resolution Policy* (I), la procédure *Uniform Rapid Enslion (URS)* (II), et la procédure relative aux noms de domaine «.ma » (III).

I- Le Règlement Uniforme des Litiges relatifs aux Noms de Domaines (UDRP).

Les principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine ont été adoptés par l'ICANN le 26 Aout 1999 et les règles d'application sont entrées en vigueur le 24 Octobre 1999. Il s'agit d'une procédure au champ d'application assez restrictif puisqu'elle ne concerne que la résolution des conflits entre les titulaires de noms de domaine et les propriétaires de marques. Ces règles s'imposent aux *registrars* agréés par l'ICANN qui doivent exécuter la décision rendue dans le cadre de l'UDRP et aux titulaires de noms de domaine qui s'engagent à se soumettre à la procédure UDRP et aux Centres d'arbitrage habilités par l'ICANN pour administrer les litiges UDRP et qui sont : L'*Asian Domain Name Dispute Resolution Center*, le *National Arbitration Forum*, le Centre d'arbitrage et de médiation de l'OMPI principal acteur des procédures UDRP et enfin, le *Czech Arbitration Court Arbitration Center for Internet Disputes*.

Toute personne qui réserve un nom de domaine s'engage lors de l'enregistrement de celui-ci, à se soumettre à la procédure UDRP dans le cas où son nom de domaine entrerait en conflit avec la marque ou un autre signe distinctif d'un tiers. Toutefois, le recours à une

procédure judiciaire n'est pas exclu puisqu'à tout moment, les parties peuvent choisir de soumettre leur litige à un juge, notamment pour obtenir des dommages et intérêts¹. Le recours à la procédure UDRP a été dans un premier temps réservé aux noms de domaines enregistrés sous les *gTLDs*. Il a été étendu en 2005 aux noms de domaines enregistrés sous les *ccTLD* de nombreux pays. Dans tous les cas, le paragraphe 4 de l'UDRP impose au requérant de prouver, contre le défendeur, cumulativement, que trois conditions sont remplies : un risque de confusion, une absence d'intérêt légitime et la mauvaise foi. Ces trois conditions, qui s'appliquent cumulativement, appellent plusieurs remarques².

D'abord la première condition qui consiste à démontrer que le nom de domaine est identique ou semblable au point de prêter à confusion avec une marque de produits ou services sur laquelle il a des droits. En premier lieu, le champ d'application de la procédure UDRP, limité selon les principes directeurs aux marques antérieures a été élargi par la jurisprudence de l'OMPI. Ont ainsi été admises les actions de titulaires de patronymes ou de noms commerciaux qui avaient été enregistrés comme noms de domaine par des cybersquatteurs ; de même, des noms de villes se sont vu protéger. Tous ces signes ont été qualifiés de marques d'usage ce qui a permis leur protection. En deuxième lieu, les droits du demandeur sur sa marque sont établis par la production de justificatifs. En aucun cas les instances UDRP n'ont compétence pour se prononcer sur la validité des marques. Seuls les juges nationaux peuvent procéder à une telle appréciation. En troisième lieu, la première condition permet de sanctionner non seulement la reproduction servile de marque, mais également les cas de *typosquatting*.

Parfois, la protection de la marque est écartée lorsque ce n'est pas le demandeur qui est titulaire des droits sur la marque invoquée. Par exemple, dans l'affaire « e-coleau.org », le panel d'experts désigné par l'OMPI a rejeté la plainte introduite par la requérante qui invoquait la marque e-Soleau, initialement enregistrée au nom de son gérant et cédée à son profit par acte sous seing privée. Il a considéré qu'elle ne pouvait invoquer de droit sur cette marque, l'acte de cession intervenu entre le gérant et la société requérante ne respectant pas les dispositions impératives du Code de la propriété intellectuelle selon lesquelles toute

¹L'article 4 des principes directeurs régissant le règlement uniforme des litiges relatifs aux noms de domaine dispose que : « la procédure administrative obligatoire (...) ne vous interdit pas, non plus qu'elle n'interdit au requérant, de porter le litige devant un tribunal compétent appelé à statuer indépendamment avant l'ouverture de cette procédure administrative obligatoire ou après sa clôture, etc ».

²Christiane FERAL-SCHUHL, *Op.cit.*, p. 1059.

transmission ou modification des droits attachés à une marque enregistrée doit pour être opposable aux tiers, être inscrite au registre national des marques¹.

Ensuite, la deuxième condition impose au requérant de montrer que le titulaire du nom de domaine n'avait aucun droit sur ce nom ni aucun intérêt légitime qui s'y attache. Le plus souvent, il appartiendra au titulaire du nom de domaine litigieux de démontrer qu'il a enregistré celui-ci dans le but de l'exploiter ou qu'il l'exploite effectivement dans le cadre d'une offre de bonne foi des produits ou services. Enfin, la troisième condition oblige au requérant de montrer que le nom a été enregistré et utilisé de mauvaise foi². L'article 4.b des UDRP apporte des précisions sur la notion de mauvaise foi, considérant que celle-ci est établie lorsque le nom de domaine a été enregistré, aux fins d'être revendu, ou en vue d'empêcher le propriétaire de la marque correspondante de l'enregistrer, et que le titulaire est engagé dans ce type de pratique é titre habituel, ou en vue de perturber les opérations commerciales d'un concurrent, ou en vue d'attirer à des fins lucratives, les utilisateurs de l'internet sur un site en créant une probabilité de confusion avec la marque du requérant. Cette preuve a pu être établie à de nombreuses reprises : lorsque le nom de domaine évoque une marque ou une personne connue, ou lorsque le déposant a multiplié les réservations douteuses de noms de domaine, ou encore lorsque le nom de domaine litigieux est redirigé vers le site d'un concurrent, ou enfin lorsqu'il y a absence totale d'un usage du nom de domaine.

Quant aux règles de procédure, chaque organisme accrédité peut appliquer ses propres règles de procédure, à la condition toutefois que celles-ci ne soient pas contraires aux principes de l'UDRP. En conséquence, la procédure à suivre devant chaque organisme est quasi-similaire : le conflit est en principe tranché par un expert rendues publique ; les taxes et honoraires dus en cas d'expert unique sont à la charge du demandeur, les parties peuvent toutefois demander à ce que le litige soit tranché par une formation collégiale constituée de trois experts, ces experts sont soumis à une obligation de déclaration d'impartialité et d'indépendance et disposent de pouvoirs propres d'investigation très étendus. La langue de

¹OMPI (Centre d'arbitrage et de médiation), décision n°D2007-1760, 28 Février 2008, Vente-Privee.com contre Mawuna Koutonin.

²Dans certains cas, cependant, la mauvaise foi a été écartée, à l'exemple de la décision du 26 Mai 2006 qui a retenu que la société française Jet Tour ne rapportait pas la preuve de la mauvaise foi de la société coréenne qui exploitait une page web comportant de nombreuses publicités accessibles à l'adresse « jettours.com » OMP (Centre d'arbitrage et de médiation), décision n° D 2006-0250, 26 Mai 2006, Jet Tour contre Société coréenne.

procédure est celle du contrat d'enregistrement du nom de domaine, sauf autre accord des parties ou mention particulière dans le contrat d'enregistrement ; la procédure dure environ 60 jours, l'intimé bénéficiant d'un délai de 20 jours à compter de la notification de la requête du plaignant pour présenter son mémoire en défense. Le Centre d'arbitrage et de médiation de l'OMPI a proposé, fin 2008, de dématérialiser entièrement les procédures UDRP considérant que cela ne préjudicierait pas aux parties, que cela leur profiterait en termes de couts et de temps, tout en préservant l'environnement. Depuis le 1^{er} Mars 2010, toutes les plaintes et réponses UDRP doivent être déposées au format électronique, y compris toutes les annexes.

Les décisions qui peuvent être prononcées par ces organismes d'arbitrage sont de trois types soit en faveur du requérant avec injonction de transférer le nom de domaine en litige à son profit, soit en faveur du requérant avec injonction de retrait du nom de domaine en litige soit en faveur du défendeur. Contrairement aux procédures judiciaires, elle ne permet pas d'obtenir des dommages-intérêts, comme le précise le point 4, i), des principes directeurs UDRP¹. La décision est notifiée aux parties, à l'ICANN et au *registrar* concerné. Elle est également publiée sur le site du centre d'arbitrage. Le *registrar* est tenu d'exécuter cette décision dans les 10 jours de la notification, sauf si la juridiction judiciaire est saisie de l'affaire, à l'initiative de l'une quelconque des parties au litige.

En effet, rien n'empêche les parties à une procédure UDRP de saisir un tribunal étatique de leur litige, soit pendant que la procédure est en cours, soit une fois qu'elle est terminée. Le point 4, k), des principes directeurs UDRP le prévoit expressément. L'expert UDRP peut même, aux termes des règles d'application, suspendre ou clôturer la procédure UDRP lorsque le nom de domaine en cause fait également l'objet d'une procédure judiciaire. Toutefois, il faut noter qu'il s'agit de procédures distinctes, et non pas d'appel ou de recours contre les décisions UDRP². En effet, les décisions UDRP ne peuvent être annulées par les tribunaux. En revanche, ces derniers peuvent connaître des mêmes affaires. Dans ce cas, si la décision UDRP a ordonné le transfert du nom de domaine, le tribunal devra toutefois prendre en compte cet élément factuel.

L'inconvénient de cette indépendance des procédures est que les décisions risquent de mener à des résultats différents, comme dans l'affaire pneuonline, dans laquelle l'OMPI avait

¹« Questions fréquemment posées : noms de domaine de l'Internet », consulté le 02-02-2022 à 10h sur <https://www.wipo.int/amc/fr/center/faq/domains.html>

²Luc GRYNBAUM, Caroline LE GOFFIC et Lydia MORLET-HAIDARA, *Op.cit.*, p. 697.

rejeté la demande de transfert des noms de domaine « pneuonline.com », « pneusonline.com » et « pneu-online.com », au motif de la non-distinctivité de la marque antérieure Pneu-Online, et les tribunaux français ont au contraire jugé la marque distinctive et ont prononcé une interdiction d'utilisation des noms de domaine en cause dans le domaine des pneumatiques¹. Les divergences sont d'autant plus envisageables que les règles appliquées dans le cadre des procédures UDRP diffèrent du droit national.

II- La procédure *Uniform Rapid Suspension System* (URS).

L'URS, procédure novatrice et alternative de suspension, uniquement dédiée aux nouvelles extensions, doit permettre de lutter a posteriori contre les atteintes manifestement illicites à des droits antérieurs établis, avant tout débat sur le fond. Elle présente l'avantage de sa rapidité, moins d'un mois, et son faible coût en comparaison avec la procédure classique UDRP. La procédure URS ne permet en effet que la suspension du nom de domaine litigieux. Elle n'autorise ni sa radiation ni son transfert au titulaire légitime qui devra attendre la fin de cette suspension pour le réserver à son nom, avec les risques que comporte l'observation de ce délai².

La plainte qui peut être déclencher par tout titulaire alerté de l'enregistrement d'un nom de domaine identique à sa marque, doit être déposée sous forme électronique devant l'un des centres d'arbitrage sélectionnés par l'ICANN et rapporter les mêmes preuves citées précédemment à savoir : la preuve de l'usage de la marque sur laquelle est fondé le recours, l'identité ou la similarité, le risque de confusion du nom de domaine avec la marque antérieure et enfin, l'absence d'intérêt légitime du réservataire et sa mauvaise foi.

L'analyse des premières décisions rendues par le National Arbitration Forum³, l'un des centres d'arbitrage habilité, fait apparaître l'importance que revêt la preuve de la mauvaise foi. Une grande majorité des plaintes rejetées le sont sur l'absence de ce critère, dont les contours, plus étroits que dans la procédure UDRP, se dégagent peu à peu des premières décisions. Ainsi, le commerce de noms de domaine pour le profit ou la détention d'un large portefeuille ne sont pas, en eux-mêmes des indices de mauvaise foi, seul l'abus

¹C. Cass., Civile, ch. Com., décision n° 08-16.752, 9 Mars 2010, la Société Delticom contre les Sociétés Pneus Online Suisse et Pneus Online France.

²L. BALLET, « Nouvelles extensions et insécurité juridique », in IP/IT, N° 2, Février 2016, Dalloz, p. 75.

³« Système de suspension rapide uniforme », consulté le 01-04-2022 à 9h sur www.adrforum.com

étant susceptible *in concreto* des circonstances, notamment la volonté de revente à un prix excédant les coûts directement liés au nom.

De manière générale, il semble inutile de choisir la voie de la plainte URS dans le cas où le nom de domaine litigieux ne fait l'objet d'aucune exploitation réelle. Dans cette hypothèse, la nécessité de procéder à la preuve, négative, de l'absence d'intérêt légitime de la part du réservataire est, en effet, particulièrement ardue face à l'indélicatesse, par nature, de ce dernier. La société *Netflix* en a fait l'amère expérience en perdant coup sur coup deux noms pour lesquels il était argué, sans la réalité d'aucun site web hébergé à l'une ou l'autre de ces adresses, d'intentions louables et non commerciales. Impossible de suspendre un nom de domaine sans existence tangible, impossible de qualifier la mauvaise foi par la détention passive d'un nom de domaine, a tranché l'examineur¹. Il y a donc un vrai choix à opérer, au regard de l'importance de l'atteinte et des enjeux financiers et commerciaux, entre les procédures URS et UDRP.

III- La Procédure Alternative de Règlement des Litiges pour le « .ma » (PARL).

Il s'agit d'une procédure extrajudiciaire, administrée par le Centre d'Arbitrage et de Médiation de l'Organisation Mondiale de la Propriété Intellectuelle (OMPI). Elle s'applique à tous les noms de domaine «.ma» enregistrés. La PARL s'applique uniquement aux litiges relatifs aux noms de domaine «.ma» ayant trait aux marques de fabrique, de commerce ou de service protégées au Maroc, entre un titulaire et une personne tierce, c'est ce qui découle de l'article 45 de la décision prise par l'ANRT en 2014. Selon le Règlement sur la Procédure alternative de résolution de litiges du domaine «.ma », il suffit de prouver l'enregistrement ou l'utilisation du nom de domaine de mauvaise foi, tandis que selon les Principes UDRP il est nécessaire de prouver ces deux éléments cumulativement.

Dans le cadre de cette procédure un expert unique est nommé par le Centre de l'OMPI pour rendre une décision. Contrairement à la formation collégiale prévue par l'UDRP². Il faut noter que cette procédure alternative de règlement de litige ne concerne que les litiges relatifs à l'enregistrement des noms de domaine entre un titulaire et un tiers et ne vise en aucun cas les litiges relatifs à la responsabilité de l'ANRT et des prestataires. Le nom de domaine objet du litige reste gelé pendant le déroulement de la procédure alternative de résolution des

¹« Décision en nom de domaine », consulté le 01-04-2022 à 11h sur www.adrforum.com/domainesecisions

²« Service de l'OMPI pour le règlement des litiges pour le domaine .MA », consulté le 01-04-2022 à 16h sur <https://www.wipo.int/amc/fr/domains/cctld/ma/index.html>

litiges. Le Registre exécutera la décision de l'expert de transférer ou de supprimer le nom de domaine litigieux après un délai de trente 30 jours, par opposition à 10 jours ouvrables selon les principes UDRP, si le registre ne reçoit pas un document attestant qu'un tribunal marocain a été saisi d'une procédure¹.

