

Livre blanc  
Une réalisation de



# Le numérique et ses déclinaisons sectorielles

En partenariat avec



MARS 2019







# Présentation

Isabelle Eid

**S**uite à la première édition du Guide du Numérique<sup>1</sup>, le cabinet DLA Piper prolonge la réflexion sur l'évolution de la transformation digitale avec la publication de ce deuxième ouvrage. L'objectif cette fois-ci est de mettre en perspective les enjeux immédiats et prospectifs du digital à travers une approche sectorielle.

Cet ouvrage intervient dans une nouvelle ère, une période pendant laquelle les technologies précédemment émergentes atteignent la maturité et sont capables d'atteindre des nouveaux objectifs plus ciblés que jamais. Avec le temps, les nouvelles technologies se sont montrées capables de pénétrer tous les marchés, et relèvent de nouveaux défis tous les jours. Si l'impact du numérique est ressenti dans tous les domaines, les enjeux et les solutions sont propres à chaque secteur et nécessitent une étude particulière. L'approche sectorielle est intéressante voire nécessaire afin d'appréhender les spécificités juridiques et économiques de chaque domaine.

Dans ce cadre, DLA Piper propose une réflexion s'articulant autour de onze thèmes, rédigés par les avocats du cabinet, afin d'analyser de manière non exhaustive les conséquences du numérique. Les sujets traités varient - ils peuvent être aussi larges que la relation entre l'éthique et les nouvelles technologies ou aussi précis que la réglementation des jetons numériques au Luxembourg ou encore la cybersécurité en Afrique francophone. Cette deuxième édition du Guide aborde par ailleurs les enjeux numériques dans les secteurs classiques comme l'aéronautique, l'hôtellerie ou la santé.

Cette déclinaison sectorielle est complétée par une série d'entretiens avec des praticiens, des entrepreneurs, des dirigeants et des philosophes, permettant d'apporter un éclairage pratique sur les différentes manières - juridique, managériale, éthique ou sociale - dont l'innovation est perçue et pratiquée mais aussi faire apparaître les facteurs non négligeables de blocage à son développement. Nous remercions infiniment ces personnalités pour leur éclairage précieux.

Un lexique et un index d'abréviations sont aussi proposés, afin de mieux appréhender le nouveau lexique associé à la transformation numérique.

---

1. Le Guide du numérique, DLA Piper & Option Finance, 2017.  
Accessible à : <http://viewer.zmags.com/publication/d061946f#/d061946f/1>

Présentation .....	4
Biographie des auteurs .....	7
Biographie des témoins .....	9
Introduction .....	12
Grand Témoin .....	13
<b>Thème 1 Aéronautique &amp; transformation numérique</b> .....	15
1. Le consommateur digital au centre de l'offre aérienne : la transformation digitale via la consécration de l'expérience utilisateur .....	18
1.1. Qui dit « utilisateur » dit « données » .....	18
1.2. La plateforme numérique : le point de rencontre de deux mondes .....	20
2. L'optimisation de la production : la transformation digitale des métiers, systèmes et méthodes .....	21
2.1. La digitalisation des méthodes de production comme gage de compétitivité .....	21
2.2. La digitalisation des outils de productivité via de nouveaux modèles de sourcing .....	22
3. La création de nouveaux métiers : la transformation digitale de l'activité commerciale .....	23
3.1. La nouvelle tendance du constructeur informaticien .....	23
3.2. La culture de l'innovation comme clé de croissance à long terme .....	24
<b>Thème 2 Immobilier &amp; transformation numérique : la Proptech change la donne</b> .....	26
1. La proptech révolutionne le secteur immobilier .....	29
1.1. Une facilitation du processus de gestion immobilière .....	29
1.2. Zoom sur les BIM .....	31
2. Les enjeux juridiques de la proptech .....	31
2.1. La caducité du modèle traditionnel .....	31
2.2. La nécessité d'une adaptation juridique .....	32
<b>Thème 3 Assurance &amp; transformation numérique</b> .....	34
1. Transition digitale du secteur des assurances : Repenser l'expérience client .....	36
1.1. Agilité des méthodes de travail .....	37
1.2. Processus et simplification de l'activité digitale .....	38
2. Apprentissage automatique et analytique avancée .....	39
2.1. Big Data .....	39
2.2. Impact des réglementations relatives à la confidentialité des données .....	40
3. Le digital transforme-t-il le paysage réglementaire ? .....	42
3.1. Les challenges réglementaires à l'innovation dans les secteurs insurtech .....	42
3.2. Que faire ? .....	42
3.3. Bacs à sable réglementaires .....	43
3.4. Un accroissement de la réglementation: quelles opportunités pour aider les innovateurs ? .....	43
Conclusion .....	44
<b>Thème 4 Hôtellerie &amp; transformation numérique</b> .....	46
1. La transition numérique du secteur de l'hôtellerie .....	48
1.1. L'émergence des plateformes d'hébergement en ligne .....	48
1.2. L'hôtellerie se réinvente sous l'impulsion de l'innovation digitale .....	49
2. Les enjeux juridiques de la numérisation du secteur de l'hôtellerie .....	50
2.1. Vers un encadrement juridique des plateformes d'hébergement en ligne .....	50
2.1.1. L'extension du régime d'autorisation préalable aux meublés de tourisme .....	51
2.1.2. Les nouvelles obligations de déclaration préalable des meublés de tourisme .....	51
2.1.3. Le changement de destination .....	52
2.1.4. L'encadrement légal de la durée des locations .....	52
2.1.5. La responsabilité renforcée des nouveaux acteurs du secteur du tourisme .....	52
2.2. L'adaptation de la législation fiscale .....	52
2.2.1. Les stratégies d'optimisation fiscale des entreprises numériques .....	53
<b>Thème 5 Juridique &amp; transformation numérique</b> .....	54
1. La transformation de l'environnement juridique .....	56
1.1. Les nouvelles offres de prestations de services juridiques .....	57
1.2. Une transformation engendrée par différents phénomènes .....	57
2. Les impacts sur les professionnels du droit .....	58
2.1. Une transformation qui affecte la justice et ses institutions .....	58
2.2. Les réponses technologiques et organisationnelles des cabinets d'avocats et des directions juridiques des entreprises .....	59
2.3. La transformation digitale au secours de la justice ? .....	60
3. Impacts sur le management dans les organisations : la collaboration des ressources humaines ou la « disruption » du management .....	61
3.1. L'empowerment .....	61
3.2. Le développement personnel de la génération Y .....	62
<b>Thème 6 Santé &amp; transformation numérique</b> .....	64
1. La numérisation de la santé : un marché en ébullition .....	67
1.1. L'influence des nouvelles technologies sur l'accès aux soins .....	67
1.2. Une meilleure qualité de soins ? .....	67
2. Focus sur les enjeux de la digitalisation de la santé .....	68
2.1. Les enjeux éthiques et juridiques .....	68
2.2. La relation médecin-patient .....	69
<b>Thème 7 Données personnelles &amp; transformation numérique en Afrique Francophone</b> .....	71
1. Le cadre légal et réglementaire applicable à la cybersécurité en Afrique francophone : un arsenal encore peu développé et à l'efficacité limitée .....	74
1.1. Des déclarations de principes au niveau régional .....	74
1.2. ... doublés de dispositions plus spécifiques au niveau national d'effet toutefois limité .....	76

2. Quelles sont les bonnes pratiques internationales en matière de sécurité des données personnelles ?	78
2.1. France : une réglementation historiquement basée sur la gestion « en amont » des risques de sécurité	79
2.2. La nouvelle réglementation européenne applicable dès le 25 mai 2018 : un arsenal juridique répondant à une logique de prévention et de réaction	80
2.3. Les principales obligations de sécurité des données aux États-Unis	81
3. Le respect d'un socle minimal d'obligations de sécurité inspiré des meilleures pratiques internationales sera difficilement contournable pour les groupes ayant des activités en Afrique	82

**Thème 8 Politique de concurrence & transformation numérique : la question de la Data** ..... 84

1. L'explosion du numérique : la collecte massive de données	86
1.1. Données et entreprises, de quoi parle-t-on?	87
1.1.1. Des données au «big data» : l'expansion des données dans tous les secteurs	87
1.1.2. L'utilisation des données dans l'économie	88
1.2. Les problématiques concurrentielles soulevées par la détention de données	89
1.2.1. L'ampleur des données : une source d'inquiétude pour les autorités de régulation	90
1.2.2. La collecte massive de données, facteur d'une transparence accrue du marché	91
1.2.3. Des problématiques déjà partiellement abordées par les autorités de concurrence	92
1.2.4. La collecte massive de données confère-t-elle un avantage concurrentiel durable ?	93
2. Analyse de l'effet des données : les défis des autorités de concurrence	95
2.1. La définition de marché	95
2.2. L'adaptation des outils et des méthodes	97
2.2.1. Vers une évolution des règles de concurrence applicables ?	97
2.2.2. Contrôle des concentrations : des seuils inadaptés	98

**Thème 9 Jetons numériques : les ICO au Luxembourg : Présentation générale et enjeux juridiques** ..... 100

1. Définition des ICO	102
1.1. Fondements juridiques	103
1.2. Mécanisme	103
2. Catégories de jetons	103
3. Avis des autorités de régulation	103
3.1. AEMF	103
3.2. OICV	104
3.3. CSSF	104
3.3.1. « Avertissement sur les ICO et tokens » publié par la CSSF	104
3.3.2. Recommandation de la CSSF	105
3.4. FINMA	105
3.5. Autorité des marchés financiers (« AMF »)	106
3.6. Ministre des Finances lituanien	106
4. Enjeux juridiques	106
4.1. Régime prospectus	107

4.2. Autorisations requises	107
4.2.1. Établissement de crédit	107
4.2.2. Établissement de paiement	108
4.2.3. Entreprise d'investissement	109
4.2.4. Fonds d'investissement : AIFM	109
4.2.5. Professionnels du secteur financier accordant des prêts	109
4.2.6. Instrument constituant une obligation perpétuelle	109
4.3. Blanchiment d'argent et lutte contre le terrorisme	109
4.4. Protection des données	110
4.5. Code de la consommation	110
5. Conclusion	110

**Thème 10 Objets connectés & transformation numérique :** ..... 111

1. Un marché en plein essor avec une demande croissante en capacité	114
2. Itinérance internationale : dans l'attente de clarifications au niveau européen, l'itinérance intra-communautaire des objets connectés est soumise à la réglementation tarifaire ex ante	114
3. Protection des données personnelles : quelles que soient les données traitées, quelle que soit la qualification retenue pour le fournisseur, les obligations du RGPD seront désormais incontournables	115
4. Le projet de règlement ePrivacy : des obligations complémentaires à prendre en compte ?	116
4.1. Articulation entre RGPD et règlement ePrivacy	116
4.2. Modalités d'application du règlement ePrivacy à l'IdO	117
4.3. Pour conclure	118

**Propos conclusif Intelligence artificielle : quel encadrement ?** ..... 119

1. Encadrement de l'intelligence artificielle dans une perspective « individualiste »	122
1.1. L'intelligence artificielle, un moyen de mise en conformité de l'entreprise au RGPD	122
1.2. Le RGPD, un moyen d'encadrer les projets basés sur l'intelligence artificielle	123
2. Encadrement de l'intelligence artificielle dans une perspective « collectiviste »	123

**Quelle vision pour le digital en France ?** ..... 126

1. La nécessaire adaptation du modèle français face à la transformation digitale actuelle	127
1.1. Vers un modèle français souverain et durable réconciliant innovation et cadre éthique	128
1.2. La dimension humaine nécessairement impactée par la transformation numérique	128
2. L'éthique comme notion régulatrice au déploiement de la transformation digitale	129
2.1. Le foisonnement avéré des usages digitaux dans les secteurs régulés	129
2.2. L'interprétabilité du digital, le nouveau challenge éthique des data scientists	131

Index des abréviations	132
Lexique	133
à propos de DLA Piper	138

## Biographie des auteurs



**Xavier Norlain**, Avocat associé, co-Managing Partner de DLA Piper France. Il conseille des fonds d'investissement pour leurs opérations d'acquisitions avec effet de levier (LBO), de capital-risque et de capital développement, et des groupes industriels ou de services pour leurs opérations de haut de bilan, de restructuration ou de croissance externe.

♥ Introduction



**Gregory Tulquois**, Avocat associé, département IP-T France. Responsable du département contrats commerciaux et droit économique. Il intervient sur les contrats stratégiques et les projets de transformation, dans les secteurs aéronautiques, industrie et produits de consommation.

♥ Thème Aéronautique



**Sonia de Kondserovsky**, Avocat associé, département Corporate France. Elle intervient dans les opérations de fusions & acquisitions complexes dans le secteur de la santé et des technologies/télécoms.

♥ Thème Santé



**Laurent Massinon**, Avocat associé, département Finance, Projects & Restructuring Luxembourg. Il intervient dans les opérations bancaires et financières ainsi que dans le domaine de la ré(assurance). Il intervient également en conseil et en contentieux dans les transactions relatives aux marchés des capitaux.

♥ Thème ICO



**Édouard Sarrazin**, Avocat associé, département Litigation & Regulatory France. Il intervient en droit de la concurrence, européen & national ainsi qu'en droit de la distribution & droit commercial.

♥ Thème Concurrence



**Mathilde Tariel-Savy**, Avocat senior, département Real Estate France. Elle intervient en conseil et en contentieux sur l'ensemble des questions de droit immobilier, notamment dans le suivi des acquisitions d'actifs immobiliers et le développement et la location d'immeubles.

♥ Thème PropTech



**Caroline Brun**, Avocat, département Real Estate France. Elle intervient dans le cadre d'investissements immobiliers, notamment pour les acquisitions et cessions d'entreprises ou de portefeuilles d'actifs immobiliers.

♥ Thème Hôtellerie



**Clara Deveau**, Avocat, département Litigation & Regulatory France. Elle intervient dans les contentieux en droit français et européen de la concurrence, notamment en matière de pratiques anticoncurrentielles et de contrôle des concentrations.

♥ Thème Concurrence



**Jonathan Rofé**, Avocat associé, Responsable du département IP-T de DLA Piper France. Il assiste tant les entreprises utilisatrices que les prestataires et fournisseurs de services, d'applications ou d'infrastructures informatiques pour l'élaboration et la négociation de leurs contrats. Il accompagne également de nombreuses entreprises de différents secteurs d'activités (santé, luxe, industrie, etc.) dans la transformation digitale de leurs activités.

♥ Thème Santé



**Florence Guthfreund-Roland**, Avocat associé, département IP-T France. Elle intervient dans le secteur des télécommunications, des technologies de l'information et les transactions relatives à l'externalisation de services.

♥ Thème Afrique & Télécoms/IoT



**Denise Lebeau-Marianna**, Avocat associé, département IP-T France. Elle intervient en matière de données personnelles et le droit des nouvelles technologies. Elle conseille également ses clients dans le domaine des données de santé.

♥ Conclusions sur l'IA



**Myriam Mejdoubi**, Avocat associé, département Real Estate France. Elle intervient dans les opérations d'acquisitions, de financements, de baux commerciaux, de droit de la construction et de droit des sociétés.

♥ Thème Hôtellerie



**Luc Bigel**, Avocat senior, département Finance & Projects. Il assiste les assureurs, des réassureurs, des banques et intermédiaires, français ou étrangers, dans toutes leurs problématiques assurantielles (vie ou non vie), réassurantielles ou de distribution, tant en conseil qu'en contentieux.

♥ Thème Assurance



**Hamza Akli**, Avocat, département Finance & Projects. Il intervient en matière de réglementation applicable aux entreprises d'assurance, de réassurance, ainsi qu'aux intermédiaires d'assurance tant en conseil qu'en contentieux.

♥ Thème Assurance



**Agnès Chavernoz**, Avocat, département IP-T France. Elle intervient dans le cadre du déploiement de projets informatiques et de transformation digitale et conseille en contrats informatiques et commerciaux, protection des données personnelles et propriété intellectuelle.

♥ Thème Aéronautique



**Mathilde Hallé**, Avocat, département IP-T France. Elle conseille des entités privées et publiques nationales et internationales pour la réalisation de projets portant sur la télécommunication, les médias, les nouvelles technologies, l'Internet et la protection des données personnelles.

♥ Thèmes Afrique & Télécoms/IoT



**Yaël Hirsch**, Avocat, département IP-T France. Elle intervient sur les problématiques liées à la protection des données, notamment dans le secteur de la santé, des communications électroniques, des technologies et du commerce électronique.

📍 **Conclusion sur l'IA**



**Aurelia Pons**, Avocat, département IP-T France. Elle intervient en conseil et en contentieux dans le secteur de l'informatique, des communications électroniques et des nouvelles technologies.

📍 **Thème Télécoms/IoT**



**Christina Nickel**, Legal Advisor, département Finances, Projects & Restructuring Luxembourg. Elle intervient dans les opérations bancaires et financières, notamment sur les questions réglementaires. Elle intervient également en conseil et en contentieux dans les transactions relatives aux marchés des capitaux.

📍 **Thème ICO**



**Isabelle Eid**, Avocat conseil, responsable des départements Knowledge Management pour la France, et du Marketing & Développement pour la France et le Benelux. Elle coordonne également des groupes de travail mêlant la doctrine et praticiens sur les enjeux prospectifs des réformes telles que le Code civil et la transformation numérique. Elle est coordinateur éditorial du présent ouvrage sur le numérique et ses déclinaisons sectorielles. Elle a été également coordinateur éditorial du Guide 1 du numérique en 2017 ainsi que des travaux sur le code civil primé par le Financial Times Innovative Lawyer (standout dans la category « sharing knowledge and business management ») en 2016.

📍 **Présentation, Thème Juridique & Conclusions sur l'éthique et la transformation digitale**

## Biographie des témoins



**Véronique di Benedetto,**  
**Vice présidente France, Econocom et**  
**Présidente de la commission du Syntec**  
**« Femmes du numérique ».**

Véronique di Benedetto a occupé différents postes de Direction générale en France et à l'International dans des entreprises informatiques. Elle est actuellement Vice-Présidente France et administratrice d'Econocom, groupe européen qui accompagne la transformation numérique des entreprises. Également administratrice du Syntec Numérique et de la Fondation Femmes@Numérique, elle est aussi au comité stratégique de plusieurs start-ups technologiques. Chevalier de la Légion d'honneur (2013).



**Jean-Pierre Bienaimé,**  
**Secrétaire Général de la 5G Infrastructure**  
**Association et Président de l'Institut**  
**de Recherches Economiques et Sociales**  
**sur les Télécommunications (IREST).**

Ayant rejoint France Télécom (FT) dès 1979, Jean-Pierre Bienaimé a été notamment Conseiller du DG des Télécoms du Maroc à Rabat, Directeur Adjoint du Marketing International à FT, DG de Nexus International, et Directeur du Support aux Opérations Internationales Mobiles pour le Groupe Orange. En 2009, Jean-Pierre fut nommé Directeur de la Stratégie et de la Communication à Orange Wholesale France, puis en 2014 Directeur d'Orange Wholesale Community et de la Communication. Jean-Pierre a été président de l'UMTS Forum de 2003 à 2016. A compter de septembre 2016, Jean-Pierre devient Secrétaire Général du 5G PPP auprès de la Commission Européenne, avec la mission de promouvoir l'écosystème et la voix de l'Europe sur la 5G. En 2014, il a été élu membre du Conseil d'ESSEC Alumni, et en 2015, il a été élu président de l'IREST technologies/télécoms. [📍 Thème Santé](#)



**François Chopard,**  
**CEO, Starburst Accelerator.**

François est le fondateur de Starburst Accelerator, le 1<sup>er</sup> incubateur/accélérateur dédié aux start-ups aérospatiales. François se spécialise dans les secteurs de l'aéronautique, de l'aérospatiale et de la défense avec des enjeux technologiques de premier plan et a développé une grande expérience des problématiques liées à l'innovation. Cela l'a amené à parler d'innovation au Forum économique mondial de Davos. Il travaille aujourd'hui sur des sujets tels que les tendances futures, la stratégie produit, l'innovation ouverte pour les entreprises principalement de l'industrie aérospatiale ainsi que les fonds d'investissement. Avant de rejoindre Impulse Partners, François était associé chez Oliver Wyman à Paris. Il a également été fondateur et CEO d'Arendi Consulting. François est diplômé de l'École Supérieure d'Electricité (Supélec) de Paris, France. Il a débuté sa carrière en tant qu'ingénieur Airbus et a passé deux ans dans un laboratoire de recherche de l'US Airforce.



**Olivier Colcombet,**  
**Directeur Général de Digit RE et Président**  
**des réseaux immobiliers Capifrance**  
**et d'OptimHome.**

Diplômé de l'ESLSCA et d'un Executive MBA, Olivier Colcombet a commencé sa carrière comme auditeur chez KPMG. Il a ensuite assumé différentes fonctions de direction financière, de direction générale chez Electronic Arts et chez Namco Bandai. Depuis 2013, Olivier Colcombet gère la croissance et le développement des actifs immobiliers d'Artémis. Il a contribué à la création de Digit RE Group dont il est le directeur général. Il assure dans ce cadre la présidence des marques de Digit RE Group à savoir : les 4 réseaux immobiliers, OptimHome, Capifrance, Immobilier Neuf et Réfleximmo, du site d'estimation en ligne Drimki, de Coworkimmo, les centres de coworking dédiés à la filière immobilière et de Dili, une offre simple et sécurisée pour raccourcir les délais de vente d'un bien immobilier.



**Michel Combet,**  
**Directeur général, Fédération Française**  
**des Télécoms.**

Ingénieur du corps des Mines, Michel Combet a pris les rênes de la Fédération début mai 2016, après un parcours de plus de 18 ans dans le domaine de l'économie numérique et des médias, au sein des autorités nationales de régulation sectorielle, l'ARCEP et le CSA, dans différents cabinets ministériels, ainsi que pendant plusieurs années aux Etats-Unis, plus particulièrement dans la Silicon Valley.



**Jean-François Gendron,**  
**Président,**  
**French Healthcare.**

Jean-François débute sa carrière professionnelle en prenant la direction de l'entreprise familiale Gendron Industrie, fonction qu'il assumera pendant 20 ans. En 2001, il reprend SOTEC médical, alors en redressement judiciaire. Très rapidement, il dynamise l'entreprise qui aujourd'hui emploie plus de 70 personnes. Vice-président de la CCI de Nantes (2000-2005), il en prend la présidence en 2005. Réélu à ce poste début 2011. Au plan national, il occupe le poste de Président de CCI International depuis juillet 2013. Fin 2016, il devient vice-président Développement de la société HAcare Medical Interior. En mars 2017, il prend la présidence de l'association French Healthcare lancée par le ministre des affaires étrangères et du développement international. Initiée comme une marque, French Healthcare contribue à promouvoir l'expertise et l'excellence française en santé. En juillet 2017, il est nommé Consul de la Principauté de Monaco à Nantes.



**Frédéric Jenny,**  
**co-directeur du Centre Européen de Droit**  
**et d'Économie de l'ESSEC (CEDE) et Président**  
**du Comité de la concurrence de l'OCDE.**

Frédéric Jenny, Ph.D en économie de l'Université de Harvard (1975), docteur en économie de l'Université de Paris (1977) diplômé de l'ESSEC (1966) est professeur d'économie à l'ESSEC Business School, Co-Directeur du Centre de Droit et d'Économie de l'ESSEC et Président du Comité de la Concurrence de l'OCDE (depuis 1994). Il a été Administrateur non-exécutif de l'Office of Fair Trading du Royaume Uni 2007 à 2014), magistrat à la Cour de Cassation (Chambre Commerciale) (2004 à 2012), Vice-Président du Conseil de la concurrence (1993-2004) et Président du Groupe de Travail sur le Commerce International et la Concurrence de l'Organisation Mondiale du Commerce OMC (1994-2003). Il a publié de nombreux articles en France et à l'étranger dans les domaines du droit et de l'économie de la concurrence, de la régulation économique, du commerce international et du développement économique.



**Nicolas Guérin,**  
**Secrétaire Général d'Orange et Président**  
**du Cercle Montesquieu.**

Nicolas Guérin est diplômé de l'Institut de droit des affaires (IDA) et du DESS droit des affaires et fiscalité Université de Paris II Panthéon Assas. Il est secrétaire général du groupe Orange depuis mars 2018, groupe dans lequel il avait auparavant exercé des fonctions de directeur juridique concurrence et réglementation (1998-2009) puis de directeur juridique groupe (2009-2018). Il est également Secrétaire du Conseil d'administration d'Orange et administrateur d'Orange Côte d'Ivoire. Il est par ailleurs Président du Cercle Montesquieu, Président de la Commission droit public économique et du Comité concurrence du Medef et Président du Comité d'évaluation et d'orientation de la Chaire Internationale de droit de l'espace et des télécommunications de l'Université de Paris XI. Il est également administrateur de l'AFJE.



**Gaspard Koenig,**  
**Philosophe, écrivain et Président du**  
**laboratoire d'idées GenerationLibre.**

Philosophe (Diplômé de l'ENS, agrégation, Columbia), Gaspard Koenig dirige le think-tank libéral Generation Libre, qu'il a fondé en 2013. Il a travaillé précédemment au cabinet de Christine Lagarde à Bercy, et à la BERD à Londres. Il est l'auteur de romans et d'essais, enseigne à HEC, et apparaît régulièrement dans les médias – notamment à travers sa chronique hebdomadaire dans Les Echos. est l'auteur d'une dizaine de romans et d'essais, notamment autour de Mandeville, de Gilles Deleuze et de l'avenir du libéralisme.



**Olivier Labbé, Directeur Général, Cap DC.**

Diplômé de l'école Centrale de Lyon, Olivier Labbé a travaillé pendant 17 ans chez IBM en tant que responsable Business et Delivery dans les services aux infrastructures. Il a rejoint en 2008 Cap Ingelec, entreprise d'ingénierie spécialisée dans l'efficacité énergétique, comme directeur général délégué. Il rejoint ensuite Hewlett-Packard pendant 5 ans où il occupe les postes de Directeur Général Technology Services France puis de Directeur du Développement France. Depuis octobre 2015, Olivier Labbé est directeur général de Cap DC, marque internationale de la société d'ingénierie girondine Cap Ingelec.



**Laurent Marochini,**  
**Président Groupe ALFI Digital/Fintech**  
**Blockchain & Crypto-currency**  
**(Association Luxembourgeoise de fonds**  
**d'investissement).**

Avant de rejoindre SGSS en 2006 en tant que Risk Manager, Laurent a travaillé chez BNP Securities Services et Crédit Suisse Private Banking. En 2010, Laurent est devenu Responsable Innovation et Qualité. Il a été reconnu deux fois 2ème meilleur Innovateur du Groupe Société Générale. Blockchain Leader pour SGSS, Il est aussi co-président du groupe de travail Blockchain & Crypto Currencies à l'ALFI et membre du Comité Exécutif Fintech & Digital. En septembre 2018, Laurent est devenu responsable du Lab d'innovation de Société Générale à Luxembourg #LePlateauLux.



**Jean-Charles Samuelian,**  
**Co-fondateur & CEO, Alan.**

Alan est la première assurance santé digitale en Europe, et la première assurance indépendante agréée par la Banque de France depuis 1986. Créée en 2016, la société a levé plus de 35 M€ avec des investisseurs internationaux dont Index Ventures, Partech et CNP. Avant cela, Jean-Charles a co-fondé Expliseat, qui a révolutionné le siège d'avion de classe éco. Il code depuis qu'il a 12 ans. Jean-Charles a reçu de nombreux prix dont la Médaille du Redressement Productif, deux Prix Montgolfier. Jean-Charles est membre du Conseil National du Numérique (CNNum), et du conseil d'administration de France Fintech. Il est ingénieur des Ponts & Chaussées, MBA du Collège des Ingénieurs et est diplômé de l'Institut des Actuaire.



**Arnaud Morvan,**  
**Responsable Digitalisation, B&B Hôtels.**

J'ai intégré B&B en 2002, au sein de l'équipe IT, en tant que webdesigner ou j'ai pu travailler sur la mise en place des plateformes web et e-commerce, ainsi que sur la mise en place des supports de com hôtels, internes, et le développement de l'intranet de l'entreprise. J'ai ensuite intégré l'équipe Marketing en tant que webmarketeur et Chef de projet web ou j'ai pu accompagner la professionnalisation de la distribution digitale, de la communication et la mise en place des première plateformes d'avis clients chez B&B. En 2011 je prends la responsabilité de l'acquisition et de la distribution. De 2014 à 2016 je prends la responsabilité du Service Médias et CRM. En 2016, je reprends la Responsabilité du service Ecommerce jusqu'en Juin 2018 ou le Groupe souhaite accompagner la Transformation Digitale par l'interne et me confie cette mission en tant que Responsable Digitalisation.

# Introduction

Par **Xavier Norlain**

**A**u rang des progrès ayant bouleversé nos comportements, le numérique irrigue inévitablement la société dans son ensemble. Le paysage macroéconomique actuel continue d'influencer fortement les investissements, le commerce mondial et entraîne subséquemment une mutation du système économique.

Face à une transition numérique aussi effrénée qu'inéluctable, les entreprises doivent relever un défi pour sensibiliser leurs salariés à ces vagues de transformations. Le numérique irrigue incontestablement tous les secteurs d'activités au sein des entreprises, de sorte qu'il conduit à s'interroger tant sur les enjeux économiques et sociaux existants et à venir, que sur les mutations formelles et matérielles que cela peut engendrer. De part l'ampleur et la profondeur de son impact, le numérique permet l'apparition de nouveaux modèles venant bouleverser des pans entiers de modèles existantes, tels que la définition et les méthodes de travail, les supports classiques de prestations de services, l'organisation et la collaboration des ressources humaines ou encore, la protection du consommateur.

En tout état de cause, le numérique est un secteur d'avenir, en perpétuelle mutation et possédant un fort potentiel de croissance. Bien que l'un des obstacles à une transition généralisée du numérique soit la nécessité de se conformer à la réglementation, la cadence de développement de certains outils technologiques a considérablement dépassé le cadre réglementaire censé les régir.

Les nouvelles technologies numériques sont ancrées au sein de toutes les pratiques professionnelles et ce, quotidiennement. Pour de nombreuses entreprises, la transformation numérique semble être «un voyage plutôt qu'une destination», car les technologies émergentes

perturbent les processus déjà numérisés, créant des pressions budgétaires non prévues lors du lancement de projets liés à la transition digitale. Le développement croissant du Big Data en tant que ressource-métier est en train de se généraliser au sein du monde de l'entreprise, des start ups, et des PME ainsi qu' à toutes les équipes financières et commerciales. Actuellement, les modes de fonctionnement de l'entreprise ne peuvent plus éviter ce phénomène. En outre, cette transformation a permis de signaler une forte hausse des applications de vente et de finance. Néanmoins, les inquiétudes concernant la sécurité des données freinent incontestablement la croissance.

Par ailleurs, sensibiliser les entreprises pour accompagner leur transformation digitale dans une démarche plus éthique, favoriserait l'édification de valeurs spécifiquement dédiées aux problématiques que posent le numérique. L'éthique recouvre effectivement des enjeux touchant à la fois au politique, à l'économie (communication, marketing, e-reputation) ou à la culture d'entreprise. L'impact du numérique sur la culture de l'entreprise et les modes de management soulève des enjeux éthiques tels que la confidentialité des données, le respect de certains principes, la nécessité de recourir à la régulation pour une meilleure politique de concurrence. De facto, alimenter un cadre éthique de manière plus généralisée, permettrait d'inciter l'exploitation du potentiel afférent aux technologies émergentes.

Ainsi, cette deuxième version du Guide constitue un éclairage essentiel pour l'appréhension de ces nouvelles problématiques juridiques, économiques et sociales, dans le cadre de la révolution numérique. L'analyse sectorielle retenue offre une étude stratégique des enjeux que représente la transformation numérique et identifie des spécificités à approfondir et exploiter.

# Grand Témoin

**Véronique di Benedetto**, Vice Présidente France, Econocom et Présidente de Femmes du numérique.

**L'expression mutation digitale tient parfois au sein des entreprises davantage d'une simple cosmétique que d'une véritable réorganisation. Comment l'entreprise peut/doit-elle véritablement embrasser cette mutation ?**

La révolution digitale que nous vivons dépasse largement le cadre purement technologique. Elle bouleverse les modèles économiques, souvent par des approches collaboratives et innovantes qui touchent directement l'utilisateur final. Nous le voyons avec l'essor des start-ups qui se concentrent au départ sur une réponse nouvelle à un besoin précis, en général pas ou mal adressé par des entreprises traditionnelles. Si cette réponse est adaptée, elle est adoptée de façon « virale » par la multitude, et donne naissance à des géants du numérique de plus en plus puissants, qui obligent les entreprises traditionnelles à se transformer en profondeur, sous peine de disparaître.

Aujourd'hui, aucune entreprise ne peut ignorer les bouleversements sociétaux, sociaux, économiques que cette révolution engendre, l'utilisateur prend le pouvoir et il doit être au centre de l'attention. Que les entreprises ne se trompent pas, il ne s'agit pas d'opérer une transformation autocentrée, mais au service des usagers. Cependant, se transformer est un processus complexe,

souvent pris par le mauvais bout. On parle solutions, outils, technologies, avant de prendre le temps de bien définir le « pour quoi » et de se concentrer sur le « pour qui ». D'expérience, j'observe que la réussite d'une transformation repose en grande partie sur la faculté de mobiliser les différentes parties prenantes internes et externes.

Et, pour aller plus loin, cette mobilisation doit s'activer autour de 3 grandes étapes :

► La construction de la cible et l'identification du catalyseur originel du besoin de transformation (concurrence nouvelle, évolution du marché, performance de l'activité, évolutions organisationnelles.)

► La clarification du point d'arrivée avec un diagnostic introspectif (qui sommes-nous ? notre mission et nos valeurs ? nos forces et nos faiblesses ? d'où partons-nous ?). De par l'évolution rapide du marché et avec l'arrivée des start-ups, les entreprises ont souvent perdu leur propre « récit ».

► La définition des passerelles pour passer du stade actuel à la vision future et l'acculturation de l'organisation interne. Le digital est un moyen, non un objectif. La définition de l'usage cible permet ensuite de définir les moyens humains, techniques et financiers qui vont porter ce projet et la feuille de route.

L'implémentation doit se faire pas à pas et non de façon radicale. Une approche « test & learn » augmente fortement l'adhésion de l'ensemble des parties prenantes car les solutions se créent avec et pour eux. Chez Econocom, par exemple, et grâce à notre expérience terrain, nous co-construisons avec nos clients et mettons en œuvre les solutions adaptées à leur transformation.



© GÉRARD UFFÉRAS

**Comment le numérique modifie-t-il l'organisation du travail au sein de l'entreprise ? Comment l'entreprise doit-elle repenser la relation sociale ? Quels sont les pièges à éviter ?**

Sous l'impulsion des nouveaux usages et de la technologie, l'entreprise comme unité de temps, de lieu et d'action va disparaître. Les entreprises seront amenées à être de plus en plus « éclatées », agiles et flexibles. Dans ce contexte et avec l'accélération des rythmes d'innovation, les entreprises doivent multiplier les collaborations internes et externes et repenser globalement leurs relations sociales. Cette nouvelle relation doit se construire par l'usage des outils technologiques (la mise en place d'outils collaboratifs, du télétravail...) et par un changement culturel et de comportements (niveau de transparence plus élevé, autonomie dans un cadre de travail plus adapté, nouveaux services aux collaborateurs).

L'entreprise doit repenser ses relations sociales autour de ce que j'appelle l'objectif de développement réciproque. Connecter les individus, par exemple, permet de créer de nouvelles formes de management venant se superposer aux traditionnelles hiérarchiques. Prenons les outils de réseaux sociaux internes : on assiste au développement de « tribus » sur des thématiques professionnelles (par expertise, projet...), comme personnelle (passion, services...). Je pense que le partage d'expertise entre les entités, les départements, les métiers, voire les autres entreprises devient une nécessité pour offrir au client final une solution globale et à forte valeur ajoutée. Les grands groupes n'hésitent d'ailleurs plus à faire collaborer leurs services de R&D avec leurs concurrents ou des start-ups.

Quels sont les pièges à éviter :

- **Croire que la transformation soit une séquence**, c'est un processus infini, presque permanent, sur un temps long.
- **Se concentrer uniquement sur la technologie**. Les ressources humaines représentent une dimension cruciale.
- **Vouloir appliquer une mutation ou projet digital réussi à sa propre organisation**.

Chaque entreprise est unique de par son patrimoine humain, son histoire et les moyens dont elle dispose.

- **Croire que l'on connaît ses utilisateurs et leurs besoins**. Il est important de sonder le terrain. L'usage doit être au cœur de la réflexion. Passer de la vente « produit » à la vente « service à l'usage » devient la priorité à mettre en œuvre.

**Pourquoi les femmes sont-elles si peu présentes au sein des entreprises du numérique ? Quels sont les freins ? Comment peut-on y promouvoir la mixité ?**

Les entreprises alertent très régulièrement sur leur difficulté grandissante à embaucher dans le numérique. Entre 170 000 et 212 000 postes dans le numérique seront à pourvoir en France en 2022.

Or en 2017 le secteur du numérique compte moins d'un tiers de femmes et ce principalement dans les fonctions dites « de support ». Seules 16 % des femmes du secteur sont des techniciennes et 27 % des femmes codeuses. Enfin, il y a seulement 20 % des femmes au sein des DSI.

Les facteurs sociohistoriques qui peuvent expliquer cette situation sont nombreux : avènement du micro-ordinateur qui a transformé l'image du secteur, naissance de la figure du geek, absence de rôles modèles, méconnaissance du secteur, puissance des stéréotypes... De ce constat alarmant, qui perdure depuis déjà des années, est née la fondation femmes@numérique qui a réussi à fédérer un large écosystème (associations, entreprises, institutions et gouvernement) pour changer d'échelle dans la mise en œuvre des actions. Ses priorités sont de cibler le grand public qui méconnaît les métiers du numérique, l'Éducation nationale pour un enseignement précoce de l'informatique, la formation professionnelle pour des cursus adaptés aux femmes en reconversion, les pouvoirs publics pour appuyer et relayer les actions lancées par les associations et les entreprises.

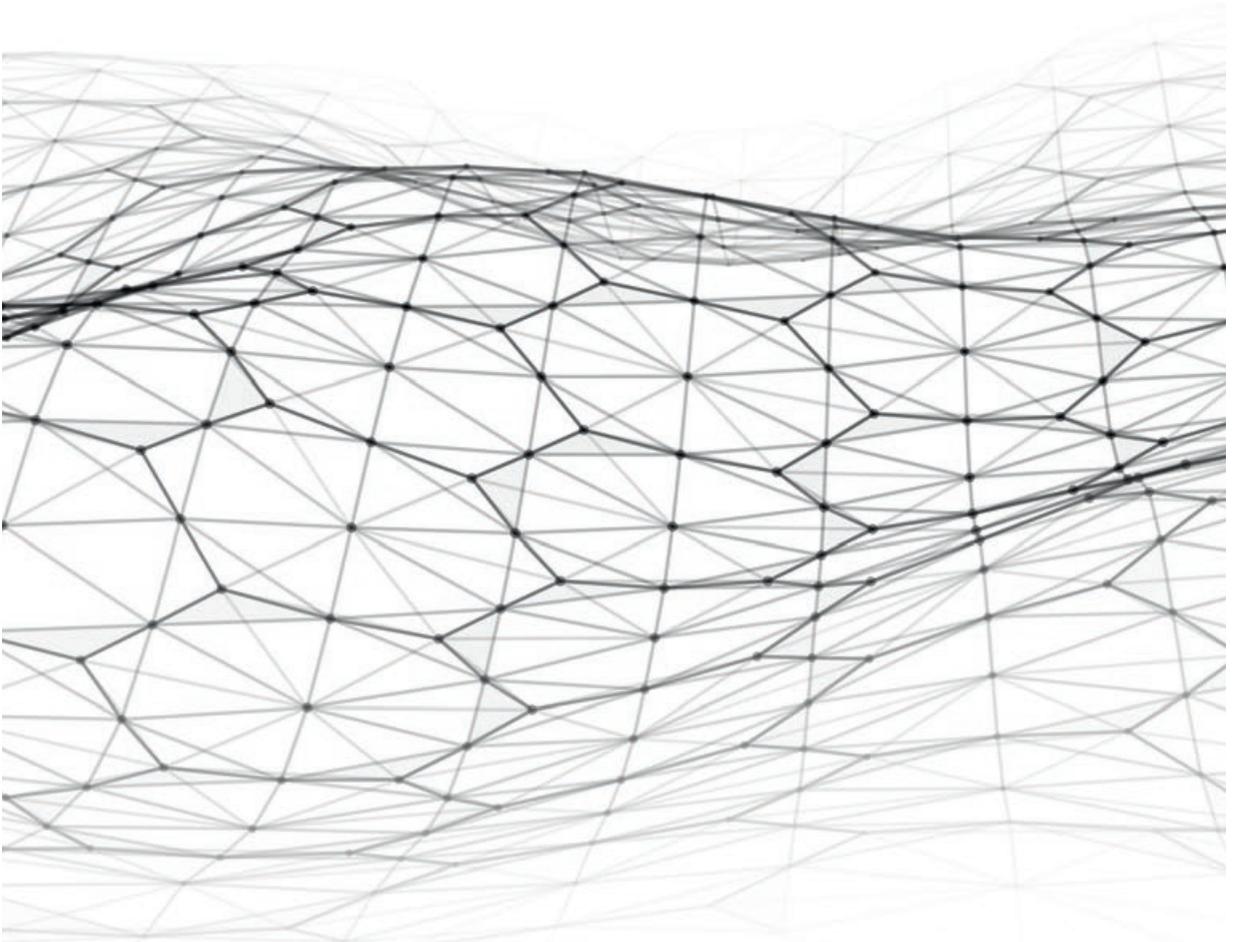
C'est une situation qui nécessite une transformation sur un temps long !

INDUSTRIE

---

THÈME 1

# Aéronautique & transformation numérique





# Le point de vue...

**François Chopard,**  
CEO, Startburst Venture

## Comment le numérique peut répondre aux problématiques de l'aéronautique ?

Concernant la conception et la construction d'un avion, les outils tels que les maquettes numériques et les outils collaboratifs de développement, comme les plateformes collaboratives, et de simulation permettent à tous les acteurs de travailler en synergie sur le même objet, avec un gain de temps formidable. Il y a moins d'itérations. Grâce à cela, on optimise l'aérodynamisme de l'appareil et sa performance, mais aussi le vieillissement du matériel en phase de conception. Dans les processus de fabrication, les outils permettent de s'assurer que tous les produits arrivent au bon moment et au bon endroit sur la liste d'assemblage, dans les mains du bon opérateur. La blockchain, qui n'en est qu'aux débuts, est parfois utilisée pour les contrats, la réception des pièces et le paiement et l'IA pour avoir une supply chain, avec les fournisseurs qui sont avertis en temps réel en cas de dysfonctionnement, de retard, d'avance. Une fois l'avion construit, les outils, grâce aux capteurs installés dans l'appareil, permettent d'avoir des informations sur l'avion et la manière dont ils fonctionnent. Il est possible de faire de la maintenance prédictive ou anticipée.

## Quelles conséquences sur les pratiques du secteur ?

La blockchain va avoir des conséquences sur la manière de payer les transactions. Il va falloir revoir tous les contrats et tous les échanges entre acheteurs et fournisseurs. Côté passagers, cela va également avoir beaucoup d'implications sur le pricing des billets d'avions et la notion actuelle de « compagnie aérienne », telle qu'elle existe aujourd'hui, pourrait disparaître. Il sera possible de rentabiliser les vols des business jets et hélicoptères, qui actuellement, voyagent quasiment à vide. Le prix des billets va donc énormément chuter, car les nouveaux outils vont permettre d'avoir plus de sièges disponibles. De nouveaux acteurs vont apparaître. Il commence à y avoir de plus en plus de start-ups qui développent des avions, sur des courtes distances, notamment, ce

qu'on appelle aujourd'hui les taxis volants, car les outils de conception deviennent plus accessibles. Quand ces entreprises auront développé leurs petits avions, elles vont vouloir grandir. Les grands groupes, qui ne maîtrisent pas ce qui se passe, mais le subissent, peuvent garder un œil sur ces entreprises grâce à la pépinière que nous développons et qui propose des partenariats. C'est un laboratoire d'innovation. Ils peuvent voir émerger ses nouveaux acteurs et se préparer à leur arrivée. À terme, ils pourraient les racheter, ou collaborer avec eux.

## Comment le numérique permet-il d'innover dans un secteur où le cadre réglementaire est très contraint ?

Ces contraintes réglementaires ont été pendant longtemps une barrière à l'entrée de nouveaux acteurs dans le secteur. Mais avec le numérique, on voit que ces barrières baissent. Il est plus facile de comprendre les règles de certification, la réglementation et tout cela coûte moins cher. Le numérique permet de faire chuter les coûts de développement et permet l'accès à de nouveaux acteurs. C'est déjà le cas dans le secteur spatial, si l'on prend l'exemple de Space X, qui a développé un moteur pour les fusées.



Par **Gregory Tulquois** et **Agnès Chavernoz**

**A**u printemps 2017, le groupe Airbus, dont le cœur de métier est la fabrication d'avions et d'hélicoptères civils et militaires, lançait Skywise, une plateforme numérique dédiée initialement à ses clients compagnies aériennes : *via* cette plateforme, l'objectif du programme est de fournir aux professionnels de l'aviation un outil numérique leur permettant d'analyser à grande échelle les données issues notamment des composants avioniques des flottes d'aéronefs et d'en tirer des résultats afin notamment d'améliorer leur performance opérationnelle (par exemple en optimisant les opérations de maintenance d'un appareil) et économique (par exemple en réduisant la consommation de carburant). Signe d'un secteur profondément impacté par l'essor des nouvelles technologies, cet exemple est surtout représentatif de la transformation des modèles économiques traditionnellement établis dans le secteur aéronautique du fait de sa digitalisation. Depuis ces dernières années en effet, le rôle des solutions technologiques non liées à l'opération des vols dans le secteur aéronautique a évolué : marginal à l'origine, il est depuis devenu l'un des piliers majeurs de la transformation des entreprises de l'aéronautique, et celles-ci considèrent aujourd'hui la nécessité de mettre en place une stratégie digitale efficace comme essentielle à leur succès économique.

Une stratégie digitale efficace permet tout d'abord d'innover : cette capacité d'innovation sert de levier afin de devancer les concurrents traditionnels, tout en prévenant la multiplication d'acteurs nouveaux du secteur, « natifs numériques » ambitieux et agiles, dont les modèles commerciaux novateurs viennent bouleverser les règles traditionnellement établies pour le jeu de la concurrence dans le secteur de l'aéronautique.

Une stratégie digitale efficace permet ensuite d'optimiser les méthodes et par suite, les coûts

de développement et de production, dans un secteur à forte intensité capitalistique. Enfin, une stratégie digitale efficace permet de créer de nouvelles perspectives de revenus tirant notamment leur origine dans la mise à disposition de solutions technologiques à forte valeur ajoutée permettant d'optimiser l'exploitation des opérations aériennes.

Par conséquent, le secteur aéronautique devient digital et digitalisé : digitalisé car la technologie y est utilisée comme un levier d'optimisation des outils de production et de productivité, et digital car la technologie y est utilisée comme un vecteur de croissance dans des domaines complémentaires au cœur de métier. Ce virage vers le numérique, s'il présente de nombreux avantages, n'est pas sans soulever plusieurs défis d'un point de vue juridique pour les entreprises concernées : il suppose en effet de s'assurer que la stratégie digitale définie est mise en place en conformité avec le cadre réglementaire applicable aux projets digitaux (réglementation applicable aux plateformes numériques, à la protection des données, etc.), de maîtriser les risques inhérents à l'externalisation des données, phénomène tendanciel du fait de l'accroissement des activités de collecte de données à grande échelle comme lame de fond de projets digitaux (sécurité et confidentialité des données hébergées, continuité et niveaux de service, etc.), de protéger les actifs immatériels innovants présentant un avantage concurrentiel avéré (logiciels, algorithmes, etc.), et généralement, de tenter d'encadrer au mieux les conditions d'engagement de sa responsabilité dans ces domaines d'activité nouveaux *via* les contrats conclus avec les partenaires, clients et fournisseurs.

Cet article a pour vocation d'agrèger autour de trois thématiques les enjeux juridiques généralement identifiés dans les projets de transformation

digitale des entreprises de l'aéronautique. En pratique en effet, la mise en place d'une stratégie digitale dans le secteur aéronautique s'observe principalement autour de trois axes : la redéfinition des expériences utilisateurs, utilisateurs devenus aujourd'hui consommateurs digitaux dont le parcours, de l'achat d'un billet d'avion à l'atterrissage, est rendu de plus en plus digital (1) ; la digitalisation des processus de production en vue de les rendre plus efficaces (2) ; et enfin, la création de nouveaux métiers à forte perspective de croissance, basés sur le déploiement industriel de solutions technologiques (3).

## 1. Le consommateur digital au centre de l'offre aérienne : la transformation digitale via la consécration de l'expérience utilisateur

Pour répondre à la demande croissante en matière de transport aérien<sup>1</sup> et capter une clientèle grandissante, les acteurs de l'industrie aéronautique redoublent de créativité et multiplient les expériences digitales destinées à attirer cette clientèle. Le passager utilisateur final, nouvel objet des attentions, est une personne physique, donc toute forme d'utilisation de ses données est soumise au règlement européen relatif à la protection des données<sup>2</sup> (le « RGPD ») (1.1), et il est consommateur, donc l'ensemble des règles applicables au commerce électronique s'applique à son expérience d'achat en ligne (1.2).

### 1.1. Qui dit « utilisateur » dit « données »

Pour séduire, il faut connaître. La volonté d'attirer une clientèle de plus en plus nombreuse ne faisant pas exception à ce principe, les opérateurs du secteur aéronautique s'efforcent de développer de solutions destinées à collecter et à analyser le plus grand nombre d'informations possible sur cette clientèle<sup>3</sup>. Les données tirées de l'« expérience utilisateur » sont précieuses : quand elles sont utilisées à bon escient (par exemple, combinées entre elles ou déduites par des procédés d'intelligence artificielle), elles servent à améliorer la connaissance

de l'utilisateur et de ses attentes et par conséquent, à lui proposer des services individualisés permettant de le fidéliser autour de l'expérience et de la marque.

D'un point de vue juridique, le réflexe induit par l'actualité générale de ces derniers mois conduit immédiatement à s'interroger sur les conditions dans lesquelles sont menées ces analyses de données : s'il s'agit de données permettant, directement ou indirectement, d'identifier un passager, le RGPD s'applique à leur traitement<sup>4</sup>. Au vu de la définition très large de la « donnée

1. Les projections pour 2036 indiquent que le nombre de passagers aériens va presque doubler, atteignant 7,8 milliards, Association internationale du transport aérien, octobre 2017.

2. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

3. Les exemples sont nombreux : alors que Thalès établit un centre de recherche dédié entièrement à l'amélioration, via sa digitalisation notamment, du divertissement à bord et de la connectivité des passagers (interaction entre l'équipement de l'avion et les équipements personnels de communication des passagers, systèmes de paiement en ligne à bord, etc.), la compagnie aérienne AirAsia s'associe à Palantir, prestataire spécialisé dans la science des données, dont les solutions de *data analytics* permettront notamment à la compagnie aérienne d'étudier le comportement de ses passagers en vol afin de leur proposer une expérience de plus en plus personnalisée et ainsi, de les fidéliser à l'image de la compagnie.

4. Selon le RGPD, la donnée à caractère personnel est « toute information se rapportant à une personne physique identifiée ou identifiable [...] ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

5. Décret n° 2014-1095 du 26 septembre 2014 portant sur la création d'un traitement de données à caractère personnel dénommé « systèmes API-PNR France » pris pour l'application de l'article L. 232-7 du Code de la sécurité intérieure.

à caractère personnel » (le numéro de siège passager en est une, par exemple<sup>5</sup>), il convient de considérer que bon nombre des données issues de l'expérience utilisateur traitées par les professionnels de l'aéronautique tombent dans cette définition, et leur traitement doit donc répondre aux exigences d'une collecte loyale, licite et proportionnée au vu de sa finalité initiale<sup>6</sup>.

Dans le contexte d'une expérience de vol, par exemple, si les données d'identification de l'utilisateur, nécessaires initialement aux fins de la vente du billet d'avion, de l'embarquement et du passage des frontières, sont ensuite utilisées par une agence de voyage en ligne ou une compagnie aérienne afin d'étudier le comportement et les habitudes de cet utilisateur pour lui proposer des services plus adaptés à ses besoins (horaires de vols moins chers, services de conciergerie, préférence de place en cabine, etc.), il faut en informer l'utilisateur, et parfois même obtenir son consentement<sup>7</sup>.

Outre le respect de ces prérequis, l'enjeu de la conformité au RGPD naît aussi du recours accru aux services d'infrastructures informatiques externalisées : les entreprises de l'aéronautique, comme d'autres secteurs d'ailleurs, utilisent le *cloud* pour héberger la masse gigantesque de données qu'ils accumulent, notamment sur leurs utilisateurs.

Dans des écosystèmes *cloud* faisant intervenir une multiplicité d'intervenants parfois localisés dans le monde entier, il convient de s'assurer que l'entreprise conclut avec son prestataire un service *cloud* en parfaite maîtrise de sa chaîne de sous-traitance, puisqu'il en va de sa propre conformité aux exigences relatives à la protection des données.

Le responsable du traitement doit en effet sélectionner ses sous-traitants, ainsi d'ailleurs que les sous-traitants de ses sous-traitants, sur la base de leur conformité au RGPD<sup>8</sup>, et cela peut s'avérer délicat dans le contexte du *cloud*, où ce responsable de traitement n'est ni décisionnaire de la façon dont le service lui est fourni, ni donc des intervenants dans la fourniture globale de ce service<sup>9</sup>.

Or les sanctions encourues du fait d'une non-conformité au RGPD peuvent être

considérables<sup>10</sup>. Le respect des règles encadrant la sous-traitance d'activités de traitement et le transfert de données à caractère personnel est donc un enjeu majeur dans l'établissement des relations contractuelles entre clients et prestataires (sans compter d'ailleurs le risque d'une potentielle perte de confiance des utilisateurs en cas de médiatisation de failles de sécurité exposant les données consommateurs<sup>11</sup>).

.....  
**6.** Article 5 du RGPD : au titre de ce texte, les données à caractère personnel (i) doivent être collectées de manière loyale et licite, (ii) ne doivent être collectées que dans la mesure strictement nécessaire à la réalisation de la finalité pour laquelle elles ont été collectées, (iii) doivent être exactes, exhaustives et à jour, et (iv) ne doivent pas être conservées pendant une durée plus longue que celle nécessaire à la réalisation de cette finalité.

.....  
**7.** Notamment dans l'hypothèse où ses données sont ensuite utilisées à des fins de prospection commerciale (art. L. 34-5 du Code des postes et des communications électroniques).

.....  
**8.** Article 28 du RGPD.

.....  
**9.** Si le RGPD admet que le choix d'un second niveau de sous-traitance puisse se faire par voie d'autorisation générale (article 28 du RGPD), la Commission nationale de l'informatique et des libertés (CNIL) en indique des contours contractuels très précis sous peine de non-conformité. Afin de pouvoir autoriser de manière générale un second niveau de sous-traitance par son propre sous-traitant, le responsable du traitement doit disposer des informations suivantes, par écrit : les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance (<https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses>).

.....  
**10.** Amende administrative pouvant s'élever jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial (article 83 du RGPD), et sanctions pénales dont l'amende peut s'élever à 1 500 000 euros pour les personnes morales.

.....  
**11.** Citons ici Yahoo, dont la proposition d'achat des parts sociales a été réduite de 350 millions de dollars après la découverte de failles de sécurité ayant compromis les données de certains des utilisateurs ou encore TalkTalk, opérateur de télécommunications britannique : la médiatisation de ses piratages répétés aurait provoqué une diminution de son chiffre d'affaires de 80 millions de livres sterling et une perte de 4,4 % de parts de marché.

## 1.2. La plateforme numérique : le point de rencontre de deux mondes

Puisque le passager se retrouve au centre des attentions de l'industrie aéronautique, le nombre de moyens mis en place pour communiquer avec lui, collecter ses données d'expérience utilisateur, faciliter son expérience de voyage, promouvoir ou distribuer des produits est en hausse depuis ces dernières années. L'avènement du « consommateur digital » est en effet sans précédent dans le secteur aéronautique, où la part de clients qui manifestent une présence en ligne est plus élevée que dans les autres secteurs<sup>12</sup>.

Dès l'achat du billet d'avion notamment, les chiffres sont édifiants : l'Association internationale du transport aérien constate qu'en 2017, 74 % des passagers ont embarqué au moyen d'une carte d'embarquement électronique stockée sur leur *smartphone*<sup>13</sup>.

Ainsi, et au-delà d'une augmentation du nombre d'agences de voyage en ligne au détriment des agences physiques (il est estimé que leur part de marché pour ce qui est de la vente de billets d'avion augmentera de 40 % en 2016 à 60 % en 2025<sup>14</sup>), nous constatons une explosion du nombre de sites internet de comparaison en ligne d'offres de transport aérien.

L'ensemble de ces moyens de communication et de promotion n'échappent pas aux règles applicables en matière de communication en ligne et de commerce électronique avec des consommateurs.

Ainsi, l'éditeur de toute plateforme numérique tombant dans la définition de « service de communication au public en ligne »<sup>15</sup> est soumis aux obligations de la loi pour la confiance dans l'économie numérique du 21 juin 2004<sup>16</sup> et notamment à celle de mettre à disposition du public des éléments d'information permettant de l'identifier lui, ainsi que son directeur de la publication et son hébergeur. En pratique donc, une attention particulière doit être portée sur la rédaction de mentions légales disponibles sur la plateforme concernée.

En outre, il convient également de s'assurer, pour ces « nouveaux acteurs du numérique »,

que les nouvelles obligations portées par la loi pour une République numérique du 7 octobre 2016<sup>17</sup> sont bien respectées, dès lors qu'ils opèrent une plateforme en ligne.

La définition large de « plateforme en ligne »<sup>18</sup> permet de conclure que sont à considérer comme telles aussi bien les sites comparateurs de vols que ceux d'agences de voyages en ligne, dès lors que dans ce dernier cas, il s'agit pour l'agence concernée de proposer entre autres à ses utilisateurs un référencement d'offres de transport aérien ou

12. Livre blanc du Forum économique mondial. Initiative Transformation digitale – Secteur de l'aviation, du voyage et du tourisme : [https://www.accenture.com/t20170116T084449\\_\\_w\\_/us-en/\\_acnmedia/Accenture/Conversion-Assets/WEF/PDF/Accenture-DTI-Aviation-Travel-and-Tourism-Industry-White-Paper.pdf](https://www.accenture.com/t20170116T084449__w_/us-en/_acnmedia/Accenture/Conversion-Assets/WEF/PDF/Accenture-DTI-Aviation-Travel-and-Tourism-Industry-White-Paper.pdf).

13. 2017 Global Passenger Survey, Association internationale du transport aérien : <https://www.iata.org/publications/store/Documents/GPS-2017-Highlights-report.pdf>.

14. Livre blanc du Forum économique mondial. Initiative Transformation digitale – Secteur de l'aviation, du voyage et du tourisme, op. cit.

15. L'article L. 32 du Code des postes et des communications électroniques définit les services de communications électroniques comme « les prestations consistant entièrement ou principalement en la fourniture de communications électroniques », ces dernières définies comme tout service d'« émissions, transmissions ou réceptions de signes, de signaux, d'écrits, d'images ou de sons, par voie électromagnétique ».

16. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

17. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

18. Au titre de l'article L. 111-7 du Code de la consommation, « est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur : 1° le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ; 2° ou 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 service ».

d'hébergements touristiques. Pour ces plateformes en ligne, les obligations de la loi pour une République numérique visent notamment une information renforcée des utilisateurs à des fins de transparence et de loyauté. Par exemple, pour ce qui est des sites comparateurs, il est maintenant obligatoire de renseigner l'utilisateur sur les modalités permettant d'arriver au résultat du référencement ; cette information doit également le renseigner sur l'existence d'un lien capitalistique entre l'opérateur de la plateforme et celui qui dont les offres de biens ou de services sont comparées, ou d'une rémunération au profit de cet opérateur, dès lors que ces éléments ont une incidence sur le référencement.

Enfin, l'ensemble des règles applicables aux relations entre professionnels et consommateurs, incluant celles relatives à leur information, aux pratiques commerciales réglementées ou interdites et à la formation et exécution de contrats à distance doivent naturellement être respectées. Outre le risque financier encouru du fait du non-respect des exigences ci-dessus<sup>19</sup>, la publicité potentielle des sanctions liées à des violations de la réglementation applicable entre professionnels et consommateurs est dissuasive pour toute velléité de non-conformité, puisque comme en matière de protection des données à caractère personnel, il en va de la confiance que peut placer le consommateur dans l'image de l'entreprise et donc de sa fidélité à ses produits et services. Au-delà des initiatives digitales développées en direction du consommateur utilisateur final, c'est au sein même de l'entreprise que se constate aussi la mise en place de stratégies digitales destinées à en optimiser l'activité.

## 2. L'optimisation de la production : la transformation digitale des métiers, systèmes et méthodes

Les entreprises repensent leurs processus en interne, transforment leurs systèmes de *back-office* et rafraîchissent leurs structures de contractualisation pour intégrer et rationaliser leurs opérations de production *via* des processus de digitalisation.

De tels changements jouent un rôle crucial pour la réalisation d'objectifs stratégiques qui visent à la fois l'optimisation des lignes de production et donc le maintien d'un avantage compétitif (2.1) et la recherche d'une efficacité maximale des outils de productivité (2.2).

### 2.1. La digitalisation des méthodes de production comme gage de compétitivité

En interne, les processus de production aussi connaissent une époque de bouleversement. En sus de la robotisation des lignes de production, fabrication additive, recours accru aux objets connectés et à la réalité augmentée, toutes les technologies nouvelles sont utilisées dans l'optique de rendre toujours plus efficace, plus rapide et plus efficiente la fonction de production.

C'est ainsi que les collaborateurs de Boeing ou d'Airbus portent maintenant, sur les chaînes d'assemblage final de leurs aéronefs, des lunettes connectées permettant, *via* des techniques de réalité augmentée, de les assister dans l'implémentation des faisceaux de câblage du système aérien concerné.

Puisque ces méthodes digitalisées de fabrication visent donc à conférer aux entreprises qui les mettent en place un avantage compétitif notable en termes de productivité, il convient, pour les acteurs du secteur aéronautique faisant preuve d'innovation technologique, de protéger les objets de cette innovation.

La protection de l'innovation comme gage de compétitivité devient ainsi un enjeu majeur : il ne s'agit pas seulement de protéger l'objet de la vente, comme propre à l'entreprise et signe de son identification auprès du marché, mais également de tenter de se réserver des droits sur la façon dont l'objet est conçu et réalisé, puisque de l'efficacité de ces méthodes de conception dépend à long terme la rentabilité économique

<sup>19</sup> L'article L. 131-4 du Code de la consommation fixe une amende administrative dont le montant ne peut excéder 75 000 euros pour une personne physique et 375 000 euros pour une personne morale. La publication de la décision peut également être exigée (art. L. 132-4 du Code de la consommation).

de l'objet vendu. Pour des procédés de fabrication digitaux, la protection par le droit d'auteur s'envisage<sup>20</sup>. Elle reste toutefois imparfaite dans la mesure où elle ne peut pas être revendiquée sur l'ensemble des éléments pouvant composer la création<sup>21</sup>. Dans ce cas, d'autres moyens de protection sont également utilisés, tels que notamment la protection de l'invention par le brevet<sup>22</sup> ou la protection d'informations, de procédés ou de méthodes *via* la conclusion d'obligations contractuelles de confidentialité dissuasives en cas de manquement.

En outre, la loi du 30 juillet 2018 relative à la protection du secret des affaires<sup>23</sup> vient apporter un régime supplémentaire de protection pour les informations protégeables au titre du secret des affaires : dès lors que ces informations ne sont pas « *généralement connues ou aisément accessibles* » pour les avertis du secteur concerné, qu'elles revêtent une valeur commerciale « *effective ou potentielle* » et qu'elles font l'objet de « *mesures de protection raisonnables* » afin d'en conserver le caractère secret, leur obtention, leur utilisation et/ou leur divulgation non autorisées sont passibles de mesures conservatoires destinées à faire cesser le trouble constaté, et du paiement de dommages-intérêts au détenteur légitime de l'information concernée.