En effet, la PARL ne fait pas obstacle à la saisine d'un tribunal compétent pour le même litige, avant, pendant ou après cette procédure. Dans ce cas, la décision définitive prise par ledit tribunal sera appliquée. L'ANRT n'intervient pas dans une PARL mise en œuvre, et elle n'est pas responsable des décisions rendues. Néanmoins, elle est tenue de fournir toute information en leur possession sur le titulaire du ou des noms de domaine objet du litige à la demande du centre d'arbitrage.

De plus, l'ANRT peut recevoir et traiter les plaintes concernant les noms de domaines mais dans des cas précisés dans l'article 44 de la décision qui portent sur la contestation de l'enregistrement d'un nom de domaine ayant trait à un terme figurant sur la liste des termes réservés ou encore la contestation relative au nom du titulaire d'un nom de domaine tel que figurant sur la base de données WHOIS. Dans ce cas l'ANRT statue sur la plainte dans un délai ne passant pas deux mois à compter de la date de réception de ladite plainte sauf circonstances exceptionnelles².

Paragraphe 4: Les plateformes du règlement amiable des différends.

Les contrats conclus en ligne génèrent des différends portant souvent sur de faibles montants, pour lesquels les voies classiques de traitement des litiges sont inadaptées. Le recours à des modes amiables de règlement des conflits permet un traitement rapide, peu onéreux de ces litiges et, lorsque ceux-ci sont des différends transfrontaliers, leur règlement extrajudiciaire permet d'éviter les conflits de lois et de juridictions qu'ils pourraient soulever. Quant à la difficulté liée à la distance géographique pouvant séparer les parties au litige, elle trouve sa solution dans le recours au même medium que celui qui a été employé pour conclure le contrat à l'origine du différend, à savoir l'internet. C'est d'ailleurs vers le règlement en ligne des différends que ce sont naturellement orientés des acteurs importants du commerce électronique. C'est par exemple, le cas d'eBay qui a eu recours à la plateforme *SquareTrade*

¹V. art. 46 de la décision ANRT/DG/N°12/14 du 21 Novembre 2014 relative aux modalités de gestion administrative, technique et commerciale des noms de domaine Internet «.ma».

²V. art. 44 de la décision ANRT/DG/N°12/14 du 21 Novembre 2014 relative aux modalités de gestion administrative, technique et commerciale des noms de domaine Internet «.ma».

pour résoudre à l'amiable les conflits entre utilisateurs, avant que ce site d'enchères ne crée son propre gestionnaire de litiges¹. Entre 1999 et 2008, la plateforme a traité, en cinq langues, deux millions de conflits impliquant des utilisateurs issus de 120 pays.

Le développement du règlement en ligne des litiges est aujourd'hui encouragé, en premier lieu par l'Union européenne qui a pris l'initiative de créer et d'administrer elle-même en 2016 une plateforme de règlement en ligne des litiges du e-commerce entre consommateur et professionnel². Le soutien apporté au développement des plateformes de règlement amiable des différends émane également de la Commission des Nations Unies pour le droit commercial international. Au terme d'une réflexion de six années, la CNUDCI a adopté en 2016 des Notes techniques sur le règlement des litiges en ligne visant spécifiquement les conflits découlant de contrats internationaux de vente ou de service qui portent sur de faibles montants et sont conclus au moyen de communications électroniques³. Il s'agit d'un descriptif non contraignant qui formule des préconisations relatives au processus de règlement des litiges en ligne, ayant pour objet de favoriser leur développement.

Les modes alternatifs de résolution des conflits ne faisant l'objet d'aucun monopole, les initiatives des *startups* dans ce domaine sont moins contraintes que lorsque celles-ci souhaitent s'aventurer sur le terrain des actions judiciaires. Ces plateformes développent des modèles divers, avec des degrés variables de digitalisation de la gestion du différend et une mobilisation plus ou moins poussée de l'intelligence artificielle. Les plateformes de règlement amiable des litiges proposent des niveaux plus ou moins élevés de dématérialisation de la procédure, la prise en charge technologique du traitement du différend peut aller de la simple demande en ligne jusqu'à la négociation automatisée d'une solution amiable.

La dématérialisation touche, en premier lieu, la demande de règlement extrajudiciaire du différend. Il s'agit alors de faciliter le recours à un médiateur en permettant de formuler une demande en ligne. Ainsi, en Europe les plateformes de règlement en ligne des litiges de consommation permettent aux consommateurs de déposer une demande en remplissant un formulaire de plainte électronique, en y joignant les pièces pertinentes. La plateforme transmet la plainte au défendeur, il appartient ensuite aux parties de choisir une entité de règlement

¹« Resolution Center eBay », consulté le 02-04-2022 à 10h sur <http://resolutioncenter.ebay.fr/>

²Règlement (UE) N°524/2013 du parlement européen et du conseil du 21 mai 2013 relatif au règlement en ligne des litiges de consommation et modifiant le règlement (CE) n°2006/2004 et la directive 2009/22/CE (règlement relatif au RLLC).

³CNUDCI, « Notes techniques sur le règlement des litiges en ligne » Nations Unies, New York, Mai 2017.

extrajudiciaire des litiges parmi celles sélectionnées par les Etats membres et répertoriées sur le site. La plateforme propose également, gratuitement, un outil de gestion électronique des dossiers permettant de développer la procédure amiable par l'intermédiaire de ce site¹.

Au-delà de la formulation en ligne de la demande, le numérique peut également être utilisées pendant le processus de règlement du différend. Les plateformes peuvent proposer un traitement entièrement dématérialisé du différend en ouvrant un espace privé de discussion en ligne. Ce sont également des modes hybrides qui peuvent être choisis mêlant présentiel et échanges à distance². Les échanges en ligne doivent naturellement être sécurisées et bénéficier d'une protection des données. La Commission des Nations Unies pour le droit commercial international préconise que « *toutes les communications effectuées au cours d'une procédure de règlement des litiges en ligne se fassent par l'intermédiaire de la plateforme* »³. Ces outils de communication sont utilisés durant les différentes phases du processus de résolution en ligne des litiges. Les Notes techniques de la CNUDCI identifient trois étapes qui correspondent au modèle retenu par de nombreuses plateformes : une première étape de négociation menée entre les parties par l'intermédiaire de la plateforme de règlement des litiges en ligne, puis une deuxième étape de règlement assisté ,qui s'ouvre en cas d'échec de la première, pendant laquelle un tiers neutre est désigné et communique avec les parties pour tenter de parvenir à un accord. Les Notes techniques de la CNUDCI mentionnent une dernière étape sur laquelle, faute de consensus, elles restent beaucoup plus vagues qui interviendrait en cas d'échec du règlement assisté, le tiers devant informer les parties des options susceptibles d'être choisies⁴.

Les différentes expériences de règlement des litiges en ligne sont caractérisées par l'intervention d'une plateforme –intermédiaire technologique- qui met à la disposition des parties et du tiers neutre une application permettant de créer des données, de les transmettre et d'en assurer la conservation de manière sécurisée. Des plateformes développées proposent des

¹S. CHASSAGNARD-PINET, « Le e-règlement amiable des différends », in IP/IT, N° 10 Octobre, 2017, Dalloz, p. 508.

²Le site Mediation.fr propose par exemple à celui qui initie la médiation en ligne, d'adopter une médiation à distance (par mail, téléphone ou visioconférence) ou pour une médiation présentielle.

³CNUDCI, « Notes techniques sur le règlement des litiges en ligne » Nations Unies, New York, Mai 2017, Section 3.

⁴Ce mode de règlement en ligne des litiges est proche de celui proposé par l'application ECODIR (Electronic Consumer Dispute Resolution) ouvert en 2001 à l'initiative, de la Commission européenne pour résoudre les conflits de la consommation en ligne. C'est un modèle similaire qui a également été utilisé par la plateforme SquareTrade, avec beaucoup plus de succès, pour résoudre les litiges entre utilisateurs du site d'enchères eBay.

méthodes de traitement des litiges utilisant un algorithme de négociation automatisée. Un premier type d'application permet de régler des litiges simples portant sur le paiement d'une créance. Les parties du différend saisissent sur la plateforme pour l'un sa demande, pour l'autre son offre, sans que ces données soient communiquées à la partie adverse¹. Si la marge différentielle entre les deux offres ne dépasse pas un pourcentage préalablement fixé. Souvent autour de 30%, l'algorithme calcule un montant médian susceptible de recueillir un accord des parties². Certains sites assurent des résolutions de différends plus complexes pouvant inclure plusieurs parties et plusieurs demandes³.

Sous l'expression de règlement en ligne des litiges, ce sont donc des services très variés qui sont proposés aux parties à un différend. Cette variété de modèles fait écho à la diversité des acteurs qui en sont les promoteurs. En effet, si les startups de la *legaltech* investissent le champ du règlement amiable des différends, elles ne sont pas les seules à vouloir prendre part au développement de ce marché. Les initiatives en matière de dématérialisation du règlement amiable des litiges également recherchées par les entreprises du secteur bancaire, c'est le cas du centre marocain de médiation bancaire⁴. Ce dernier gère le dispositif de médiation bancaire destiné au règlement à l'amiable des différends nés ou pouvant naître entre les établissements de crédit et leurs clients⁵. Il s'agit d'un dispositif de médiation institutionnelle conventionnelle ou judiciaire au profit des personnes physiques ou morales régi par la loi 08-05 relative à la médiation. C'est finalement la question de la nécessité de créer un service public de médiation en ligne qui est soulevée, afin d'assurer une protection renforcée des droits des justiciables.

L'instauration des audiences virtuelles durant la période de Covid-19 pourrait être l'occasion de conduire une réflexion sur l'articulation de cette phase judiciaire dématérialisée avec une phase amiable qui pourrait être développée via une plateforme publique de règlement amiable des petits litiges. La mise en place d'un traitement entièrement

¹On parle de blind-bidding services (procédure d'offre aveugle).

²Le site Cybersettle, créée en 1998 aux Etats-Unis et qui a connu un grand succès dans le secteur de l'assurance, fonctionnait selon ce modèle.

³C'est le cas du site Smartsettle qui propose un processus de règlement du conflit consistant pour les parties à identifier les différents points du litige puis à les classer en donnant une valeur à chacune de ces questions. L'algorithme formule ensuite des blocs de propositions, en mobilisant certaines techniques de la théorie des jeux, pour aider les parties à atteindre la résolution la plus efficace et la plus satisfaisante pour elles.

⁴« Centre Marocain de Médiation Bancaire », consulté le 23-05-2022 à 10h sur <https://cmmb.ma/>

⁵La saisine du centre de médiation bancaire est faite par courrier, par mail, ou par un dépôt auprès du CMMB.

dématérialisé du litige devrait toutefois s'accompagner d'une réflexion sur l'accessibilité de ce e-règlement des différends pour des justiciables peu familiers des outils numériques. Si la dématérialisation du règlement amiable des différends semble difficilement pouvoir être contenue, elle gagnerait à ne pas être pensée séparément de celle du règlement judiciaire des litiges et à s'enrichir d'une réflexion sur l'accessibilité de cette justice numérique en cours de déploiement.

Conclusion du Titre II

Il apparaît finalement d'une part, que la notion de responsabilité numérique paraît s'imposer dans un monde marqué par la transformation numérique ayant permis le développement de l'économie numérique. Pourtant, les questions de responsabilités propres au monde numérique présentent, d'un point de vue juridique des facettes variées qu'il est difficile de conclure à l'émergence d'une notion générale et compréhensible de responsabilité numérique. D'autre part, les règles du droit international privé, qu'elles soient tirées du droit commun marocain ou des conventions internationales, permettent d'apporter des réponses aux problèmes classiques de la détermination du tribunal compétent, de la loi applicable dans le cadre de l'économie numérique ainsi qu'au régime applicable à la responsabilité des acteurs de l'internet. Quant aux règles du droit pénal international, elles autorisent largement les autorités marocaines à procéder à la répression des infractions commises sur ou par l'internet.

Pour autant, on ne peut affirmer que toutes les solutions auxquelles conduit les applications de ces règles soient satisfaisantes. En effet, pour être efficace la sécurité juridique doit s'étendre à toute la planète, eu égard à la nature transnationale de l'internet. Le phénomène de la transformation digitale des entreprises, contribue en effet à poser ces problèmes en termes renouvelés, car la localisation géographique et matérielle des relations juridiques, qui est à la base de la démarche conflictualiste, prête à discussion lorsque ces relations se nouent dans le monde virtuel des réseaux numérique. Pour autant, il est difficile de soutenir que cette localisation soit impossible. Mais en l'état actuel du droit, des incertitudes subsistent. Des précisions, voire des adaptations sont préconisées, afin de rendre juridiquement plus claire et plus efficace la pratique de la transformation digitale des entreprises.

Conclusion de la deuxième partie

L'environnement numérique et les échanges électroniques accélèrent et participent à la mondialisation et à la globalisation de l'économie, et par là, multiplie la dimension internationale dans les litiges tout en générant sans cesse de nouveaux problèmes juridiques. En effet, l'entreprise dans son processus de digitalisation est dans l'obligation d'assurer une sécurité juridique à l'égard de son environnement externe que ce soit envers l'administration, les concurrents ou même des particuliers qui souhaitent porter atteinte à son système d'information et ses données.

C'est dans ce contexte que le législateur marocain a adopté toute une panoplie de dispositions législatives, que ce soit au niveau du code pénal ou au niveau des lois spéciales, qui visent à lutter contre le phénomène de la cybercriminalité et contre les cyberattaques et surtout combler le vide juridique. Il a, en effet, déployé des efforts énormes, pour lutter contre ce fléau. Cependant, les cyberattaques prennent plusieurs formes et aspects, et cela complique la tâche du législateur. En effet, il ne se passe pas un jour sans que de multiples failles soient découvertes. La fragilité de l'outil numérique conduit le législateur à tenter d'assurer la plus grande sécurité, afin d'éviter des fraudes qui prennent des formes diverses.

Par ailleurs, dans sa relation avec les acteurs de l'internet, l'entreprise en transition digitale risque de se trouver face à des litiges qui engagent sa responsabilité ou celle des acteurs de l'internet et l'assignent devant des tribunaux ou devant des centres d'arbitrage. Dans ce cadre, le paysage institutionnel du règlement des litiges en ligne se modifie constamment. Nombreux sont les centres qui annoncent leur création. La plupart de ces centres sont le résultat d'initiatives privées et en conséquence, ils s'avèrent susceptibles de partialité ou de dépendance à l'égard des intérêts de leurs fondateurs. La légitimité du centre de l'OMPI pour les noms de domaines est, sur ce plan, exemplaire. Son efficacité en témoigne.

Enfin, pour l'entreprise, l'insécurité juridique des systèmes numériques a un coût effroyable. Ses répercussions sont généralement similaires à celle du crime économique, notamment par l'altération des mécanismes de régulation économique (espionnage, vol, etc.). Cela se traduit concrètement par la perte des marchés pour les entreprises victimes. En effet, il semble que tous ces efforts déployés par le législateur n'ont pas pu réprimer tous les actes, il est impératif d'envisager d'autres lois plus modernes et plusieurs efforts restent à faire.