La protection de l'innovation (et notamment des informations commerciales ou techniques qui la composent) est donc une question essentielle : puisqu'elle permet le maintien d'un avantage compétitif, elle devient également un point de risque pour l'entreprise qui la développe et l'exploite dans un environnement digital dématérialisé.

## 2.2. La digitalisation des outils de productivité *via* de nouveaux modèles de sourcing

En plus de la transformation digitale de la fonction de production, celle de ses outils de productivité venant au support de l'ensemble des métiers est aussi notable.

Le secteur aéronautique ne fait pas figure d'exception pour ce qui est de la propension du

monde commercial à externaliser vers des prestataires de service tiers ses ressources informatiques, en ce compris notamment l'hébergement de ses données<sup>24</sup> et ses ressources logicielles<sup>25</sup>. Les avantages attendus de l'externalisation dans le *cloud* sont en effet nombreux : le *cloud* serait moins cher, puisqu'il épargne à l'entreprise l'achat et la maintenance en interne de ses serveurs de données, ce qui lui permet par ailleurs de recentrer ses efforts sur son cœur de métier, et il serait aussi plus sûr, puisque sa sécurité est assurée par des spécialistes de la sécurité informatique, expertise qui n'est pas nécessairement toujours présente dans une entreprise dont ce ne serait pas le métier et dont la taille ne permet pas de se doter de cette expertise. Mais

.....  
**20.** Le Code de la propriété intellectuelle confère à l'auteur un monopole d'exploitation comprenant le droit de reproduction et le droit de représentation de la création. Le droit d'auteur peut porter sur les logiciels, les plans d'impression 3D, un objet connecté en lui-même, etc.  
 .....

**21.** « *Les idées et principes qui sont à la base de la logique, des algorithmes et des langages de programmation ne sont pas protégés* » (considérant de la directive 91/250/CEE du 14 mai 1991 concernant la protection juridique des programmes d'ordinateur).  
 .....

**22.** Un objet peut bénéficier de la protection par le brevet sous certaines conditions cumulatives : l'invention doit être nouvelle, susceptible d'application industrielle et impliquer une activité inventive, c'est-à-dire qu'elle ne doit pas découler de manière évidente de la technique connue par « l'homme du métier » (article L. 611-10 du Code de propriété intellectuelle).  
 .....

**23.** Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires.  
 .....

**24.** Nous constatons que les projets de référencement des prestataires de services d'infrastructure et de plateforme *cloud* se multiplient dans les grands groupes de sociétés de l'industrie aéronautique (par exemple, *Amazon Web Services Boasts It Is GE's Cloud of Choice*, Fortune : <http://fortune.com/2017/10/06/ge-amazon-web-services/>).  
 .....

**25.** Nous constatons un recours accru aux solutions logicielles distribuées sous un modèle industriel *Software as a Service* (SaaS), en remplacement des outils logiciels traditionnels sur site (par exemple, *Airbus to shift employees to Google's GSuite*, communiqué Reuters : <https://uk.reuters.com/article/uk-airbus-alphabet/airbus-to-shift-employees-to-googles-g-suite-memo-idUKKCN1GR28Y>).

des contraintes juridiques sont soulevées par ces nouvelles méthodes de *sourcing*. Outre les risques liés à une non-conformité réglementaire en matière de protection des données à caractère personnel<sup>26</sup>, ceux liés à la sécurité et à la protection de l'ensemble des données externalisées ainsi que ceux inhérents au concept même d'externalisation doivent être relevés. En remettant à un tiers la maîtrise de l'infrastructure informatique ou des ressources logicielles, c'est aussi la maîtrise de la continuité du fonctionnement de ces éléments qui est déléguée au prestataire de services *cloud* : par suite, sur des processus internes critiques, le risque lié à une potentielle discontinuité d'activité doit être encadré.

De même, la question de la confidentialité des données chargées dans le *cloud* demeure cruciale : dans des écosystèmes faisant intervenir une multiplicité d'acteurs ayant accès, pour diverses raisons, aux données des clients du service (support, maintenance, évolution du service, etc.), comment s'assurer que ces données, qui peuvent parfois porter sur des éléments confidentiels de l'entreprise et dont la divulgation pourrait avoir des conséquences négatives majeures, sont bien gardées confidentielles, et que leur sécurité est assurée ? De tels projets d'externalisation dans le *cloud* requièrent par conséquent une négociation attentive des sujets généralement identifiés afin de prévenir ces risques ; ils peuvent également requérir la mise en place de règles de gouvernance interne destinées à encadrer l'utilisation des services *cloud* au sein de l'entreprise afin de limiter les possibilités d'occurrence de ces risques.

Outre l'optimisation de l'activité, c'est son développement qui est aussi au centre des stratégies de digitalisation du secteur aéronautique. Il s'agit de créer de nouvelles activités basées sur la mise à disposition de solutions digitales ou technologiques en lien avec le cœur de métier.

### 3. La création de nouveaux métiers : la transformation digitale de l'activité commerciale

Dans un secteur initialement industriel, nous observons que les constructeurs et prestataires

de maintenance d'aéronefs ou de composants avioniques tentent maintenant de se distinguer dans la fourniture de services informatiques en rapport avec leur activité cœur (3.1), et que parallèlement, les partenariats avec le secteur de la technologie et les investissements dans ce secteur s'accroissent (3.2).

#### 3.1. La nouvelle tendance du constructeur informaticien

Imaginez : il paraît qu'en 2026, le volume annuel de données collectées *via* les composants avioniques de la flotte mondiale atteindra 98 millions de téraoctets, étant entendu qu'à date, les long-courriers les plus récents génèrent déjà en moyenne 30 fois plus de données en vol que ceux de la génération précédente<sup>27</sup>.

Cette course effrénée à la collecte de données techniques n'est pas anodine : tout comme les données des passagers<sup>28</sup>, celles issues d'un vol d'aéronef sont cruciales pour comprendre comment celui-ci et chacun de ses composants se comportent en trajet et détecter les potentielles anomalies survenues ou encore les phénomènes d'usure de matériaux.

Une fois ces données transformées en résultats concrets, l'activité de MRO (maintenance, repair and operations) et le recours à cette activité pour le détenteur du système aérien concerné s'en trouvent impactés : la maintenance des aéronefs étudiés peut devenir prédictive, puisque chaque composant du système est maintenu au besoin et non plus en fonction d'une périodicité arbitraire préétablie, ce qui permet de réduire le temps d'arrêt au sol de l'aéronef concerné, d'augmenter la durabilité de ses composants et donc *in fine* de maximiser sa rentabilité.

Les plateformes digitales, alimentées massivement en données analysées notamment *via* des

<sup>26</sup>. Voir *supra* (1.1).

<sup>27</sup>. *Sondage MRO*, Oliver Wyman : <https://www.oliverwyman.com/our-expertise/insights/2016/apr/mro-survey-2016.html>.

<sup>28</sup>. Voir *supra* (1.1).

procédés de *big data* et d'intelligence artificielle, mettent à la disposition des opérateurs de l'aéronef les résultats de la maintenance prédictive. Les effets positifs attendus de ces initiatives sont tels que tant les constructeurs d'aéronefs<sup>29</sup> que ceux d'éléments majeurs des aéronefs<sup>30</sup> se sont lancés dans la prestation de services digitaux et à terme, ce sont de nombreuses activités que les opérateurs du secteur aéronautique se proposent d'optimiser *via* la mise à disposition de solutions digitales (perfectionnement des processus d'opérations de vol, optimisation des flottes en *leasing*, amélioration des conceptions de cabines, etc.).

Nous observons également le recours accru à des solutions logicielles tierces comme composants de la solution proposée aux clients.

Afin de mettre en œuvre la technologie la plus pointue, l'entreprise de l'aéronautique n'hésite pas à créer avec des experts du domaine informatique et de la science des données des partenariats aux termes desquels la technologie est i) apportée par ces experts et ii) appliquée par ces acteurs au secteur de l'aéronautique. Dans cette logique de « *go-to-market* », où le fournisseur de la solution (ici, le constructeur d'aéronefs ou de pièces) met à disposition de ses clients un ensemble digital global notamment composé de solutions propriétaires tierces, l'enjeu lié à la circulation des droits de propriété intellectuelle sur cet ensemble devient essentiel : il s'agit en effet de s'assurer que les droits nécessaires à l'utilisation par les clients (compagnies aériennes, etc.) de l'ensemble final (et donc des solutions tierces qui le composent) ont bien été obtenus, et que ces clients n'excèdent pas les droits qui leur sont confiés, au risque pour le fournisseur de devoir en répondre devant les éditeurs de ces solutions tierces.

En outre, lorsque ces solutions sont elles-mêmes distribuées sous un modèle *cloud* (i.e., mise à disposition de, et accès à, l'ensemble final *via* internet, certains de ses composants propriétaires tiers pouvant également être fournis depuis le *cloud*), il convient de porter une attention particulière aux engagements de performance et de niveaux de service pris par

chacun des prestataires de service impliqués dans la fourniture de l'ensemble final. Le fournisseur de cet ensemble doit être vigilant quant aux engagements qu'il accepte lui-même de prendre envers ses clients, comparativement à ceux obtenus de la part de ses propres fournisseurs (ce réflexe doit aussi s'appliquer à ces fournisseurs envers leurs propres prestataires de service d'hébergement de leur solution propriétaire, par exemple) ; pour le client, il s'agit d'être vigilant quant au découpage des responsabilités qui peut parfois être opéré contractuellement par le fournisseur dans le contrat de mise à disposition de l'ensemble final : il pourrait en effet être tenté de s'exonérer du mauvais fonctionnement de certaines caractéristiques de cet ensemble final (e.g., son niveau de disponibilité), sur le fondement du fait qu'il n'en a pas techniquement la charge.

Dans de telles hypothèses, une stratégie commerciale claire de développement pour le constructeur acheteur, développeur et éditeur paraît nécessaire afin d'anticiper les risques juridiques liés à ces relations commerciales distinctes mais interdépendantes d'un point de vue projet. De même, une anticipation des risques notamment liés à l'intégrité et à l'exactitude des résultats fournis par ce type de solutions, venant au support du cœur de métier, paraît primordiale pour les clients.

### 3.2. La culture de l'innovation comme clé de croissance à long terme

Bien que la nature consommatrice de capitaux du secteur aéronautique constitue une barrière à l'entrée pour beaucoup d'acteurs dans l'écosystème digital, les avancées technologiques et la multiplicité des cas d'usage que propose cet écosystème créent des rôles pour les nouveaux acteurs, et le secteur reste donc marqué par une forte concurrence. Ce

29. Tels qu'Airbus avec sa plateforme Skywise d'analyse de données multi-source.

30. Comme Rolls-Royce et son service TotalCare d'analyse des données moteur Rolls-Royce.

phénomène stimule l'innovation non seulement au sein des start-ups et des entreprises du digital, mais aussi chez les acteurs traditionnels du secteur aéronautique qui cherchent à investir et/ou à nouer des partenariats afin d'anticiper et de façonner les changements de marché.

Par exemple, GE Aviation a créé une division « *digital* » qui combine toute l'expertise digitale de son unité opérationnelle au sein d'une seule unité commerciale. De même, le groupe Airbus a mis en place le fonds Airbus Ventures, ainsi qu'un centre d'innovation technologique et commerciale dans la Silicon Valley, baptisé A<sup>3</sup>, tous deux ayant pour vocation de définir l'avenir de la mobilité et du transport aérien. D'autres entreprises privilégient au contraire des accords de partenariat pour investir dans des start-ups qui produisent des solutions innovantes pertinentes à leur cœur de métier. Ainsi, International Airlines Group (IAG) s'est associée avec L Marks pour lancer Hangar 51, un programme d'incubation sur 10 semaines qui permet aux start-ups de travailler avec les équipes dirigeantes d'IAG afin de tester leurs produits et services auprès des compagnies aériennes et de négocier avec elles des projets d'investissements. Hangar 51 se concentre sur l'amélioration des processus aéroportuaires, sur la digitalisation des processus économiques ainsi que sur l'identification de nouveaux cas d'usage d'utilisation des données dans la prise de décision opérationnelle et la satisfaction client.

De telles initiatives aident les entreprises du secteur aéronautique à tenir le rythme de l'innovation digitale en intégrant en permanence les nouvelles technologies dans leurs opérations et à anticiper le prochain bouleversement technologique. D'un point de vue juridique, la forme de l'investissement ou du partenariat choisi entraîne des conséquences en termes de titularité de la propriété intellectuelle qui pourrait

naître sur les créations qui en sont issues, ainsi que sur le degré d'implication requis de chaque acteur pour le succès de l'entreprise. En outre, dans l'hypothèse de constructions de partenariats ou de création de « *hubs* » technologiques, il convient de trouver le juste équilibre entre d'une part, la nécessité d'encadrer les responsabilités de chaque acteur, et d'autre part, de faciliter les méthodes de travail « agiles », prégnantes dans les modes de fonctionnement des acteurs de l'innovation digitale.

Même lorsque l'investissement ou le partenariat n'est pas recherché, nous constatons un recours accru aux accords de conception de prototypes (*proof of concept*, *proof of value*, etc.) ou de programmes pilotes, destinés à tester des technologies émergeant sur le marché et à confirmer les solutions que ces technologies peuvent apporter à des cas d'usage identifiés.

Une fois les preuves des objets de l'innovation faites et le passage en production industrielle envisagé, il reste encore, pour les opérateurs de l'industrie aéronautique, à s'assurer que ces objets sont bien conformes aux exigences réglementaires particulièrement nombreuses dans ce domaine.

Les défis juridiques liés à la transformation digitale du secteur de l'aéronautique sont nombreux : ils passent notamment par la prise en compte des exigences réglementaires dans le cadre de l'achat de solutions digitales et de leur mise à la disposition d'utilisateurs, par la protection des éléments de l'innovation, et par la nécessité de prévoir une répartition adéquate des responsabilités dans les différentes relations contractuelles avec l'ensemble des parties prenantes à ces processus de transformation. Demain, ces mêmes défis juridiques et d'autres resteront d'actualité quand les avancées technologiques permettront de déposer par drone un colis à domicile, de transporter des passagers par voie aérienne sans pilote, ou de disposer d'un réseau urbain de mobilité aérienne.

INDUSTRIE

---

THÈME 2

# Immobilier & transformation numérique :

LA PROPTECH CHANGE LA DONNE

# Le point de vue...



**Olivier Colcombet, Directeur général de Digit RE Groupe et président des réseaux immobiliers OptimHome et Capifrance**

## **Comment le numérique a-t-il révolutionné le secteur immobilier ?**

C'est une révolution qui a eu lieu en deux temps, dirais-je. La première étape s'est déroulée il y a 10-15 ans avec la présentation numérique des annonces, qui a permis aux vendeurs d'avoir une meilleure visibilité et aux acquéreurs d'avoir une meilleure information sur les biens, sans avoir à se déplacer. C'est en partie sur ce socle que nous avons bâti notre business model. Dans un second temps, la numérisation et l'évolution des outils technologiques ont agi comme des moteurs qui nous ont obligés à innover et à nous réinventer. Cette deuxième étape est récente et a 3-4 ans seulement. Elle a permis l'émergence de nouveaux outils et de nouveaux services. Les acteurs traditionnels du secteur se sont d'ailleurs fait distancer ils n'ont pas été aussi agiles que les nouveaux acteurs, qui partaient *ex nihilo*, et qui ont tout de suite embrassé ces nouvelles technologies. Pour répondre aux attentes des particuliers et leur proposer des solutions innovantes pour améliorer l'accompagnement et sécuriser les transactions.

## **Quelles opportunités cela permet et avez-vous identifié des freins ?**

La révolution, l'évolution que nous sommes en train de vivre est à la fois technologique, sociétale et servicielle. Il est symptomatique de constater, par exemple, que les conseillers immobiliers qui utilisent des outils « modernes » ont plus de temps à passer avec leurs clients. Ces derniers, mieux informés, peuvent les solliciter pour des conseils à forte valeur ajoutée après avoir en amont eu

des informations générales, sur le quartier, par exemple, grâce à la géolocalisation et aux autres outils qui agissent comme des filtres. Le temps accordé au client est ainsi de meilleure qualité et la technologie aide paradoxalement, à améliorer la relation humaine. Par ailleurs, dans le secteur de l'immobilier, la digitalisation n'est pas totale, car il y a toujours des contraintes réglementaires qui font que l'on est obligé de passer par un mandat, un acte de vente, etc. Mais cela rassure, eu égard aux montants élevés en jeu. L'un des freins les plus importants à l'expansion de solutions digitales que j'identifie est l'utilité, il faut qu'elles répondent avant tout à un besoin, à une attente.

## **Quel est votre regard sur le RGPD, est-ce un frein ou une opportunité ?**

Les acteurs doivent s'armer pour que les informations sur les clients soient utilisables. Nous développons en interne un projet sur ce point, et nous avons réussi à faire de ce qui peut sembler être un frein une opportunité, mais il faut avoir du temps, des ressources et de l'énergie. Comme à chaque fois que l'on pose une restriction pour protéger les usagers, il est regrettable que ces restrictions ne soient pas homogènes et que certains s'en affranchissent car ils sont trop petits et passent entre les mailles du filet. Dans le cas des sollicitations au client, il me semble de surcroît qu'il existe des freins naturels, car les personnes trop envahies de messages vont trouver cela rédhibitoire. Mais comme toujours concernant l'expérience utilisateur, les choses sont plus faciles à dire qu'à mettre en œuvre.

# Le point de vue...



**Frédéric Augier,**  
directeur du digital, Nexity

## Comment le numérique a-t-il révolutionné le secteur de la construction ?

Dans le secteur de la construction, nous n'en sommes qu'au début de la révolution. Le phénomène est désormais engagé, mais, au fil des années, le secteur a accumulé beaucoup de retard en matière de digitalisation. C'est un secteur notoirement sous-investi en innovation, recherche et développement et digital, et c'est seulement maintenant, avec plusieurs années de décalage avec d'autres secteurs d'activité que commencent à apparaître des outils numériques de pilotage, de collaboration et de simplification de process. Je pense notamment au BIM, à la dématérialisation de documents, aux applications mobiles qui facilitent la réalisation des tâches sur les chantiers ainsi qu'à des solutions plus récentes comme l'Internet des objets (IOT *Internet of things*), qui permet de rendre les objets communicants et de mieux gérer le fonctionnement des équipements.

## En quoi consiste le *building information modeling* (BIM) ?

Le BIM est la représentation numérique d'un immeuble en trois dimensions, à laquelle s'ajoutent les informations techniques sur les différents équipements de construction. Cette base de données décrit avec une précision industrielle les éléments nécessaires à la conception, à la réalisation et l'exploitation d'un bâtiment. Ces outils sont très transformants car on a désormais la capacité de construire l'immeuble à l'écran, de détecter les anomalies et les incohérences et d'éviter des travaux supplémentaires sur le chantier. En termes de répartition des tâches, cela signifie plus de temps passé sur l'étude et moins de temps d'exécution. La maquette 3D BIM permet aussi d'animer des visites virtuelles très immersives de bureaux et de logements et de renforcer la co-conception

avec les clients. Et pour le bon fonctionnement de l'immeuble au quotidien, le BIM incite à développer la maintenance prédictive et permet de gagner du temps dans le diagnostic et la résolution des désordres éventuels. Globalement, le BIM est une opportunité majeure pour réduire les coûts de construction, renforcer le professionnalisme de la filière et *in fine* transformer la relation client.

## De nouveaux métiers ont-ils émergé grâce à ces progrès techniques ?

Du fait de la collaboration plus poussée entre les différents acteurs, naissent des métiers chargés de faire l'interface. Par exemple, celui de BIM manager, chargé de la coordination entre le maître d'ouvrage et le maître d'œuvre, par exemple pour réaliser la synthèse des maquettes ou des revues de chantier BIM. Il y a aussi le métier d'assistant BIM à la maîtrise d'ouvrage, chargé de rédiger les cahiers des charges BIM. Les métiers traditionnels qui interviennent dans la création et la gestion d'un bâtiment doivent être également capables de travailler sur une maquette BIM. Dans le cadre de la charte de la filière du bâtiment pour la construction numérique, l'objectif est de généraliser le recours au BIM d'ici 2022. C'est un délai à la fois ambitieux et réaliste. Les freins à la numérisation que j'identifie, c'est en premier lieu le manque de standardisation technique, parce que chacun travaille avec des logiciels et des maquettes qui lui sont propres qu'il faut convertir ou compiler, ainsi que le manque de règles relatives à la responsabilité des acteurs sur ces nouveaux outils. Mais surtout, l'ampleur de la transformation exige une mise à niveau de toute la filière, de la grande entreprise au petit artisan, afin de pouvoir travailler sur une plateforme commune. Or, il faut du temps pour se familiariser avec les méthodes de travail digitales.



Par **Mathilde Tariel-Savy**

« **P**roptech », le mot était sur toutes les lèvres lors du MIPIM qui s'est déroulé à Cannes du 13 au 16 mars 2018 avec notamment la mise en place d'un nouvel événement, « *le Proptech Lab* », qui a pris la forme d'un espace d'exposition permettant à la proptech de se faire connaître auprès des acteurs du secteur de l'immobilier.

La numérisation accélérée touche aujourd'hui tous les secteurs de l'économie tels que la finance avec la fintech, le secteur médical avec la medtech, le secteur assurantiel avec l'insurtech, etc. Par le biais de la proptech, c'est désormais le secteur de l'immobilier – l'un des plus gros secteurs de l'économie française et mondiale – qui est concerné. Le terme « proptech » vient de *property* et de *technology* et désigne les sociétés qui utilisent le numérique dans le secteur de l'immobilier.

Par le biais de start-ups innovantes, la proptech révolutionne aujourd'hui le secteur de l'immobilier (1) engendrant des problématiques et enjeux juridiques nouveaux (2).

## 1. La proptech révolutionne le secteur immobilier

Toutes les dimensions du secteur de l'immobilier ont vu les proptechs s'imposer. Les technologies innovantes touchent notamment le processus de gestion immobilière (1.1) et s'imposent aussi au domaine de la construction (1.2).

### 1.1. Une facilitation du processus de gestion immobilière

La révolution numérique a su s'imposer dans le cadre d'opérations telles que l'acquisition et le financement de biens immobiliers.

Un outil a pris de plus en plus d'ampleur lors d'acquisitions immobilières : la blockchain. Selon l'article L. 223-12 du Code monétaire et

financier issu de l'ordonnance du 28 avril 2016, relatif aux « *minibonds* », la blockchain est « *un dispositif d'enregistrement électronique partagé permettant l'authentification de ces opérations, dans des conditions, notamment de sécurité, définies par décret en Conseil d'État* ». La doctrine s'est questionnée sur la définition à donner au concept de blockchain. Le site Blockchain France la définit ainsi comme « *une technologie de stockage et de transmission d'informations, transparente, sécurisée, et fonctionnant sans organe central de contrôle* »<sup>1</sup>. La blockchain est présentée comme inviolable en raison de son mode de fonctionnement particulier qui s'apparente à une chaîne de blocs. Selon le site Blockchain France, « *les transactions effectuées entre les utilisateurs du réseau sont regroupées par blocs, chaque bloc est validé par les nœuds du réseau appelés les "mineurs", selon des techniques qui dépendent du type de blockchain, et une fois le bloc validé, il est horodaté et ajouté à la chaîne de blocs. La transaction est alors visible pour le récepteur ainsi que l'ensemble du réseau* »<sup>2</sup>.

L'utilisation du système de la blockchain permettrait de sécuriser encore davantage les transactions immobilières et d'arriver au même niveau de sécurité qu'un acte notarié<sup>3</sup>.

1. <https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/>.

2. *Ibid.*

3. *Les mystères de la blockchain*, Recueil Dalloz 2017 p. 2160, Mustapha Mekki.

4. Amendement n° 227 présenté par la députée Laure de La Raudière : « *Les opérations effectuées au sein d'un système organisé selon un registre décentralisé permanent et infalsifiable de chaîne de blocs de transactions constituent des actes authentiques au sens du deuxième alinéa de l'article 1317 du Code civil.* »

Un amendement a d'ailleurs été déposé le 13 mai 2016 afin que la blockchain soit pourvue de la même force qu'un acte notarié, mais cet amendement a finalement été rejeté<sup>4</sup>.

Dans les opérations de financement immobilier, on retrouve la proptech sous la forme d'un type de conseillers financiers 2.0 : les « *robo-advisors* ». Les robo-advisors sont des sites Internet qui, grâce à des algorithmes, vont gérer des portefeuilles d'actifs et optimiser des placements financiers. Cette solution présente l'avantage de la simplicité et peut coûter quatre à cinq fois moins cher qu'un conseiller humain<sup>5</sup>.

Au cours de ces dernières années, de nombreuses innovations ont été développées et révolutionnent aujourd'hui le marché de la location immobilière. La proptech a donné naissance à de nombreux services qui peuvent être utilisés aussi bien par les propriétaires/bailleurs que par les locataires.

Ainsi la géolocalisation des biens, telle que la propose par exemple GoogleMaps, permet aujourd'hui de situer virtuellement son bien sur Internet mais aussi de visualiser le quartier et l'environnement situé autour du bien ciblé. Dans le même domaine, la société Bien'ici annonce avoir « *cartographié la France entière en 2D et en 3D* »<sup>6</sup>. Ainsi, ce site permet aux futurs locataires de « *découvrir en détail les villes et les quartiers et [de se] repérer facilement grâce à plus de 200 bâtiments remarquables modélisés en HD partout en France* », et également de localiser « *simplement les commerces, les transports, les écoles et tous les autres points d'intérêt autour du bien qui [les] intéresse* »<sup>7</sup>.

De nombreuses start-ups ont également fait leur apparition et développé des services innovants. À ce titre, la start-up Matterport ayant pour objet la fabrication de caméras dédiées et la capture d'images 2D et 3D, permet de visiter des biens immobiliers en 3D et à 360°, sans se déplacer, grâce à un casque de réalité virtuelle. L'idée est de permettre aux utilisateurs de se projeter plus facilement dans le bien qui fait l'objet de leur futur projet d'acquisition ou de location<sup>8</sup>.

Dans un autre registre, la société HappyRenting

propose aux locataires de noter leur logement, permettant ainsi aux futurs habitants de se faire une idée plus précise du bien qu'ils s'appêtent à habiter et ce, sur les critères suivants : quartier, appartement, immeuble et agence/propriétaire<sup>9</sup>. Enfin, les « *smart contracts* » (« contrats intelligents ») se développent également. Les *smart contracts* sont des programmes informatiques, utilisant la blockchain, et permettant de générer automatiquement des contrats sur un modèle de « *si... alors...* »<sup>10</sup>.

Les parties complètent les informations requises par le système informatique, et le programme en tire automatiquement les conséquences afin de construire le contrat. Les *smart contracts* peuvent aussi être utiles en matière de location de bien. Certaines start-ups utilisent cette technologie afin de générer automatiquement des contrats de location de bien saisonniers.

Les *smart contracts* ouvrent une série de questions relatives à leur encadrement juridique. La doctrine s'interroge notamment sur la qualification de « contrat » en tant que tel<sup>11</sup>. D'autres problématiques liées à la responsabilité en cas de défaillance du système, à la charge de la preuve ou encore à la responsabilité sont également discutées<sup>12</sup>.

5. <http://www.lesmeilleursfonds.com/article.php?post=51>.

6. <https://www.bienici.com/>.

7. *Ibid.*

8. <https://www.journaldelagence.com/1143495-matterport-agents-immobiliers-peuvent-proposer-visite-virtuelle-3d-qualite-4k-sami-belmokadem-directeur-france-de-matterport>.

9. <https://happyrenting.fr>

10. *Considération sur les smart contracts*, Gaëtan Guerlin, Dalloz IP/IT 2017, p. 512.

11. Fintech – Blockchain et smart contracts : premiers regards sur une technologie disruptive, *Revue de droit bancaire et financier*, n° 1, janvier 2017, dossier 4, Étude par Cécilia Zolynski.

12. *Ibid.*

## 1.2. Zoom sur les BIM

La proptech impacte toutes les dimensions du secteur de l'immobilier. Un bien immobilier peut ainsi être touché par le numérique à n'importe quelle étape, et ce dès sa construction. L'exemple le plus marquant dans le domaine de la construction est le BIM (*building information modelling* ou maquette numérique en français) qui est, selon le Plan de transition numérique, « une méthode de travail basée sur la collaboration autour d'une maquette numérique. Dans un processus BIM, chaque acteur de la construction crée, renseigne et utilise cette maquette, et en tire les informations dont il a besoin pour son métier. En retour, il alimente la maquette de nouvelles informations pour aboutir au final à un objet virtuel renseigné, représentatif de la construction, de ses caractéristiques géométriques et des propriétés de comportement »<sup>13</sup>.

L'intérêt majeur du BIM est de permettre une meilleure synergie entre les acteurs de la construction et d'avoir une compréhension plus globale de la construction tout au long de la durée de vie de l'ouvrage.

La dimension collaborative du BIM a ouvert de multiples interrogations quant à la responsabilité des constructeurs des articles 1792 et suivants du Code civil et notamment à l'imputabilité d'un dommage à un constructeur donné<sup>14</sup>. La collaboration des acteurs du BIM rend floue la mission de chaque acteur et complexifie donc l'imputabilité d'un éventuel dommage. Ce problème, qui pourrait être facilement contourné par une répartition conventionnelle des responsabilités, se heurte aujourd'hui à l'article 1792-5 du Code civil<sup>15</sup> qui prohibe les clauses limitatives ou exonératoires de responsabilité.

## 2. Les enjeux juridiques de la proptech

Les innovations technologiques au sein du secteur de l'immobilier soulèvent de nombreuses problématiques juridiques nouvelles. Face à l'évolution d'un secteur traditionnel

(2.1), la mise en place d'un arsenal juridique adapté aux nouveaux risques engendrés par les progrès technologiques est un enjeu fondamental (2.2).

### 2.1. La caducité du modèle traditionnel

La particularité du secteur de l'immobilier est que le marché est traditionnel, et immobile. De ce fait, la transition numérique paraît moins évidente que dans d'autres secteurs voisins tels que les secteurs bancaire ou assurantiel. L'immobilier repose sur une multitude d'acteurs qui interviennent à différentes étapes tout en conservant chacun leur spécificité et leur calendrier. Cette diversité ne participe pas à une transition numérique rapide, tous les acteurs n'étant pas capables d'adapter leur offre dans le même temps et dans la même mesure.

Cette chaîne d'acteurs peut aussi voir son équilibre remis en cause par la proptech. L'arrivée de certains outils comme la blockchain peut impacter très fortement l'offre de certains acteurs, d'où la nécessité urgente d'intégrer ces nouveaux instruments dans le quotidien, pour qu'ils ne soient pas perçus comme un frein mais bien comme l'atteinte de nouveaux objectifs : venir en soutien des acteurs de l'immobilier, et du secteur en général, afin d'améliorer la productivité et l'offre, de baisser les

<sup>13</sup>. Plan de transition numérique dans le bâtiment et mission interministérielle pour la qualité des constructions publiques, BIM et maquette numérique, Guide de recommandations à la maîtrise d'ouvrage, juill. 2016, 4. <http://www.batiment-numerique.fr/uploads/DOC/PTNB%20-%20Guide%20Methodo%20MOA.pdf>.

<sup>14</sup>. BIM : analyse et perspectives de l'immeuble numérique, *Construction – Urbanisme*, n° 12, décembre 2017, étude 11.

<sup>15</sup>. Article 1792-5 du Code Civil : « Toute clause d'un contrat qui a pour objet, soit d'exclure ou de limiter la responsabilité prévue aux articles 1792, 1792-1 et 1792-2, soit d'exclure les garanties prévues aux articles 1792-3 et 1792-6 ou d'en limiter la portée, soit d'écarter ou de limiter la solidarité prévue à l'article 1792-4, est réputée non écrite. »

coûts, et de gagner en efficacité et en rapidité. En France, les acteurs de l'immobilier sont plus en retard que dans d'autres régions du monde. Si l'on reprend l'exemple du BIM, le Royaume-Uni a imposé en 2016 l'utilisation du BIM pour sa commande publique<sup>16</sup>. Par ailleurs, l'Autorité de construction pour l'habitation de Hong Kong a rendu le BIM obligatoire pour tout nouveau projet de construction du marché public dès 2014<sup>17</sup>.

En France, la directive 2014/24/UE du Parlement européen et du Conseil du 26 février 2014 sur la passation des marchés publics fait mention du BIM à l'article 22.4 qui prévoit que « pour les marchés publics de travaux et les concours, les États membres peuvent exiger l'utilisation d'outils électroniques particuliers tels que des outils de modélisation électronique des données du bâtiment ou des outils similaires ». Cependant la transposition en droit français de cette directive ne rend pas l'utilisation du BIM obligatoire, contrairement à certains de ses voisins européens comme le Royaume-Uni, les Pays-Bas ou encore le Danemark<sup>18</sup>.

Or, les acteurs du numérique ont pour ambition des marchés internationaux. Il est donc primordial pour la France de poursuivre dans la voie de la transition du numérique.

## 2.2. La nécessité d'une adaptation juridique

Aujourd'hui, la législation française n'est pas armée, ou tout du moins pas suffisamment, pour pouvoir répondre à tous les enjeux que soulève la proptech.

En effet, aucune définition juridique n'est donnée à la proptech et à ses déclinaisons. Or, sans définition juridique, aucun statut ou régime n'est applicable. Ce retard est logique dès lors que l'implantation du numérique dans la société française s'est faite très rapidement et avec une très grande ampleur. Les lois actuelles ont été écrites à une époque où le digital n'était pas présent et où il n'était pas possible de prévoir une telle révolution. Une évolution juridique leverait les freins existants en permettant aux entreprises de tirer

pleinement parti des progrès technologiques et de rendre le secteur plus dynamique.

C'est en ce sens qu'un rapport intitulé « La révolution numérique et le marché du logement, Nouveaux usages, nouveaux acteurs, nouveaux enjeux » a été rendu à la ministre du Logement et de l'Habitat durable et au ministre de l'Économie et des Finances en novembre 2016 par Bernard Vorms. Ce rapport vise à « *décrire l'impact du numérique sur les métiers de la transaction et de la gestion immobilières, pour leur partie résidentielle* », suite à la révolution numérique. Ledit rapport ambitionne d'analyser « *les évolutions du secteur et [de] faire des propositions visant à aider les professionnels mais aussi la puissance publique à saisir ces nouvelles opportunités* »<sup>19</sup>.

Sur la base des propositions formulées, une réflexion interministérielle va s'ouvrir pour apporter des réponses aux questions soulevées. Parmi la liste de recommandations figurent les objectifs suivants<sup>20</sup> :

- lever l'insécurité juridique liée à la dématérialisation des documents et des correspondances ;
- traiter les nouveaux usages de location temporaire avec des textes spécifiques en distinguant chacune des situations ;
- imposer aux plateformes collaboratives d'assortir chacune de ces modalités d'occupation d'exigences spécifiques en matière d'information des occupants ;
- garantir un égal accès de tous aux données

16. Le Royaume-Uni toujours à la pointe du BIM, Antoine Hudin, *CTB*, n° 356.

17. <https://bimbtp.com/decouvrir-le-bim/le-bim-dans-le-monde/>.

18. BIM, maquette numérique et assurance construction, Jean Roussel, *RDI*, 2017 p. 515.

19. « Rapport à la ministre du Logement et de l'Habitat durable et au ministre de l'Économie et des Finances », [http://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/rapport-logement-vorms-11-2016\\_0.pdf](http://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/rapport-logement-vorms-11-2016_0.pdf).

20. *Ibid.*

de prix et de loyers dont la puissance publique rend la communication obligatoire (données de prix transmises par les notaires et données de loyers transmises par les administrateurs de biens, dans certaines localisations) ;

- fiabiliser les avis en ligne en imposant aux plateformes d'informer sur le fait que les avis ont fait l'objet d'une vérification et le cas échéant d'en préciser les modalités ;

- conduire une étude comparative sur le fonctionnement du marché immobilier dans les principaux pays comparables à la France.

Seulement, la numérisation du secteur de l'immobilier s'accompagne de craintes telles que celle de la cybercriminalité. Devenue un élément nouveau et crucial, la cybersécurité ne peut qu'être anticipée. Les bâtiments peuvent ainsi être très facilement victimes d'un hacker déterminé. Le secteur de l'immobilier doit

donc rapidement s'armer pour lutter contre les attaques liées à toutes les innovations et aux objets connectés.

Mais d'autres risques existent également et sont liés à des domaines aussi variés que le droit à l'oubli, la sécurité des données personnelles ou encore la question du droit applicable.

En ce sens, une mission d'information sur la blockchain est actuellement en cours à l'Assemblée nationale afin d'analyser notamment les enjeux de souveraineté qu'implique la blockchain.

Un MIPIM dédié à la proptech a eu lieu à Paris le 20 et 21 juin 2018, et un autre aura lieu en juillet 2019, dernière preuve de l'intérêt des acteurs du marché pour ce qui s'annonce comme une inévitable révolution technologique.

SERVICES

---

THÈME 3

# Assurance & transformation numérique





# Le point de vue...

**Jean-Charles Samuelian,**  
CEO et co-fondateur, Alan

## **Qui est Alan ? Quelles sont les étapes suivantes pour Alan ?**

Créé en 2016 par Jean-Charles Samuelian et Charles Gorintin, Alan est une start-up parisienne dédiée à l'assurance complémentaire santé. Surfant sur le développement des nouvelles technologies, la jeune pousse propose une nouvelle offre d'assurance santé entièrement dématérialisée, plus simple à utiliser, plus rapide, dotée d'un excellent rapport qualité/prix et accessible à tous. Elle s'adresse déjà à plus de 10 000 personnes physiques et près de 1500 entreprises, principalement des PME et TPE.

La société a déjà levé plus de 35 millions d'euros depuis sa création. Le dernier tour de table, datant d'avril dernier, ayant réuni 23 millions d'euros grâce au soutien d'Index Ventures, de Partech, de la CNP et de plusieurs business angels. La majorité du capital reste cependant concentrée dans les mains des fondateurs et des salariés.

## **Vous êtes un nouvel entrant sur le marché, comment l'arrivée de nouveaux entrants – challengers - (notamment) modifie le visage plus traditionnel de l'assurance ?**

Alan ré-invente l'assurance complémentaire santé vers plus de transparence et de simplicité. Nous transformons la santé en une expérience simple grâce à des outils beaux et bien pensés. Notre vision ultime est de devenir la référence technologique qui rend la santé et le bien-être simples et accessibles à tous.

## **Que représente l'arrivée du digital dans le secteur de l'assurance ?**

Le digital permet de simplifier les relations avec les utilisateurs, rendant les échanges plus rapides et sûrs. Il recrée de la confiance dans un secteur où les assurés avaient historiquement l'habitude de lutter pour se faire rembourser leurs soins ou en tous cas de perdre beaucoup de temps dans leurs démarches. Dans le secteur de l'assurance, le digital est donc un gage de transparence et

d'efficacité permettant à l'utilisateur de prendre sa décision dans les meilleures conditions.

## **Le réglementaire est-il aujourd'hui un frein au développement d'acteur disruptif comme le votre ?**

Dans ce secteur, l'émergence de nouveaux acteurs est rare car l'entreprise est longue et souvent difficile, notamment en raison des exigences réglementaires. Alan a dû faire preuve auprès du régulateur du sérieux et de la qualité de son offre 100% dématérialisée. Elle est d'ailleurs la première société d'assurance indépendante à avoir reçu un agrément depuis trente ans par l'Autorité de contrôle prudentiel. Il est certain que le réglementaire est une barrière d'entrée, mais elle est indispensable car l'enjeu touche à la santé des personnes.

C'est la parfaite connaissance de cet environnement réglementaire qui a guidé d'ailleurs nos premiers recrutements. Parmi nos premiers salariés, la plupart d'entre eux a déjà exercé dans un groupe d'assurance ou chez le régulateur.



Par **Luc Bigel** et **Hamza Akli**

**D**ans le secteur des assurances comme dans tout secteur soumis aux évolutions technologiques, une stratégie digitale efficace est devenue désormais une préoccupation majeure afin de satisfaire des preneurs d'assurance de plus en plus enclins à adapter leurs habitudes qu'ils soient « *digital native* » ou non. C'est pourquoi les assureurs mais également les distributeurs d'assurance se doivent d'innover, tant pour devancer leurs concurrents traditionnels que pour anticiper les innovations et les modèles dits « *disruptifs* » censés révolutionner le secteur de l'assurance. Ce livre blanc aborde la question de la transition digitale dans le secteur des assurances et s'intéresse aux défis juridiques, réglementaires et commerciaux que devront relever les acteurs de ce marché déjà qualifié d'hyper concurrentiel afin d'optimiser leurs opérations et processus. L'objectif : favoriser une révolution digitale au sein de leur organisation et plus largement au sein du marché de l'assurance entendu dans son sens large. Les conditions *sine qua non* d'une mise en œuvre efficace de la mutation digitale de ce secteur nous semblent résider dans plusieurs champs dont notamment la transformation de l'expérience client principalement ou encore l'évolution de la gestion des sinistres intégrant les outils insurtech en passant par l'amélioration des délais de commercialisation et de la rétention client. Toutes ces évolutions contribueront à améliorer la compétitivité des assureurs, leur rentabilité et partant les services offerts aux preneurs d'assurances.

## 1. Transition digitale du secteur des assurances : Repenser l'expérience client

Dans toutes les parties du globe disposant d'un accès effectif à internet, la digitalisation

transforme les attentes des clients. Le nombre d'internautes est passé ces 15 dernières années de 400 millions à 3,2 milliards, selon les derniers chiffres du rapport ICT 2015 de l'ITU<sup>1</sup>. Selon le rapport 2017 de l'ITU<sup>2</sup> les souscriptions de forfaits mobiles ont augmenté annuellement de 20% depuis les cinq dernières années de sorte que l'on recense aujourd'hui presque autant d'abonnements de téléphonie mobile que d'habitants sur la planète. Toujours selon l'ITU<sup>3</sup>, 7 milliards de personnes (soit 95 % de la population mondiale!) habitent dans une zone couverte par un réseau de téléphone cellulaire. Le rythme et l'ampleur de ce phénomène digital impliquent une transformation de l'expérience client de la part des acteurs de l'assurance afin de s'adapter aux exigences de la génération des *millennials* ou génération connectée.

Par ailleurs, une récente étude sur le digital dans le secteur des assurances<sup>4</sup> révèle que les deux premiers facteurs qui motivent les stratégies digitales des sociétés d'assurance sont l'enrichissement de l'expérience client et un contrôle plus direct de la relation client. Ces exigences nouvelles permettront aux acteurs traditionnels de faire évoluer leurs offres de services et de produits et laisseront le champ libre à des nouveaux acteurs 2.0.

En dépit de cette prise de conscience, nombre d'acteurs du secteur sont novices en matière

1. <http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf>

2. <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf>

3. <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf>

4. [http://www.ey.com/Publication/vwLUAssets/EY\\_Insurance\\_in\\_a\\_digital\\_world:\\_The\\_time\\_is\\_now/\\$FILE/EY-Digital-Survey-1-October.pdf](http://www.ey.com/Publication/vwLUAssets/EY_Insurance_in_a_digital_world:_The_time_is_now/$FILE/EY-Digital-Survey-1-October.pdf)

digitale, avec moins de la moitié des assureurs qui proposent la fonction mobile pour fournir un devis et seulement 23 % de ces derniers en capacité de soumettre et de traiter les sinistres via une procédure digitalisée.<sup>5</sup> De même que les investissements considérables nécessaires à la transformation des technologies existantes (souvent dépassées), la prise en compte d'exigences réglementaires évolutives et les contraintes liées à la culture interne des acteurs traditionnels constituent autant de freins à la croissance digitale dans le secteur de l'assurance.

Néanmoins, certains assureurs se montrent moins frileux et ont commencé à repenser le modèle économique classique de l'assurance avec la prise en compte notamment de la montée en puissance de l'économie collaborative. Ces nouvelles façons d'appréhender la relation d'assurance s'écartent d'une relation transactionnelle épisodique classique pour adopter une interaction et un engagement avec les clients de plus en plus constants mais néanmoins souples. Ce nouveau virage pris par certains acteurs du monde de l'assurance favorise ainsi la confiance que leur témoignent leurs clients. Pour illustration, le service « *Panasonic Smart Home & Allianz Assist* », partenariat entre Panasonic et Allianz, relie les systèmes de suivi et de contrôle de maison connectée à des services de protection domestique. Cette solution intégrée emprunte aux principales garanties des polices d'assurance multirisques et protège le domicile des assurés empêchant ainsi les dommages complémentaires dus aux cambriolages, aux bris de vitre/fenêtre et aux fuites d'eau, afin notamment de fournir un service renforcé aux clients par rapport aux produits d'assurance habitation traditionnels. La « *Health Keeper Platform* » d'AXA constitue un autre exemple de cette évolution, avec une application qui assure un suivi des activités de l'utilisateur et propose également des services médicaux à prix réduit en fonction du degré d'activité du client. Ces nouvelles façons de penser la relation d'assurance permettent ainsi aux assureurs de multiplier leurs opportunités

d'interagir directement avec leurs clients. Par ailleurs, le développement de la digitalisation en matière d'assurance via l'utilisation du *big data* confronte les assureurs à la maîtrise de nouveaux concepts particulièrement techniques et difficiles à maîtriser. Figurent au rang de ceux-ci par exemple la Blockchain et les smart contracts permettant de dématérialiser, sécuriser et tracer des transactions qui devront à notre sens absolument faire partie de l'arsenal digital des assureurs. L'intelligence artificielle joue également un rôle considérable sur la matière assurable tant sur la nature que l'amplitude des risques pris en charge par l'assureur. Enfin, on pourra citer l'assurance collaborative qui connaît un essor important grâce notamment aux réseaux sociaux. Cette « *assurance* » (sa nature peut être débattue) qui consiste à regrouper des individus afin qu'ils mettent en commun leurs risques et s'assurent mutuellement apparaît comme un système collaboratif de partage des risques au sein d'une communauté à taille humaine. Le but commun de ces récents programmes de transformation des compagnies d'assurance reste l'amélioration de la place du client dans la relation d'assurance et la satisfaction de ses besoins de plus en plus évolutifs et souples. Ces nouveaux programmes ont par ailleurs favorisé l'agilité des méthodes de travail et d'organisation des entreprises afin d'adapter au mieux cette mutation digitale aux attentes des clients et leur proposer des services innovants et robustes (1.1). Leur principal défi à ce sujet réside dans la simplification de leur activité digitale (1.2).

### 1.1. Agilité des méthodes de travail

De la même manière que le développement « *agile* » bouscule le paysage informatique traditionnel, le « *travail agile* » et les « *méthodes agiles* » (qui prévoient que les organisations adoptent de nouveaux modes,

5. [http://www.ey.com/Publication/vwLUAssets/EY\\_Insurance\\_in\\_a\\_digital\\_world:\\_The\\_time\\_is\\_now/\\$FILE/EY-Digital-Survey-1-October.pdf](http://www.ey.com/Publication/vwLUAssets/EY_Insurance_in_a_digital_world:_The_time_is_now/$FILE/EY-Digital-Survey-1-October.pdf)

approches et technologies de collaboration souvent au sein de laboratoires ou de plateformes) contribuent au programme digital d'une société d'assurance et lui permettent de mettre en œuvre des changements de manière plus rapide et extensible. Les processus et méthodes agiles sont ainsi plus susceptibles de fournir une mise en œuvre adaptée à l'ampleur de la transition digitale en cours. Avec le « *Digital Garage* » d'Aviva, par exemple, et le « *Digital Accelerator* » d'Allianz, des assureurs d'envergure créent de nouvelles plateformes réunissant différentes entités de l'entreprise pour créer des groupes de travail agiles en charge d'opérer une rupture avec les modèles d'activité traditionnels, et de piloter ce bouleversement digital. Les assureurs plus traditionnels peuvent également développer cette agilité en interne par le biais de partenariats commerciaux avec des entreprises technologiques très dynamiques ou des cabinets de conseil innovants.

Quels que soient les avantages offerts, ces nouveaux modes de travail ont toutefois un coût et les entreprises doivent se préparer aux principales problématiques juridiques et commerciales qui peuvent se poser quand elles s'associent avec des entreprises tierces – qu'il s'agisse de cabinets de conseil ou d'entreprises technologiques – dans l'optique de soutenir leurs activités de transition digitale. La mise en place de contrats ultra-normés prenant en compte l'ensemble des exigences liées aux politiques de conformité des assureurs peut toutefois se révéler contre-productive privant ainsi de la flexibilité nécessaire au succès d'un développement agile.

On assiste par conséquent à l'avènement d'une méthode de contractualisation hybride. Cette approche paraît plus adaptée à des organisations plus conservatrices, mêlant garanties minimales en termes juridiques, tout en bénéficiant des avantages, des méthodes et des processus agiles.

Le degré de spécificité, la fidélisation du client et la structure commerciale doivent être minutieusement envisagés en insistant sur le volet contractuel des résultats stratégiques et

commerciaux (avec des facteurs d'incitation adaptés et des correctifs si ceux-ci ne sont pas réalisés).

En pratique, l'agilité du travail et de ses méthodes doit reposer également sur une expertise technique certaine et irréprochable. L'utilisation de nouvelles méthodes de souscription des produits d'assurance, de mise en place de canaux de distribution, de gestion de la sinistralité doit être réalisée de pair avec un expertise technique et ne pas se limiter aux seuls aspects juridiques. À titre d'exemple, la souscription de risques Blockchain doit être réalisée avec précaution de manière à mettre en place une déclaration des risques précise et un contours des garanties correspondant exactement à ce que l'assureur peut ou souhaite assurer. Une analyse combinée tant juridique que technique est fortement recommandée de manière à cantonner ou du moins appréhender les risques liées à ces nouvelles méthodes de travail.

---

### 1.2. Processus et simplification de l'activité digitale

---

Le principal défi à relever pour les assureurs vise à concrétiser la transition digitale « *véri- table* » des systèmes back-office, des processus internes, des modèles d'interaction avec le client, de souscription et de gestion des sinistres pour tout le cycle de l'assurance, ce qui implique plus que la simple création d'un « *vernís digital* » pour leurs modèles économiques existants.

Nombre de sociétés d'assurance consistent en des organisations complexes d'une certaine envergure, œuvrant sur des plateformes variées et soutenant des centaines de processus d'activités différents, dans de nombreux pays et régions. Pour s'adapter au monde digital, les assureurs doivent consolider et simplifier leurs processus.

Les assureurs sont traditionnellement perçus comme des structures lourdes avec des processus complexes et il a pu être indiqué que leur capacité à réagir aux évolutions du marché de manière réactive était souvent

restreinte par des réglementations contraignantes et des investissements dans des systèmes patrimoniaux coûteux. En réalité, la réglementation a pour objectif de permettre le développement de produits dans un objectif de solvabilité d'une part mais également de protection des consommateurs d'autre part. Dès lors, garantir une stratégie digitale est conforme aux objectifs stratégiques de l'assureur, simplifier leur paysage technologique et leurs processus, favoriser une culture de start-up, et permettre le changement digital constituent autant d'éléments pour faire évoluer une activité d'assurance traditionnelle. Les assureurs sont conscients que cette révolution digitale leur permet de relever un nouveau défi, celui d'être en mesure de transformer avec succès leur interaction avec le client et d'accroître leur part de marché dans un monde toujours plus perméable aux mutations technologiques.

## 2. Apprentissage automatique et analytique avancée

Les besoins du secteur de l'assurance sont multiples et variés, qu'il s'agisse de comprendre et d'anticiper les comportements clients, d'évaluer les risques complexes ou d'améliorer l'efficacité des processus de production. La technologie est un moyen de parvenir à une fin très précise : élaborer des solutions opérationnelles plus rapides, plus sûres et plus efficaces. Le traitement des données personnelles est également l'enjeu majeur que pose l'essor du numérique. Le respect de la vie privée de chacun, le devenir d'une donnée stockée dans n'importe quelle base et l'utilisation qui en est faite par les GAFAs doivent être réglementés. Il est donc nécessaire de lier l'important développement du Big Data (2.1) à une législation appropriée, garantissant le respect et la confidentialité des données (2.2).

### 2.1. Big Data

L'émergence de technologies toujours plus sophistiquées améliore la capacité à saisir

et à extraire de la valeur de donnée client. Le « *Big data* » utilise des volumes considérables de données, qui englobent souvent les « *données personnelles* » des individus à partir d'un large éventail de sources, dans l'optique de démontrer des modèles de comportement et fournir des perspectives qui peuvent éclairer le développement de nouveaux produits et services. La nature et la portée de la *data* impliquent qu'il peut être difficile de la traiter à l'aide des techniques logicielles et des bases de données traditionnelles. Mais la valeur du *Big Data* ne cesse de croître et les nouvelles technologies comme l'apprentissage automatique et l'intelligence artificielle, qui fournissent une analyse efficace, deviennent incontournables. Cette technologie identifie des schémas afin de produire des décisions, des prédictions et des résultats fiables à grande échelle. Le *Big Data* peut permettre aux assureurs d'améliorer le « profilage » des assurés et de cibler au mieux leurs besoins avec une individualisation poussée de l'offre d'assurance et le développement de nouveaux services de prévention en vue d'éviter les sinistres.

L'apprentissage automatique peut fournir une analyse de la *data* dès que celle-ci est enregistrée – par exemple, la mise à jour d'une information pour aider à l'identification de la fraude. Il est en mesure d'identifier les opportunités de subrogation, de raccourcir les délais de dépôt de déclarations de sinistres, d'améliorer la prévision des sinistres et le calcul des réserves, et peut contribuer à prévoir quels sinistres sont les plus susceptibles d'entraîner une compensation. Ces avantages peuvent transformer la relation client et générer des économies considérables pour les sociétés d'assurance.

L'apprentissage automatique peut également permettre de surmonter efficacement les silos internes. Compte tenu du mode de stockage et d'obtention de la *data*, les organisations font souvent face à des obstacles quand elles essaient d'en extraire de la valeur. Nombre de sociétés collectent ainsi des volumes considérables de données non vérifiées et ne disposent pas d'une vision adaptée de la *data* ainsi stockée. Celle-ci peut être conservée par différentes entités ou départements, et avoir été obtenue selon des

consentements et notifications variés. Par conséquent, même si les entreprises acceptent d'extraire de la valeur de la *data* qu'elles possèdent, elles ne savent pas où est stockée leur *data* la plus précieuse ni sur quelle base celle-ci a été collectée. L'apprentissage automatique peut servir à casser les silos internes en analysant un éventail de sources, de types et de formes de *data* opérable.

Mais le phénomène *Big Data* pourrait être également synonyme de la fin de la mutualisation des risques, principe directeur qui définit la notion même d'assurance. La doctrine universitaire majoritaire définissant la notion d'assurance insiste sur le caractère consubstantiel du contrat d'assurance avec les éléments techniques qui le caractérisent, en particulier la mutualisation du risque qui permet la dilution du risque individuel dans la multitude des risques de même nature, selon la loi des statistiques ; cet aspect particulier est présenté comme un élément inhérent à l'opération d'assurance en ce qu'il justifie le régime particulier applicable, par exemple la proportionnalité entre la prime et l'indemnité ou les règles actuarielles sous-jacentes au régime prudentiel. La mutualisation des risques est ce principe qui permet à l'assurance de remplir son objet social de couverture historique et de protection de tous. Mais en affinant à l'extrême les profilages des assurés permettant une individualisation extrême de la tarification des primes d'assurance, la notion même de mutualisation pourrait être vidée de sa substance et remettre en cause le principe même d'assurance.

## 2.2. Impact des réglementations relatives à la confidentialité des données

À mesure que le volume et la diversité de la *data* augmentent, les difficultés et les défis associés à son utilisation s'accroissent également. Bien que l'analyse du *Big Data* n'implique pas toujours de données personnelles, une grande part de ses opérations s'appuie souvent sur un traitement exhaustif de ce type de données. C'est dans ce contexte, que dans quasiment tous les systèmes

juridiques, le législateur cherche à tenir le rythme de ces évolutions technologiques en mettant en place un arsenal de lois et de réglementations encadrant l'utilisation du *Big Data* et en s'assurant de la bonne utilisation et de la conservation de ces données.

Au sein de l'Union européenne, le traitement des données personnelles est régi par un corpus juridique qui, s'il garantit efficacement aux individus des droits spécifiques, est souvent considéré comme incompatible avec les opérations relatives au *Big Data*. Par exemple, la directive 95/46/EC de l'Union européenne (« *Directive pour la protection des données* ») dispose que les contrôleurs de données, concept qui englobe les assureurs qui traitent le *Big Data* à l'aide de l'apprentissage automatique, ne collectent les données personnelles que pour les « usages spécifiés, explicites et légitimes ». Elle exige en outre que les données personnelles soient « adaptées, pertinentes et en nombre raisonnable compte tenu de l'objectif pour lequel elles sont collectées et/ou traitées. Or, l'analytique du *Big Data* implique en général la collecte du volume maximal de données auprès du plus grand nombre de sources possibles, avant leur exploitation et leur réaffectation à d'autres utilisations.

Le Parlement européen a adopté dernièrement le Règlement général sur la protection des données (RGPD) qui a modifié en profondeur la manière dont les entreprises et les individus gèrent leurs données. Le Règlement est appelé à se substituer à la Directive sur la protection des données et s'appliquer automatiquement dans tous les États membres. Les organisations soumises au Règlement ont eu jusqu'au 25 mai 2018 pour se préparer et nombre de sociétés d'assurance ont mis en place les chantiers nécessaires même si en pratique, certains aspects ne sont pas totalement finalisés. Ce besoin est d'autant plus pressant que la CNIL a manifesté son intérêt particulier pour cette industrie. En ce sens, l'autorité administrative indépendante a émis par la voie de cinq délibérations en date du 11 octobre 2018, des mises en demeure adressées à différentes sociétés d'assurance. Il a été prouvé que ces sociétés rappelées à l'ordre se servaient

des données recueillies dans le cadre de leur mission d'intérêt général auprès des fédérations professionnelles de secteur afin de réaliser de la prospection commerciale. Or, ces données personnelles n'étant censées servir qu'à recouvrer les cotisations et payer les allocations de retraite, la CNIL a estimé qu'il s'agissait là d'un détournement de finalité et leur a accordé 1 mois pour faire cesser ce détournement.

L'un des principaux changements proposés tend à renforcer notamment les conditions d'utilisation de données dans l'optique d'un « *profilage* » des clients. Les individus auront le droit de ne pas être soumis à une décision qui serait fondée uniquement sur un traitement automatisé et qui produirait des effets juridiques ayant un impact sur l'individu. Ce qui est susceptible d'inclure par exemple les calculs de primes d'assurance et l'analyse de la probabilité qu'un individu dépose un sinistre pour son assurance automobile ou maladie. Cela pourrait éventuellement inclure les calculs automatiques de primes d'assurance. Le profilage fondé uniquement sur des données sensibles, à l'instar des données médicales, est interdit. Le profilage fondé sur des données anonymes est acceptable, sous réserve que les données ne puissent pas être associées à un individu en particulier.

En pratique, l'impact du RGPD est également présent en matière de distribution d'assurance. Les conventions et protocoles de distribution doivent contenir des dispositions lourdes en matière de respect de RGPD ce qui est parfois difficilement compatible avec la nécessité de manager la distribution commerciale avec des intermédiaires d'assurance qui ne sont pas en mesure de gérer ces dispositions. Là encore, un renouveau des modèles est à anticiper.

Le nouveau Règlement requiert un modèle de consentement plus actif, dans l'optique de soutenir le traitement juridique des données personnelles. Chaque fois que le consentement est requis pour le traitement des données personnelles, celui-ci doit être explicite et non pas implicite. Le Règlement requiert des organisations qui utilisent les informations pour l'analytique

de données qu'elles soient en mesure de prouver que les individus comprennent et approuvent réellement l'utilisation de leurs données. Cette nouvelle exigence pourrait poser problème aux assureurs et est susceptible de nécessiter une évolution considérable de la manière dont le consentement est obtenu auprès des clients et géré au sein des sociétés d'assurance (y compris dans les bases de données historiques).

Avec la récente décision du Royaume-Uni de sortir de l'Union européenne, le Règlement ne s'appliquera plus directement aux assureurs du Royaume (sauf si l'assureur en question cible des ressortissants de l'Union européenne). Le Royaume-Uni reste et restera toutefois engagé en faveur de la conformité en matière de protection des données. *L'Information Commissioner's Office* (ICO) a ainsi déclaré récemment qu'il souhaite la mise en place au Royaume-Uni de lois équivalentes à celles instituées par le Règlement, dans l'optique de fournir la « *pertinence* » nécessaire pour soutenir les transferts de données au Royaume-Uni depuis l'UE.

Parallèlement, la cybersécurité représente un risque croissant et un domaine d'attention réglementaire renforcé. De nouvelles recommandations actualisées ont été publiées par le législateur en Asie par exemple. À la lumière de ces différents développements, les équipes risque et conformité des assureurs en Asie doivent non seulement se concentrer sur les obligations de conformité en matière de cybersécurité immédiate qui proviennent des dernières réglementations mais aussi garantir que des programmes de conformité proactifs soient développés pour tenir compte de la dépendance toujours plus forte à la technologie et à *la data*.

Avec cette évolution du paysage réglementaire, on devrait continuer d'observer une augmentation de la réglementation autour du *Big Data*. Une nouvelle fois, il peut être également considéré qu'il s'agit là d'une opportunité pour les assureurs. La recherche active de solutions pour garantir la conformité leur permettra non seulement de consolider des méthodes innovantes pour monétiser leurs

données client, mais également de garantir que l'organisation maintient et assoit la confiance auprès de sa base clientèle. La mise en place d'une infrastructure et du cadre de gouvernance adaptés pour soutenir efficacement l'utilisation du *Big Data* peut permettre aux entreprises de consolider une meilleure relation avec leurs clients et prospects, notamment quand il s'agit d'utiliser des techniques d'analytique avancée et de *Big Data*.

### 3. Le digital transforme-t-il le paysage réglementaire ?

L'assurance tendant à devenir un secteur de plus en plus régulé au point d'apparaître comme un problème majeur dans ce secteur, les compagnies d'assurance vont devoir consacrer d'importants moyens financiers et humains pour répondre à ce challenge juridique.

Ainsi, si le digital apporte plusieurs transformations dans les différents secteurs du droit, l'innovation amorcée par le digital se voit opposer néanmoins plusieurs challenges (3.1), que des plateformes ont tenté de détourner (3.2). Ces solutions proposées par des organismes indépendants (3.3) n'attendent plus que d'être soutenues par une législation de plus en plus conséquente, devant concilier droit de la consommation et protection des données personnelles (3.4).

#### 3.1. Les challenges réglementaires à l'innovation dans les secteurs insurtech

Un des premiers challenge réglementaire dans le secteur de l'insurtech est de définir dans quelle mesure une nouvelle activité est réglementée ou soumise à des contraintes particulières.

Ce travail est parfois d'autant plus complexe qu'aux dates auxquelles ont été rédigées les textes du Code des assurances ou du Code Monétaire et Financier, ces nouvelles technologies et ces concepts étaient encore inconnues. Par conséquent, il sera d'autant plus nécessaire d'interpréter la loi dans son but téléologique initial et de la concilier avec les nouveaux

impératifs de protection du consommateur. Par ailleurs, dans plusieurs pays, les réglementations imposent des règles de protection des consommateurs pour la vente de produits d'assurance qui ne sont pas adaptées à un environnement digital très évolutif. Par conséquent, l'utilisation du passeport européen et en particulier du régime de la libre prestation de services est rendue plus complexe à mettre en œuvre en l'absence de textes harmonisés. Enfin, et surtout, il convient de faire coïncider les exigences du Code des assurances et du Code Monétaire et Financier à l'activité Insurtech ainsi qu'avec les préconisations de l'Autorité de Contrôle Prudentiel et de Résolution (« ACPR »). À titre d'exemple, lors de la distribution d'un produit d'assurance, le parcours client devra être en mesure de remplir les conditions du devoir de conseil nécessitant un travail pédagogique de recueil des besoins et de reformulation des capacités du client et cela, indépendamment de la forme de souscription utilisée. L'utilisation de nouvelles technologies devra être réalisée de manière à respecter ces impératifs.

#### 3.2. Que faire ?

Diverses initiatives ont été prises par les autorités de régulation européennes afin d'aider à l'accompagnement des entreprises d'assurance dans ce nouveau contexte technologique et réglementaire.