Conclusion générale

Tout au long de cette thèse, nous témoignons de la densité exceptionnelle du cadre juridique mise en place pour accompagner l'entreprise dans son processus de digitalisation. Au travers la problématique soulevée au départ, de la présentation des différents acteurs, du rappel des différentes réponses juridiques apportées, la thèse aborde de manière transversale toutes les thématiques juridiques majeures et actuelles liées à la transformation digitale des entreprises en relation avec son environnement interne ainsi que son environnement externe. Si la digitalisation des entreprises est nouvelle, les interrogations qu'elle soulève ne le sont pas tellement : sécurité, confidentialité, preuve, protection des consommateurs, responsabilité professionnelle, respect des droits de la personne et de la propriété, droit applicable, juridiction compétente. Il s'agit avant tout d'offrir la maîtrise des normes assurant la sécurité juridique mais aussi de s'interroger sur celles-ci ainsi que sur celles adoptées à l'étranger.

On peut alors, suite aux développements précédents, affirmer que le Maroc tente pas à pas de se rapprocher des standards internationaux en matière du numérique par l'adoption de plusieurs lois encadrant ce domaine. De plus, quand il n'y a pas de réglementation spécifique, le Maroc arrive à s'adapter aux nouvelles données en appliquant le droit commun qui s'avère indéboulonnable et indémodable. Certes, le Maroc suit de très près les tendances internationales en matière de sécurité juridique des entreprises numériques, mais il faut attendre que le projet de loi objet de la sécurité passe par le circuit législatif avant de voir la loi approuvée et promulguée. Malheureusement, le temps que le projet de loi arrive à bon port, on se rend compte que la loi est déjà dépassée du fait de l'accélération du monde numérique.

En conséquence, il reste aujourd'hui plusieurs domaines non réglementés, ni réprimés, en droit marocain et qui devraient l'être prochainement pour assurer une sécurité juridique aux entreprises en phase de digitalisation. Le paysage juridique marocain a été, au fil de ces décennies, très imprégné par l'ère de la dématérialisation et en particulier par le numérique. Cependant, plusieurs questions restent aujourd'hui sans réponses faute d'un arsenal juridique complet rassemblant les diverses lois applicables en la matière. Nous déplorons l'absence d'un cadre juridique global qui réunit les dispositions éparses du régime juridique marocain en matière numérique.

Par ailleurs, le numérique franchit les frontières nationales. Il a une place importante dans la vie économique et la quantité de transactions échangées menées par l'intermédiaire d'internet est en spectaculaire progression. Si le numérique participe de manière positive au développement économique, il présente des dangers non négligeables. De ce fait, les réponses doivent être recherchées dans l'invention de nouveaux modes de régulation entre les Etats et l'intensification de la coopération internationale. Une harmonisation du droit des procédures ainsi qu'une étroite coopération judiciaire s'avère donc inévitable et particulièrement nécessaire pour faire face aux cyberattaques de plus en plus organisées. Les Etats appelés à un double effort, d'harmonisation de leurs législations et pratiques nationales et de coopération de leurs autorités policières et judiciaires.

En outre, la transformation digitale des entreprises est mise en place par les dirigeants, acteurs d'internet et experts. Il est indispensable de créer un lien de coordination et de coopération avec les acteurs publics et privés concernés par la transition digitale, en profitant de leurs connaissances en la matière. Il s'agit donc de créer un seul canal comprenant les juristes et les experts au numérique qui vise à couvrir les différents actes numériques. De plus, le droit régissant le monde numérique mêle ainsi, de façon subtile et simultanée, des apports issus de la loi, de la jurisprudence qui s'est emparée très rapidement de la matière, de contrats, ainsi que de générations spontanées d'usages forgés par les utilisateurs eux-mêmes au fil de leurs pratiques.

En effet, malgré les efforts déployés par le législateur, il reste encore des défis sécuritaires à relever, car le terrain de la criminalité est très glissant, mais cela ne veut nullement dire se focaliser uniquement sur la machine judiciaire et législative et négliger des volets qui sont aussi importants et qui se basent sur la sensibilisation, la prévention, la concertation et la coopération. En matière de sécurité juridique, il n'existe qu'un maître mot : anticiper, car aujourd'hui tous les spécialistes le confirment : PME, ETI comme très grandes entreprises. Mettre en place des outils de prévention et de protection juridique contre une cybermenace d'ailleurs consubstantielle à la transformation numérique des entreprises.

La transformation digitale fait couler beaucoup d'encre sur son potentiel impact sur la fonction de juriste, elle pourrait le conduire à s'émanciper. Armé de nouveaux outils, il serait capable de gagner en compétence. Et il pourrait s'avérer être un acteur incontournable dans la résolution des problématiques juridiques nées de la digitalisation des entreprises. L'argument selon lequel la numérisation stimule l'activité économique a été renforcé par la pandémie de

la Covid-19. Les technologies numériques étant des technologies polyvalentes utilisables pour diverses activités économiques, la généralisation des services numériques pourrait produire des gains importants. Ainsi pour tirer les bénéfices économiques les plus rapides de la numérisation, la priorité est au rôle du juriste, l'ange gardien de l'entreprise.

Cette recherche entamée pour rédiger cette thèse nous a permis de formuler des propositions qui pourront encourager les entreprises à aller vers plus de digitalisation en toute sécurité juridique :

L'appel à une adoption d'un code numérique rassemblant toutes les lois en la matière, qui constituera une référence aux différents acteurs de l'internet. Le législateur marocain est amené à faire un travail méthodique et rigoureux afin de réunir tous les textes juridiques réglementant le monde numérique dans un seul code pour faciliter et généraliser l'accès aux lois.

Par ailleurs, le législateur marocain est invité à actualiser ses outils de travail et combler le vide juridique en la matière en se basant sur une approche participative qui englobe plusieurs intervenants. L'adoption d'une approche participative aura pour but d'intégrer les différents acteurs de l'internet : professionnel et consommateurs dans le processus de légifération.

Aussi, compte tenu de la nature transfrontière du numérique, une harmonisation des lois marocaines avec les lois étrangères et une coopération judiciaire entre les Etats s'avèrent indispensable.

A elle seule, l'approche législative est insuffisante pour assurer une sécurité juridique efficace et cela se justifie par la nature particulière du monde numérique. C'est pourquoi le juriste et les experts du numérique sont invités à collaborer de façon très originale et concomitante pour assurer ensemble une sécurité juridique au sein de l'entreprise en phase de digitalisation. Le juriste doit accompagner les parties prenantes du numérique pour préparer le cadre juridique qui permettra le développement d'un environnement numérique durable dans lequel l'équilibre entre sécurité et liberté est respecté.

Enfin, l'anticipation de l'entreprise contre les différentes cybermenaces à travers non seulement la réglementation mais également la prévention et la sensibilisation. Il est aujourd'hui impératif pour l'entreprise, quelle que soit sa taille, d'avoir en amont des outils de prévention et de protection, et en aval des outils de supervision et de détection pour être capable de réagir à temps et éviter les dégâts irréparable.

BIBLIOGRAPHIE

I. Ouvrages

I.1. Ouvrages généraux

- AUBERT J, L'essentiel de l'introduction au droit, Ellipses, Paris, 2010.
- BLAISE J-B et DESGORGES R, Droit des Affaires : Commerçant, Concurrence, Distribution, LGDJ, 8^{ème} éd., Paris, 2015.
- BOUDAHRAIN A, Droit social marocain, Socheppress-Université, Casablanca, 1984.
- CACHARD O et KLOTGEN P, Droit international privé, Bruylant, 9^{ème} éd., coll. Paradigme, Paris, 2021.
- CARREAU D, JUILLARD P, BISMULT R et HAMANN A, Droit International Economique, Dalloz, 6^{ème} éd., Paris, 2017.
- CHARBONNIER O et ENKART S, Société digital : Comment rester humain?, DUNOD, Malakoff, 2018.
- COLLART DUTILLEUL F et DELEBECQUE P, Contrats civils et commerciaux, Dalloz, 10^{ème} éd., Paris, 2015.
- COLLART DUTILLEUL F et DELEBECQUE P, Contrats civils et commerciaux, Dalloz, 11^{ème} éd., coll. Précis, Paris, 2019.
- COMBE E, Economie et politique de la concurrence, Dalloz, 2^{ème} éd., Paris, 2020.
- EL HAJOU S, Le nouveau droit de la concurrence au Maroc, REMALD, Casablanca, 2016.
- ESSAID M-J, Introduction à l'Etude du Droit, Fondation M. J. ESSAID et Fondation Education et Culture du Groupe Banque Populaire, 4^{ème} éd. Rabat, 2010.
- GHESTIN J, LOISEAU G et SERINET Y-M, La formation du contrat : le contrat, le consentement, LGDG, 4^{ème} éd. coll. Traités, 2013, Paris.
- JOURDAIN P, Les principes de la responsabilité civile, Dalloz, 10^{ème} éd., Paris, 2021.
- LACHIEZE C, Droit des contrats, llipses, 3^{ème} éd., Paris, 2012.
- LARROOUMET C et BROS S, Traité de droit civil Tome 3 : Les obligations, Le contrat, Economica, 10^{ème} éd., Paris, 2021.
- LE TOURNEAU P, Droit de la responsabilité et des contrats, Dalloz, 11^{ème} éd., Paris, 2018-2019.
- LEVEQUE F, Les entreprises hyperpuissantes, Odile Jacob, Paris, 2021.
- MAYER P, HEUZE V et REMY B, Droit international privé, LGDJ, 12^{ème} éd., Paris, 2019.
- NMILI M, Les impôts au Maroc Techniques et Procédures, Maarif Al jadida, 5^{ème} éd., 2015.
- PITRON G, L'enfer numérique : voyage au bout d'un like, éd. Les liens qui libèrent, 2021.
- SALIN P, La concurrence, Presse Universitaire de France, 1^{ère} éd., Paris, 1995.
- SCHWAB K, La quatrième révolution industrielle, DUNOD, Malakoff, 2017.
- SECONDAT C-L (Montesquieu), De l'esprit des lois, Paris, 1748.
- SOUAIDI M, Droit Pénal des Affaires, Najah Al jadida, 1^{ère} éd., Casablanca, 2015.

I.2. Ouvrages spéciaux

- AZEMA J et GALLOUX J-C, Droit de la propriété industrielle, Dalloz, 8ème éd. Paris, 2017.
- BABINET G, Big data, penser l'homme et le monde autrement, Le passeur, Paris, 2015.
- BAZIN E, Le droit de repentir en droit de la consommation, Dalloz, Paris, 2008.
- BEN MERZOUK-GLON E, La sécurité juridique en droit positif, une valeur irréductible à la norme, Edition universitaires européennes, Saarbrücken, 2010.
- BERNIER J, L'intelligence artificielle et les mondes de travail, Perspectives sociojuridiques et Enjeux éthiques, Presse de L'Université de Laval, Québec, 2021.
- BILLETTE DE VILLEMEUR M, Le Télétravail en pratique, GERESO, coll. L'essentiel pour agir, Paris, 2019.
- BOY L, RACINE J-B et SIRIAINEN F, Sécurité juridique et droit économique, Larcier, Bruxelles, 2008.
- BRUNAUX G, Le contrat à distance au XIXème siècle, LGDJ, Paris, 2010.
- CACHARD O, La régulation internationale du marché électronique, LGDJ, Paris, 2002.
- CAPRIOL E, Droit international de l'économie numérique, Lexis Nexis, 2ème éd., Paris, 2007.
- CHAINTREUIL J-N, RH et digital, Diateino, Paris, 2015.
- COUPEZ C, Le digital interne en entreprise, Mardaga, coll. Gestion, Entreprise, Finance, Paris, 2019.
- DAOUDI T, Techniques du Commerce International, Arabian Al Hilal, Rabat, 1997.
- DIK A, La Fraude informatique au Maroc, Librairie Dar Essalam, 1ère éd. Rabat, 2017.
- DIRKSEN U et HERBERG M, Syndicats et Transformation 4.0 : Histoires de syndicats qui confrontent le nouveau monde du travail, Friedrich-Ebert-Stiftung, Berlin, 2021.
- DOUET F, Fiscalité 2.0 : Fiscalité du numérique, LexisNexis, 3ème éd., Paris, 2020.
- DULONG DE ROSNAY M, Les Golems du numérique, Droit d'auteur et Lex Electronica, Presses des Mines, Paris, 2016.
- EL AZZOUZI A, La cybercriminalité au Maroc, Bishops Solutions, Casablanca, 2010.
- ENNASHI K, La criminalité numérique en droit marocain, Librairie Rachad, Settat, 2020.
- FAUCHOUX V, DEPREZ P et BRUGUIERE J-M, Le droit de l'internet : Lois, contrats et usages, LexisNexis, 2ème éd, Paris, 2013.
- FERAL-SCHUHL C, Cyberdroit: le droit à l'épreuve de l'Internet, Dalloz, 8ème éd., Paris, 2020-2021.
- FRISON ROCHE M-R, Internet, Espace d'Interrégulation, Dalloz, Paris, 2016.
- GANASCIA J-G, Intelligence artificielle vers une domination programmée ?, Le Cavalier bleu, 2ème éd., Paris, 2017.
- GHAZOUANI C, Le contrat de commerce électronique international, Laatrache, 1ère éd., Tunis, 2011.
- GOURION P-A et RUANO-PHILIPPEAU M, Le droit de l'internet dans l'entreprise, LGDJ, Paris, 2003.
- GREFFE F et GREFFE P, La publicité et la loi, Litec, 11ème éd., Paris, 2009.
- GRYNBAUM L, LE GOFFIC C et MORLET-HAIDARA L, Droit des activités numériques, Dalloz, 1ère éd., Paris, 2014.

- HURBULOT C, Manuel d'intelligence économique, Presses Universitaires de France, coll. Major, Paris, 2012.
- KRIVIN H, L'IA peut-elle penser ? Miracle ou Mirage de l'intelligence artificielle, De Boeck, Paris, 2021.
- LE LOUP L, Blockchain : La révolution de la confiance, Librairie Eyrolles, Paris, 2017.
- LE TOURNEAU P, Contrats du numérique ; Informatiques et Electroniques, Dalloz, 10ème éd., Paris, 2018-2019.
- LUCAS A, Droit d'auteur et numérique, Litec, Paris, 1998.
- MATTATIA F, Droit d'auteur et propriété intellectuelle dans le numérique, Eyrolles, 3ème éd., Paris, 2021.
- MORIN F, BRIERE J-Y, ROUX D et VILLAGGI J-P, Le droit de l'emploi au Québec, Wilson & Lafleur, 4ème éd., Montréal, 2010.
- QUEMENER M, DALLE F et WIERRE C, Quels droits face aux innovations numériques : Législation, jurisprudences et bonnes pratiques du cyberspace. Défis et protections face aux dérives du numérique, Gualino, 1ère éd., Paris, 2020.
- RACINE J-B, Droit de l'arbitrage, PUF, 1ère éd., Paris, 2016.
- RODER S, Guide pratique de l'intelligence artificielle dans l'entreprise, Eyrolles, Paris, 2019.
- SCHMIDT-SZALEWSKI J et PIERRE J-L, Droit de la propriété industrielle, Litec, 4ème éd., coll. Manuels, Paris, 2007.
- TOUMLILT M-D, Le commerce électronique au Maroc aspects juridiques, Editions Maghrébines, Casablanca, 2008.
- VAMPARYS X, La Blockchain au service de la finance : Cadre juridique et Applications pratiques, éd. Revue Banque, Paris, 2018.
- VIVANT M et BRUGIERE J-M, Droit d'auteur et droits voisins, Dalloz, 2ème éd., Paris, 2012.