C'est dans ce contexte que le *Project Innovate* de la FCA, autorité de contrôle britannique, a communiqué sur sa volonté d'ouvrir ses portes aux entreprises développant des approches innovantes, à même de profiter à tous les consommateurs. Elle considère l'innovation digitale comme essentielle pour consolider son objectif statutaire de promouvoir la concurrence. En ceci, elle est alignée sur la politique du gouvernement britannique qui souhaite la promotion du secteur digital. La plateforme d'innovation offre aux acteurs qui souhaitent développer de nouveaux concepts des assistants dédiés, des conseils et le cas échéant des recommandations sur les questions

réglementaires spécifiques. L'organisme cherche en priorité à fluidifier le processus d'autorisation pour les entreprises innovantes, afin de soulever intérêt et innovation dans ce domaine. L'autorité a ainsi aidé 177 start-ups au cours de sa première année d'exploitation et a refusé les candidatures de plus de 150 autres entreprises ayant échoué à satisfaire à ses critères.

En France, on soulignera l'initiative de l'ACPR qui a mis en place une cellule dite «Fintech et Innovations» (qui s'applique également à l'assurance). L'objectif est de permettre la mise en place d'une plateforme permettant aux acteurs traditionnels et émergents de pouvoir appréhender la législation applicable et d'identifier des interlocuteurs susceptibles de les accompagner dans les démarches réglementaires. Cette cellule est d'autant plus importante qu'elle permet d'avoir une interprétation des textes, le cas échéant, par le régulateur prudentiel.

### 3.3. Bacs à sable réglementaires

Parallèlement à l'accompagnement des entreprises d'assurance au niveau du respect des exigences réglementaires, les autorités de contrôle ont également fait montre d'innovation en créant des structures adaptées permettant le développement de nouveaux produits d'assurance considérés comme « à risque ». C'est ainsi qu'au Royaume-Uni, la FCA a officiellement lancé son « bac à sable » qui consiste en un espace sécurisé dans lequel les produits insurtech et/ou fintech peuvent être testés par des start-ups non autorisées ou encore des entreprises déjà habilitées souhaitant tester des concepts n'entrant pas facilement dans le cadre réglementaire existant. Cette approche devrait permettre de réduire le délai de commercialisation et d'améliorer l'accès au financement (en réduisant les incertitudes réglementaires) afin de permettre à terme, l'introduction de nouveaux produits favorisant la concurrence et donc les services offerts aux consommateurs. Dans l'enceinte du bac à sable, des entreprises peuvent rester soumises à des restrictions tout en testant leurs idées. Quand la FCA est satisfaite et

considère que tous les critères d'autorisation réglementaire sont respectés, les restrictions peuvent être suspendues.

Par ailleurs, d'autres législateurs suivent l'exemple de la FCA et encouragent l'innovation digitale

En Australie par exemple, l'autorité de contrôle locale, l'ASIC, cherche à mettre en place un bac à sable sur un modèle similaire et l'organisme a déjà déployé une plateforme d'innovation. L'ASIC se targue également d'un processus d'autorisation beaucoup plus rapide pour les nouvelles entreprises – celles-ci sont ainsi habilitées dans un délai de 60 jours après candidature. Au Royaume-Uni et dans d'autres juridictions, le processus peut nécessiter jusqu'à un an. La *Singapore Monetary Authority* (MAS) cherche également à développer un bac à sable et de manière plus générale à aider Singapour à développer une plateforme asiatique insurtech et fintech.

D'autres législateurs se montrent pour le moment beaucoup plus frileux à l'instar de l'Allemagne, par exemple, où la Bafin a refusé les demandes pour un bac à sable et insiste pour que les organisations insurtech et fintech qui opèrent dans un domaine soumis à autorisation se conforment aux mêmes réglementations que les organismes déjà établis.

### 3.4. Un accroissement de la réglementation: quelles opportunités pour aider les innovateurs ?

Dans plusieurs juridictions, les législateurs et les pouvoirs publics sont de plus en plus enclins à adapter les réglementations existantes afin d'encourager l'innovation et la croissance du digital. La FCA a ainsi déclaré, envisager un assouplissement des réglementations juridiques pour faciliter l'innovation. Au sein de l'Union Européenne, et plus particulièrement dans le secteur des assurances, la mise en place de la réglementation de cette matière a été récemment plus forte notamment avec la récente mise en œuvre du *corpus* Solvency II, la transposition de la Directive sur la Distribution de l'Assurance ou encore,

les changements mis en œuvre à la suite du Règlement sur la protection des données. Ces réglementations ont un impact fort dans l'utilisation et la mise en place de modèles relatifs aux nouvelles technologies dans le secteur des assurances et devront être pris en compte qu'il s'agisse d'intelligence artificielle, de blockchain ou d'assurance collaborative.

À l'heure actuelle, législateurs et gouvernements nationaux de l'Union Européenne disposent d'une marge de manœuvre réduite s'ils souhaitent agir individuellement pour réduire l'impact des règles édictées à l'échelle européenne. Il appartient donc à d'autres types d'acteurs de permettre une interprétation favorable des textes et des pratiques aux développements des initiatives digitales. En ce sens, l'ACPR et sa cellule Fintech et Innovation en sont un exemple. Pour les assureurs, il nous semble que l'alliance de la maîtrise technique et juridique des nouveaux projets sont la clef d'une réussite pour profiter de la révolution digitale.

Au plan européen, on soulignera également que le Brexit peut être une chance pour attirer le secteur technologique hors du Royaume-Uni vers des territoires qui garantissent un accès moins restreint à un vivier de talents élargi et permettant le rattachement au marché unique européen. Surtout, les libertés communautaires de régime de liberté d'établissement et de libre prestation de services sont des outils permettant aux acteurs d'intervenir sur un marché plus large et de manière réglementaire simplifiée. Ainsi, à l'heure où chaque juridiction cherche à se présenter comme un endroit favorable aux évolutions technologiques, ces libertés communautaires pourraient conduire une fois de plus à une évolution et une modernisation de la réglementation de l'Union européenne. Quel que soit le cadre réglementaire qui s'appliquera, le législateur continuera à tendre vers un équilibre oscillant entre favoriser l'innovation et réaliser ses objectifs de protection des assurés, preneurs et bénéficiaires d'assurance.

La déclaration de Bob Ferguson, chef du Project Innovate de la FCA en est l'illustration parfaite : « *l'innovation n'est en aucun cas une sorte de dissolvant universel qui s'affranchirait*

*du besoin de respecter les exigences destinées à protéger les consommateurs ou l'intégrité des systèmes financiers. Elle ne doit pas servir d'excuse pour se monter moins vigilant ».*

---

## Conclusion

---

Pour le secteur des assurances, la transition digitale est aujourd'hui une question cruciale. À l'évidence, les assureurs en ont conscience et s'attèlent à la recherche de nouveaux moyens pour optimiser leurs opérations et processus avec des méthodes de travail, plus agiles, plus souples.

Une stratégie de transition digitale est ici essentielle pour créer des parcours client plus fluides, plus efficaces, mais surtout pour améliorer l'expérience client dans son ensemble. Bâtir la confiance avec les clients tout en restant dynamique et en optimisant la stratégie digitale reste un réel défi. Le *Big Data* ou encore la *Blockchain* offrent un large éventail d'opportunités pour s'engager auprès des clients et aider les entreprises d'assurance à mieux les comprendre (ainsi que leurs habitudes).

Pour acter le changement et se tourner vers l'avenir, les assureurs doivent repenser les modèles traditionnels. Les assureurs qui mettent en place ces nouveaux modèles bénéficient déjà d'une traction vitale et gagnent des parts de marché, deux avantages qui devraient aller croissant avec le temps et le développement de la technologie.

Le moment est décisif pour le secteur. Ces nouvelles technologies sont considérées comme des sources de solution aux sujets de préoccupation des assureurs, concernant leurs nécessaires innovations technologiques.

Aussi, les organisations qui sont en mesure de tirer profit de la transition digitale et de cette rupture au sein du secteur, tout en négociant les risques juridiques, réglementaires et commerciaux, seront celles qui en sortiront gagnantes. On l'aura compris, l'innovation doit devenir un élément central de la stratégie des entreprises d'assurance d'où la nécessité de changer la culture et la structure d'organisation des assureurs traditionnels dans un contexte d'hyper-réglementation, tel est le challenge à relever.

SERVICES

---

THÈME 4

# Hôtellerie & transformation numérique



# Le point de vue...

**Arnaud Morvan,**  
Responsable de la Digitalisation, B&B Hôtels

## Comment le numérique a-t-il transformé le secteur de l'hôtellerie ?

Depuis quelques années, le secteur hôtelier fait face à une tendance forte à l'ultra digitalisation, qui concerne aussi bien les services et produits proposés que les usages des consommateurs.

Nous avons ainsi été parmi les pionniers de l'hôtellerie économique à déployer sur ses 268 hôtels en France, un réseau WIFI haut débit via la fibre, car ce sont nos clients qui le disent, "un bon Wifi est aussi important qu'un bon lit". Par ailleurs, nous avons su nous adapter rapidement aux nouveaux usages des clients, avec notamment la mise en place d'une plateforme d'avis clients 100 % vrais et certifiée AFNOR. Au-delà des transformations liées à l'expérience client, la plus grande transformation de ces trois dernières années concerne principalement notre modèle de distribution. Après l'arrivée d'acteurs comme AirBnB (au nom de marque très proche de la nôtre), qui sont venus cannibaliser et capter notre clientèle sur les canaux digitaux, ou encore l'omniprésence des OTA (booking/expédia/...) sur tous les canaux de distribution digitaux, nous avons dû réadapter rapidement nos stratégies de distribution avec une approche très ROI-ste de nos investissements sur l'ensemble des leviers digitaux, et revoir notre organisation interne en intégrant les expertises nécessaires pour une meilleure maîtrise. Aujourd'hui 40 % de notre CA est réalisé en ligne. Sans compter tout le business fait par téléphone ou directement dans nos hôtels après consultation de notre site web, de notre appli ou des avis clients. Tout l'enjeu est de préparer notre entreprise à être plus agile, plus rapide, devant les changements de ces environnements de distribution ou l'arrivée de nouveaux concurrents ou start-ups sur le marché.

## Quels sont les principaux challenges / défis du numérique pour les hôteliers ?

Le numérique n'est pour nous pas une finalité en soi, mais un moyen d'améliorer l'expérience client et le quotidien de nos hôteliers, de leur faciliter la vie dans l'exploitation de leur hôtel.

Le principal défi aujourd'hui, est d'amener l'ensemble de notre réseau à une maturité sur les

usages digitaux, en créant les conditions d'un travail plus collaboratif, en décloisonnant nos services, ce qui nécessite la mise en place de ressources dédiées à la sensibilisation, à la formation et à l'accompagnement sur ces nouveaux usages, d'où la création de mon poste.

L'intelligence collective sera un facteur clé pour amener l'innovation dans notre entreprise, et la digitalisation ne se fera selon nous qu'avec les hommes et les femmes de notre réseau.

## Quel sera le visage de l'hôtellerie de demain ?

Elle devra s'adapter bien plus rapidement à son environnement et aux usages des clients, être plus agile pour ne pas subir les changements externes, mais savoir les transformer en réelles opportunités business.

L'usage mobile sera omniprésent pour nos clients, et nous devons les accompagner plus fortement dans l'expérience qu'ils vivent avec notre marque, leur permettre de vivre une expérience unique dans nos hôtels à produit et service équivalent. Être présent à chaque étape du parcours client est ainsi un enjeu prioritaire :

- En amont lors de la recherche : avec l'explosion programmée de la recherche vocale, chez lui, dans sa voiture, depuis son mobile,
  - Pendant son séjour en lui apportant des services qui facilitent son quotidien ou l'organisation de ses déplacements
  - Après son séjour en lui permettant de partager les valeurs de notre marque et son expérience.
- L'expérience client sera donc personnalisée, avec une utilisation maîtrisée de la data, une transparence vis-à-vis de nos clients sur leur utilisation avec un objectif unique, lui proposer la meilleure expérience en adéquation avec ses propres valeurs dans un environnement et des usages en constante évolution. Enfin, l'hôtellerie de demain, aura avant tout un visage humain, celui de nos hôteliers que nous devons accompagner, en digitalisant, automatisant une partie des processus opérationnels actuels, en les accompagnant à ces changements, afin de leur permettre une meilleure gestion de leur client et de leurs besoins.



Par Myriam Mejdoubi et Caroline Brun

**L'**émergence de l'économie numérique a entraîné une mutation profonde et rapide du secteur touristique – l'un des plus réceptifs à cette révolution – constituant un véritable facteur de croissance et d'innovation pour le secteur de l'hôtellerie.

En dépit des attentats terroristes qui ont sensiblement affecté le secteur touristique, rendant particulièrement atypiques les saisons 2015 et 2016<sup>1</sup>, l'activité hôtelière en France a connu un rebond significatif touchant toutes les régions et gammes d'hôtels en 2017<sup>2</sup> et apparaît encore au beau fixe en 2018<sup>3</sup>.

Toutefois, l'accueil touristique n'est plus l'apanage des acteurs traditionnels du tourisme. Les particuliers y contribuent notamment à travers les plateformes de mise en relation en ligne en utilisant ou en mettant à disposition d'autrui des biens ou des services.

Cette nouvelle économie numérique présente de nouveaux défis à relever pour le secteur de l'hôtellerie et incite à de nouvelles interactions avec les institutionnels. L'État semble favorable à ces efforts d'innovation qui constituent une richesse pour l'attractivité touristique en France, à l'heure où elle se prépare à accueillir successivement la Coupe du monde de rugby en 2023 et les Jeux olympiques et paralympiques en 2024. Les pouvoirs publics restent néanmoins attentifs aux préoccupations qui en découlent et interviennent afin de soutenir et d'encadrer le secteur tout en préservant la liberté d'entreprendre et d'innover. Ainsi, face à la transition numérique du secteur de l'hôtellerie (1), le législateur multiplie les efforts de régulation afin de répondre aux nouveaux enjeux juridiques (2).

## 1. La transition numérique du secteur de l'hôtellerie

Sous l'impulsion de l'innovation digitale, l'émergence fulgurante des plateformes

d'hébergement en ligne (1.1) a incité l'hôtellerie à se réinventer (1.2).

### 1.1. L'émergence des plateformes d'hébergement en ligne

En l'espace de quelques années, l'ère du numérique a intensifié la concurrence entre les acteurs traditionnels de l'hôtellerie – auparavant confrontés à leurs pairs – et les nouveaux acteurs du numérique. Avec l'essor des nouvelles technologies, les concurrents numériques de l'hôtellerie se sont rapidement développés par le biais de plateformes en ligne simplifiant les échanges et facilitant la mise en relation entre les individus.

En effet, le secteur de l'hôtellerie a été confronté à une multiplication de ces plateformes en ligne, pour certaines venues d'Outre-Atlantique, et animées d'un esprit *start-up* dont les hôteliers traditionnels étaient peu familiers<sup>4</sup>.

À titre d'illustration, Booking.com et AirBnb se sont imposés comme des opérateurs emblématiques de l'e-tourisme de l'hébergement,

1. *Tendances du tourisme et de l'hôtellerie – Réinventer l'Hôtellerie*, Deloitte – InExtenso, 16 février 2018.

2. *L'industrie hôtelière française en 2018*, KPMG, 25 septembre 2018, <https://home.kpmg.com/fr/fr/home/media/press-releases/2018/09/industrie-hoteliere-francaise-2018.html>.

3. *Bilan de l'activité hôtelière au 1<sup>er</sup> semestre 2018 : un marché au beau fixe malgré les grèves du printemps*, communiqué de presse MKG Consulting, 24 juillet 2018.

4. *L'hôtel... rit*, Xavier Delpech, *Juris tourisme* 2015, n° 176, p. 3.

5. *Ibid.*

6. Décision 15-D-06 du 21 avril 2015 de l'Autorité de la concurrence ; *Plateformes de réservation hôtelière*, communiqué de presse de l'Autorité de la concurrence, 9 février 2017.

chacun avec un modèle économique propre<sup>5</sup>. Booking.com est devenue la plateforme de référence en matière de réservation d'hôtels en ligne. L'Autorité de la concurrence a néanmoins remis en cause les clauses de parité mises en œuvre par Booking.com dans ses contrats avec les hôteliers<sup>6</sup>, permettant aux hôtels la possibilité de proposer des tarifs inférieurs sur les plateformes concurrentes de Booking.com ainsi que les canaux directs hors ligne (téléphone, mailings, agences de voyages physiques etc.), mais pas sur leur site internet. La loi Macron du 6 août 2015 a également interdit toute clause venant limiter la liberté tarifaire de l'hôtel, permettant ainsi aux hôtels de proposer sur leur site internet des tarifs inférieurs à ceux proposés par les plateformes de réservation en ligne.

AirBnb est devenue quant à elle le leader incontesté en matière de location meublée de courte durée et a créé le concept de plateforme collaborative permettant l'utilisation partagée de biens entre particuliers<sup>7</sup>. La plateforme de location AirBnb, qui a fêté ses dix ans d'existence, est passée du statut de *start-up* à celui de géant de l'économie collaborative. Elle propose aujourd'hui près de 5 millions de logements, dans 81 000 villes et près de 200 pays<sup>8</sup> quand un groupe hôtelier mondial comme AccorHotels propose 4 300 hôtels à travers le monde et environ 620 000 chambres dans moins de 100 pays<sup>9</sup>.

Une multitude d'offres dérivées ont également fait leur apparition, à l'instar de plateformes comme Spotted by Locals qui met à disposition des applications pour smartphone ou des guides touristiques dans une quarantaine de villes européennes, CouchSurfing, service d'hébergement en ligne temporaire et gratuit regroupant une cybercommunauté de plus de 10 millions de membres répartis dans plus de 200 000 villes dans le monde et permettant aux personnes de proposer un lit ou un canapé pour dormir, ou encore Gamping, plateforme communautaire permettant de camper chez l'habitant.

Face à l'émergence des plateformes collaboratives, la loi Lemaire<sup>10</sup> est venue préciser la notion d'opérateur de plateforme à l'article

L. 111-7 du Code de la consommation : « *Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur :*

*1° le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ;*

*2° ou 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 service. »*

Les hôteliers ont pris conscience du poids des plateformes collaboratives dont l'activité en France représente désormais 2 milliards d'euros, soit 15 % du chiffre d'affaires de l'activité d'hébergement des hôtels<sup>11</sup>. Force est de constater que ces nouveaux acteurs ont perturbé l'équilibre de l'hébergement touristique et que l'innovation digitale incite plus que jamais l'hôtellerie à se réinventer.

## 1.2. L'hôtellerie se réinvente sous l'impulsion de l'innovation digitale

Le développement du numérique dans le secteur de l'hôtellerie a amené à repenser entièrement les relations professionnels-clients et a incité les hôteliers à investir dans la

7. *Les particuliers, nouveaux acteurs du tourisme*, Nathalie Fabry, Juris tourisme 2016, n° 189, p. 35.

8. Source AFP.

9. <https://www.accorhotels.group/fr-FR/hotel-development/accorhotels-choice/a-leading-hotel-operator#nu-0>

10. Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (dite « loi Lemaire »).

11. *Hôtellerie : la stratégie des professionnels face à leurs concurrents numériques*, J.-C. Catalon, *La Tribune*, 2 février 2017.

12. *Quel impact du numérique sur les métiers du tourisme ?* Youma Dieng, Juris tourisme 2016, n° 189, p. 33.

transformation numérique afin de valoriser leur offre et de répondre aux attentes des consommateurs<sup>12</sup>.

Le rebond de l'activité hôtelière en 2017 a en partie discrédité les critiques à l'encontre d'Airbnb et de ses concurrents les accusant de capter massivement les clients de l'hôtellerie et de provoquer une chute de leurs taux d'occupation. En 2017, Airbnb n'a jamais proposé autant de logements en France, ce qui n'a pas empêché l'industrie hôtelière d'enregistrer une hausse de fréquentation de près de 4 % par rapport à 2016<sup>13</sup>.

Avec l'émergence des sites comparateurs, le séjour du client débute lors de la préparation du voyage et continue même après son voyage *via* le partage de son expérience et la fidélisation. Ainsi, le client devient plus exigeant concernant les services et le confort lors de son séjour : l'hôtel n'est plus un simple lieu de résidence ou de travail temporaire, c'est plutôt un lieu qui lui procure une expérience différenciée.

Sur ce point particulier, le numérique fournit de nombreuses possibilités pour répondre aux besoins à la fois fonctionnels et émotionnels du client. D'ailleurs, ce dernier, multi-équipé, emporte ses terminaux partout avec lui y compris à l'hôtel, et s'attend en outre à une offre numérique complète : accès au réseau wifi, location d'appareils numériques, espaces professionnels high-tech, signalétique et actualités sur écrans dans les halls.

Le tout-digital est perçu par conséquent comme un luxe par les usagers car il répond aux besoins de personnalisation et de fluidité à l'aide d'applications, d'équipements intelligents et des services désintermédiés depuis la chambre.

En ce sens, le groupe AccorHotels souhaite s'imposer en leader de l'hôtellerie digitale et revendique une stratégie ambitieuse fondée sur un plan à 5 ans de 225 millions d'euros destiné à améliorer l'expérience digitale des clients, partenaires et collaborateurs<sup>14</sup>. Parmi les huit programmes dédiés à ce plan, le groupe entend développer de puissantes campagnes d'« acquisition » afin d'attirer et orienter la demande des consommateurs (par la présence significative sur les réseaux sociaux, des

références à fort impact sur les moteurs de recherche, et en concluant des partenariats avec les comparateurs de prix les plus influents comme TripAdvisor, Kayak, Trivago, etc.), d'optimiser la « distribution » de l'hôtel (notamment par les sites internet, les applications et les partenariats avec les agences de voyage en ligne) ou encore d'accroître la fidélisation en veillant à l'e-réputation (commentaires de clients et service client en ligne)<sup>15</sup>.

Les consommateurs d'aujourd'hui sont en permanence connectés, et l'interaction avec le client à travers ces canaux digitaux est primordiale, en particulier dans le secteur de l'hôtellerie.

---

## 2. Les enjeux juridiques de la numérisation du secteur de l'hôtellerie

---

Si l'économie numérique est de nature à dynamiser le secteur de l'hôtellerie en proposant des modes de consommation alternatifs et innovants, celle-ci ne peut se développer sans une véritable régulation, au risque de mettre en péril l'économie traditionnelle.

L'encadrement juridique des plateformes d'hébergement en ligne (2.1) et l'adaptation corrélative de la législation fiscale (2.2) se sont révélés indispensables afin de maintenir une concurrence loyale et transparente entre les opérateurs.

---

### 2.1. Vers un encadrement juridique des plateformes d'hébergement en ligne

---

L'essor rapide des plateformes d'hébergement numériques a fait surgir des interrogations juridiques nouvelles pour les entreprises qui les gèrent, les utilisateurs qu'elles mettent en relation et les acteurs traditionnels du secteur hôtelier.

---

**13.** *Tendances du tourisme et de l'hôtellerie – Réinventer l'hôtellerie*, Deloitte – In Extenso, 16 février 2018.

**14.** <https://www.accorhotels.group/fr-FR/hotel-development/accorhotels-choice/leading-digital-hospitality#nu-3>

**15.** *Ibid.*

Ainsi, une première série de lois a été promulguée afin d'encadrer l'activité des plateformes d'hébergement en ligne, de limiter le risque de concurrence déloyale et de tenter de réguler les dysfonctionnements du marché.

### 2.1.1. L'extension du régime d'autorisation préalable aux meublés de tourisme

En premier lieu, la loi ALUR du 24 mars 2014<sup>16</sup> a étendu le régime de changement d'usage des locaux d'habitation aux meublés de tourisme de manière générale en ajoutant un nouvel alinéa à l'article L. 631-7 du Code de la construction et de l'habitation : « *Le fait de louer un local meublé destiné à l'habitation de manière répétée pour de courtes durées à une clientèle de passage qui n'y élit pas domicile constitue un changement d'usage au sens du présent article.* »

Les meublés de tourisme sont des villas, appartements, ou studios meublés, à l'usage exclusif du locataire, offerts en location à une clientèle de passage qui y effectue un séjour caractérisé par une location à la journée, à la semaine ou au mois et qui n'y élit pas domicile. Est un local meublé au sens du II de l'article 324-1-1 du Code du tourisme tout meublé de tourisme ainsi défini<sup>17</sup>.

Désormais, toute location de locaux meublés d'habitation est soumise au régime d'autorisation préalable dès lors que (i) lesdits locaux sont situés dans une commune de plus de 200 000 habitants ou celles des départements des Hauts-de-Seine, de la Seine-Saint-Denis et du Val-de-Marne, et que (ii) les locations sont effectuées de façon répétée et pour de courtes durées à une clientèle de passage qui n'y élit pas domicile.

### 2.1.2. Les nouvelles obligations de déclaration préalable des meublés de tourisme

Par ailleurs, la loi pour une République numérique (dite « loi Lemaire »)<sup>18</sup> a renforcé les obligations déclaratives. L'article L. 324-1-1, alinéa 1<sup>er</sup>, du Code du tourisme imposait déjà une obligation de déclaration aux loueurs de locaux meublés en précisant que

« *toute personne qui offre à la location un meublé de tourisme, que celui-ci soit classé ou non au sens du présent code, doit en avoir préalablement fait la déclaration auprès du maire de la commune où est situé le meublé* ».

Le loueur n'est pas soumis à cette obligation si le local constitue sa résidence principale.

La loi Lemaire est venue ajouter une obligation de déclaration préalable soumise à enregistrement auprès de la commune, applicable aux résidences principales comme aux résidences secondaires, pour toute location de courte durée d'un local meublé de tourisme. Cette extension n'est cependant pas de droit et suppose au préalable une délibération du conseil municipal dans les communes où le changement d'usage des locaux destinés à l'habitation est soumis à autorisation préalable (communes de plus de 200 000 habitants ou celles des départements des Hauts-de-Seine, de la Seine-Saint-Denis et du Val-de-Marne et communes de plus de 50 000 habitants en zone tendue<sup>19</sup>).

La procédure d'enregistrement commence avec une demande auprès du maire de la commune où se trouve le local et la déclaration se fait au moyen d'un téléservice imposant un contenu obligatoire minimum. Le déclarant reçoit un accusé de réception avec un numéro de déclaration qui devra être indiqué dans le bail, lors de la mise en location et sur l'annonce en ligne<sup>20</sup>. L'enregistrement constitue un moyen de contrôle effectif des locations de courte durée et permet, en conséquence, la taxation par l'administration. Cependant, il sera impossible au loueur de mettre une annonce de location en ligne sur

.....  
16. Article 16 de la loi n° 2014-366 du 24 mars 2014 pour l'accès au logement et un urbanisme rénové (dite « loi ALUR »).

.....  
17. Article D. 324-1 du Code du tourisme.

.....  
18. V. *supra*.

.....  
19. *La location Airbnb ou la « disruption » rattrapée par la réglementation de la République numérique*, D. Richard, *AJDI* 2017, p. 336.

.....  
20. Article L. 324-2-1 du Code du tourisme.

une plateforme collaborative s'il ne présente pas son numéro d'enregistrement<sup>21</sup>.

### 2.1.3. Le changement de destination

Les changements de destination sont régulés par le Code de l'urbanisme. L'article R. 151-27 énonce cinq destinations possibles, dont l'habitation ainsi que le commerce et les activités de service, comprenant chacune des sous-destinations. Ainsi, la destination « Habitation » comprend les sous-destinations logement et hébergement et la destination « Commerces et activités de service » comprend, entre autres, la sous-destination hébergement hôtelier et touristique<sup>22</sup>.

Le changement d'une destination à une autre (mais non le changement de sous-destinations) est soumis à des déclarations préalables ou à des demandes de permis de construire le cas échéant.

### 2.1.4. L'encadrement légal de la durée des locations

La loi Lemaire a également introduit à l'article L. 324-2-1 du Code du tourisme l'interdiction de mettre en location un logement meublé pendant plus de 120 jours par an lorsque le logement constitue la résidence principale du loueur<sup>23</sup>. Au-delà de 120 jours, le loueur n'est plus considéré comme un particulier mettant en location sa résidence principale de façon occasionnelle mais comme un professionnel soumis au régime juridique et fiscal du loueur meublé professionnel. Le propriétaire qui n'observe pas cette limite voit en principe son annonce supprimée de la plateforme.

Dans certaines villes à l'étranger, le nombre de jours est encore plus restreint – à Amsterdam, Londres ou San Francisco, il est interdit de louer un logement meublé pour une durée excédant 90 jours<sup>24</sup>.

Le projet de loi portant évolution du logement, de l'aménagement et du numérique (dite « loi ELAN ») devrait entrer en vigueur avant la fin d'année 2018 et apporter sa pierre à l'édifice de l'encadrement des locations meublées touristiques.

### 2.1.5. La responsabilité renforcée des nouveaux acteurs du secteur du tourisme

Dans la mesure où cette nouvelle économie numérique emporte des conséquences économiques et juridiques non négligeables, le législateur a souhaité étendre la responsabilité des nouveaux acteurs du tourisme.

De nouvelles obligations figurent désormais dans le Code du tourisme<sup>25</sup> et imposent notamment aux plateformes d'hébergement d'informer le loueur sur les obligations de déclaration et d'autorisation préalable, de publier dans l'annonce du local le numéro de déclaration ou encore de veiller à ce que la location ne dépasse pas la durée de 120 jours précitée en ce qui concerne les résidences principales. Une obligation de loyauté<sup>26</sup> s'impose également aux nouveaux opérateurs, ces derniers ayant l'obligation de délivrer une information loyale, claire et transparente aux consommateurs. À défaut, leurs activités pourraient être considérées comme de véritables pratiques déloyales au sens des articles L. 121-2 et L. 121-6 du Code de la consommation.

## 2.2. L'adaptation de la législation fiscale

L'apparition des nouveaux concurrents numériques dans le secteur hôtelier et touristique a également mis en évidence de nouvelles

21. *Airbnb et plateformes collaboratives : quelles incidences sur le droit immobilier ?* Hebdo édition privée n° 710 du 7 septembre 2017, n° LXB N9927BWL.

22. Article R. 151-28 du Code de l'urbanisme.

23. La résidence principale est définie comme celle où l'occupant demeure au moins huit mois par an au sens de l'article 2 de la loi n° 89-462 du 6 juillet 1989 tendant à améliorer les rapports locatifs tel que modifié par la loi ALUR du 24 mars 2014.

24. *Le Monde*, 14 novembre 2017, *Locations saisonnières : que dit la loi ?* [http://www.lemonde.fr/les-decodeurs/article/2017/08/04/locations-saisonnières-que-dit-la-loi\\_5168615\\_4355770.html](http://www.lemonde.fr/les-decodeurs/article/2017/08/04/locations-saisonnières-que-dit-la-loi_5168615_4355770.html)

25. Article L. 324-2-1 du Code du tourisme tel que modifié par la loi Lemaire.

26. Articles L. 111-6 et L. 111-7 du Code de la consommation.

problématiques fiscales. Les acteurs traditionnels ont souligné le manque à gagner résultant du succès des activités de location en ligne non soumises aux mêmes contraintes fiscales.

Afin de rapprocher les obligations fiscales des non-professionnels de celles existant pour les professionnels, la loi de finance rectificative pour 2016 a créé une nouvelle obligation figurant à l'article 1649 quater A bis du Code général des impôts. Cette obligation, qui entrera en vigueur à compter du 1<sup>er</sup> janvier 2019, oblige les plateformes en ligne à déclarer automatiquement à l'administration fiscale les revenus engrangés par les particuliers. Plus précisément, la déclaration devra mentionner, outre le statut de particulier ou de professionnel caractérisant l'utilisateur sur la plateforme, le montant total des revenus bruts perçus par l'utilisateur au cours de l'année civile au titre de ses activités sur la plateforme en ligne, ou versés par l'intermédiaire de celle-ci<sup>27</sup>.

Cette déclaration permettra à l'administration d'alimenter automatiquement la déclaration préremplie des contribuables alors qu'il appartient aujourd'hui à ces derniers de reporter manuellement sur leur déclaration les revenus locatifs. L'automatisme de la transmission est ainsi de nature à éviter toute omission, intentionnelle ou non.

La pression fiscale a encore été accentuée par la loi de finance rectificative pour 2017 dont l'article 45 modifie l'article L. 2333-33 du Code général des collectivités territoriales en imposant, à compter de 2019, la collecte de la taxe de séjour. Cette mesure s'accompagne de l'instauration d'une taxe de séjour spécifique pour les logements ne faisant pas l'objet d'un classement, lesquels représentent l'immense majorité des biens proposés à la location par des particuliers *via* les plateformes collaboratives<sup>28</sup>.

Afin de réduire cet écart d'obligations fiscales qui se justifie de moins en moins, certaines municipalités (dont Paris dès 2015) ont mis en place une taxe de séjour pour les locaux touristiques loués par des particuliers. Face au succès de cette collecte, d'autres villes françaises ont progressivement mis en place cette taxe.

### 2.2.1. Les stratégies d'optimisation fiscale des entreprises numériques

Contrairement au modèle hôtelier classique, celui des plateformes de location en ligne permet à ces dernières, souvent localisées à l'étranger, d'exercer une activité significative en France tout en diminuant leur assiette taxable.

En effet, les géants des plateformes d'hébergement, qui offrent pour la plupart des biens et services par l'intermédiaire des technologies numériques, ne facturent pas directement leurs ventes dans l'Hexagone. Ils profitent ainsi des différents niveaux de fiscalité au sein de l'Union européenne afin de réduire l'impôt dont ils doivent s'acquitter. Les opérations européennes des géants du web sont en effet imposables uniquement dans le pays où est implantée la filiale du groupe.

À titre d'exemple, en 2016, le Trésor public français n'a perçu que 92 944 euros<sup>29</sup> d'impôts de la part de la plateforme Airbnb, ce qui constitue un montant dérisoire eu égard aux revenus engrangés par son activité sur le sol français.

En somme, l'effort de régulation des pouvoirs publics a pour conséquence une superposition de nouvelles règles juridiques et fiscales qui complexifie quelque peu l'encadrement légal et réglementaire de cette économie numérique porteuse de croissance pour le secteur de l'hôtellerie.

.....  
27. Article 1649 quater A bis du Code général des impôts modifié par la loi n° 2016-1918 du 29 décembre 2016 de finances rectificative pour 2016.  
.....

28. *La location entre particuliers à l'ère des plateformes numériques*, Alexandre Riéra, *AJ Contrat* 2018, p. 206. *L'Opinion* – <https://www.lopinion.fr/edition/economie/deputes-votent-taxe-airbnb-a-250-millions-d-euros-139553>  
.....

29. *Le Figaro* – [http://www.lefigaro.fr/flash-eco/2017/08/07/97002-20170807FILWWW00006-en-2016-airbnb-a-payee-92944-euros-d-impots-en-france.php?redirect\\_premium](http://www.lefigaro.fr/flash-eco/2017/08/07/97002-20170807FILWWW00006-en-2016-airbnb-a-payee-92944-euros-d-impots-en-france.php?redirect_premium)

SERVICES

---

THÈME 5

**Juridique  
&  
transformation numérique**

# Le point de vue...



**Nicolas Guérin, secrétaire général d'Orange  
et président du Cercle Montesquieu**

*« Le digital permet de réorienter les juristes vers des activités à plus forte valeur ajoutée. »*

## Comment le digital est-il concrètement utilisé au sein de la direction juridique ?

Chez Orange, un juriste a été chargé de regarder les 140 legaltechs existantes. Deux d'entre elles ont été choisies et nous les avons expérimentées sur des dossiers contentieux passés. Le traitement par l'une des legaltech a abouti dans 80 % des cas au même résultat, avec un gain en termes de temps, de coût et de simplicité. Nous avons également développé des outils en interne, notamment un chatbot, ainsi qu'un outil qui permet de générer des non-disclosure agreements (NDA), sur lesquels nos juristes passaient beaucoup de temps. Ils sont réorientés vers des activités à plus forte valeur ajoutée. L'objectif, à terme est d'industrialiser ces outils, afin d'améliorer la productivité. Pas question pour autant de supprimer des postes de juristes. Au contraire, ces avancées technologiques nécessiteront peut-être de créer une direction juridique des opérations.

## Avez-vous identifié des menaces liées à cette transformation digitale ?

La menace pour moi est double. D'abord, le risque de voir se développer, de manière totalement régulée et non contrôlée, les outils développés aux États-Unis et subventionnés par les GAFAM. En France et en Europe, les budgets pour développer ces outils sont sous-dimensionnés et il existe même une forme de résistance au digital. Le risque porte aussi sur l'externalisation des directions juridiques. Il est désormais possible d'exercer le droit n'importe où vers n'importe quel autre pays, avec des outils

américains. L'enjeu est donc celui de la compétitivité. Il faut que les juristes cessent de se retrancher derrière des monopoles ou des silos. Ils doivent proposer des solutions digitales efficaces et constituer des fonds pour subventionner l'offre européenne ou française de legaltechs. Il faut ancrer le droit et ses outils en France. La seconde menace est celle de la division des professions du droit. Il ne faut pas croire que le digital permettra aux directions juridiques de se passer des avocats ou, à l'inverse aux entreprises de se passer de direction juridique en recourant seulement à l'avocat. C'est une utopie. Il ne faut pas que le digital soit un outil de guerre au sein des professions du droit.

## Comment la direction accompagne-t-elle cette transformation digitale ?

Chez Orange, le fonctionnement est un peu particulier. Il existe un important comité de direction qui aide la direction juridique au quotidien sur des projets transverses. Des programmes ont été élaborés et des budgets dégagés.

Plus généralement, les entreprises françaises doivent financer les legaltech, conclure des partenariats avec elles, éventuellement les racheter. La BPI et les cabinets d'avocats doivent aussi financer le développement des legaltechs. Même si les entreprises ne les financent pas, ou ne les rachètent pas, elles doivent les utiliser, car c'est toujours valorisant pour une legaltech d'avoir pour client et pour partenaire une grande entreprise. Les partenariats aussi permettent aux legaltechs de lever des fonds.



Par **Isabelle Eid**

**L**es nouvelles technologies bouleversent bon nombre de secteurs d'activité, et l'industrie juridique n'échappe pas à ce phénomène. À l'ère de l'économie numérique, le monde du droit voit naître de nouvelles initiatives ayant vocation à servir une profession de plus en plus confrontée à l'innovation. C'est sous l'impulsion de ces dernières que naissent de nouveaux cadres, de nouveaux outils, de nouveaux axes de développement essentiels à l'avenir de la profession. Avec l'émergence des legaltechs, de nouveaux acteurs bousculent le marché du droit.

Selon la Charte éthique commune établie entre la legaltech et les professions du droit rédigée par l'Association pour le développement de l'informatique juridique (ADIJ) et Open Law, « est défini comme acteur de la legaltech toute organisation qui propose, fournit et/ou développe des technologies au service du droit ou de l'accès à la justice ». L'Observatoire permanent de la legaltech du Village de justice compte aujourd'hui au moins 164 acteurs de la legaltech en France, ces derniers étant majoritairement des start-ups (75 %).

L'une des idées de ces start-ups est de pronostiquer les décisions de justice grâce à des algorithmes brassant les jurisprudences et de les « quantifier ». Elles proposent aux professionnels du droit d'évaluer leurs chances de succès dans un litige, de trouver les arguments les plus pertinents, voire de prévoir le montant d'éventuelles indemnités. Parmi les grands changements annoncés dans les années à venir, la justice prédictive fait beaucoup parler. D'autres proposent des logiciels qui peuvent simplifier les recherches juridiques, le travail collaboratif ou la relecture des contrats. Les legaltechs proposent de plus en plus de services juridiques variés grâce aux nouveaux outils numériques tels que l'intelligence artificielle et la blockchain.

L'entrée en scène des nouvelles technologies dans le secteur de droit a perturbé (et perturbe encore) les spécialistes. Dans son rapport intitulé « L'avenir de la profession d'avocat » de février 2017, Me Kami Haeri indique que cette confrontation assez violente entre les praticiens et l'innovation était inévitable, puisque « la culture prédominante (des juristes) est celle de la censure, de l'autocensure, du scepticisme et de l'incrédulité. Dans un tel environnement, proposer une nouvelle page de site internet, voire une nouvelle manière de travailler avec ses clients suscite plus souvent la critique systématique que l'adhésion enthousiaste ». Cette tendance est par ailleurs fortement renforcée par la question de savoir si les métiers de droit survivront la révolution numérique.

En analysant les facteurs et produits de la transformation digitale (1), nous pourrions constater que les effets de ces derniers sont plutôt positifs, les legaltechs apportant une plus-value substantielle aux professions juridiques sans pour autant supprimer le besoin d'une intervention humaine (2). Le développement du numérique contribue par ailleurs à la création de nouvelles formes de travail et du management dans tous les secteurs, y compris celui de l'industrie juridique (3).

## 1. La transformation de l'environnement juridique

Les unes après les autres, les professions réglementées « s'uberisent ». L'impact sur la profession d'avocat se fait *via* les *legal start-ups*, ou des plateformes facilitant la création d'actes standardisés ou la mise en relation des avocats avec leurs clients. Mais l'innovation technologique, *via* les blockchains par exemple, s'apprête à bouleverser encore plus les métiers juridiques. Un nouveau genre de

prestations de services juridiques voit le jour grâce la révolution numérique (1.1). Cette transformation du monde juridique résulte de plusieurs facteurs sociaux (1.2).

### 1.1. Les nouvelles offres de prestations de services juridiques

L'environnement des professions juridiques se transforme, à l'image des legaltechs qui se développent avec de nouvelles offres de prestations de services juridiques à bas prix. C'est le cas notamment de services de génération automatique de documents juridiques : Captain contrat, Legal start... Plusieurs sites ont émergé et proposent des contrats clés en main pour un prix très compétitif. Lorsque l'on s'intéresse aux investissements, on constate que 16,5 % des legaltechs françaises ont levé des fonds en 2017 pour un montant total de 17,8 millions d'euros. La majorité de ces levées ont été effectuées auprès d'avocats, d'huissiers et d'autres professionnels du droit. On y voit ainsi un vrai intérêt dans ces nouvelles offres de la part des professionnels.

Dans le domaine des recherches juridiques en particulier, la start-ups Doctrine.fr qui avait levé 2 millions d'euros en 2016 a récemment annoncé une levée de 10 millions d'euros auprès d'Otium Venture et Xavier Niel, soit « *la plus grande levée de fonds d'une legaltech en Europe* »<sup>1</sup>. Nicolas Busmante, CEO de Doctrine.fr, nous a expliqué que l'apport de l'intelligence artificielle dans le domaine juridique était de simplifier la recherche juridique. Selon lui, « *l'avocat peut maintenant se concentrer sur son inventivité juridique et déléguer la recherche juridique à une intelligence artificielle* ».

D'ailleurs, le développement de la technologie blockchain révolutionne le domaine de droit, notamment dans des relations contractuelles. « *(La blockchain) permet le stockage, et la transmission, sans intermédiaire, d'informations transparentes, sécurisées et infalsifiables.* »<sup>2</sup> Sans intermédiaire, les frais de transaction sont réduits voire inexistantes et

l'exécution des obligations contractuelles ne peut pas être altérée. En effet, « *la confiance contractuelle est refondée. Elle est absolue, affranchie de tout système juridique, sans intermédiaire ni contentieux* »<sup>3</sup>.

### 1.2. Une transformation engendrée par différents phénomènes

Si cette transformation de l'environnement juridique peut paraître soudaine mais également extrêmement imprécise, elle pourrait pourtant trouver ses fondements à travers deux phénomènes assez bien connus du milieu juridique.

Premièrement, plusieurs études ont démontré que les citoyens avaient le sentiment de faire face à une justice lente, coûteuse, compliquée et incompréhensible. Si la majorité d'entre eux se disent prêts à faire appel à un avocat expérimenté, pour obtenir un œil d'expert sur un litige complexe, ils regrettent cependant d'avoir à déboursier le prix d'un avocat collaborateur junior pour des tâches administratives, qu'une personne moins qualifiée, telle qu'un assistant juridique, aurait pu accomplir. Pour la majorité de la population, l'accès au droit est extrêmement difficile et par conséquent, il n'est pas envisagé de faire valoir ses droits pour des problèmes pouvant survenir au quotidien.

Le second phénomène est évidemment celui de la robotisation de la société. Un grand nombre de tâches répétitives n'ont plus besoin d'une intervention humaine et il est aussi probable que certains robots ou logiciels auront un rôle de conseillers juridiques. C'est d'ailleurs déjà le cas aux États-Unis où des robots procurent des conseils pour contester des infractions de la route. En Europe, cette robotisation est

1. Legaltech : Doctrine lève 10 millions d'euros, *Le Monde du droit* (29 juin 2018). <https://www.lemondedudroit.fr/professions/337-legaltech/58623-legaltech-doctrine-leve-10-millions-euros.html>.

2. Les facteurs de transformation du droit, Guy Canivet. *Enjeux numériques*, n° 3, septembre 2018.

3. *Ibid.*

déjà bien présente puisqu'il existe déjà de nombreux logiciels et plateformes sur Internet qui fournissent, par exemple, des contrats standards préconçus. Stephen Hawking a un jour dit dans un entretien à la BBC en 2014 : « *Réussir à créer une intelligence artificielle serait un grand événement dans l'histoire de l'homme. Mais cela pourrait aussi être le dernier...* » L'essor de l'intelligence artificielle engendre de véritables bouleversements dans la société et particulièrement dans l'environnement juridique, à tel point que certains spécialistes parlent d'une quatrième révolution industrielle. Mais la question se pose de savoir quelle sera la place de la justice et des avocats suite à cette révolution...

## 2. Les impacts sur les professionnels du droit

Les nouvelles technologies de l'information et de la communication (NTIC) ouvrent le champ à la dématérialisation du juridique. Rapidité et souplesse des échanges, l'activité juridictionnelle ne peut que bénéficier d'une telle mutation (2.1). Cette transformation, de par son ampleur, a un impact substantiel sur la profession d'avocat et les directions juridiques (2.2) et cela d'une manière positive et enrichissante (2.3).

### 2.1. Une transformation qui affecte la justice et ses institutions

Lors du Forum parlementaire de la legaltech tenu le 18 juin 2018, Nicole Belloubet, la garde des Sceaux, a confirmé l'importance et l'inévitabilité de la transformation de la justice par le numérique<sup>4</sup>. Un rapport publié en novembre 2017 avait déjà préconisé qu'« *un certain nombre de litiges de la vie courante, simples, répétitifs et de faible montant* » puissent « *être jugés par des moyens électroniques : la formulation des demandes, la production des preuves et de mémoires pourraient être traitées et même, éventuellement, le jugement rendu et exécuté en ligne* »<sup>5</sup>. Par le biais de son projet de loi de programmation

2018-2022 et de réforme pour la justice, le ministère envisage la dématérialisation de la justice, afin de la rendre plus accessible pour les justiciables tout comme pour les professionnels. Par ailleurs, le développement et le renforcement de Portalis<sup>6</sup> font partie des projets visés par cette loi, avec un déploiement progressif jusqu'en 2021.

Les mécanismes de la « *justice prédictive* » s'inscrivent dans cette même perspective. En effet, certains outils permettent désormais de calculer ses chances de gagner son procès et de connaître le montant approximatif des indemnités à en attendre, voire même de trouver des arguments décisifs devant telle ou telle juridiction. Selon le professeur Bruno Dondero, la justice prédictive consiste à « *identifier quelle solution sera donnée à un litige X par un juge Y, soit au vu des données du litige X, soit par une analyse des écritures des parties* »<sup>7</sup>. Cette justice prédictive permettrait alors de véritables gains de temps et d'argent mais aussi et surtout une réelle transparence judiciaire. En effet, sans la subjectivité innée aux humains, les décisions rendues seront impartiales. De plus, l'entrée en scène des *big data* changera comment les juges travaillent. Contrairement aux humains, ces machines ont une mémoire infailible et sont capables d'enregistrer tous les détails de chaque affaire – on parle ainsi d'« *un nouveau savoir juridique* »<sup>8</sup>.

4. Forum parlementaire de la legaltech, Table ronde n° 3 : Éthique et régulation (18 juin 2018). [http://videos.senat.fr/video.702718\\_5b279a92a5b47](http://videos.senat.fr/video.702718_5b279a92a5b47). forum-parlementaire-de-la-legal-tech--apres-midi-?timecode=17789000.

5. Institut Montaigne, Justice : faites entrer le numérique, Rapport (novembre 2017).

6. Portalis : le ministère de la Justice présente le projet aux avocats, *LJA* (17 mars 2015). <https://www.lja.fr/portalis-le-ministere-de-la-justice-presente-le-projet-aux-avocats>.

7. B. Dondero, La justice prédictive, Le blog du professeur Bruno Dondero (10 février 2017). <https://brunodondero.com/2017/02/10/la-justice-predictive>.

8. A. Garapon, J. Lassègue, *Justice digitale*, Presses universitaires de France, 2018.

Toutefois, ces outils font débat dès lors qu'ils posent le risque de tomber dans un effet de performativité, c'est-à-dire la standardisation des décisions juridictionnelles avec l'utilisation à l'infini de la même motivation dans des cas similaires (justice « figée »). D'ailleurs, ce processus soulève évidemment plusieurs enjeux éthiques tels que la désymbolisation de l'activité juridictionnelle, à laquelle on substitue la certitude du chiffre, entraînant ainsi une crainte de déshumanisation et de « justice au rabais » doublée de la crainte de la manipulation des bases de données.

S'il est vrai que la transformation digitale de la justice entraîne certaines difficultés et suscite de nombreuses questions non encore réglées, les apports positifs d'une maîtrise du numérique dans ce domaine sont devenus incontestables. Ainsi, Bertrand Louvel, premier président de la Cour de cassation, avait déclaré : « *Cette meilleure visibilité et prévisibilité devrait également développer le recours par les avocats aux modes alternatifs de règlement des litiges. Les juridictions devraient ainsi être déchargées du poids du contentieux pour lesquels la voie judiciaire n'apparaîtra plus la mieux adaptée.* »<sup>9</sup> L'impact de cette transformation digitale s'effectuera non seulement sur les professionnels du droit mais également sur la justice tout entière avec un possible désengorgement des institutions judiciaires qui n'est certainement pas à déplorer.

## 2.2. Les réponses technologiques et organisationnelles des cabinets d'avocats et des directions juridiques des entreprises

De nombreux cabinets apportent des réponses à cette transformation en proposant de nouvelles organisations ainsi que des solutions technologiques innovantes. Certains ont ainsi pu créer un réseau pluridisciplinaire de juristes et techniciens informatiques afin d'apporter une réponse juridique et numérique à leurs clients. D'autres ont adopté des innovations technologiques ou d'intelligence artificielle afin de proposer des solutions innovantes.

C'est l'exemple de Kira, un outil qui permet aux équipes mises en place sur un audit d'analyser une quantité importante de contrats et de clauses en un temps considérablement réduit, en même temps qu'il facilite, par une interface dédiée, une organisation d'équipes avec notamment plusieurs niveaux de contrôle, de relecture et de réalisation des travaux d'analyse<sup>10</sup>.

Les cabinets repensent également leur organisation et innovent en adoptant les avocats « à la demande » (ou *flexible lawyering*)<sup>11</sup>, principe permettant d'apporter des réponses aux défis suivants : faire face au surcroît d'activité dans le cabinet, répondre aux requêtes variées des clients, et enfin maintenir les avocats et talents dans le réseau du cabinet<sup>12</sup>. Plus largement, les cabinets internationaux repensent globalement l'offre de service juridique, à laquelle est appliquée une véritable organisation en mode « gestion de projet » (*legal project management*). Est ainsi sollicitée en amont la palette des services internes de la firme (facturation, finance, marketing, ou autres services à valeur ajoutée, tel le knowledge management) aux côtés des avocats souvent répartis sur plusieurs juridictions afin d'identifier, de façon globale et intégrée, les besoins exprimés par les clients, et d'évaluer en détail le processus

9. Discours de Bertrand Louvel lors du colloque « La jurisprudence dans le mouvement de l'open data, 14 octobre 2016.

10. DLA Piper partners with Kira Systems to leverage artificial intelligence tool for M&A due diligence, DLA Piper Newsroom (14 juin 2016). <https://www.dlapiper.com/en/us/news/2016/06/dla-piper-partners-with-kira-systems>.

11. Flexible Lawyers, DLA Piper Publications (25 avril 2016). <https://www.dlapiper.com/en/uk/insights/publications/2016/04/flexible-lawyers>.

12. Lawyers on Demand data highlights surging flexible legal resourcing market, The Lawyer (12 février 2015). <https://www.thelawyer.com/issues/online-february-2015/lawyers-on-demand-data-highlights-surging-flexible-legal-resourcing-market>.

13. Steven B. Levy, *Legal Project Management: Control Costs, Meet Schedules, Manage Risks, and Maintain Sanity*, DayPack Books (2009).

de réalisation des prestations juridiques, ainsi que leurs conditions<sup>13</sup>.

De même, une étude récente menée auprès des directions juridiques de 99 entreprises de tailles différentes a démontré que ces dernières considèrent que l'exploitation des outils du numérique est un enjeu majeur<sup>14</sup>. Les priorités des directions juridiques sur l'usage du digital restent comparables à celles des cabinets d'avocats, c'est-à-dire la dématérialisation de la documentation, les processus et le reporting (22 %) ainsi que la facilitation du travail en équipe (29 %). Malgré cette prise de conscience des enjeux numériques, 50 % des directions juridiques jugent que leur maturité digitale est encore faible. Cela dit, ce serait inexact de dire que les directions juridiques ne prennent pas d'initiatives pour favoriser le numérique.

Au contraire, à la faveur de nouvelles fonctions internes alliant technicité juridique et nouveaux outils, telles que le knowledge management, la révolution digitale s'intègre de plus en plus dans les directions juridiques. Les tâches juridiques telles que la création de contrats, les données sur les résolutions des litiges, les suivis des contentieux sont désormais informatisées, et deviennent ainsi accessibles plus rapidement, ce qui permet aux juristes de se concentrer sur les missions à haute valeur ajoutée<sup>15</sup>. L'avenir des professions juridiques passera forcément par de nouveaux outils et une transformation du mode de travail et des offres de services, ce dont la nouvelle génération de juristes et d'avocats a bien conscience, et nécessite que ces derniers ajoutent ainsi à leurs connaissances juridiques celles sur l'approche stratégique de leurs organisations, ainsi que sur les grands enjeux du monde du droit, afin d'appréhender les défis juridiques des grandes mutations contemporaines et à venir.

### 2.3. La transformation digitale au secours de la justice ?

À travers l'adoption des nouveaux outils par une variété de professionnels de droit, il est

évident que la transformation digitale ne constitue pas nécessairement une menace. On pourrait même aller jusqu'à dire que cette transformation pourrait être une bouée au secours de la justice, une aide précieuse tant pour les professionnels du droit que pour les justiciables. La transformation de l'environnement juridique et notamment l'essor des legaltechs permettent de tirer quelques enseignements pour les professions juridiques. En effet, tous les professionnels s'accordent à dire qu'on assiste à une judiciarisation de la société, et qu'on observe des juridictions en surchauffe, des délais de justice qui s'allongent et des magistrats qui n'arrivent plus à faire face au flux croissant de contentieux. Pour l'avocat, il s'agira de mieux conseiller et orienter son client, en privilégiant les modes alternatifs de règlement des litiges plutôt que la procédure ordinaire. De même au niveau stratégique, de meilleurs arguments pourront être soulevés par l'avocat et de meilleures stratégies juridiques pourront être adoptées par les entreprises. Tout changement de notre société induit un choc évolutif et il est fort à craindre que l'avocat remplacé sera celui qui n'aura pas su ou pu s'adapter et adopter de nouveaux outils.

Une analyse de F. Levy et D. Remus, respectivement du Massachusetts Institute of Technology et de l'University of North Carolina School of Law, a montré que pas plus de 13 % de l'emploi juridique ne pouvait être automatisé<sup>16</sup>.

14. Digitalisation de la fonction juridique : quelles priorités en 2018 ? PwC Société d'Avocats (31 mai 2018). <https://www.pwcavocats.com/fr/assets/files/pdf/2018/05/pwc-etude-digitalisation-fonction-juridique.pdf>.

15. Orange convertit ses juristes au digital, *Les Echos Executives* (2 mai 2016). <https://business.lesechos.fr/directions-juridiques/droit-des-affaires/contrats-et-clauses/021874947620-orange-convertit-ses-juristes-au-digital-210074.php>.

16. D. Remus, F. Levy, Can Robots Be Lawyers? Computers, Lawyers and the Practice of Law (11 décembre 2016). Accessible en anglais à l'adresse [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2701092](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2701092).

D'ailleurs, de nombreux spécialistes comme James E. Katz confirment que la collaboration entre les machines et les humains permettra à ces derniers d'avancer plus rapidement. En effet, les humains qui maîtrisent les outils numériques seront dans une position beaucoup plus avantageuse que ceux qui refusent les atouts du numérique ou les machines toutes seules. En outre, plusieurs aspects essentiels du rôle d'avocat ne pourront jamais être remplacés. Premièrement, l'intelligence artificielle ne fera usage que d'argumentations qui ont déjà été créées, elle ne pourra donc pas innover. Naîtrait alors un risque de cristallisation de la justice. Seul l'être humain pourra apporter de la créativité, si utile à l'évolution de la société. Pour finir, l'intelligence artificielle ne pourra jamais apporter le contact humain ni cette capacité de ressentir les émotions de son client. Un robot n'arrivera jamais à se mettre à la place d'autrui.

Pour toutes ces raisons, on peut raisonnablement affirmer que, malgré la transformation radicale de l'environnement juridique, les professions juridiques et notamment celles de l'avocat auront encore un grand rôle à jouer dans les années à venir.

Nous pouvons affirmer, avec Richard Susskind, que « *dans le futur, le travail (dans le domaine juridique) subsistera. La prochaine décennie sera caractérisée par une réorganisation du travail et non une disparition de ce dernier. Actuellement, cette réorganisation n'est pas urgente mais durant les cinq prochaines années, nous devrions nous préparer pour ce changement. De plus en plus de services légaux nous seront disponibles à l'appui des nouvelles technologies* »<sup>17</sup>.

### 3. Impacts sur le management dans les organisations : la collaboration des ressources humaines ou la « disruption » du management<sup>18</sup>

L'économie numérique promeut le développement du management collectif, ou « participatif ». Il est construit autour de trois piliers :

donner un sens à la mission du collaborateur, lui octroyer plus de liberté et d'autonomie dans la confiance de l'entreprise (« *empowerment* ») (3.1), et enfin la mise en place par cette dernière d'une politique permettant le développement personnel du collaborateur (3.2). Cette transformation de modèle impactera sans doute les équipes de juristes, qu'elles soient en directions juridiques ou en cabinets d'avocats.

#### 3.1. L'empowerment

L'objectif est d'atteindre une « intelligence collective » en passant par une participation aux décisions et une délégation de pouvoir. La hiérarchie n'est donc plus tout à fait pyramidale, tout du moins elle n'est plus ressentie comme telle, et devient plutôt « horizontale », ou *flat* (plate).

Le salarié ou collaborateur, responsable de sa mission en toute autonomie, est impliqué au maximum dans le processus de construction du projet sur lequel il travaille. C'est sur ce modèle de management 2.0 qu'a parié notamment l'entreprise Criteo. Pour mettre en pratique le management par tous, cette ancienne start-ups salarie tous ses collaborateurs au niveau cadres, qui rime avec autonomie, et leur offre des actions gratuites à chaque nouveau salarié qui rejoint l'équipe (c'est le « *power-up* »).

La mobilité interne notamment est l'un des outils du management participatif : un salarié qui est sous la responsabilité d'un chef de

<sup>17</sup> R. Susskind, You have five years to reinvent the legal profession, The Law Society Gazette (27 avril 2016). <https://www.lawgazette.co.uk/law/susskind-you-have-five-years-to-reinvent-the-legal-profession/5054990>. article. Traduit de l'anglais : « *It is not that there are no jobs in the future, but the 2020s will be a decade of redeployment, not unemployment. It is not an emergency but over the next five years we have to prepare. More and more legal services will be enabled by the support of new technology.* »

<sup>18</sup> Cette partie reprend des passages du thème « Économie collaborative » introduit dans le *Guide du numérique* 1.

projet aujourd'hui pourra avoir la tête d'un nouveau projet demain et supervisera dans ce cadre son ancien responsable. L'engouement pour les nouvelles technologies a un impact au niveau de la communication interne des entreprises. Parmi les pionniers, Google propose à ses salariés de s'auto-évaluer pour définir qui obtiendra une prime, ou encore récompense toute initiative visant à améliorer la vie au sein de l'entreprise.

C'est « l'esprit start-ups », une agilité et un rapport direct au management : celui-ci étant accessible, n'importe quel salarié peut alors discuter avec le CEO et lui apporter des idées nouvelles. Cela engendre plus de fluidité dans la circulation de l'information qui n'est pas juste détenue par une petite poignée de « sachants » en haut de la pyramide.

La suppression de la hiérarchie pyramidale fait redescendre la responsabilité du management sur chaque collaborateur individuellement, chaque salarié est autonome, s'investit personnellement dans sa mission comme s'il en était seul responsable. Il y gagne alors de voir ses actions impacter directement l'activité de la société qui lui fait confiance *a priori* ; en contrepartie, cette autonomisation peut aussi confiner à l'isolement et génère une dose de stress et d'implication importante puisque le salarié est seul décideur. D'aucuns disent que les salariés, tous au même niveau, entrent donc inconsciemment en compétition, et tendent vers l'individualisme. L'effacement de la barrière entre la vie privée et la vie professionnelle induit une culture du travail sans limite : puisqu'il fait si bon vivre au travail, pourquoi rentrer chez soi ? En réalité, si le contrôle n'est plus imposé par la hiérarchie, il a été transféré, avec le management et la responsabilité, aux salariés eux-mêmes. On est dans l'autocontrôle. Ce n'est plus le supérieur qui va s'étonner de l'absence de tel collègue mais ses pairs, qui évaluent son investissement à la lumière du leur.

Le principe est le même pour le secteur juridique. Face à la mutation technologique et organisationnelle, les cabinets d'avocats et les directions juridiques doivent s'adapter. Ces

derniers, d'habitude plutôt individualistes, sont amenés aujourd'hui à travailler de plus en plus ensemble, *via* des plateformes collaboratives. Selon le rapport « *La nécessaire transformation des cabinets d'avocats* »<sup>19</sup> publié par Wolters Kluwers et LJA en collaboration avec des cabinets de droit et de conseil, cette transformation s'appuie forcément sur la confiance (en soi et envers les autres) et la bienveillance. Ces deux éléments contribuent à rapprocher tous les professionnels au sein d'une équipe, toute hiérarchie confondue : les associés, les collaborateurs, les juristes et les salariés.

---

### 3.2. Le développement personnel de la génération Y

---

Enfin, le management participatif met l'accent sur le développement personnel, *via* notamment l'environnement de travail du collaborateur. Celui-ci doit être agréable, car un collaborateur qui se sent bien au travail est plus productif.

De grandes entreprises s'inscrivent dans cette mouvance « *best place to work* », en créant des espaces de travail agréables et des open spaces lumineux, en multipliant les espaces de détente. En améliorant la qualité de vie au bureau, on favorise l'envie de venir travailler et on accroît la productivité.

Dans ce cadre, on observe une convergence des comportements professionnels et personnels. Alors que le droit du travail aujourd'hui tente de toujours plus renforcer la scission entre ces deux aspects qu'il considère comme antagonistes, l'économie collaborative les interconnecte et utilise le fruit de ce mélange pour créer de la richesse.

Les entreprises nouvelles sont dirigées par des jeunes qui jouent au baby-foot entre deux réunions et viennent au travail en jean. Les dirigeants ont le même âge que leurs collaborateurs, et se montrent tels qu'ils sont avec leurs

---

19. La nécessaire transformation des cabinets d'avocats, Wolters Kluwer, LJA (2014). <https://www.wkf.fr/media/pdf/La-necessaire-transformation-des-cabinets-d-avocats.pdf>.

qualités et leurs défauts (Mark Zuckerberg pour Facebook, Sean Parker pour Napster, etc.). Ils personnalisent ainsi la fonction hiérarchique, rendant la direction plus accessible en s'éloignant du modèle traditionnel du CEO invisible et tout-puissant.

De même, les collaborateurs sont incités à être davantage proactifs pour promouvoir leur entreprise à l'extérieur *via* les réseaux sociaux (LinkedIn, Twitter, Instagram).

Comme les entreprises, les cabinets d'avocats et les directions juridiques mettent en place de nouvelles techniques de management. Les locaux sont aménagés différemment aujourd'hui, pour comprendre des bureaux open space facilitant le travail collaboratif, des espaces collectifs pour déjeuner, une bibliothèque au centre du cabinet, une salle de sport, etc. Le bien-être des avocats et des juristes est pris en compte pour booster la productivité, l'innovation et la communication.

Ce nouveau management, induit par les nouvelles technologies, semble en tout cas correspondre aux attentes de la génération Y.