I.3. Ouvrages Collectifs

- AMAUDRIC DU CHAFFAUT B, « « Web 2.0 » et titularité des droits : une complexité renforcée » in L'entreprise et la titularité des droits de propriété intellectuelle, Ouvrage collectif sous la direction Jean-Michel BRUGIERE, Dalloz, Paris, 2015.
- AUROUX J-B, « La publicité ciblée sur internet à l'épreuve du droit des données à caractère personnel » in L'entreprise à l'épreuve du droit de l'Internet, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2014.
- AZZI T, « Les créations multimédias (bases de données, jeux vidéos...) » in L'articulation des droits de propriété intellectuelle, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2011.
- BARLOW J-P, « Déclaration d'indépendance du cyberspace » in Libre enfant du savoir numérique, Ouvrage collectif sous la direction d'Olivier BLONDEAU, L'Eclat, Paris, 2000.
- BEKALE NGUEMA G-B, « La concurrence déloyale et le numérique : le détournement de la clientèle par l'utilisation du dévoiement (pharming) » in L'entreprise face aux défis du numérique, Ouvrage collectif sous la direction d'Alexandre RIERA et Sylvain CHATRY, MARE & MARTIN, Paris, 2018.

- BENABOU V-L, « Essai de prospective juridique sur les modes de valorisation des données : fonds informationnel, droit à la probabilité et dividende de la donnée » in *Le Big Data et Le Droit*, Ouvrage collectif sous la direction de Florence G'SELL, Dalloz, Paris, 2020.
- BOOTHERSTONE T, « Sécuriser les transactions par la notion de e-fonds de commerce » in *La propriété intellectuelle et la transformation numérique de l'économie*, Ouvrage collectif sous la direction de Fatima GHILASSENE et Laurence JOLY, INPI, 1ère éd., France, 2015.
- BOUHENIC J-D, « L'entreprise et la titularité des droits de propriété intellectuelle. L'œuvre collective » in *L'entreprise et la titularité des droits de propriété intellectuelle*, Ouvrage collectif sous la direction Jean-Michel BRUGUIERE, Dalloz, Paris, 2015.
- BRUGUIERE J-M, « Les conditions générales d'utilisation sur l'internet. Nouvelles réglementations de droit privé ? » in *L'entreprise à l'épreuve du droit de l'internet*, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris 2014.
- CAPRIOLI E et GURFINKIEL A, « Cybersurveillance des salariés et communications électroniques », in *L'entreprise à l'épreuve du droit de l'Internet* », Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014.
- CHAIEHLOUDJ W, « Innovation et préparation du marché à l'entrée de concurrents » in *L'articulation des droits de propriété intellectuelle et du droit de la concurrence*, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020.
- CHATRY S, « Les données collectées par l'entreprise : documenter sa conformité au RGPD », in *L'entreprise face aux défis du numérique*, Ouvrage collectif sous la direction de Alexandre RIERA et Sylvain CHATRY, MARE & MARTIN, Paris, 2018.
- CHOLET S, « La publicité digitale encouragée » in *L'articulation des droits de propriété intellectuelle et du droit de la concurrence*, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020.
- CLAVIER J-P, « La publicité par voie électronique », in *L'entreprise face aux défis du numérique*, Ouvrage collectif sous la direction de Jean-Marc MOULIN, Sylvain CHATRY et Alexandre RIERA, Mare&Martin, Paris, 2018.
- CURIEN N, « La régulation réflexive à travers le miroir de la transition numérique » in *Internet, Espace d'Interrégulation*, Ouvrage collectif sous la direction de Marie-Anne FRISON ROCHE, Dalloz, Paris, 2016.
- DUMONT F, « Les contrats de publicité. Les nouvelles techniques d'achat publicitaire sur internet » in *L'entreprise à l'épreuve du droit de l'Internet*, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014.
- FAVREAU A, « Remarque sur le droit de la concurrence et nouvelles technologies : perturbateurs des systèmes en place » in *L'articulation des droits de propriété intellectuelle et du droit de la concurrence*, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020.
- FAVREAU A, « Protéger la e-réputation de l'entreprise » in *L'entreprise à l'épreuve du droit de l'Internet*, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris 2014.
- GALOKHO C, « Droit des entreprises en difficulté et numérique » in *L'entreprise face aux défis du numérique*, Ouvrage collectif sous la direction d'Alexandre RIERA et Sylvain CHATRY, Mare & MARTIN, Paris, 2018.
- GELLES V et POIDEVIN B, « Réflexions autour de la création numérique dans l'entreprise : problématiques juridiques, enjeux et pistes de réforme » in *La propriété*

intellectuelle et la transformation numérique de l'économie, Ouvrage collectif sous la direction de Fatima GHILASSENE et Laurence JOLY, INPI, 1ère éd., France, 2015.

- GIRARDET A, « Articuler les droits de propriété intellectuelle sans les confondre ou la difficile recherche de frontières ! » in L'articulation des droits de propriété intellectuelle, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2011.
- GODEFROY L, « L'émergence de nouvelles responsabilités autour des plateformes » in Quelles régulations pour l'économie collaborative, Ouvrage collectif sous la direction d'Irina PARACHKEVOVA et Marina TELLER, Dalloz, Paris, 2017.
- LAURRIEU J, « Les territoires disputés de la concurrence déloyale et de la propriété intellectuelle » in La propriété intellectuelle dans les droits du marché et de la rivalité concurrentielle, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2016.
- MACREZ F, « Logiciel : le cumulard de la propriété intellectuelle » in L'articulation des droits de propriété intellectuelle, Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2011.
- MAGNIER V, « La Blockchain, un choix de gouvernance pertinent ? » in Blockchain et droit des sociétés, Ouvrage collectif sous la direction de Véronique MAGNIER et Patrick BARBAN, Dalloz, Paris, 2019.
- MANOUBI M, « Réflexions sur la notion de fonds de commerce électronique », in Mélanges offerts en l'honneur du professeur Hafed BEN SALAH, Centre de publication universitaire, Carthage, 2018.
- MARTIN G-J, « Quelle régulation pour l'économie collaborative ? Un défi pour le droit économique. Réflexions à mi parcours » in Quelles régulations pour l'économie collaborative ? Un défi pour le droit économique, Ouvrage collectif sous la direction d'Irina PARACHKEVIVA et Marina TELLER, Dalloz, Paris, 2017.
- MOULIN J-M, « Numérique et droit des sociétés », in L'entreprise face aux défis du numérique, Ouvrage collectif sous la direction de Jean-Marc MOULIN, Sylvain CHARTRY et Alexandre RIERA, Mare&Martin, Paris, 2018.
- NICOLI M, PALTRINIERI L et PREVOT-CARPENTIER M, « Travail et plateformes numériques : entre exploitation et opportunités » in Travail e(s)t liberté ?, Ouvrage collectif sous la direction d'Enrico DONAGGIO, José ROSE et Mariagrazia CAIRO, Erès, coll. Clinique du travail, Paris, 2022.
- PEUCHOT R, « Gestion des données personnelles : quels changements le règlement européen apportera-t-il ? » Ouvrage collectif sous la direction de Jean-Michel BRUGIERE, Dalloz, Paris, 2014.
- PIERSON F, « L'organisation syndicale : du communautaire vers le réticulaire » in Où va le travail à l'ère numérique ?, Ouvrage collectif sous la direction d'Anne-France SAINT LAURENT-KOGAN et Jean-Luc METZGER, Presses des Mines, coll. Sciences sociales, Paris, 2007.
- ROSIER K et DELFORGE A, « Le régime de la responsabilité civile du responsable du traitement et du sous-traitant dans le RGPD » in Le règlement général sur la protection des données Analyse approfondie, Ouvrage collectif sous la direction de Cécile de TERWANGNE et Karen ROSIER, Larcier, Paris, 2018.
- SAINT PULGENT M, « Les besoins d'interrégulation engendrés par Internet. Propos introductifs » in Internet, Espace d'Interrégulation, Ouvrage collectif sous la direction de Marie-Anne FRISON ROCHE, Dalloz, Paris, 2016.

- SOLTSMANN W, « L'encouragement à l'innovation par la concurrence, malgré les contraintes du droit de la concurrence » in L'articulation des droits de propriété intellectuelle et du droit de la concurrence, Ouvrage collectif sous la direction de Pascale TREFIGNY, Dalloz, Paris, 2020.
- TOURNAUX S, « Droit du travail et numérique : de quelques aspects relatifs aux relations individuelles de travail » in L'entreprise face aux défis du numérique, Ouvrage collectif sous la direction d'Alexandre RIERA et Sylvain CHATRY, MARE & MARTIN, Paris, 2018.
- TREFIGNY P, « Les liens commerciaux et le droit des marques » in L'entreprise à l'épreuve du droit de l'Internet, Ouvrage collectif sous la direction de Jean-Michel BRUGUIERE, Dalloz, Paris, 2014.

II. Thèses et Rapports

II.1. Thèses

1.1. En Français

- AIT OUKRIM J, Etude et appréciation critique du système d'imposition des affaires internationales au Maroc, Thèse de Doctorat en Sciences Economiques, Université Hassan II, Casablanca, 2010.
- BELKHEIRI M, La fiscalisation des sociétés étrangères : le cas des établissements stables au Maroc, Thèse de Doctorat d'Etat en Sciences économiques, Université Hassan II, Casablanca, 2006.
- GUILLEMARD S, Le droit international privé face au contrat de vente cyberspatial, Thèse de Doctorat en Droit, Université Laval Québec et Université Panthéon-Assas Paris II, Paris, 2002.
- IHRAI O, La propriété intellectuelle à l'ère de l'économie numérique, Thèse de Doctorat en Droit privé, Université Mohammed V- Souissi, Rabat, 2012.
- LARHER Y-M, Les relations numériques de travail, Thèse de Doctorat en Droit privé, Université Panthéon-Assas Paris II, Paris, 2017.
- PIAZZON, T, La sécurité juridique, Coll. de thèse, Lextenso 2^{ème} éd., Paris, 2006.

1.2. En Arabe

- بشرى النية، العقد المبرم بطريقة الكترونية، رسالة لنيل الدكتوراه في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، اكدال الرباط، السنة الجامعية 2012-2011.
- المختار لمجردي، الحماية القانونية للمصنفات الرقمية، رسالة لنيل الدكتوراه في القانون الخاص، جامعة محمد الخامس، كلية العلوم القانونية والاقتصادية والاجتماعية، اكدال الرباط، السنة الجامعية 2017-2016.
- خليل زكرياء، المسؤولية المدنية للبائع المهني وتطبيقاتها على عقد البيع الإلكتروني، رسالة لنيل الدكتوراه في القانون الخاص، جامعة القاضي عياض، كلية العلوم القانونية والاقتصادية والاجتماعية، مراكش، السنة الجامعية 2013-2012.
- سلطان بن ناصر بن سالم البلوشي، التحكيم في المنازعات الإلكترونية، رسالة لنيل الدكتوراه في القانون الخاص، جامعة محمد الأول، كلية العلوم القانونية والاقتصادية والاجتماعية، وجدة، السنة الجامعية 2014 – 2013.

II.2. Rapports

2.1. En Français

- ADD, « Note d’Orientations Générales pour le Développement du Digital au Maroc à horizon 2025 », Royaume du Maroc, Mars 2020.
- BERNIE J, VALLEE G et JOBIN C, « Les besoins de protection sociale des personnes en situation de travail non traditionnelle », Rapport final, Québec, 2003.
- BIT, « Les plateformes de travail numérique et l’avenir du travail: pour un travail décent dans le monde en ligne », 1ère éd., Genève, 2019.
- BOUHLAL R et LAHLOU S, « Contrat et Immatériel », Rapport Marocain, 2014.
- BOUVARD M, CARCENAC T, CHIRON J, DALLIER P, GENEST J, LALANDE B et MONTGOLFIER A, « Le e-commerce : propositions pour une TVA payée à la source », Rapport d’information, 17 Septembre 2015.
- CE,
 - « Proposition de directive du conseil établissant les règles d’imposition des sociétés ayant une présence numérique significative », 21 Mars 2018.
 - « Puissance publique et plateformes numériques : accompagner l’ubérisation », Etude annuelle, Juill. 2017.
- CEPEJ, « Charte éthique européenne d’utilisation de l’intelligence artificielle dans les systèmes judiciaires et leur environnement », Strasbourg, 2018.
- CNN, « Ambition numérique. Pour une politique française et européenne de la transition numérique », Rapport remis au Premier ministre, Paris, 2015.
- CNUDCI, « Notes techniques sur le règlement des litiges en ligne » Nations Unies, New York, Mai 2017.
- Commission Ad hoc, « L’arbitrage en ligne », Rapport du Club des juristes, Paris, Avril 2019.
- CUSOLITO A-P, GEVAUDAN C, LEDERMAN D et WOOD C-A, « Les avantages du numérique pour les pays du Moyen-Orient et d’Afrique du Nord », Rapport de la Banque mondiale, 2021.
- DAUGAREILH I, DEGRYS C et POCHET P, « Économie de plateforme et droit social : enjeux prospectifs et approche comparative », ETUI, Bruxelles, 2019.
- Emploi et Développement social Canada, « Rapport du Comité d’experts sur les normes du travail fédérales modernes », Ottawa, 2019.
- HCP, « Intégration des Tic au niveau des entreprises au Maroc », 2021.
- INTERPOL, « Evaluation 2021 des Cybermenaces en Afrique », Rapport, Singapore, Octobre 2021.
- McKinsey Global Institute « Accélérer la mutation numérique des entreprises : un gisement de croissance et de compétitivité pour la France », France, 2014.
- METTLING B, « Transformation numérique et vie au travail », 2015,
- Ministère de l’Economie, des Finances et de la Réforme de l’Administration, « Guide pratique des mesures préventives dans les services publics », Royaume du Maroc, Mai 2020.
- OCDE,
 - « Le commerce électronique au temps de la pandémie de Covid-19 », 7 Octobre 2020.
 - « Le rôle des plateformes numériques dans la collecte de la TVA/TPS sur les ventes en ligne », Paris, 2019
 - « Algorithmes et entente », Synthèse de la table ronde, Direction des Affaires Financière et des Entreprises Comité de la Concurrence, 17 octobre 2018.

- « Empêcher les mesures visant à éviter artificiellement le statut d'établissement stable, Action 7 », Rapport final, éd. OCDE, Paris, 2016.
- « Relever les défis fiscaux posés par l'économie numérique », Projet OCDE/G20 sur l'érosion de la base d'imposition et le transfert de bénéfices, éd. OCDE, 2014.
- « Commentaires du modèle de convention fiscale concernant le revenu et la fortune », 2008.
- OIT,
 - « Le télétravail Durant la pandémie de Covid-19 et après », Guide Pratique, 1ère éd. Genève, 2020.
 - « Déclaration de l'OIT relative aux principes et droits fondamentaux au travail et son suivi, Conférence internationale du travail », Genève, 18 juin 1998.
- OIT et Eurofound, « Travailler en tout temps, en tout lieu: les effets sur le monde du travail », Rapport, Genève, 2017.
- OMPI, « Rapport final concernant le premier processus de consultations de l'OMPI sur les noms de domaines de l'Internet », Genève, 30 avril 1999.
- SNE, « Questions juridiques relatives aux œuvres multimédia », Livre blanc du Groupe de travail audiovisuel et multimédia, 1994.
- VALENDUC G et VENDRAMIN P, « Le travail dans l'économie digitale : continuités et ruptures », ETUI, Bruxelles, Mars 2016.