SERVICES

---

THÈME 6

# Santé & transformation numérique



# Le point de vue...



**Jean-François Gendron,  
Président, French Healthcare**

## Comment le numérique a-t-il révolutionné le secteur de la santé ?

L'impact du numérique est visible dans tous les domaines de la santé : la prévention et le suivi avec les objets et dispositifs médicaux connectés qui permettent la surveillance des patients ou des personnes âgées à domicile ; la télémédecine bien sûr, avec une prise en charge par l'Assurance maladie de la téléconsultation et de la téléexpertise depuis le 15 septembre 2018 ; la chirurgie robotique, avec notamment le robot Da Vinci qui équipe de plus en plus d'établissements en France ; le traitement des données médicales par des supercalculateurs, tels IBM Watson qui diagnostique des cancers... Les services rendus aux patients et les pratiques des professionnels évoluent rapidement avec les avancées du numérique. La filière française du numérique en santé représenterait aujourd'hui 30 000 emplois et 3 milliards d'euros de chiffre d'affaires. Logiquement, les perspectives à l'international pour les entreprises et établissements français évoluent également. Le numérique est d'ailleurs transversal aux groupes de travail actuels de French Healthcare (Hôpital, Maladies chroniques, Cancer, Technologies médicales, Accueil de la patientèle internationale).

## Le cadre réglementaire est-il un frein à cette révolution numérique ? Ou est-il davantage un gardien d'une révolution pérenne et plus réfléchie ?

Pour être pérenne, la « révolution numérique » se doit d'être réfléchie et encadrée. Si on lie l'usage des technologies numériques à des objectifs

d'amélioration de la santé, il est par exemple essentiel de se pencher sur la fracture numérique, à l'échelle du monde mais aussi de notre pays. Tous les Français n'ont pas accès à internet, et parmi les internautes tous n'ont pas accès au haut débit, ce qui les prive de facto de télémédecine. Si on souhaite que les patients s'approprient ces nouveaux outils, se prennent davantage en charge et participent à la télésurveillance de leurs maladies chroniques, il faut leur assurer que leurs données médicales sont en sécurité et correctement utilisées. Tout cela fait partie d'un contrat social – peut-être pas suffisamment explicite - autour du développement du numérique.

## Quel sera le visage de la santé de demain ?

Les perspectives sont importantes en matière de décryptage du génome et de réparation des gènes, de prévention et de diagnostic avec l'intelligence artificielle, d'impression d'organes en 3D et de médecine régénératrice, de progrès de la robotique, d'interventions plus nombreuses en ambulatoire... Ces évolutions apporteront bien sûr leur lot de questionnements éthiques, autour de l'allongement de la durée de vie, du déferlement de connaissances en dehors du cabinet médical et sans la supervision d'un médecin, du sentiment de « toute-puissance » qui pourrait naître et de ses dérives... Des sujets passionnants !



Par **Sonia de Kondserovsky & Jonathan Rofé**

**A** l'heure du numérique, il n'est pas un secteur qui soit épargné par la transformation digitale. À l'instar du secteur hôtelier où de nouveaux intermédiaires ont révolutionné les usages et ébranlé les acteurs historiques, l'écosystème du secteur de la santé évolue considérablement avec le développement de nouveaux outils numériques et l'arrivée de nouveaux acteurs.

Les nouvelles technologies ont en effet permis des évolutions considérables dans le domaine de la santé. Les outils matériels et logiciels deviennent de plus en plus précis, permettant, par exemple, au chirurgien de recourir à la robotique pour les opérations les plus délicates, ou encore à l'oncologue de diagnostiquer un cancer dans des délais toujours plus réduits en exploitant les logiciels dotés d'intelligence artificielle (IA).

D'un autre côté, les relations traditionnelles entre le patient et le médecin, et entre les praticiens eux-mêmes, sont en pleine mutation. Les patients prennent leurs rendez-vous médicaux sur Internet, télé-consultent leur médecin, sollicitent des « *chatbots* », des robots dotés d'intelligence artificielle et capables de répondre à certaines questions ou de fournir un suivi de dossier (grossesse, rendez-vous, etc.). En parallèle, la télé-expertise<sup>1</sup> permet à différents spécialistes impliqués sur un même dossier de collaborer beaucoup plus facilement et de manière plus efficace.

Le rapport Villani soulignait récemment que « *de nombreux résultats permettent d'illustrer en quoi l'intelligence artificielle pourra être à l'origine de bénéfices importants pour la recherche, la pratique médicale, le système de santé national, les personnes malades et l'ensemble des citoyens* »<sup>2</sup>. Pour ces raisons, l'intervention des nouvelles technologies est perçue favorablement par 76 % des Français<sup>3</sup>. Mais si les nouvelles technologies sont capables

de révolutionner le domaine de la santé, cette transition soulève de nouvelles problématiques. De prime abord, la protection des données personnelles, et de manière encore plus flagrante depuis l'entrée en vigueur du RGPD, concentre encore une grande partie de l'attention. Le stockage et les traitements induits par tout logiciel doté de l'IA peuvent avoir des effets négatifs dès lors que les données accumulées ne bénéficient pas d'une protection maximale. Selon Elizabeth Denham, la commissaire à l'information du Royaume-Uni, the « *price of innovation does not need to be the erosion of fundamental privacy rights* ». Au-delà des problématiques juridiques, il convient de s'interroger sur d'autres questions d'ordre éthique, déontologique et sociétal. Dans un domaine aussi sensible que celui de la santé, la transparence, la traçabilité et la fiabilité des résultats de l'IA sont critiquées. En outre, de nombreux acteurs s'inquiètent de l'avenir de leur profession. *In fine*, la question de savoir comment les professionnels de santé peuvent (et doivent) garder la main face aux outils intelligents se pose.

Nous verrons que le domaine de la santé n'est pas en manque d'innovation. Au contraire, de

1. La télé-expertise permet « à un professionnel médical de solliciter à distance l'avis d'un ou de plusieurs professionnels médicaux par l'intermédiaire des technologies de l'information et de la communication ». La télémédecine, ministère des Solidarités et de la Santé, 14 septembre 2018. Accessible à <https://solidarites-sante.gouv.fr/soins-et-maladies/prises-en-charge-specialisees/telemedecine/article/la-telemedecine>.

2. Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne, C. Villani, Mission parlementaire du 8 septembre 2017 au 8 mars 2018.

3. Prévention santé : les Français favorables aux nouvelles technologies, 6 mars 2018, L'Argus de l'Assurance.

plus en plus d'entreprises (petites et grandes) proposent des services pouvant améliorer l'accès aux soins ou la qualité des soins (1). Ces initiatives sont néanmoins susceptibles d'engendrer des risques importants en l'absence de mécanismes d'encadrement réfléchis (2).

## 1. La numérisation de la santé : un marché en ébullition

La numérisation de la santé a ouvert de nombreuses brèches dans le domaine médical, dans lequel fourmillent des acteurs intermédiaires proposant des services aux médecins et aux patients afin de faciliter l'accès aux soins (1) ou d'améliorer la qualité des traitements (2).

### 1.1. L'influence des nouvelles technologies sur l'accès aux soins

La prise de rendez-vous sur Internet est l'un des services qui s'est le plus développés ces dernières années grâce à plusieurs acteurs. Doctolib, par exemple, qui a levé 85 millions d'euros depuis sa création en 2013<sup>4</sup>, revendique 70 000 médecins utilisateurs de ses services et 200 millions de rendez-vous pris à partir de sa plateforme. Les raisons d'un tel succès ne sont pas difficiles à comprendre. Du côté du patient, la prise de rendez-vous n'a jamais été aussi simple : le contact par Internet est plus rapide que par téléphone (et sans intermédiaire) et permet de voir clairement les offres de soin proposées par le professionnel ainsi que les différents créneaux disponibles. Du côté du médecin, l'outil permet de réduire les frais de secrétariat mais aussi d'optimiser le taux de remplissage du cabinet, notamment en gérant les annulations. Les résultats concrets d'un tel service sont prometteurs. Depuis 2017, Doctolib a été déployé dans 30 hôpitaux de l'Assistance publique-hôpitaux de Paris (AP-HP) dans l'objectif de réduire les délais d'attente et de fidéliser les patients<sup>5</sup>. Au bout d'un mois de déploiement, le nombre de consultations non honorées a baissé significativement (de 15 %-25 % à 8 %) et l'activité a augmenté (hausse de 7,5 % du nombre de rendez-vous).

Au-delà des simples prises de rendez-vous, les nouvelles technologies en général, et Internet en particulier, permettent aux individus de trouver des réponses à leurs questions – et des solutions à leurs symptômes – de manière de plus en plus autonome.

De la simple recherche sur les sites spécialisés – avec néanmoins les risques d'auto-diagnostic voire d'auto-médication que cela pose – à la consultation téléphonique, en passant par la visioconférence avec le médecin professionnel et jusqu'à la télé-médecine, il n'est plus toujours indispensable pour les patients de se déplacer pour avoir un avis médical personnalisé. Cela constitue également une réponse à des difficultés auxquelles certaines populations sont confrontées. En particulier, la multiplication des déserts médicaux encourage au développement de solutions alternatives aux prestations médicales traditionnelles. De plus en plus de plateformes technologiques lancent des services de téléconsultation, certaines revendiquant aujourd'hui plus de 10 000 téléconsultations<sup>6</sup>.

### 1.2. Une meilleure qualité de soins ?

Les outils technologiques sont devenus indispensables pour assister les médecins dans la recherche des diagnostics en réduisant les délais et en améliorant la précision et la fiabilité des résultats. La qualité des soins augmente ainsi avec l'assistance des outils intelligents, capables de détecter automatiquement des dysfonctionnements ou anomalies. Therapixel, start-up française qui développe un logiciel permettant de diagnostiquer un cancer à partir de son système d'intelligence artificielle, en est l'un des nombreux exemples. Une étude « *à paraître, montrera[it] que, pour*

4. La révolution de la télémédecine : la santé au bout du clic, 8 janvier 2019, Les Echos.

5. Le passage à Doctolib profite aux hôpitaux de Paris, 8 janvier 2019, Le Figaro.

6. La révolution de la télémédecine : la santé au bout du clic, 8 janvier 2019, Les Echos.

*30 % d'un groupe de femmes atteintes du cancer du sein, l'IA a été capable de détecter la tumeur sur des images prises un an avant qu'elle ne soit diagnostiquée* »<sup>7</sup>.

À l'instar des appareils « smart » pour la maison comme Echo (d'Amazon) ou encore HomeKit (d'Apple), les objets connectés sont très présents dans le domaine de la santé. Les nouvelles montres connectées proposent par exemple un suivi très précis des utilisateurs afin de leur permettre de mener une vie « saine ».

Les montres peuvent ainsi surveiller le niveau de stress, les calories dépensées, le rythme cardiaque de l'utilisateur, ses rythmes de sommeil et un grand nombre d'autres données qui, combinées, permettent d'établir une cartographie « santé » très précise. Certaines montres vont jusqu'à alerter l'utilisateur lorsqu'elles détectent une anomalie voire même appeler les urgences dans certaines hypothèses (par exemple : détection de chute). Les investissements majeurs des géants du web dans le domaine de la santé sont à la mesure des enjeux économiques et sociétaux soulevés. Et certains considèrent que « *c'est un marché insensible aux aléas politiques et à la conjoncture économique, c'est un marché inefficace où leurs moyens technologiques et financiers sont un atout et, enfin, c'est vertueux (...)* »<sup>8</sup>.

## 2. Focus sur les enjeux de la digitalisation de la santé

Il existe un besoin infini quant aux outils pouvant améliorer le fonctionnement du système de santé. Mais la numérisation doit être abordée avec prudence. La numérisation de la santé implique de nouveaux enjeux à la fois sur les plans éthique et juridique (2.1) et sur le futur des relations entre les professionnels de santé et leurs patients (2.2).

### 2.1. Les enjeux éthiques et juridiques

Les acteurs de la santé sont aujourd'hui confrontés aux mêmes interrogations que les acteurs des autres secteurs : comment profiter des formidables opportunités qu'offrent les

technologies sans risquer l'ubérisation ? Ce terme récemment introduit dans le dictionnaire sous la définition de « *transformation d'un secteur avec un modèle économique innovant tirant parti du numérique* » inquiète de plus en plus les professionnels de santé. Le Conseil national de l'ordre des médecins (CNOM) a ainsi fait part de son inquiétude quant à l'ubérisation de la santé en observant « *une tendance accélérée vers "l'ubérisation de la santé", par des offres en ligne qui correspondent à du commerce électronique non régulé et qui tendent à réduire la pratique médicale à une simple prestation électronique moyennant rétribution, via des plateformes du secteur marchand* »<sup>9</sup>. En effet, la transformation digitale, dans certains de ses aspects et bien que répondant à des besoins du corps médical et des patients, peut poser un problème éthique. Rappelons en effet que selon l'article 19 du Code de déontologie médicale, « *la médecine ne doit pas être pratiquée comme un commerce* ». Que dire des plateformes dont la finalité médicale n'est que secondaire par rapport aux autres finalités – affichées ou non – poursuivies ? Certaines plateformes de téléconsultation ont ainsi d'ores et déjà perçu la manne formidable que constituent les milliards de données (médicales) collectées, et dont la valeur va (et de manière grandissante) bien au-delà des frais perçus pour les consultations. En particulier, le développement de la médecine prédictive, marché sur lequel les acteurs majeurs investissent des sommes considérables, ne peut se faire qu'au travers de l'analyse des mégabases de données ainsi constituées.

Outre la marchandisation de la santé, les nouvelles technologies, et surtout l'intelligence artificielle, soulèvent la problématique de la transparence. Dans un domaine aussi sensible

7. Trois start-ups de l'intelligence artificielle appliquée à la santé à suivre, 5 octobre 2018, Les Echos.

8. Jean-David Zeitoun, « En médecine, le besoin est quasiment illimité », 5 octobre 2018, Les Echos.

9. Télémédecine et autres prestations médicales électroniques, février 2016, avis public du Conseil national de l'ordre des médecins.

que celui de la santé, il demeure absolument nécessaire que les médecins comprennent pourquoi un patient est malade et de quoi ce dernier souffre. Si l'intelligence artificielle – ou le robot – est capable de déceler les anomalies chez les patients avec des taux de précision impressionnants, son raisonnement doit être clair pour permettre aux médecins de vérifier l'exactitude des résultats et traiter le patient par la suite. Le processus décisionnel doit donc être transparent mais cette transparence peut se heurter à la confidentialité (voire au secret des affaires) attachée aux méthodes, algorithmes et autres éléments ayant permis d'aboutir à la décision, avec le risque de porter atteinte à l'avantage compétitif – et donc à la valeur – de ceux qui l'ont développé. Il est donc nécessaire de trouver un équilibre entre un encadrement juridique strict et les bénéfices sanitaires de ces outils.

En toute hypothèse, le législateur doit équilibrer innovation et précaution, l'objectif n'étant pas de freiner l'évolution des nouvelles technologies mais de proposer un cadre sécurisé afin d'éviter les risques d'abus. Il est également important de veiller à une approche coordonnée des pays européens. L'exemple de l'e-commerce des médicaments est assez significatif. Très réglementé en France, il l'est beaucoup moins dans d'autres pays européens comme le Royaume-Uni, où la vente « (est ouverte) à tous les médicaments et autoris[é] [aux] pure players (les vendeurs qui opèrent seulement sur Internet) »<sup>10</sup>. A contrario, la mise en œuvre du RGPD a montré qu'une approche cohérente au niveau européen pouvait apporter des résultats positifs.

En ce sens, le projet de loi relatif à l'organisation et à la transformation du système de santé<sup>11</sup>, déposé à l'Assemblée nationale le 13 février 2019, prévoit la création d'un espace numérique de santé où les utilisateurs peuvent stocker leurs dossiers médicaux tout en leur laissant la possibilité de paramétrer les données affichées. L'espace numérique permettra à l'utilisateur de « gérer ses données de santé et de participer à la construction de son parcours de santé en lien avec les professionnels, les établissements et les autres acteurs de santé »<sup>12</sup> et devrait être compatible avec les

différentes applications et objets connectés des utilisateurs. Tout cela, sans pour autant sacrifier le respect de sa vie privée puisqu'il peut choisir quelles informations sont disponibles, qui pourra accéder à ses records médicaux et pendant quelle période de temps cet accès sera possible. Le projet de loi prévoit également l'élargissement du champ du Système national des données de santé (SNDS), pour comprendre « l'ensemble des données cliniques obtenues dans le cadre de soins remboursés par l'Assurance maladie »<sup>13</sup> afin d'améliorer la recherche médicale et la qualité du suivi. Toutefois, dans le souci de protéger davantage les informations privées, le projet de loi milite pour la pseudonymisation complète des données.

## 2.2. La relation médecin-patient

Les nouvelles technologies soulèvent de nombreuses craintes, tous secteurs économiques confondus, quant à la profonde mutation des professions et des relations qu'elles induisent. Certains métiers vont se transformer – ainsi les secrétaires médicales voient progressivement la prise de rendez-vous disparaître de leurs attributions. Des tâches simples vont pouvoir être automatisées – un logiciel IA bien alimenté trouvera des solutions plus rapidement et avec la même (voire plus de) précision qu'un humain. Les dispositifs médicaux connectés vont progressivement impliquer une évolution de la relation patient-médecin dans la mesure où le lien est à la fois plus direct (le médecin peut avoir accès aux données de son patient en « temps réel ») et plus distendu (sentiment de médecine « virtuelle »).

10. O. Debarge, Le commerce électronique des médicaments : une mutation inachevée, 24 janvier 2019, Petites affiches, n° 18.

11. Projet de loi relatif à l'organisation et à la transformation du système de santé, Accessible à <http://www.assemblee-nationale.fr/15/pdf/projets/pl1681.pdf>.

12. Ibid, art. 12.

13. Ibid.

Ces enjeux sont pertinents dans le domaine médical et la question de savoir comment (ou si) les médecins et les autres professionnels continueront de pratiquer leur métier se pose. Le rapport Villani et la plupart des auteurs analysant ce sujet militent pour une relation de « complémentarité » entre machine et homme.

Dans un premier temps, « *les professionnels de santé vont jouer un rôle fondamental dans l'expérimentation et l'entraînement des IA à des fins médicales dans des conditions réelles* »<sup>14</sup>. Le rôle bénéfique des nouvelles technologies dans le domaine de la santé est évident, il n'est plus possible d'ignorer leurs capacités. Le rapport propose dans ce sens d'adapter le métier de médecine, en transformant les voies d'accès aux études de médecine et en ajoutant des formations sur les usages de l'IA. Le développement des nouvelles technologies entraînera certainement l'automatisation, mais cela pourra être abordé par un remaniement des institutions et des missions des professionnels de santé. La transformation digitale permet d'augmenter la productivité du personnel médical en réduisant par exemple le temps consacré à des analyses qui pourraient être réalisées par des logiciels performants. La machine assistera le professionnel dans son travail sans pour autant le remplacer – on parle alors du « *praticien augmenté* ».

La pratique médicale sera donc obligée d'évoluer avec le temps. Mais ce n'est pas seulement le médecin qui en sentira les effets. L'expérience médicale se transformera également pour le patient, qui recevra les soins administrés par le « *praticien augmenté* ». La téléconsultation par exemple est intéressante pour ceux qui ne peuvent pas se déplacer facilement ou qui habitent dans des régions rurales. Elle n'est toutefois pas accessible à ceux qui n'ont pas d'accès à l'Internet, risquant d'alimenter la fracture numérique voire la fracture sociale.

Un autre enjeu pour le patient : le régime de la responsabilité médicale est susceptible d'évoluer. La relation traditionnelle patient-médecin

évolue pour comprendre un tiers, le concepteur du produit ou logiciel assistant le médecin. En cas de dysfonctionnement ou d'erreur du système, vers qui le patient peut-il se retourner pour obtenir une indemnisation pour son dommage ? Peut-il tenir le médecin responsable du fait de son utilisation du logiciel ? Dans l'exemple de la montre connectée cité plus haut, comment déterminer la chaîne des responsabilités (le logiciel, la montre, le réseau, etc.). Si la montre ne déclenche pas d'alerte alors que les paramètres permettraient clairement d'identifier un symptôme majeur ? Qui blâmer si, au contraire, des milliers de montres, par exemple en raison d'un bug, se mettent à appeler les urgences en même temps, saturant ainsi les services et mettant la vie des autres patients en danger ?

Le droit positif n'apporte pas de réponses définitives à ces questions. Pour l'instant, il n'accorde pas la personnalité juridique aux systèmes d'IA. Par ailleurs, l'application du régime des produits défectueux n'est pas satisfaisante, en particulier en raison de la double composante – matérielle et logicielle – des dispositifs et la difficulté d'attribuer un dysfonctionnement à l'un ou l'autre de ces composants.

Il est important que ces questions soient réglées le plus rapidement possible pour apporter une sécurité juridique essentielle à la confiance des différents acteurs.

.....  
<sup>14</sup>. Donner un sens à l'intelligence artificielle, Pour une stratégie nationale et européenne, p. 198, C. Villani, Mission parlementaire du 8 septembre 2017 au 8 mars 2018.

RÉGLEMENTAIRES

---

# **Données personnelles & transformation numérique en Afrique Francophone :**

**SÉCURITÉ & RÉGLEMENTATION**

# Le point de vue...



Olivier Labbé,  
directeur Général, Cap DC

## La révolution numérique a un impact quasi-systémique sur l'économie africaine. Pour quelles raisons ?

L'Afrique est un continent avec un énorme potentiel économique, notamment en raison de la croissance de la population. Son développement la conduit à sauter des étapes technologiques que nous avons connues en Europe. J'ai souvent l'habitude de dire qu'en France, l'arrivée d'internet a été retardée à cause du minitel. En Afrique, au contraire, la pénurie de distributeurs de billets par exemple a conduit à passer directement à l'étape suivante, le paiement mobile, secteur dans lequel le Kenya est désormais leader.

## Quels secteurs sont concernés ?

Les besoins numériques sont très importants partout, mais trois secteurs se distinguent pour le moment. Le secteur bancaire, avec l'exemple cité ci-dessus du paiement mobile, mais aussi le secteur de la santé et de l'agriculture. Concernant la santé, il y a en Afrique un médecin spécialiste pour un million d'habitants. Dans cette configuration, la télémédecine est incontournable. Dans le secteur de l'agriculture, environ 30 % de la production se dégrade avant d'être vendue, faute d'acheteur. Le numérique permet de créer des places de marché pour écouler la production. Dans ces trois secteurs, il y a indubitablement une opportunité technologique.

## Par quelles étapes doit passer cette révolution numérique ?

Le développement de l'informatique repose sur deux types de leviers. Tout d'abord celui des équipements individuels : téléphones, ordinateurs etc. En Afrique, le taux d'équipement est en pleine croissance. Le second levier est celui des infrastructures lourdes, qui sont de deux types : les réseaux et les data center. Il y a un gros travail à faire de ce point de vue et il y a d'importantes disparités

entre l'Afrique côtière, qui profite des réseaux de câbles sous-marins et les pays plus enclavés. Il faudrait garantir à tous la même qualité, ce qui n'est pas le cas aujourd'hui, car dans les terres, en ce qui concerne les réseaux, la mise en place de câbles terrestres nécessite d'importants investissements. Pour les Data Centers, il y a un véritable enjeu, un vrai besoin d'infrastructures locales. Encore aujourd'hui, beaucoup d'adresses mails de membres du gouvernement sont sur gmail, ce qui signifie qu'elles sont hébergées en dehors du pays ! L'avènement de ces infrastructures nécessite cependant le développement préalable d'autres secteurs, et notamment celui de l'énergie. La puissance de production électrique annuelle africaine est seulement de 15 % supérieure à celle de la France. Pour créer des Data Centers en Afrique, l'investissement n'est pas si lourd. La mise en place d'un Data Center National coûterait entre 10 et 20 millions d'€, ce qui est un investissement limité par rapport à d'autres infrastructures, telles qu'un barrage ou un réseau autoroutier. Il faut être prêt à investir dans ce domaine. Un autre problème vient des coûts d'exploitations, en raison du climat chaud, peu propice au refroidissement des serveurs. Il faut donc développer des nouvelles technologies comme le froid solaire ou un grid énergétique basé sur une production renouvelable, que nous ne développons pas en Europe, parce que cela est moins une priorité.

## Faut-il également adapter le cadre juridique ?

Il est indispensable d'adopter une régulation numérique, comme nous l'avons fait en Europe. Certains pays, comme le Bénin, le Mali ou le Sénégal ont instauré des règles de protection des données, mais il faudrait le faire de manière plus large, à l'échelle du continent ou de plusieurs pays. Ces cadres juridiques doivent être mis en place par les gouvernements, car ils amènent la confiance aux investisseurs numériques.



Par **Florence Guthfreund-Roland** et **Mathilde Hallé**

**A** lors que près de 25 % de sa population dispose d'un accès à Internet (principalement mobile)<sup>1</sup>, l'Afrique est désormais une cible potentielle des cybermenaces, et donc partie prenante aux discussions sur la cybersécurité. Malgré la faiblesse des infrastructures de télécommunications, et le coût encore élevé des services d'accès à Internet (fixe ou mobile), en particulier s'agissant du haut débit, l'essor des smartphones illustre l'emballement de la population africaine pour l'ensemble des services (et réseaux sociaux) offerts sur Internet. Si une importante partie du continent reste encore sans aucun accès à Internet, la rendant *de facto* immune aux risques de cybersécurité, le développement de l'accès à Internet en Afrique met les utilisateurs et fournisseurs de services face à de nouveaux risques technologiques, commerciaux, juridiques et réputationnels liés aux attaques et autres violations de sécurité. Parallèlement à l'essor des services internet auprès des utilisateurs, les entreprises se reposent désormais largement sur Internet pour les besoins de leurs activités. Or, la généralisation de la fourniture de services ayant recours au réseau internet s'accompagne de nouvelles menaces de cybersécurité. Peu de secteurs de l'économie sont épargnés. Entre les données de trafic et de facturation traitées par les opérateurs télécoms, les fichiers marketing réalisés par les entreprises de *retail* et distribution, les réseaux sociaux dont l'essor est considérable en Afrique, il est peu de secteurs de l'économie qui ne soient directement ou indirectement dépendant du réseau internet, que ce soit à des fins de collecte d'information, de transmission, de communication ou encore d'hébergement (*cloud*).

Aussi, l'Afrique se retrouve de fait au cœur des problématiques de sécurité en ligne, à la fois en tant que cible potentielle mais aussi en tant que nouveau partenaire dans la lutte contre ces nouvelles menaces. L'actualité de ces dernières années illustre cette tendance. Les victimes sont

principalement les établissements bancaires, les institutions et agences gouvernementales, ainsi que les branches locales d'entreprises internationales et entreprises locales de taille moyenne. En Côte d'Ivoire, Microsoft Afrique a annoncé en avril 2017 que plus de 554 millions de données (*data points*) avaient été « volées » au cours du premier semestre de l'année précédente, constatant ainsi une hausse de plus de 30 % par rapport à la période antérieure<sup>2</sup>. Au Sénégal en juin 2017, les services officiels en charge des élections ont accidentellement mis en ligne un fichier contenant les données personnelles de plus de 5 millions d'électeurs<sup>3</sup>. En Afrique du Sud, les données personnelles de 17 millions de bénéficiaires d'aides sociales ont été communiquées à des tiers à des fins commerciales en 2014, sans que les personnes concernées n'en aient été informées<sup>4</sup>. Et à l'été 2017, l'ensemble du continent a été massivement touché par les cyberattaques globales « Wannacry » et « GoldenEye »,

1. Par comparaison, le taux de pénétration de l'accès à Internet en Europe est autour de 77 %.

2. Ces données, que l'on peut retrouver, sur le site Gemalto, sont relayées par Serge Ntamack, directeur régional des affaires publiques, Microsoft Afrique. Pour chacune de ces sources, les données sont mondiales et ne concernent pas spécifiquement la Côte d'Ivoire. Data breach statistics 2016 : First half results, <https://blog.gemalto.com/security/2016/09/20/data-breach-statistics-2016-first-half-results/> (consulté le 16 février 2018).

3. [www.lequotidien.sn/retrait-des-listes-du-site-de-la-dge-la-cdp-met-a-jour-les-donnees-l-mamadou-niane-directeur-des-affaires-juridiques-de-la-commission-nous-navons-pas-ordonne-le-retrait-des-liste/](http://www.lequotidien.sn/retrait-des-listes-du-site-de-la-dge-la-cdp-met-a-jour-les-donnees-l-mamadou-niane-directeur-des-affaires-juridiques-de-la-commission-nous-navons-pas-ordonne-le-retrait-des-liste/) (consulté le 16 février 2018).

4. <https://afrique.latribune.fr/politique/gouvernance/2017-03-12/afrique-du-sud-une-fraude-massive-aux-donnees-personnelles-defraye-la-chronique.html> ; <https://blogs.mediapart.fr/jacqueline-derens/blog/140317/comment-faire-du-gras-sur-le-dos-des-pauvres>

et plusieurs agences nationales en charge du développement des nouvelles technologies, telles que la NITDA au Nigeria, ont immédiatement relayé l'alerte afin d'encourager les entreprises à prendre rapidement des mesures de protection et de prévention<sup>5</sup>. Globalement, l'augmentation de la criminalité informatique aurait fait perdre au continent près de 3,5 milliards de dollars en 2017<sup>6</sup>. Parallèlement, les autorités sont déjà sensibilisées à la nécessité de lutter contre les failles de sécurité affectant les données personnelles des citoyens. Ainsi, en janvier 2016, le Centre de réponse aux incidents informatiques de Côte d'Ivoire (CI-CERT) a-t-il annoncé avoir prévenu des failles importantes de sécurité signalées dans les smartphones Huawei et systèmes d'exploitation de smartphones Android qui auraient à défaut affecté la sécurité des données personnelles de millions d'utilisateurs<sup>7</sup>.

Pour autant, et bien que le niveau de sophistication de la cybercriminalité en Afrique soit jusqu'à présent resté globalement limité, la faiblesse du cadre légal et réglementaire (excepté quelques rares exceptions) applicable en matière de cybersécurité et sécurité des données personnelles en Afrique, tant au niveau national qu'au niveau régional, fait craindre à terme une multiplication des actes cybercriminels, au détriment du développement de l'économie numérique et du droit des individus à la protection de leurs données (1). Aussi convient-il de s'interroger sur les bonnes pratiques internationales de nature à suppléer les dispositions légales applicables, en examinant les réglementations françaises, communautaires et américaines, afin de dégager un corpus de principes applicables à l'échelle internationale en matière de sécurité des données (2). Pour les entreprises établies en Afrique, ces pratiques s'avèrent difficilement contournables (3).

## 1. Le cadre légal et réglementaire applicable à la cybersécurité en Afrique francophone : un arsenal encore peu développé et à l'efficacité limitée

L'Afrique est un marché en plein bouleversement digital, le continent connaît une

révolution numérique sans précédent. Le continent innove et l'usage des nouvelles technologies y est très répandu. Le revers de la médaille de ces avancées technologiques, au demeurant, réside dans le développement de la cybercriminalité dont la propagation est très rapide sur le continent africain comme ailleurs. Encore imparfaitement appréhendée, celle-ci représente un défi majeur pour les pays africains. Ce qui constitue un risque mais aussi une opportunité en termes d'innovation. La cybersécurité en Afrique francophone est l'un des points majeurs de développement que pose l'essor du numérique. Afin de tenter de remédier aux problèmes posés par les failles dans les systèmes qui favorisent la cybercriminalité, et d'endiguer les risques dus à la prolifération des données personnelles, plusieurs dispositions législatives ont été mises en place. Cependant, ce cadre légal est encore peu développé et son efficacité peine à se faire ressentir. L'arsenal de dispositions du législateur s'est tout d'abord ressenti au niveau régional (1.1) où plusieurs textes et conventions ont vu le jour, pour ensuite s'étendre au niveau national sous forme de loi, dont l'utilité semble parfois discutée et dont l'efficacité reste encore à prouver (1.2).

### 1.1. Des déclarations de principes au niveau régional...

Plusieurs textes ont été adoptés au niveau régional concernant la sécurité des données en Afrique. Les principaux textes résultent d'initiatives de l'Union africaine, de la Communauté

5. <https://afrique.latribune.fr/africa-tech/2017-06-28/cyberattaques-l-afrique-sur-le-qui-vive-742056.html>

6. <http://geopolis.francetvinfo.fr/cybercriminalite-l-afrique-a-perdu-35-milliards-de-dollars-en-2017-185873>

7. « Côte d'Ivoire : des failles importantes de sécurité signalées dans les smartphones Huawei et systèmes Android », *CIOmag*, 16 janvier 2016, <https://cio-mag.com/cote-divoire-des-failles-importantes-de-securite-signalees-dans-les-smartphones-huawei-et-systemes-android/> (consulté le 16 février 2018).