2.2. En Anglais

- COUNTOURIS N & DE STEFANO V, « New Trade Union Strategies for New Forms of Employment », ETUC, Brussels, 2019.
- International Labor Organization, « Working from home: From invisibility to decent work », Geneva, 2021.
- International Post Corporation, « Cross-border E-Commerce Shopper Survey », 2017.
- IPSOS, « Digital Trends Morocco 2023 », 13 February 2023.

III. Articles de Revues

III.1. En Français

- AIT OUAKRIM J, « Les techniques d'élimination des doubles impositions Internationales dans la réglementation fiscale marocaine », Université Hassan 1er – Settat.
- ATTIAS ASSOULINE A-V et GLON G, « Fiscalité du digital, digitalisation de la fiscalité », in Revue d'économie financière, N° 131, Mars 2018.
- AZDDOU N, « Le droit marocain des marques », in Revue Marocaine Droit, Economie et Gestion, N° 57, 2018.
- AZOURY N, « Une révolution enclenchée par le changement numérique », in Questions de management, N° 7, Septembre 2014, EMS Editions.
- BALLEST L, « Nouvelles extensions et insécurité juridique », in IP/IT, N° 2, Février 2016, Dalloz.
- BARREAU C, « La régulation des smart contracts et les smart contracts des régulateurs », in Annales des Mines- Réalités industrielles, N° 3, Aout 2017.
- BASSIME L, « Le Dahir des obligations et contrats à l'ère des nouvelles technologies : la signature électronique. », in Revue Marocaine de Droit d'Economie et de Gestion, N° 55, 2016.

- BAUJARD C, « Formation numérique : quel dispositif juridique de protection des savoirs ? », in Revue Recherches en Sciences de Gestion-Management, N° 94, 2013.
- BENARERAF J-A, « Qualification et responsabilité des sites contributifs », in IP/IT, N° 4, Avril 2016, Dalloz.
- BENSAMOUN A, « Droit souple et lutte contre la contrefaçon en ligne », in IP/IT, N° 4, Avril 2016, Dalloz.
- BESSERMANN B, « Les enjeux du développement de la responsabilité numérique pour les assureurs », in IP/IT, N° 03, Mars 2020, Dalloz.
- BEVIERE-BOYER B, « Responsabilité numérique : le défi d'une responsabilité spécifique « humanisée » », in IP/IT, N° 03, Mars 2020, Dalloz.
- BOIZARD M, « La valorisation des données numériques par la protection juridique des algorithmes », in IP/IT, N° 2, Février 2018, Dalloz.
- BOUAYAD H, « Autorité de concurrence et autorités de régulation du secteur des technologies de l'information et des communications « TIC » », in Revue Marocaine de Droit Economique, N° 1, Octobre 2007.
- BOUTRIG A, « Le contrôle, l'assistance et le renforcement des capacités nationales en matière de cybersécurité. D'autres fonctions de la DGSSI », in Revue de police, N° 42, Décembre 2021.
- BYK C, « Présentation des enjeux de la responsabilité numérique », in IP/IT, N° 03, Mars 2020, Dalloz.
- CANAS S, « Blockchain et preuve le point de vue du magistrat », in IP/IT, N° 2, Février, 2019, Dalloz.
- CARON C, « L'interopérabilité au service de la libre concurrence », in Revue de Commerce Electronique, Janvier 2012.
- CHAMBET-FALQUET C, « L'intelligence économique de l'entreprise à l'heure du numérique », in I2D : Information, données & documents, N° 4, 2015.
- CHANG M, FABIANO M, APOLLINE O et VACHON V, « Le traitement des décisions de justice en droit français », in IP/IT, N° 5, Mai 2021, Dalloz.
- CHASSAGNARD-PINET S,
- « Les usages des algorithmes en droit : prédire ou dire le droit », in IP/IT, N° 10 Octobre 2017, Dalloz.
- « Le e-règlement amiable des différends », in IP/IT, N° 10, Octobre 2017, Dalloz.
- CHIBANI I et KABIR H, « Le télétravail comme mode alternatif : Quel statut juridique ? », in Revue du Chercheur dans les Etudes et les Recherches Juridiques et Judiciaires, N° 38, Janvier 2022.
- CORONE F, « Liens commerciaux sur internet et contrefaçon de marque », in LEGICOM N° 44, 2010, Victoires éd.
- CUNY D, « Folie des cryptomonnaies : même Kodak lance Kodakcoin », in La Tribune, N° 11, Janvier 2018.
- DE HASS C, « L'omnipotence du juge français de la propriété intellectuelle face à l'internet ou l'histoire d'une incompétence largement ignorée », in LPA, N° 226, 13 Novembre 2001.
- DEFFAINS B, « Le monde du droit face à la transformation numérique », in Pouvoirs, N° 170, Mars 2019, Seuil.
- DEGRYSE C, « Du flexible au liquide : le travail dans l'économie de plateforme », in Revue Industrielle, N° 4, 2020.
- DELMAS-LINEL B et MUTZ C, « Le Cloud computing à l'épreuve des souverainetés nationales. Faut-il avoir peur du USA Patriot Act ? », in RLDI, N° 090, 2013.

- DELMAS-LINEL B, SABAILA B et LIZZIT F, « Promesses du Cloud computing et protection des données à caractère personnel : la remise en question du cadre juridique français et européen », in Lexbase Hebdo, N° 292, 12 avril 2012, éd. Affaires.
- DEZIEL P-L et JOLICOEURJ M-P, « Vers une approche synergique de la dématérialisation des dossiers judiciaires : la protection de la vie privée des justiciables comme vecteur d'accès à la justice », in IP/IT, N° 5, Mai 2021, Dalloz.
- DOM J-P, « Matérialité et localisation de l'entreprise numérique », in IP/IT, N° 12, Décembre 2019, Dalloz.
- DORMONT S, « Quel régime de responsabilité pour l'intelligence artificielle ? », in Communication Commerce Electronique, N° 11, 2018.
- DOUVILLE T, « Le contrat en matière de responsabilité conjointe de traitement de données », in IP/IT, N° 4, Avril 2021, Dalloz.
- DOUET F, « Fiscalité des initial coin offerings (ICOs) », in IP/IT, N° 4, Avril 2019, Dalloz.
- DROSS W, « L'encadrement des technologies par le droit : nécessité et source de changements », in Revue du Notariat, N° 3, 2004.
- DOUVILLE T, « Le fonds de commerce électronique : de sa reconnaissance à sa marginalisation », in IP/IT, Dalloz, N° 12, Décembre 2019.
- DUPRE J et LEVY VEHEL J, « L'intelligence artificielle au service de la valorisation du patrimoine jurisprudentielle », in IP/IT, N° 10, Octobre 2017, Dalloz.
- ECHARD R, « Cybersécurité en entreprise, comment protéger votre patrimoine intellectuel et industriel ? », in IP/IT, N° 12, Décembre 2017, Dalloz.
- EDDE R, « Le droit : Un outil de régulation du cyberspace ? Le cas du droit à l'oubli numérique », in L'Homme & la Société, N° 206, Janvier 2018, L'Harmattan.
- EL AHDAB J et MAKO M, « Arbitrage international versus intelligence artificielle », in Revue Droit et Affaires, 2018
- EL HAJOUÏ S, « Les interférences entre le droit de la concurrence et le droit de la propriété intellectuelle », in Revue marocaine de droit économique, N° 1, Octobre 2007.
- EL HAOUD N, « L'intelligence économique au service de l'entreprise innovante », in Revue internationale d'intelligence économique, N° 2, 2011, Lavoisier.
- EL KASSIMY S, « Les smart contrats : la révolution de la confiance », in Revue de Droit Commercial, N° 7, 2020-2021.
- EL MADANI M, « L'arsenal pénal et aspects de la protection juridique en matière de la criminalité informatique au Maroc », in Revue Marocaine de Droit Pénal et de Sciences Criminelles, N° 6-7, 2019.
- EL MOSTAFA R, « La DGSSI : Rempart contre les cyberattaques et garant de la cybersécurité des systèmes d'information vitaux de notre pays », in Revue de police, N° 42, Décembre 2021.
- EL OUFIR C et DIK A, « La complémentarité du droit et de la sécurité en matière informatique », in Revue Marocaine de Droit Commercial et des Affaires, N° 3, 2015.
- FORASACCO C, « Démystifier, piloter, accompagner, apprendre à faire confiance pour changer de paradigme », in Questions de management, N° 7, Septembre 2014, EMS, Editions.
- FOURNIER P, « Les apports de l'ordonnance en matière de pourparlers et d'avant-contrats », in IP/IT, N° 5, Mai 2016, Dalloz.
- FRIMOUSSE S et PERETTI J-M,
 - « Repenser la culture d'entreprise après la crise Covid-19 », in Questions de Management, N° 31, Janvier 2021, EMS Editions.

- « Comment accompagner la transformation digitale des entreprises en Afrique ? », in Questions de management, N° 8, Mars 2017, EMS Editions.
- GALLE P-R : « Ubérisation et difficultés de l'entreprise », in IP/IT, N° 7-8, Juillet-Aout 2017, Dalloz.
- GAVANON I, « Blockchain et PI et mode : enjeux de la blockchain au regard des règles relatives à la preuve électronique », in IP/IT, N° 2, Février 2019, Dalloz.
- GEUZE F, « Trois points clefs pour accompagner la révolution digitale », in Questions de management, N° 7, Septembre 2014, EMS Editions.
- GHALI A, « Le télétravail et le droit du travail », in Revue du droit marocain, N° 14, Avril 2009.
- GIUDICELLI G, « La publicité digitale en France », in IP/IT, N° 9, Septembre 2021, Dalloz.
- GOMES V.B, « Le crowdworking : essai sur la qualification du travail par intermédiation numérique », in RDT, N° 7, 2016, Dalloz.
- GOSSA J, « Les Blockchains et Smart contracts pour les juristes », in IP/IT, N° 7-8, Juillet-Aout 2018, Dalloz.
- GRATTON L, « Révolution numérique et négociation collective », in Revue Droit social, N° 12, Décembre 2016.
- GRANGE M, « Internet rattrapé par le droit », in Politique étrangère, N° 4, 2019, IFRI.
- GRUSELLE B, « Le défi des nouveaux usages numériques : La sécurité des entreprises à la peine », in Sécurité et stratégie, N°11, Avril 2012, Club des Directeurs de Sécurité des Entreprises.
- GRYNFOGEL C, « Une illustration de la confrontation entre concurrence et propriété intellectuelle : les licences FRAND », in RJDA, N° 5, 2016, Francis Lefebvre.
- G'SELL F, « Vers l'émergence d'une responsabilité numérique ? », in IP/IT, N° 3, Mars 2022, Dalloz.
- GUERINI F, « L'intelligence économique d'entreprise face au défi du numérique », in Revue du chercheur en sciences mathématiques et sociales, N° 6, Université d'Alger.
- GUERLIN G, « Considérations sur les smart contract », in IP/IT, N° 10, Octobre 2017, Dalloz.
- GUEZMIL J, « L'hébergement du fonds de commerce électronique », in Revue de la Jurisprudence et de la Législation, N° 4, Avril 2015.
- GUINIER D, « Modèle de représentation des cyberattaques, mesures génériques et prospective », in IP/IT, N° 3, Mars 2018, Dalloz.
- GUYADER H, « Avant-propos sur les enjeux de la publicité digitale », in IP/IT, N° 9, Septembre 2021, Dalloz.
- HAOUDI A et BENNAGEM TOUATI M, « Les TIC en intelligence économique : quels développements en Afrique ? », in Dossiers de Recherche en Economie et Gestion, N° 1, Juin 2020, Dossier 9, p. 148
- HASS G, « La cybercriminalité à la fois coté obscur et face cachée du Big Data », in IP/IT, N° 1, Janvier 2016, Dalloz.
- HASS G et BAMDE A, « Un statut juridique pour le nom de domaine », in IP/IT, N° 2, Février 2016, Dalloz.
- HONORAT F, « La marque face au nom de domaine », in LEGICOM, N° 44, 2010, Victoires éd.
- HOULIERE S et DE BLOTEAU D, « Faire du digital un levier », in Questions de management, N° 7, Septembre 2014, EMS Editions.

- IZDI S, « La preuve du contrat électronique en droit marocain », in Revue Marocaine du droit commercial et des affaires, N° 4-5, 2018.
- JOLY L, « La Blockchain est-elle une révolution pour la propriété intellectuelle ? », in IP/IT, N° 10, Octobre 2018, Dalloz.
- KHALED S, « Le fonds de commerce électronique », in Infos juridiques, N° 190-191, Décembre 2014.
- LACHIEZE C, « Intelligence artificielle : quel modèle de responsabilité ? », in IP/IT, N° 12, Décembre 2020, Dalloz.
- LAMENSH M et TRAVERSA E, « Plateformes numériques : développement récents en matière fiscale », in Revue International de droit économique, 3^{ème} trimestre, 2019.
- LANERET N et BAUDEQUIN A, « Données personnelles quelle circulation demain », in IP/IT, N° 12, Décembre 2017, Dalloz.
- LANERET N, KNITTEL R et BAUDEQUIN A, « Protection des données personnelles : quand le droit de la concurrence s'en mêle », in IP/IT, N° 12, Décembre 2017, Dalloz.
- LANGE T, « Cloud computing et Données personnelles : Les clauses à maîtriser », in IP/IT, N° 10, Octobre 2016, Dalloz.
- LARROUMET C, « La responsabilité du fait des produits défectueux après la loi du 19 mai 1998 », in Recueil Dalloz, N° 33, 1998, Dalloz.
- LATOURNERIE J-Y, « Cybermenaces et protection des entreprises : une priorité de l'Etat », in IP/IT, N° 1, Janvier 2016, Dalloz.
- LEGRAND S, « Enjeux de la blockchain du point de vue du praticien », in IP/IT, N° 2, Février 2019, Dalloz.
- LOISEAU G, « Intelligence artificielle et conditions de travail des salariés : un impact à prendre au sérieux », in IP/IT, N° 7-8, Juillet et Aout 2018, Dalloz.
- MAGNIER V, « Enjeux de la blockchain en matière de propriété intellectuelle et articulation avec les principes généraux de la preuve », in IP/IT, N° 2, Février 2019, Dalloz.
- MARAURIE-VIGNAL M, « Enjeux et défis de la Blockchain dans ses relations avec la propriété intellectuelle », in IP/IT, N° 10, Octobre 2018, Dalloz.
- MARIQUE E, « Les smart contracts en Belgique : une destruction utopique du besoin de confiance », in IP/IT, N° 1, Janvier 2019, Dalloz.
- MATHIEU C, PERETIE M-M et PICAULT A, « Le droit à la déconnexion : une chimère ? », in Revue de droit du travail, N° 10, 2016.
- MEINGAN D, « Pourquoi parle-t-on de transformation dans la transformation digitale ? » in Questions de management, N° 7, Septembre 2014, EMS Editions, p. 164.
- MEKKI M,
 - « Les fonctions de la responsabilité civile à l'épreuve du numérique : l'exemple des logiciels prédictifs », in IP/IT, N° 12, Décembre 2022, Dalloz.
 - « Le contrat, objet des smart contracts (Partie I) », in IP/IT, N° 7-8 juillet- Aout, 2018, Dalloz.
- MENECEUR Y, « Justice et intelligence artificielle : la confiance naîtra d'une réglementation internationale », in IP/IT, N° 5, Mai 2021, Dalloz.
- MOATI A, « Le numérique rattrapé par le digital ? », in Le Débat, N° 188, Janvier 2016, Gallimard.
- MONINO J-L et SEDKAOUI S, « Les TIC un outil indispensable pour une démarche d'intelligence économique », in Marché et Organisations, N° 18, 2013, L'Harmattan.
- MOREL L, « Le droit à la déconnexion en droit français. La question de l'effectivité du droit au repos à l'ère du numérique », in Labour and Law Issues, N°2, 2017.

- MOREL M, « Le télétravail, mode de travail en évolution ou en révolution ? », in Revue française de comptabilité, N° 551, Mars 2021
- MOSSE M, « Quand le Cloud rime avec la cybersécurité », in IP/IT, N° 1, Janvier 2016, Dalloz.
- MOTAIS E, BLONS E et PFEIFFER L : « L'adoption stratégique du numérique », Questions de management, N° 7, Septembre 2014, EMS Editions.
- NEGGAOUI M, « La sécurité juridique en droit fiscal lecture comparative », in Revue scientifique arbitral semestrielle des études juridiques juridictionnelles et jurisprudentielles N°4, 2018.
- PASQUIER T, « Le droit social confronté aux défis de l'ubérisation », in IP/IT, N° 7-8, Juillet-Aout 2017, Dalloz.
- PECH Y, « Vers une intelligence cyber ? », in Prospective et stratégie, N° 10, Janvier 2019, APORS Editions.
- PEREIRA B, « Mutation du rapport de subordination : le salarié « autonome » ou l'indépendant « subordonné » en France », in Management et Avenir, N° 104, Octobre 2018, Mangement Prospective.
- PISANI C, « L'acte dématérialisé », in Arch. Phil. Droit, N° 43, 1999.
- PIGNATARI O et COUSIN A, « L'originalité des logiciels », in IP/IT, N° 5, Mai 2016, Dalloz.
- POUPART G, « Le droit au service de la cybersécurité », in IP/IT, N° 3, Mars 2018, Dalloz.
- QUEMENER M, « Enquêtes dans le Darkweb », in IP/IT, N° 2, Février 2017, Dalloz.
- QUONIAM L et LUCIEN A, « L'Intelligence Economique 2.0 », in Les Cahiers du numérique, N° 4, 2009, Lavoisier.
- RAY J-E, « Naissance et avis de décès du droit à la déconnexion, le droit à la vie privée du XXI siècle », in Revue de Droit Social, N° 11, Novembre 2002, Dalloz.
- SASSI M, « La lutte contre la cybersécurité », in Revue de police, N° 42 Décembre, 2021.
- SEDALLIAN V, « La responsabilité de l'employeur en tant que fournisseur d'accès à internet », in LEGICOM, N° 27, Février 2002.
- SENECHAL J, « Responsabilité Ab initio, Régulation Ex ante et responsabilités A Posteriori : le cœur des débats européens sur les systèmes d'intelligence artificielle, hors et dans le secteur du commerce électronique », in IP/IT, N° 12, Décembre 2020, Dalloz.
- SERVAIS J-M, « Travailleurs des plateformes numériques de services : quelles garanties sociales ? », in Revue Interventions Economiques, N° 60, 2018.
- SIRINELLI P, « Première vues sur la directive droit d'auteur dans le marché unique numérique », in IP/IT, N° 5, Mai 2019, Dalloz.
- SLASSI MOUTABIR A,
- « L'acte authentique à l'ère de la signature électronique », in Revue de Droit Commercial, N° 4, 2017.
- « Le juge face à la preuve électronique », in Revue du Droit Marocain, N°23, 2012.
- SQALLI HOUSSAINI M, « Pratiques de sécurité informationnelle des PME exportatrices : le volet défensif de l'intelligence économique », in Revue internationale d'intelligence économique, N° 1, Janvier 2020, VA Presse Editions.
- THOMAS-SERTILLANGES J-B, « Droit et Technologies : Concilier l'Inconciliable ? », in Les Cahiers du numérique, N° 2, 2014, Lavoisier.
- VERBIEST T, « le fonds de commerce électroniques : vers une reconnaissance juridique ? », in Communication commerce électronique, N° 4, 2008.

- VERCKEN G, « La révolution du Cloud : A quoi sert encore le contrat ? », in IP/IT, N° 10, Octobre 2016, Dalloz.
- WILLMANN C, « La déconnexion des salariés : un droit « mou », aux forts enjeux », in IP/IT, N°12, Décembre 2019, Dalloz.
- ZOM C, « Contrats de Cloud computing et Données personnelles : éléments de rénovations des techniques contractuelles », in IP/IT, N° 10, Octobre 2016, Dalloz.

III.2. En Anglais

- BERNSTEIN E & LEE T-J. « Where the Consumer is the Commodity: The Difficulty with the Current Definition of Commercial Speech», 2013.
- CHANDRASEKARAN N, « Is Data the new Currency? », 14 August 2015.
- DE STEFANO V,
 - «Negotiating the Algorithm: Automation, Artificial Intelligence and Labour Protection», in Comparative Labor Law & Policy Journal, N° 1, 2019.
 - « The Rise of the Just-in-Time Workforce: On-Demand Work, Crowdwork, and Labor Protections in the Gig-Economy », in Comparative Labour Law & Policy Journal, Geneva, 2016.
- GENIN E, « Proposal for a Teoretical Framework for the Analysis of Time Porosity », in International Journal of Comparative Labour Law and Industrial Relations, N° 3, 2016.
- HYMA G-M & DIGESTI M-P, « New Nevada Legislation Recognizes Blockchain and Smart contracts Technologies », Nevada Lawyer, Nevada, August 2017.
- PRASSEL J & RISAK M, « Uber, Taskrabbit, and Co: Platforms as Employers – Rethinking the Legal Analysis of Crowdwork », in Comparative Labor Law & Policy Journal, N° 8, 2016.
- RODA J-C, « Smart contracts, Dumb Contracts », in IP/IT, N° 7-8, Juillet-Aout 2018, Dalloz.
- SHI G & ZHANG T, « Comments on Chinese civil subject qualification of artificial intelligence », in IP/IT, N° 12, Décembre 2020, Dalloz.

III.3. En Arabe

- أحمد الشرقاوي، التوقيع الإلكتروني وحجيته في الإثبات بين التشريع الوطني والقوانين الدولية، مجلة منازعات الأعمال الدولية، ع. 58، أكتوبر 2020.
- أحمد محمود المساعدة، الشيك الإلكتروني كأحد وسائل الدفع الإلكترونية الحديثة، مجلة القانون المغربي، ع. 18، مارس 2012.
- محمد اهتوت، شكلية الإثبات في العقود الإلكترونية، مجلة القانون التجاري، ع. 5 و 6، 2019.
- بخيت طريبيش المنصوري، الجرائم الإلكترونية الماسة بالأشخاص، مجلة القانون المغربي، ع. 43، يناير 2020.
- رانيا جعفر، فعالية التحكيم الإلكتروني في تسوية النزاعات الناشئة عن التجارة الإلكترونية، مجلة القانون و الأعمال الدولية، ع. 29، أكتوبر 2020.
- أيوب رابح، الحماية الجنائية من القرصنة الإلكترونية في ظل جائحة كورونا مجلة منازعات الأعمال، ع. 52، يونيو 2020.

IV. Législation

- Code Marocain de Bonnes Pratiques de Gouvernance d'Entreprise, Commission national de gouvernance d'entreprise, CGEM, Mars 2008.
- Dahir n° 1-22-34 du 23 chaoual 1443 (24 mai 2022) portant promulgation de la loi n° 95-17 relative à l'arbitrage et à la médiation conventionnelle.
- Dahir n° 1-22-35 du 23 chaouel 1443 (24 mai 2022) portant loi n° 66-19 modifiant et complétant la loi n° 2-00 relative aux droits d'auteur et droits voisins.
- Dahir n° 1-20-100 du 16 joumada I 1442 (31 décembre 2020) portant promulgation de la loi n° 43-20 relative aux services de confiance pour les transactions électroniques.
- Dahir n° 1-20-69 du 4 hija 1441 (25 juillet 2020) portant promulgation de la loi n° 05-20 relative à la cybersécurité.
- Dahir n° 1-19-08 du 18 joumada I 1440 (25 janvier 2019) portant promulgation de la loi n°121-12 modifiant et complétant la loi n°24-96 relative à la poste et télécommunication
- Dahir n° 1-18-110 du 2 joumada I 1440 (9 janvier 2019) portant promulgation de la loi n°88-17 relative à la création d'entreprises par voie électronique et leur accompagnement.
- Dahir n° 1-18-79 du 23 kaada 1439 (6 Aout 2018) portant promulgation de la loi n° 87-17 modifiant et complétant la loi n° 13-99 portant création de l'Office marocain de la Propriété Industrielle et Commerciale.
- Dahir n° 1-17-27 du 8 hija 1438 (30 aout 2017) portant promulgation de la loi 61-16 portant création de l'Agence de développement du Digital.
- Dahir n° 1-14-188 du 27 Muharam 1436 (21 Novembre 2014) portant promulgation la loi n° 23-13 modifiant et complétant la loi n° 17-97 relative à la protection de la propriété industrielle.
- Dahir n°1-13-46 du 23 Joumada 1434 (4 Avril 2013) portant promulgation de la loi 75-12 portant approbation de la Convention arabe pour la lutte contre les crimes liés aux technologies de l'information et de la communication (TIC), faite au Caire le 21 décembre 2010.
- Dahir n° 1-11-140 du 16 ramadan 1432 (17 août 2011) portant promulgation de la loi n° 24-09 relative à la sécurité des produits et des services et complétant le dahir du 9 ramadan 1331 (12 août 1913) formant code des obligations et des contrats.
- Dahir n°1-11-91 du 27 Chaabane 1432 (29 Juillet 2011) portant promulgation du texte de la constitution.
- Dahir n° 1-11-03 du 14 rabii I 1432 (18 février 2011) portant promulgation de la loi n° 31-08 édictant des mesures de protection du consommateur.
- Dahir n° 1-09-15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.
- Dahir n° 1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la loi n° 53-05 relative à l'échange électronique de données juridiques.
- Dahir n° 1-07-43 du 28 rabii I 1428 (17 avril 2007) portant promulgation de la loi n° 29-06 modifiant et complétant la loi n° 24-96 relative à la poste et aux télécommunications.
- Dahir n°1-05-192 du 15 moharrem 1427 (14 Février 2006) portant promulgation de la loi n° 34-05 modifiant et complétant la loi n°2-00 relative aux droits d'auteur et droits voisins.

- Dahir n° 1-03-197 du 16 ramadan 1424 (11 novembre 2003) portant promulgation de la loi n° 07-03 modifiant et complétant le Code pénal.
- Dahir n° 1-96-124 du 14 rabii II 1417 (30 août 1996) portant promulgation de la loi n° 17-95 relative aux sociétés anonymes.
- Décision ANRT/DG/N°12/14 du 21 Novembre 2014 relative aux modalités de gestion administrative, technique et commerciale des noms de domaine Internet «.ma».
- Décision du Premier ministre n°3-33-11 du 23 rabii II 1432 (28 Mars 2011) approuvant le règlement intérieur de la Commission nationale de contrôle de la protection des données à caractère personnel.
- Décret n° 2-21-406 du 15 juillet 2021 pris en application de la loi n° 05-20 relative à la cybercriminalité.
- Décret n° 2-20-956 du 22 Chaaban 1442 (5 avril 2021), consacrant la digitalisation de la publicité au registre du commerce et du dépôt des états de synthèse des sociétés.
- Décret n° 2-15-712 du 22 Mars 2016 qui a pour objet de fixer le dispositif de protection des Systèmes d'information sensibles (SIS) des Infrastructures d'importance vitale.
- Décret n° 2-11-509 du 21 septembre 2011 portant création de la Direction Générale de la Sécurité des Systèmes d'Information.
- Décret n° 2-09-165 du 25 jourmada I 1430 (21 mai 2009) pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel.

V. Jurisprudence (par ordre de date)

- Tribunal de commerce, décision n° 8350, 27 Septembre 2021, Al arabia lilawlama contre Ecart Service Morocco, Casablanca.
- CNDP, Délibération n° D-108-EUS/2020 du 23/04/2020 relative à la définition de l'usage des technologies de reconnaissance faciale dans le cadre du dispositif du compte à distance par les banques et établissements de paiement.
- C. Cass, Civile, ch. Sociale, décision n°19-13.316, 4 Mars 2020, Société Uber contre un chauffeur X.
- C. Cass., ch. Com., 23 Janvier 2020.
- CNDP, Délibération n° D-194-2019 du 30/08/2019 relative à un moratoire sur la reconnaissance faciale.
- C. Appel, 3ème circuit, décision n° 18-1041, 3 Juillet 2019, Société Obedorf contre Société Amazon, Etats-Unis.
- CE, décision n° C/369/6, Affaire AT.40411, 20 Mars 2019, Google Search (AdSense) et Alphabet Inc.
- C. Cass., Civile, ch. Social, décision n° 17-20.079, 28 Novembre 2018, Société Take Eat Easy contre le Livreur X.
- Tribunal de commerce, décision du 17 Octobre 2017, Société Autoconfiance 25 contre la Société IES, Belfort.
- CE, décision n° C 9/08, Affaire AT.39740, 27 Juin 2017, Moteur de recherche Google (Shopping).
- C. Cass., Civile, ch. Com., décision n° 15-18.470, 6 Décembre 2016, Société Pressimmo on ligne contre Société La Cote immobilière.
- C. Appel, 3ème ch. Correct., 13 Avril 2016, J. B., C.L., le Ministère public contre le Partenaire Européen, Montpellier.
- C. Appel, ch. Com., décision n° 15/00172, 29 Mars 2016, Grenoble.

- C. Cass, Civile, ch. Com., décision n° 14-20.486, 2 Février 2016, Société Les Vents du Nord contre Société Cuivres et bois.
- TGI, 3ème ch., 23 Mai 2014, Société Red Bull contre M. Mohamed B., Paris.
- CE, décision n° C 350/08, Affaire AT.39939, 29 Avril 2014, Société Samsung.
- CNDP, Délibération n°17-2014 du 10/01/2014 portant modification de la délibération n°402-2013 du 12 Juillet 2013 portant sur les conditions nécessaires à la mise en place d'un dispositif de géolocalisation dans des véhicules utilisés par des employés.
- C. Appel, 18 Décembre 2013, Société Autorefle.com contre David P., Paris.
- TPI, décision n°2013/2103/5538, 12 Décembre 2013, Marrakech.
- C. Cass., Civile, ch. Civile, décision n° 12-20.687, 14 Novembre 2013, MM. X. et Y. contre Société Microsoft corporation.
- CNDP, Délibération n° 478-2013 du 1er novembre 2013 portant sur les conditions nécessaires à l'utilisation des dispositifs biométriques pour le contrôle d'accès.
- TGI, ch. Correct., 28 Juin 2013, Blogmusik, Sacem et autres (Deezer) contre M. Jérôme G., Nîmes.
- CNDP, Délibération n°350-2013 du 31/05/2013 portant sur les conditions nécessaires à la mise en place d'un système de vidéosurveillance dans les lieux de travail et dans les lieux privés communs.
- C. Appel, ch. Civile, décision n° 12/00023, 20 Mars 2013, M. B. et Société Iris Media contre Mme Angela A., Bastia.
- C. Appel, 1ère ch., 27 février 2013, David D. contre Thomas M. et Pascal F., Paris.
- CJUE, 1ère ch., décision n° C-235/10, 19 Avril 2012, Wintersteiger AG contre Products 4U Sondermaschinenbau GmbH.
- CJUE, Grande ch., décision n° C-324/09, 12 Juillet 2011, Société L'Oréal contre Société eBay International.
- CJUE, Grande ch., décision n° C-236/08, 23 Mars 2010, la société Google contre la société Louis Vuitton.
- C. Cass., Civile, ch. Com., décision n° 08-16.752, 9 Mars 2010, Société Delticom contre les Sociétés Pneus Online Suisse et Pneus Online France.
- OMPI (Centre d'arbitrage et de médiation), décision n°D2007-1760, 28 Février 2008, Vente-Privée.com contre Mawuna Koutonin.
- C. Appel, 3ème ch. civile, décision n° 06/05922, 31 Janvier 2008, Société PNEUS-ONLINE SUISSE et Société PNEUS-ONLINE SARL contre Société DELTICOM AG, Lyon.
- OMPI (Centre d'arbitrage et de médiation), décision n° D 2006-0250, 26 Mai 2006, Jet Tour contre Société coréenne.
- TGI, 3ème ch., décision n° 05/16184, 27 Avril 2006, Société Rue du Commerce contre Société Brainfire Group et Société Moniker Online, Paris.
- C. Appel, décision n° 23-2005-50, 7 Avril 2006, Rabat.
- C. Appel, 2ème ch. Civile, décision n° 03/15440, 13 Mars 2006, Aix-en-Provence.
- C. Cass. ch. Civile, décision n° 02-21.259, 13 Décembre 2005.
- C. Cass. 1ère ch. Civile, décision n° 00-12.932, 3 Avril 2002, Mme X contre Société Editions Larousse.
- CJEC, 6ème ch., decision n° 102/86, 8 Mars 1988, Apple and Pear Development Council contre Commissioners of Customs and Excise.
- C. Cass., Ass. Plén., décision n° 83-10477, 7 Mars 1986, Société anonyme BABOLAT MAILLOT WITT contre Monsieur Jean X.

VI. Webographie

- BENSETTI A, AL ASSAIRE S, « Usage des moyens de visioconférence dans les sociétés anonymes », Chambre française de commerce et d'industrie du Maroc, 1 Avril 2015, http://www.cfcim.org/wp-content/uploads/2015/04/CFCIM_01042015_%C2%AB-Usage-des-moyens-de-visioconfe%CC%81rence-dans-les-socie%CC%81te%CC%81s-anonymes-%C2%BB.pdf.
- BOUGEROL D, « L'utilisation d'internet par les salariés : quels risques pour les employeurs ? », 23 Avril 2013, <https://business.lesechos.fr/entrepreneurs/ressources-humaines/dossier/10028444/tpepme-00010028444-1-l-utilisation-d-internet-par-les-salaries-quels-risques-pour-les-employeurs-58112.php#:~:text=Virus%2C%20fichier%20ind%C3%A9sirable%2C%20diffamation%2C,sur%20internet%20sont%20potentiellement%20nombreux>
- BOUZIAR I, « Les défis de l'intelligence économique au Maroc » le 6 Novembre 2020, <https://www.archimag.com/veille-documentation/2020/11/06/defis-intelligence-economique-maroc>
- CAPRIOLI E-A, « Droit et Intelligence Economique dans l'Economie Numérique », 17 Octobre 2013, <https://www.caprioli-avocats.com/fr/informations/droit-et-intelligence-economique-dans-leconomie-numerique-elements-de-reflexion-sur-21-30-0.html>
- Déclaration sur la Solution pour résoudre les défis fiscaux soulevés par la numérisation de l'économie, <https://www.oecd.org/fr/fiscalite/beps/declaration-sur-une-solution-reposant-sur-deux-piliers-pour-resoudre-les-defis-fiscaux-soulevés-par-la-numerisation-de-l-economie-octobre-2021.pdf>
- CHEMLA L, « Accord historique : ce qu'il faut savoir sur la nouvelle législation de l'UE contre les dérives d'internet », 23 avril 2022, <https://www.franceinter.fr/societe/accord-historique-ce-qu-il-faut-savoir-sur-la-nouvelle-legislation-de-l-ue-contre-les-derives-d-internet>
- Communiqué de presse du 19/09/2014 sur l'opération de contrôle de sites web <https://www.cndp.ma/fr/presse-et-media/communiqué-de-presse/253-communiqué-presse-19-09-2014.html>
- CORERA G, « Volkswagen turns o Blackberry email after work hours », in BBC News, 8 Mars 2012, <https://www.bbc.com/news/technology-16314901>
- EL AKKANI H, « L'intelligence économique: Quels défis pour le Maroc ? », 2 Janvier 2021, <https://www.mapnews.ma/fr/actualites/economie/lintelligence-%C3%A9conomique-quels-d%C3%A9fis-pour-le-maroc>
- GOULARD H, « Régulation des Gafa : le DSA et le DMA en 4 questions », in les Echos, 25 juin 2021, <https://www.lesechos.fr/tech-medias/hightech/regulation-des-gafa-le-dsa-et-le-dma-en-4-questions-1326964>
- H.G., « Protection du consommateur: ce qui va changer dans la loi », in Media24, 26 Novembre 2019, <https://medias24.com/2019/11/26/protection-du-consommateur-ce-qui-va-changer-dans-la-loi/>
- HINKES A, « Blockchains, smart contracts and the death of specific performance », <https://www.otcpm24.com/2019/05/22/blockchains-smart-contracts-and-the-death-of-specific-performance-inside-counsel/>.
- HUET J, « Contrat électronique -Présentation générale », 27 Juin 2021, https://beta-lexis360-fr.ressources.imist.ma/encyclopedies/JurisClasseur Contrats - Distribution/CX8-TOCID/document/EN KEJC-211526_0KRR?q=contrat%20%C3%A9lectronique#EN_4 .

- IBACH C : « La blockchain en entreprise : des applications concrètes », <https://www.cadre-dirigeant-magazine.com/manager/la-blockchain-en-entreprise/>
- JOLY C-R, « Le numérique au cœur des enjeux de l'intelligence économique », 31 Janvier 2016, <https://www.droit-technologie.org/actualites/le-numerique-au-coeur-des-enjeux-de-lintelligence-economique/>
- KERMARREC P, « Numérique et responsabilité des organisations », <https://pascalkermarrec.com/2021/02/09/numerique-et-responsabilite-des-organisations/>
- Modèle de la Convention fiscale concernant le revenu et la fortune : Commentaires sur l'article 5, Version abrégée 2017, https://read.oecd-ilibrary.org/taxation/modele-de-convention-fiscale-concernant-le-revenu-et-la-fortune-version-abregee-2017/commentaires-sur-l-article-5_mtc_cond-2017-8-fr#page1
- MOUMEN H, « Le Fonctionnement des Sociétés Anonymes et l'Etat D'Urgence Sanitaire au Maroc », 25 Mai 2020, <https://www.village-justice.com/articles/les-travaux-des-organes-direction-des-societes-anonymes-leurs-assemblees,35435.html>
- MOUNTAJ I, « Visioconférence : les règles en matière d'organisation des assemblées générales », in Média 24, 2 Juin 2020, <https://medias24.com/2020/06/02/visioconference-les-regles-en-matiere-dorganisation-des-assemblees-generales>
- NACIRI-BENNAN Z, « La loi marocain 95-17 sur l'arbitrage et la médiation conventionnelle », <https://www.village-justice.com/articles/loi-marocaine-sur-arbitrage-mediation-conventionnelle,43044.html>
- PELLEGRINI F et CANEVET S, « Le droit du numérique : une histoire à préserver », 2012, <https://hal.inria.fr/hal-00768912/document>
- ROSEN R.J, « Daimler Employees Can Set Emails to Auto-Delete During Vacation », in Atlantic, 14 Août 2014, <https://www.theatlantic.com/business/archive/2014/08/daimlers-german-employees-can-set-emails-to-auto-delete-during-vacation/376068/>

INDEX

C

Commerce électronique · 14, 22, 27, 38, 39, 42, 43, 44, 45, 46, 47, 48, 119, 145, 152, 156, 157, 158, 160, 182, 202, 240, 243, 295, 323, 333, 334, 335, 336, 337, 338, 339, 340, 341, 353, 367, 377, 378, 380, 382, 385, 386, 388, 396, 399

Concurrence · 10, 14, 66, 107, 114, 170, 180, 185, 191, 208, 217, 231, 235, 241, 243, 247, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 265, 270, 271, 272, 273, 274, 275, 279, 282, 301, 340, 342, 376, 378, 379, 380, 384, 385, 386, 387, 400

Conflit · 56, 63, 80, 95, 267, 275, 302, 332, 333, 338, 344, 349, 351, 355, 361, 363, 369

Conflit de lois · 332

Consommateur · 28, 92, 143, 157, 158, 159, 160, 161, 162, 174, 210, 236, 237, 238, 239, 240, 241, 242, 243, 261, 311, 312, 319, 349, 367, 390, 393, 399

Contrat numérique · 110, 113, 118, 119, 120, 138, 141, 398

Contrats électroniques · 112

Contrats internationaux · 116, 333, 334, 367

Contrefaçon · 25, 196, 198, 199, 204, 205, 206, 270, 271, 272, 273, 275, 276, 277, 278, 279, 280, 313, 314, 342, 383, 384

Cybersécurité · 10, 22, 29, 217, 250, 281, 283, 284, 289, 290, 292, 293, 295, 296, 297, 300, 384, 385, 387, 388, 390, 400, 401

D

Dialogue sociale · 104, 398

Données personnelles · 25, 26, 49, 54, 69, 70, 93, 95, 99, 120, 125, 126, 127, 128, 130, 169, 170, 171, 172, 173, 177, 178, 179, 210, 237, 245, 246, 247, 248, 249, 250, 252, 254, 258, 268, 286, 287, 288, 296, 297, 304, 310, 317, 355, 380, 387, 397, 399, 400

E

Economie numérique · 2, 17, 22, 26, 27, 28, 33, 38, 109, 180, 216, 218, 224, 226, 227, 228, 229, 237, 238, 239, 241, 242, 245, 251, 267, 307, 329, 330, 371, 377, 381, 382, 400

Entreprises en difficulté · 57, 61, 62, 63, 64, 65, 66, 67, 68, 379, 397

E-réputation · 33, 36, 57, 58, 59, 60, 379, 397

F

Fonds de commerce · 39, 42, 43, 44, 45, 46, 47, 48, 336, 379, 380, 385, 386, 396

G

Gouvernance · 13, 30, 35, 36, 37, 38, 48, 49, 54, 56, 109, 281, 292, 296, 298, 318, 380, 390, 397

I

Imposition · 10, 217, 218, 219, 220, 221, 224, 225, 227, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 244, 245, 248, 381, 382, 400

Intelligence économique · 58, 251, 261, 262, 263, 264, 265, 266, 378, 384, 385, 386, 387, 388, 393, 400

Internet · 17, 20, 21, 22, 23, 25, 26, 27, 34, 42, 43, 44, 45, 46, 47, 49, 57, 58, 60, 61, 94, 101, 102, 108, 112, 119, 120, 123, 135, 145, 147, 151, 152, 153, 156, 160, 164, 168, 169, 170, 172, 173, 174, 175, 181, 182, 183, 184, 185, 186, 193, 197, 198, 199, 200, 209, 211, 219, 237, 246, 247, 248, 256, 265, 269, 271, 275, 276, 277, 278, 281, 282, 283, 285, 286, 290, 291, 292, 293, 294, 299, 302, 304, 305, 306, 307, 308, 309, 310, 312, 313, 314, 332, 333, 334, 335, 336, 338, 340, 341, 342, 343, 344, 346, 347, 348, 349, 350, 351, 352, 362, 367,

371, 372, 374, 377, 378, 379, 384, 388, 393, 398, 399, 401, 402

J

Juridiction · 134, 227, 236, 238, 239, 240, 241, 242, 270, 271, 280, 285, 332, 337, 348, 349, 363, 373

L

Litiges · 10, 32, 159, 184, 214, 215, 301, 302, 332, 333, 342, 348, 349, 352, 353, 358, 359, 361, 365, 366, 367, 368, 369, 370, 372, 382, 401, 402

N

Négociation collective · 82, 89, 104, 105, 106, 107, 386, 398

O

Organes sociaux · 49, 50, 51, 53, 56, 104, 397

P

Procédures collectives · 64, 65, 66, 143, 397

Propriété intellectuelle · 10, 25, 31, 47, 110, 111, 137, 148, 149, 178, 180, 181, 190, 192, 194, 196, 197, 200, 201, 202, 203, 204, 206, 207, 208, 252, 253, 259, 260, 261, 274, 275, 277, 278, 294, 304, 307, 320, 343, 344, 358, 362, 378, 379, 380, 381, 384, 385, 386, 387, 399

Publicité numérique · 162, 399

R

Relations collectives · 69, 100, 101, 397

Responsabilité numérique · 302, 304, 317, 318, 319, 320, 321, 322, 323, 328, 329, 371, 384, 386, 401

S

Salarié · 34, 35, 36, 59, 60, 66, 69, 70, 71, 72, 73, 74, 76, 77, 79, 81, 86, 87, 89, 91, 92, 93, 94, 95, 96, 98, 99, 100, 101, 102, 104, 105, 106, 107, 109, 180, 193, 195, 199, 200, 201, 226, 288, 302, 310, 312, 313, 314, 379, 387, 388, 393, 397, 399, 401

Sécurité juridique · 2, 10, 17, 18, 19, 20, 21, 25, 26, 28, 29, 30, 31, 32, 34, 93, 109, 116, 121, 201, 210, 213, 214, 215, 216, 230, 243, 264, 333, 335, 354, 371, 372, 373, 374, 375, 377, 381, 387, 396, 399

Signature électronique · 22, 26, 49, 117, 120, 121, 122, 123, 133, 134, 203, 209, 299, 354, 358, 383, 388, 398

Smart contract · 34, 138, 139, 140, 141, 142, 143, 144, 203

T

Télétravail · 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 104, 109, 282, 320, 383, 384, 385, 387, 397

V

Vidéoconférence · 51

Vie privée · 27, 69, 73, 79, 81, 93, 95, 98, 99, 109, 125, 128, 130, 131, 170, 179, 211, 264, 296, 297, 302, 304, 314, 353, 384, 388

Visioconférences · 104

Vote électronique · 37, 101, 102, 103, 398

TABLE DES MATIERES

Résumé	3
Liste des abréviations	8
Sommaire	11
Introduction générale	13
Partie I : La transformation digitale des entreprises et ses mesures de sécurité juridique internes	34
Titre I : L'impact de la transformation digitale sur la vie de l'entreprise	37
Chapitre I : L'intégration du digital au droit des sociétés	39
Section 1 : L'entreprise face aux services du numérique	40
Sous-section 1 : Création et accompagnement de l'entreprise par voie électronique	40
Paragraphe 1 : La création d'entreprises par voie électronique	41
Paragraphe 2 : Inscription au registre de commerce dématérialisé	43
Paragraphe 3 : Le fonds de commerce électronique	44
I- La reconnaissance du fonds de commerce électronique	44
II- La remise en cause du fonds de commerce électronique	46
III- Une adaptation délicate du fonds de commerce électronique au régime juridique	48
Sous-section 2 : La gouvernance des entreprises numériques	50
Paragraphe 1 : L'accueil du numérique dans l'organisation des organes sociaux	51
I- L'intégration certaine du numérique dans l'organisation des organes sociaux	51
II- La permanence d'une défiance vis-à-vis du numérique dans l'organisation des organes sociaux	52
III- La protection des données à caractère personnel en matière d'organisation des organes sociaux	55
Paragraphe 2 : Le recours à la blockchain dans la gouvernance des entreprises	56
Section 2 : L'entreprise face aux enjeux du numérique	59
Sous-section 1 : L'e-réputation de l'entreprise	59
Paragraphe 1 : La gestion préventive de l'e-réputation de l'entreprise	61
Paragraphe 2 : Les actions préventives de l'e-réputation de l'entreprise	62
Sous-section 2 : Le numérique et le droit des entreprises en difficulté	63
Paragraphe 1 : Le rôle du numérique dans la déstabilisation du droit des entreprises en difficulté	63
I- Le numérique favorise la circulation de l'information	64
II- Le numérique favorise l'apparition d'entreprises vulnérables	65
Paragraphe 2 : Le rôle du numérique dans le renforcement du droit des entreprises en difficulté	67
I- Le numérique au service des procédures collectives	68
II- Le numérique : un outil de prévention des difficultés des entreprises	69

Chapitre II : Le numérique et la transformation des relations de travail	71
Section 1 : Le numérique et les relations individuelles de travail	72
Sous-section 1 : La dématérialisation du travail : le télétravail	72
Paragraphe 1 : Le cadre général du télétravail	73
I- Lieu et temps du télétravail	75
II- Les avantages et les inconvénients du télétravail	76
III- Les formes du télétravail	77
Paragraphe 2 : Le cadre juridique du télétravail	79
I- L'appel à une réglementation du télétravail	79
II- Le droit à la déconnexion	82
Sous-section 2 : Le travail par intermédiation des plateformes numériques	86
Paragraphe 1 : Le travail en réseau ou le crowdworking	86
Paragraphe 2 : La situation des travailleurs des plateformes numériques	89
I- L'impact des nouvelles technologies sur les conditions de travail des travailleurs des plateformes numériques	89
II- La qualification juridique des travailleurs de plateformes numériques	91
III- La classification des plateformes de travail par intermédiation	94
Sous-section 3 : La protection des données des employés dans le cadre de la relation du travail	95
Paragraphe 1 : L'encadrement d'utilisation d'Internet au sein de l'entreprise	96
Paragraphe 2 : Le respect de la vie privée de l'employé	97
I- La biométrie et la reconnaissance faciale dans l'entreprise	98
II- Accès à l'entreprise : géolocalisation et vidéosurveillance	100
Section 2 : Le numérique et les relations collectives de travail	103
Sous-section 1 : Le rôle pratique du numérique dans les relations collectives du travail	103
Paragraphe 1 : Le numérique : un outil d'informations des syndicats et des salariés	104
Paragraphe 2 : Le numérique : un outil de vote électronique et de visioconférence	105
Sous-section 2 : Le rôle du numérique dans la modernisation du dialogue sociale	107
Paragraphe 1 : La reconnaissance syndicale à l'ère du numérique	107
Paragraphe 2 : Le droit à la négociation collective à l'ère du numérique	109
Conclusion du Titre I	112
Titre II : Les instruments digitaux de l'entreprise	113
Chapitre I : Les contrats numériques	115
Section 1 : Processus de contractualisation en ligne	116
Sous-section 1 : Préparation et conclusion du contrat numérique	116
Paragraphe 1 : Ouverture des pourparlers	116
Paragraphe 2 : Les contrats préparatoires	118
Paragraphe 3 : La formation du contrat définitif	119
Paragraphe 4 : Les obligations des parties	121
Sous-section 2 : La sécurisation des échanges	123
Paragraphe 1 : Les services de confiance	123
I- La signature électronique	123
II- Le prestataire de service de confiance	125
Paragraphe 2 : Le paiement en ligne	126

Paragraphe 3 : La protection des données à caractère personnel en matière d'échange numérique	128
I- Les conditions de traitement des données à caractère personnel sur Internet	129
II- Les obligations du responsable du traitement et du sous-traitant à l'égard des personnes	131
III- Le rôle de la CNDP face aux traitements des données à caractère personnel	133
Paragraphe 4 : La preuve de l'écrit électronique	134
I- Le principe de la preuve écrite dans le contrat numérique	135
II- La manipulation et la falsification de la preuve électronique	138
III- Enjeux de la blockchain aux regards des règles relatives à la preuve électronique	140
Sous-section 3 : L'exécution du contrat numérique : les smart contracts	141
Paragraphe 1 : La technologie de smart contracts	142
I- Regard exploratoire sur les smart contracts	142
II- La révolution contractuelle des smart contracts	144
Paragraphe 2 : La valeur juridique des smart contracts	145
I- Les smart contracts : une optimisation de la phase d'exécution du contrat	145
II- Les difficultés liées à la réglementation des smart contracts	146
 Section 2 : Les contrats relatifs à l'Internet.	148
Sous- section 1 : Le contrat du site Internet	149
Paragraphe1 : Le contrat de conception et de réalisation du site Internet	149
I- L'objet du contrat	149
II- Les étapes de création du site Internet	151
III- Les obligations du prestataire et du client	151
Paragraphe 2 : Le contrat de maintenance du site Internet	153
I- Définition et objet du contrat	153
II- Les obligations des parties : prestataires et clients	154
Paragraphe 3 : le contrat de fourniture d'accès	154
I- Définition et objet du contrat	155
II- Les obligations du fournisseur d'accès et du client	155
Paragraphe 4 : Le contrat d'hébergement du site Internet	157
I- L'objet du contrat d'hébergement du site Internet	157
II- Les obligations découlant du contrat d'hébergement	159
Sous-section 2 : Le contrat de commerce électronique	160
Paragraphe 1 : L'obligation d'information loyale, claire et transparente	162
Paragraphe 2 : Les modalités d'acceptation de l'offre par le consommateur et de formation du contrat	164
Paragraphe 3 : Le droit de rétractation	165
Sous-section 3 : Le contrat de publicité numérique	167
Paragraphe 1 : L'achat d'espace publicitaire	168
I- Le contrat d'achat d'espace publicitaire	169
II- Le contrat de régie publicitaire	170
Paragraphe 2 : Le référencement	172
I- Le référencement par un moteur de recherche ou un annuaire	172
II- Le référencement par affiliation	173
Paragraphe 3 : La protection des données à caractère personnel en matière de publicité ciblée	174
I- Les techniques d'identification et de suivie de navigation	175
II- Le cadre légal applicable à la publicité ciblée	176
Sous-section 4 : Le contrat de Cloud computing	178
Paragraphe 1 : Les éléments du contrat de Cloud computing	180
Paragraphe 2 : Les données hébergées dans le Cloud	182

Chapitre II : La propriété intellectuelle et la transformation digitale de l'entreprise	185
Section 1 : Le nom de domaine	186
Sous-section 1 : Attribution du nom de domaine	187
Paragraphe 1 : Les organismes attributifs des noms de domaine sur Internet	188
Paragraphe 2 : Les modalités d'attribution des noms de domaines	190
Sous-section 2 : La réglementation des noms de domaines	193
Paragraphe 1 : Le statut juridique des noms de domaines	193
Paragraphe 2 : La protection des noms de domaines	195
Section 2 : Les créations numériques de l'entreprise	197
Sous-section 1 : La protection de l'œuvre numérique de l'entreprise	197
Paragraphe 1 : La protection du logiciel	198
Paragraphe 2 : La protection des bases de données : exemple du site Internet	202
Paragraphe 3 : Le régime juridique de l'œuvre numérique créée par des salariés	204
Sous-section 2 : Enjeux et défis de la blockchain en propriété intellectuelle	207
Paragraphe 1 : Les étapes d'inscription d'une transaction dans la blockchain	207
Paragraphe 2 : L'admission de la blockchain comme moyen de preuve en matière de propriété intellectuelle	209
Paragraphe 3 : Les risques et les incertitudes entravant la preuve par blockchain	212
Conclusion du Titre II	215
Conclusion de la première partie	216
Partie II : La transformation digitale des entreprises et ses mesures de sécurité juridique externes	218
Titre I : L'impact de la transformation digitale sur l'environnement externe de l'entreprise	221
Chapitre I : L'imposition des entreprises numériques	223
Section 1 : Localisation de l'assiette fiscale des entreprises du secteur du numérique	224
Sous-section 1 : Détermination du droit d'imposer les bénéfices entre les Etats contractants : le plan BEPS de l'OCDE	225
Paragraphe 1 : Notion de l'établissement stable au sens du modèle de convention fiscale de l'OCDE	226
I- Installation fixe d'affaires	226
II- Agent sans statut indépendant	228
III- Insuffisance de la seule existence d'une filiale	228
Paragraphe 2 : Actualisation des règles de localisation des bénéfices au Maroc	229
Paragraphe 3 : Les obstacles relatifs à l'actualisation des règles de localisation des bénéfices au Maroc	231
Paragraphe 4 : Les tentatives de taxation de l'économie numérique.	233
Sous-section 2 : Elimination des doubles impositions	236
Paragraphe 1 : Les mesures de droit interne marocain pour l'élimination de la double	238

imposition internationale	
Paragraphe 2 : Les méthodes d'élimination des doubles impositions dans les conventions Internationales	239
Section 2 : TVA et économie du numérique	241
Sous-section 1 : Le recouvrement de la TVA sur les ventes en ligne	242
Paragraphe 1 : Le recouvrement de la TVA sur les ventes en ligne de service	244
Paragraphe 2 : Le rôle des plateformes numériques dans la collecte de la TVA	247
Sous-section 2 : La TVA et les données à caractère personnel collectées	250
Paragraphe 1 : Le champ d'application de la TVA en matière de données personnelles.	252
Paragraphe 2 : L'assiette, le fait générateur et l'exigibilité de la TVA en matière de données personnelles	254
Chapitre II : L'entreprise digitale entre concurrence et cybersécurité.	256
Section 1 : La régulation concurrentielle de l'économie numérique	257
Sous-section 1 : La détention de la donnée comme facteur de pouvoir du marché	257
Paragraphe 1 : Le marché numérique dominé par les « Big tech »	258
Paragraphe 2 : Les pratiques anticoncurrentielles algorithmiques	262
Paragraphe 3 : L'interopérabilité dans le marché numérique	264
Sous-section 2 : L'intelligence économique à l'ère du numérique	267
Paragraphe 1 : L'intégration de l'intelligence économique au sein de l'entreprise	268
Paragraphe 2 : Les enjeux numériques de l'intelligence économique	271
Sous-section 3 : L'impact de la concurrence numérique sur la propriété intellectuelle de l'entreprise	273
Paragraphe 1 : Les contentieux de concurrence liés au nom de domaine	273
I- Les agissements parasitaires	274
II- Conflit entre nom de domaine et droit des marques	278
Paragraphe 2 : La violation des créations numériques de l'entreprise	281
I- Le droit des marques face à la contrefaçon sur Internet	282
II- Les actes illégaux relatifs aux œuvres numériques de l'entreprise	284
Section 2 : La cybermenace et la protection des entreprises numériques	287
Sous-section 1 : Les menaces numériques	288
Paragraphe 1 : Les modes opératoires des cyberattaques	289
Paragraphe 2 : La donnée : une cible principale des cyberattaques visant l'entreprise	292
Sous-section 2 : Les moyens de lutte contre les cyberattaques	296
Paragraphe 1 : L'arsenal organisationnel de lutte contre la cybermenace	297
Paragraphe 2 : La coopération internationale comme instrument de lutte	300
Paragraphe 3 : La protection des données, un enjeu cardinal de la cybersécurité	303
Paragraphe 4 : Les bonnes pratiques pour faire face aux cyberattaques	305
Conclusion du Titre I	308

Titre II : L'engagement de la responsabilité et la résolution des litiges au numérique	309
Chapitre I : La responsabilité à l'ère du numérique	311
Section 1 : La responsabilité des acteurs d'Internet	311
Sous-section 1 : La responsabilité des prestataires de service Internet.	312
Paragraphe 1 : Le régime spécial de la responsabilité des prestataires de services Internet	313
Paragraphe 2 : Le régime général de la responsabilité des prestataires de services Internet	316
Sous-section 2 : La responsabilité des autres acteurs du numérique	317
Paragraphe 1 : La responsabilité du professionnel commerçant en ligne	318
Paragraphe 2 : La responsabilité de l'employeur du fait de l'usage d'Internet par ses salariés	319
Paragraphe 3 : La responsabilité civile du responsable de traitement et du sous-traitant	322
Section 2 : La construction d'une responsabilité numérique	324
Sous-section 1 : Le défi de la responsabilité numérique du XXI^{ème} siècle	325
Paragraphe 1 : La construction d'une responsabilité numérique originale	326
Paragraphe 2 : Le risque de déshumanisation de la responsabilité numérique	328
Sous-section 2 : Les nouvelles formes de responsabilité numérique	330
Paragraphe 1 : La responsabilité de l'intelligence artificielle	331
Paragraphe 2 : La responsabilité des plateformes numériques	336
Chapitre II : La compétence des litiges nés sur Internet	340
Section 1 : La détermination de la loi applicable dans l'environnement numérique	341
Sous-section 1 : Les lois applicables aux contrats conclus sur Internet	341
Paragraphe 1 : Le rattachement subjectif	342
Paragraphe 2 : Le rattachement objectif	345
Paragraphe 3 : L'admissibilité de la <i>lex electronica</i> en tant que loi du contrat électronique	346
Sous-section 2 : Les lois applicable aux fautes civiles et pénales commises sur Internet	350
Paragraphe 1 : La loi applicable en matière délictuelle	350
Paragraphe 2 : La loi applicable aux infractions de cybercriminalité	353
Section 2 : Les modes de résolution de litiges nés du numérique	356
Sous-section 1 : Les juridictions compétentes pour trancher les litiges sur Internet	356
Paragraphe 1 : Les juridictions compétentes pour trancher les litiges civils et commerciaux sur Internet	357
Paragraphe 2 : Les juridictions compétentes pour trancher les infractions pénales sur Internet	359
Sous-section 2 : La dématérialisation des modes de résolution de litige	360
Paragraphe 1 : La dématérialisation des procédures judiciaires	361
Paragraphe 2 : La pratique de l'arbitrage en ligne	364
Paragraphe 3 : Les procédures alternatives de résolution des conflits en matière de nom de domaine	369
I- Le Règlement Uniforme des Litiges relatifs aux Noms de Domaines (UDRP)	369
II- La procédure Uniform Rapid Suspension System (URS)	373
III- La Procédure Alternative de Règlement des Litiges pour le « .ma » (PARL)	374
Paragraphe 4 : Les plateformes du règlement amiable des différends	375
Conclusion du Titre II	380

Conclusion de la deuxième partie	381
Conclusion générale	382
Bibliographie	385
Index	404