économique et monétaire d'Afrique centrale (CEMAC) de la Communauté économique des États d'Afrique de l'Ouest (CEDEAO) et de l'Union économique et monétaire ouest-africaine (UEMOA).

Après plusieurs années de négociations, l'Union africaine a adopté la Convention sur la cybersécurité et protection des données le 23 juin 2014 pour « *renforcer et harmoniser les législations actuelles des États membres et des Communautés économiques régionales (CER) en matière de TIC* », en créant « *un cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social africain* »<sup>8</sup>. La Convention décline ses principes en trois chapitres, consacrés respectivement aux transactions électroniques, à la protection des données personnelles, et à la promotion de la cybersécurité et à la lutte contre la cybercriminalité.

S'agissant de la protection des données personnelles, la Convention reprend les principes posés par la directive européenne n° 95/46/CE du 24 octobre 1995 en prévoyant que tout traitement de données personnelles doit être licite et loyal, être mis en œuvre pour une finalité définie, pour une durée limitée, sur la base de données pertinentes et exactes, et dans le respect d'exigences de transparence, de confidentialité et de sécurité. La Convention prévoit également différents régimes déclaratifs, ainsi qu'un encadrement spécifique pour les transferts internationaux.

S'agissant de la sécurité des données, la Convention est assez lapidaire. Rien n'est prévu au-delà de l'obligation générale d'assurer la sécurité des données traitées. En particulier, elle ne donne aucun détail quant au contenu de cette obligation selon les types de données collectées ou de traitements mis en œuvre, ou encore les secteurs d'activité. Elle ne prévoit pas non plus d'obligations *ex post*, telles que des obligations de notification applicables en cas de faille de sécurité.

Le chapitre relatif à la cybersécurité de la Convention prévoit des dispositions générales imposant aux États de mettre en place une réglementation appropriée (criminalisation

de certaines infractions, sensibilisation des acteurs, définition des infrastructures essentielles, gouvernance, coopération judiciaire internationale, etc.). Il vise notamment les infractions pénales afférentes à l'accès ou au maintien dans un système d'information, à l'entrave au fonctionnement d'un système d'information, ou à l'introduction frauduleuse de données dans un système d'information. Des infractions relatives aux données contenues dans un tel système sont aussi prévues, telles que l'interception frauduleuse de données lors de leur transmission informatique, l'introduction ou l'altération de données informatiques, ou encore l'usage frauduleux de données informatiques. Le volet répressif de la Convention semble ainsi plus étoffé que son chapitre plus réglementaire relatif aux obligations à la charge des organismes collectant et traitant des données personnelles.

Cependant, la Convention est d'effet limité en pratique. En effet, pour être pleinement applicable aux États membres de l'Union africaine, le texte doit faire l'objet d'une ratification interne. Or, à ce jour, seul le Sénégal l'aurait ratifiée. En raison d'une certaine inertie politique (nourrie par des controverses sur certains aspects du texte susceptibles de limiter la liberté d'expression des internautes), la logique volontariste du texte limite considérablement son effet contraignant.

Au niveau de la CEDEAO, dont 15 pays d'Afrique de l'Ouest sont membres<sup>9</sup>, plusieurs textes prévoient des dispositions juridiques relatives à la sécurité des données personnelles. En particulier, l'Acte additionnel A/SA. 1/01/10 relatif à la protection des données à caractère personnel (adopté en 2010) prévoit une obligation pour les États membres de mettre en place une réglementation applicable aux traitements de données personnelles. Il prévoit également l'obligation pour les États de mettre en place une autorité

8. Les États membres de l'Union Africaine sont listés ici : <https://au.int/fr/memberstates>

9. Bénin, Burkina Faso, Cap Vert, Côte d'Ivoire, Gambie, Ghana, Guinée, Guinée-Bissau, Liberia, Mali, Maroc, Niger, Nigeria, Sénégal, Sierra Leone, Togo.

indépendante dédiée, de respecter pour tout traitement les principes directeurs de légitimité, de loyauté et de transparence, et de mettre en place un régime de formalités administratives préalables. Il prévoit enfin une obligation générale de confidentialité et de sécurité<sup>10</sup>, sans plus de détail. À l’instar de la Convention de l’Union africaine, aucune disposition applicable en cas de violation de données n’est prévue.

La directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans la CEDEAO (adoptée en 2011) prévoit également une liste des infractions devant être criminalisées et réprimées par les États membres. Cette liste inclut principalement les infractions pénales « classiques » en lien avec les systèmes d’information (accès frauduleux ; maintien frauduleux et entrave au bon fonctionnement ; introduction et interception frauduleuse de données, etc.). La directive prévoit également des dispositions procédurales relatives à la preuve par voie électronique, aux perquisitions électroniques, à la coopération judiciaire, etc. La directive est silencieuse quant aux obligations des responsables de traitement en cas de faille de sécurité affectant les données personnelles. Les États membres de la CEDEAO ont l’obligation de se conformer aux dispositions des actes additionnels pris par la communauté, et d’adopter les dispositions législatives, réglementaires et administratives nécessaires pour se conformer aux directives dans les délais qu’elles prévoient. La directive C/DIR/1/08/11 prévoit également une obligation pour les États membres de communiquer à la Commission de la CEDEAO les mesures prises pour se conformer à la directive et de lui notifier les difficultés de mise en œuvre. Toutefois, en pratique, le nombre d’États membres de la CEDEAO ayant adopté ces textes reste très limité et même si la CEDEAO dispose d’une Cour de justice dont la principale mission est d’assurer le respect du droit de la communauté parmi les États membres, son activité reste relativement limitée et les décisions de condamnation des États membres pour manquement n’ont (encore) qu’une portée réduite. La CEDEAO souffre en effet d’un manque de moyens qui limite sa capacité à vérifier le

respect du droit communautaire et à sanctionner les manquements des États membres. Ces textes sont ainsi des pétitions de principe reflétant les bonnes pratiques internationales, mais restent d’une efficacité juridique limitée pour les citoyens et acteurs économiques.

D’autres initiatives internationales soutiennent les actions des États dans la lutte contre la cybercriminalité, notamment au niveau de l’Organisation internationale de la francophonie (OIF), ou encore dans le cadre des rapprochements entre la CEDEAO et le Conseil de l’Europe ou l’East African Community (EAC) et l’ONU. Par ailleurs quelques pays africains ont adhéré<sup>11</sup> (ou sont en voie d’adhésion<sup>12</sup>) à la Convention de Budapest, du Conseil de l’Europe, déjà ratifiée par 44 pays (majoritairement européens)<sup>13</sup>.

Ces initiatives régionales sont salutaires en ce qu’elles créent les conditions permettant une mobilisation législative dans la sous-région, mais aussi parce qu’elles font intervenir des acteurs extra-africains (organisations internationales ou États) qui disposent de l’expertise (formation, entraînement, connaissance des menaces) et/ou de moyens financiers et matériels à même de soutenir les efforts des États africains.

---

## 1.2. ... doublés de dispositions plus spécifiques au niveau national d’effet toutefois limité

---

Les initiatives nationales, et notamment législatives, en matière de lutte contre la cybercriminalité et les violations de données sur le continent africain se développent malgré leur efficacité encore limitée. Dans la majorité des pays francophones de la sous-région ayant

---

10. Acte additionnel A/SA. 1/01/10 relatif à la protection des données à caractère personnel, article 28.

11. Île Maurice, Sénégal et Tunisie.

12. Maroc, Cap Vert et Ghana.

13. Cybersécurité en Afrique : état des lieux et perspectives – <https://www.riskinsight-wavestone.com/2016/05/cybersecurite-en-afrique-etat-lieux-perspectives/> (consulté le 16 février 2018).

adopté un Code pénal (soit une large majorité), les infractions d'intrusion frauduleuse dans un système d'information (et autres infractions s'y rapportant) sont criminalisées. Certains pays disposent même d'une autorité administrative dédiée aux problématiques de cybersécurité<sup>14</sup>. Cependant, l'efficacité de ces instruments juridiques reste souvent limitée en raison du manque sévère de moyens, non seulement au plan financier, institutionnel et politique, mais également en termes d'expertise.

De plus, peu de ces pays disposent aujourd'hui d'une loi de protection des données personnelles. La douzaine de lois ayant été adoptées (sur un total de 54 pays) sont, pour la plupart, inspirées des principes issus de la loi française « Informatique et libertés »<sup>15</sup> tels que repris par la directive communautaire n° 95/46/CE. Elles prévoient ainsi généralement différents régimes déclaratifs, les principes directeurs à respecter par tout responsable de traitement, une obligation générale de sécurité, les différents droits des personnes concernées, et des restrictions en cas de transferts internationaux. Parmi ces pays, moins d'une dizaine ont à notre connaissance institué une autorité indépendante dédiée. Ces autorités sont pour la plupart réunies au sein de l'Association francophone des autorités de protection des données personnelles (AFAPDP), qui joue un rôle important à l'échelle internationale en matière de coordination et de promotion de la réglementation applicable à la protection des données. Certaines sont particulièrement actives, y compris au plan régional. Par exemple, la Commission nationale de la protection des données à caractère personnel (CNDP) du Maroc a initié en février 2018 l'organisation d'une conférence internationale sur le thème « La protection de la vie privée et des données personnelles : un levier de développement en Afrique », permettant ainsi l'organisation d'une rencontre pour la Communauté africaine des autorités de protection des données personnelles et de la vie privée<sup>16</sup>. Enfin, seuls deux pays sur le continent, à savoir le Ghana et l'Afrique du Sud,

imposent une notification aux autorités en cas de violation de données personnelles<sup>17</sup>.

La Côte d'Ivoire fait figure d'exemple dans la sous-région. Adoptée en 2013, la loi ivoirienne n° 2013-450 relative à la protection des données à caractère personnel est conforme aux meilleures pratiques internationales et plus particulièrement aux standards communautaires. Elle prévoit expressément des obligations de confidentialité, de protection et de sécurité des données personnelles traitées<sup>18</sup> et va même plus loin que la directive en imposant une obligation de remettre chaque année à l'Autorité un rapport détaillant les mesures effectivement mises en place pour assurer le respect de ces obligations<sup>19</sup>. Dans le cas où l'Autorité considère qu'un responsable de traitement n'a pas respecté ses obligations, elle a la possibilité de prononcer à son encontre des sanctions, allant de l'avertissement à l'interdiction définitive de poursuivre le traitement, en passant par des sanctions pécuniaires proportionnelles à la gravité et aux bénéfices du manquement pour le responsable dans la limite de 10 millions de francs CFA<sup>20</sup>.

Ceci étant, le respect de l'obligation de sécurité des données par les responsables de traitement reste là encore difficile à établir,

14. Cybersécurité en Afrique : état des lieux et perspectives (<https://www.riskinsight-wavestone.com/2016/05/cybersecurite-en-afrique-etat-lieux-perspectives/> consulté le 16 février 2018).

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

16. <https://www.cndp.ma/rapdp/> ; <https://afriquemidi.com/2018/03/13/reseau-africain-des-autorites-de-protection-des-donnees-personnelles-rapdp-2/>

17. Il s'agit de l'Afrique du Sud et du Ghana. [https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za\\_Privacy\\_is\\_Paramount-Personal\\_Data\\_Protection\\_in\\_Africa.pdf](https://www2.deloitte.com/content/dam/Deloitte/za/Documents/risk/za_Privacy_is_Paramount-Personal_Data_Protection_in_Africa.pdf).

18. Articles 19, 40 et 41 de la loi n° 2013-450 relative à la protection des données à caractère personnel en Côte d'Ivoire.

19. Article 43 de la loi n° 2013-450.

20. Soit 15 250 euros environ.

d'autant qu'à notre connaissance aucune recommandation n'a été publiée concernant les mesures de sécurité minimales à mettre en œuvre. De même, le manque de ressources et l'agenda chargé de l'Autorité (également en charge de la poste, des télécommunications et des transactions électroniques) conduit à s'interroger sur sa capacité à assurer l'application de la loi en pratique, en particulier s'agissant d'obligations aux contours flous dont le respect est par nature délicat à évaluer en dehors de références à des normes sectorielles ou pratiques de marché.

Cette opacité est renforcée par le fait qu'aucune obligation de notification des violations de sécurité n'est prévue par la loi ivoirienne, ni à l'attention des personnes concernées ni à l'attention de l'autorité de protection des données personnelles. En d'autres termes, il est non seulement impossible pour les personnes concernées d'être assurées que leurs données sont traitées dans des conditions de sécurité minimales, mais de plus les violations de sécurité affectant ces données peuvent passer totalement inaperçues, tant de l'Autorité que des personnes concernées.

En parallèle, la Côte d'Ivoire dispose d'une loi de lutte contre la cybercriminalité, adoptée en 2013. Son texte est court mais néanmoins relativement sophistiqué et en phase avec les pratiques législatives en matière d'infractions de cybersécurité. Y sont notamment prévues les infractions pénales « classiques » en la matière telles que l'accès et le maintien frauduleux dans un système d'information, l'entrave au bon fonctionnement d'un système d'information, ou encore l'introduction et l'interception frauduleuse de données<sup>21</sup>. Une infraction de « vol d'information » est également prévue et définie de manière relativement large<sup>22</sup>.

Par ailleurs, d'autres États ont déployé des efforts para-législatifs remarquables en matière de cybersécurité. En particulier, le Maroc<sup>23</sup>, la Tunisie<sup>24</sup>, le Mali, le Sénégal<sup>25</sup>, le Cap Vert, le Kenya et l'Afrique du Sud se sont récemment distingués par différentes initiatives. Néanmoins, les effets de ces projets nationaux restent encore limités en termes

d'obligations applicables aux acteurs impliqués dans le traitement des données personnelles et de droits pour les personnes concernées.

## 2. Quelles sont les bonnes pratiques internationales en matière de sécurité des données personnelles ?

21. Articles 4 à 16 de la loi n° 2013-451 relative à la lutte contre la cybercriminalité ([http://www.artci.ci/images/stories/pdf/lois/loi\\_2013\\_451.pdf](http://www.artci.ci/images/stories/pdf/lois/loi_2013_451.pdf)).

22. Article 26 de la loi n° 2013-451 relative à la lutte contre la cybercriminalité.

23. La stratégie du Maroc en matière de cybersécurité et les efforts déployés pour faire face aux attaques informatiques ont notamment été exposés à l'occasion de la 4<sup>e</sup> conférence mondiale sur le cyberspace (GCCS), qui s'est tenue à La Haye en 2015. Lors de cette réunion, il a été décidé d'inscrire dans le cadre des plans d'action de la Direction générale de la sécurité de systèmes de l'information (DGSSI), une batterie de mesures visant à renforcer le dispositif marocain de sécurité des systèmes de l'information (SSI) des administrations, des organismes publics et des opérateurs chargés de la gestion des infrastructures d'importance vitale (<http://www.menara.ma/fr/2015/04/16/1602574-le-maroc-expose-%C3%A0-la-4%C3%A8me-conf%C3%A9rence-mondiale-sur-le-cyberspace-sa-strat%C3%A9gie-en-mati%C3%A8re-de-cybers%C3%A9curit%C3%A91.html>). La même année, une déclaration d'intention a été signée entre le Maroc et l'Espagne pour renforcer l'échange d'expériences et de savoir-faire en matière de cybersécurité, soutenir la formation et le développement des capacités en la matière, et consolider la coopération bilatérale en matière juridique et législative (<http://www.maroc.ma/fr/actualites/signature-madrid-dune-declaration-dintention-en-matiere-de-cyber-securite-entre-le-maroc>).

24. [https://telquel.ma/2018/02/27/en-lafrique-protection-vie-privée-donnees-personnelles\\_1582074](https://telquel.ma/2018/02/27/en-lafrique-protection-vie-privée-donnees-personnelles_1582074).

25. Récemment, le Sénégal s'est doté d'un centre national de cybersécurité et d'un laboratoire dédiés à la lutte contre la cybercriminalité. Par ailleurs, un accord de coopération international en matière de cybersécurité a été signé avec la France le 15 mars 2016 afin de mettre en place des dispositifs opérationnels pouvant répondre aux éventuelles attaques numériques. Voir notamment : <http://www.osiris.sn/Cybercriminalite-Le-Senegal-une.html> ; [http://afrique.lepoint.fr/actualites/cybersecurite-la-france-renforce-ses-partenariats-en-afrique-18-03-2016-2026407\\_2365.php](http://afrique.lepoint.fr/actualites/cybersecurite-la-france-renforce-ses-partenariats-en-afrique-18-03-2016-2026407_2365.php) ; <https://www.agencecofin.com/securite/3103-18818-le-senegal-va-se-doter-d-un-centre-national-de-cyber-securite>

Au niveau international, la sécurité des données personnelles est principalement traduite au plan réglementaire par une obligation générale d'assurer la sécurité des données personnelles traitées, applicable à tout responsable de traitement, et à l'obligation de notifier les violations de sécurité affectant ces données dès leur découverte.

Néanmoins, ces obligations aux contours initialement flous (en ce qui concerne l'obligation générale de sécurité) ou limités (en ce qui concerne l'obligation de notification en cas de violation de données) se sont récemment développées, au niveau européen comme outre-Atlantique.

Au niveau mondial, la France met en œuvre depuis toujours une réglementation préventive en termes de gestion des risques de sécurité (2.1) ; par ailleurs, la réglementation européenne relative à la protection des données personnelles met en œuvre un arsenal juridique répondant à une logique de prévention et de réaction (2.2). Aux États-Unis, la réglementation applicable en matière de sécurité des données s'articule autour d'un dispositif légal conséquent (2.3).

### 2.1. France : une réglementation historiquement basée sur la gestion « en amont » des risques de sécurité

Historiquement, le cadre légal applicable à la sécurité des données en France était plutôt de nature pénale. En effet, le Code pénal criminalise depuis le début des années 1990 l'introduction frauduleuse et le maintien dans un système de traitement automatisé de données (STAD), parmi d'autres infractions assimilées<sup>26</sup>.

Ceci étant, ni le Code pénal ni la loi Informatique et libertés ne prévoient d'obligation générale de notification en cas de violation de données personnelles. Par exception, les fournisseurs de services de communications électroniques (opérateurs télécoms) sont depuis 2011 soumis à l'obligation de notifier les violations de sécurité affectant les données personnelles qu'ils traitent, en tant que responsables, aux

autorités de contrôle et dans certains cas aux personnes concernées<sup>27</sup>. En cas de non-respect de ces obligations, les fournisseurs de services de communications électroniques sont passibles de sanctions pénales allant jusqu'à 300 000 euros d'amende et 5 ans de prison.

En revanche, il existe dans la loi Informatique et libertés une obligation générale de sécurité et de confidentialité pesant sur tout responsable de traitement, c'est-à-dire toute personne définissant les finalités et les moyens d'un traitement de données personnelles<sup>28</sup>. Si la CNIL a publié de nombreuses recommandations concernant les mesures de sécurité envisageables pour assurer le respect de cette obligation dans certains secteurs d'activité ou pour certains types de traitement<sup>29</sup>, ces publications n'ont pas de caractère directement contraignant ni exhaustif<sup>30</sup>. En d'autres termes, il appartient au responsable de définir par lui-même l'éventail des mesures de sécurité physiques et logiques nécessaires pour assurer de fait la sécurité des données

26. Articles 323-1 et s. du Code pénal. Ces infractions ont été introduites dans le Code pénal par la loi n° 92-685 du 22 juillet 1992 portant réforme des dispositions du Code pénal relatives à la répression des crimes et délits contre les biens.

27. Article 34 bis de la loi n° 78-17 du 6 janvier 1978.

28. Article 34 de la loi n° 78-17 du 6 janvier 1978.

29. Voir notamment les fiches sécurité publiées par la CNIL (<https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles>). Par ailleurs, la CNIL publie régulièrement des recommandations sur des thèmes spécifiques (ex. : données hébergées dans le *cloud*, données traitées par les établissements de santé, etc.).

30. La CNIL adopte régulièrement des délibérations visant à établir les conditions de mise en œuvre de certains traitements courants, et les entreprises se conformant à ces conditions ont la possibilité de bénéficier de formalités déclaratives simplifiées en s'engageant simplement à respecter les conditions de la délibération de la CNIL. Néanmoins ces délibérations ne sont pas *per se* directement applicables aux responsables de traitement n'y ayant pas adhéré.

31. Article 35 de la loi n° 78-17 du 6 janvier 1978.

personnelles traitées pour son compte, en prenant en compte les recommandations de la CNIL le cas échéant mais sans s'y arrêter. Dans le cas où il est fait appel à des sous-traitants, l'obligation de sécurité et de confidentialité doit leur être contractuellement répercutée<sup>31</sup>. Les responsables se trouvent ainsi dans une situation délicate, devant respecter une obligation aux contours relativement flous.

C'est pourtant sur le fondement de cette obligation générale de sécurité que la CNIL a par le passé prononcé des sanctions à l'encontre de responsables de traitement lors de violations de données significatives. Par exemple, en mars 2014, la société Orange a été sanctionnée par la CNIL à la suite d'une faille de sécurité ayant affecté 1,3 million de personnes. Si la sanction prononcée à l'époque était relativement clémente (la CNIL s'étant contentée d'un avertissement public), au vu des données exposées (celles-ci étant incluses dans un fichier d'e-mailing marketing), la CNIL dispose d'un pouvoir de sanction financière susceptible de s'appliquer en cas de violation de sécurité, selon la gravité des faits. Ainsi, en janvier 2018, la CNIL a déjà prononcé plus d'une dizaine de sanctions financières à l'encontre de responsables de traitement sur le fondement de l'article 34 de la loi Informatique et libertés, la plus élevée et récente étant une sanction de 100 000 euros prise à l'encontre de la société Darty pour violation de sécurité des données personnelles (les données personnelles communiquées par les clients de la société dans le cadre de son service client en ligne n'avaient pas été sécurisées contre l'accès de tiers non autorisés)<sup>32</sup>. Dans ce contexte de relative incertitude réglementaire, les clarifications apportées par la réforme européenne du droit applicable aux traitements de données personnelles ne peuvent ainsi qu'être bienvenues, tant pour les entreprises françaises et européennes que pour l'ensemble des acteurs internationaux intéressés par le marché européen et ses bonnes pratiques.

### 2.2. La nouvelle réglementation européenne applicable dès le 25 mai 2018 : un arsenal juridique répondant à une logique de prévention et de réaction

En matière de sécurité des données personnelles, le nouveau règlement général de protection des données personnelles (RGPD) étend largement les obligations applicables aux responsables de traitement et à ses sous-traitants, et en particulier (i) l'obligation générale d'assurer la sécurité et la confidentialité des données traitées, et (ii) l'obligation de notifier toute violation de sécurité.

L'obligation d'assurer la sécurité des données est mise à la charge du responsable du traitement, c'est-à-dire la personne déterminant les finalités et les moyens du traitement, par différentes dispositions du RGPD<sup>33</sup>. Le RGPD liste expressément, de manière illustrative, les mesures qui peuvent être mises en œuvre par le responsable pour satisfaire cette obligation (cryptage, tests réguliers, etc.).

Par ailleurs, le RGPD généralise l'obligation de notification des violations de données personnelles applicable jusqu'ici aux seuls opérateurs de communications électroniques à tous les responsables de traitement<sup>34</sup>. En cas de violation, le responsable du traitement doit notifier la violation en question à l'autorité de contrôle compétente dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation ne soit susceptible d'engendrer un risque pour les droits et libertés des personnes concernées. De plus, si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes

32. Voir délibération n° SAN-2018-001 du 8 janvier 2018 à l'encontre de la société Darty : <https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000036403140&fastReqlId=306045536&fastPos=1>.

33. Articles 5 1° f) et 32 du GDPR.

34. Articles 33 et 34 du GDPR.

35. Article 80 du GDPR.

concernées, ces dernières doivent également être informées dans les meilleurs délais. Le RGDP prévoit également l'obligation pour tout sous-traitant intervenant dans le traitement des données ayant été affectées de notifier toute violation de données au responsable de traitement pour le compte duquel il intervient. Le RGDP donne également des précisions concernant les informations devant être incluses dans la notification à l'autorité. En particulier, le responsable de traitement doit mentionner (i) la nature de la violation (y compris les catégories et le nombre de données concernées), (ii) les conséquences probables de la violation, et (iii) les mesures prises par le responsable pour remédier à la violation.

En cas de non-respect de ces obligations, les sanctions générales prévues par le RGDP sont applicables. Ainsi, un responsable de traitement n'ayant pas assuré la sécurité des données personnelles traitées pourra être passible de sanctions financières jusqu'à 20 millions d'euros ou jusqu'à 4 % du chiffre d'affaires global de l'entreprise au cours de l'année précédente. Une entreprise n'ayant pas respecté ses obligations de notification en cas de violation de sécurité pourra voir sa responsabilité engagée à hauteur de 10 millions d'euros ou jusqu'à 2 % du chiffre d'affaires global de l'entreprise au cours de l'année précédente.

Outre ces amendes particulièrement importantes – d'ambition dissuasive – le RGDP laisse ouverte la possibilité d'une action de groupe à l'initiative des personnes affectées par la violation commise par le responsable, telle qu'une faille de sécurité exposant leurs données personnelles<sup>35</sup>.

Dans ces circonstances, les entreprises soumises au RGDP devront mettre en place des mesures techniques et organisationnelles de sécurité physique et logique adaptées aux traitements mis en œuvre et aux données traitées. Elles devront également revoir les contrats conclus avec leurs sous-traitants et partenaires, mais aussi plus largement adopter (et mettre en œuvre) de véritables politiques de sécurité cohérentes et adaptées.

Quoiqu'il soit fréquent d'opposer Union

européenne et États-Unis dans leur manière d'approcher les problématiques de protection des données personnelles, l'adoption du RGDP participe d'une tendance internationale vers l'harmonisation du cadre réglementaire applicable en matière de sécurité des données personnelles, en reprenant certaines obligations déjà fermement établies aux États-Unis.

### 2.3. Les principales obligations de sécurité des données aux États-Unis

Aux États-Unis, la réglementation applicable en matière de sécurité des données s'articule principalement autour de deux corpus : (i) les lois de notification de violation de sécurité, et (ii) les *orders* pris par la Federal Trade Commission (FTC) sur le fondement de la Section 5 du Sherman Act sur les pratiques déloyales.

Depuis la première loi sur la notification des violations de données en Californie en 2002, 48 États des États-Unis ont adopté des lois similaires<sup>36</sup>. La plupart de ces lois exigent une notification des violations des données personnelles aux personnes concernées, dans des délais souvent relativement courts (quelques jours). La plupart de ces lois ne prévoient pas de seuil, ce qui implique que les entreprises ont l'obligation de notifier toute violation de données. Néanmoins, certains États ont pris le parti de réduire le périmètre de l'obligation de notification aux violations de sécurité affectant des données non cryptées uniquement.

Depuis l'adoption de ces lois, les entreprises établies aux États-Unis ont développé une forte sensibilité aux violations de sécurité. En effet, au-delà du risque juridique, les entreprises cherchent autant que possible à éviter des situations de communication difficile, nécessitant des ressources supplémentaires importantes, et mettant potentiellement à mal leur réputation.

L'exemple récent de la faille de sécurité ayant

<sup>36</sup> La National Conference of State Legislatures tient une liste exhaustive de ces lois et des liens qui y renvoient : [www.ncsl.org](http://www.ncsl.org).

affecté les *credit reports* traités par l'agence américaine de *credit scoring* Equifax est éclairant. Ayant affecté plus de 145,5 millions de personnes, et des données de nature particulièrement sensible telles que leurs numéros de sécurité sociale et leurs numéros de carte de crédit, elle a créé un véritable scandale médiatique et, *in fine*, a mené à la démission de son CEO<sup>37</sup>.

En parallèle de ces obligations de notification des failles de sécurité, la FTC a développé au cours de ces dernières années de nouvelles compétences en matière de sécurité des données des consommateurs, dans le cadre des pouvoirs lui étant dévolus par la Section 5 du Sherman Act réprimant les pratiques déloyales. Si la régulation par la FTC des mesures de sécurité mises en place par les entreprises reste relativement récente, et que la FTC n'est pas en mesure de prononcer des sanctions de prime abord (la FTC est uniquement habilitée en la matière à prendre des *orders* aux termes desquels l'entreprise contrevenante est formellement et publiquement mise en demeure de respecter certains engagements sous peine de sanctions financières), ses nombreuses publications récentes en matière de sécurité<sup>38</sup> semblent indiquer que la sécurité des données des consommateurs constitue désormais une préoccupation majeure de la FTC.

---

### **3. Le respect d'un socle minimal d'obligations de sécurité inspiré des meilleures pratiques internationales sera difficilement contournable pour les groupes ayant des activités en Afrique**

---

Si le RGPD a été adopté au niveau de l'Union européenne, son champ d'application territorial déborde les frontières de l'Europe. D'une part, le RGPD s'applique au traitement des données à caractère personnel effectué dans le cadre des activités des entités établies en Union européenne (que les activités de traitement aient lieu ou non dans l'Union). D'autre part, le RGPD s'applique aussi lorsque le

traitement de données personnelles porte sur des personnes se trouvant sur le territoire de l'Union, même si le responsable (ou sous-traitant) mettant en œuvre le traitement n'est pas établi dans l'Union, lorsque le traitement est lié à l'offre de biens ou de services à ces personnes, ou au suivi du comportement de ces personnes<sup>39</sup>.

Aussi, de nombreuses entreprises établies sur d'autres continents, et par le passé non soumises à la réglementation communautaire applicable à la protection des données personnelles, devront dès le 25 mai 2018 se mettre en conformité avec l'ensemble des dispositions du RGPD. En particulier, les entreprises établies en Afrique devront se conformer au RGPD dès lors qu'elles offrent des produits ou services au public européen sur Internet.

À défaut d'être directement soumises au RGPD, d'autres entreprises établies en Afrique seront probablement amenées à respecter le RGPD afin de se mettre en conformité avec les meilleures pratiques internationales, en particulier si certaines des filiales de leur groupe les ont déjà adoptées, dans le cadre d'une approche cohérente des problématiques réglementaires et techniques de la sécurité des données.

De même, les entreprises présentes en Afrique et ayant également une présence (directe ou bien *via* les sociétés affiliées de leur groupe) non seulement en Europe mais aussi aux États-Unis se verront directement ou indirectement dans l'obligation de respecter la réglementation américaine applicable en matière de sécurité des données personnelles, et

---

37. Voir notamment : [http://www.lemonde.fr/pixels/article/2017/10/03/le-piratage-d-equifax-du-a-une-faille-informatique-non-corrigee\\_5195179\\_4408996.html](http://www.lemonde.fr/pixels/article/2017/10/03/le-piratage-d-equifax-du-a-une-faille-informatique-non-corrigee_5195179_4408996.html) ; [https://www.washingtonpost.com/news/the-switch/wp/2017/09/26/equifax-ceo-retires-following-massive-data-breach/?utm\\_term=.3a1d9daed9a3](https://www.washingtonpost.com/news/the-switch/wp/2017/09/26/equifax-ceo-retires-following-massive-data-breach/?utm_term=.3a1d9daed9a3) ; <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html>

38. Pour plus d'informations : <https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series>

39. Article 3 du GDPR.

notamment l'obligation de mettre en œuvre des mesures de sécurité adaptées et de notifier les autorités en cas de faille de sécurité.

Dans ces circonstances, il est recommandé pour les entreprises ayant des activités en Afrique de définir et mettre en place une stratégie de prévention et de réaction afin de limiter l'occurrence et d'encadrer les conséquences des failles de sécurité de données personnelles. En termes de prévention, il s'agit de développer une véritable stratégie d'entreprise en matière de cybersécurité. Cette stratégie peut être déclinée selon trois axes. Le premier axe concerne l'intégration des problématiques de sécurité des données au cœur de la gouvernance de l'entreprise. Cela passe notamment par la revue des procédures internes, la mise à jour de la documentation de l'entreprise, et la revue et la renégociation des contrats conclus avec les sous-traitants et prestataires externes. Dans ce cadre, l'entreprise devra également veiller à adapter ses polices d'assurance afin d'intégrer les cyber-risques. Le second axe concerne les technologies déployées par l'entreprise pour effectivement assurer la protection des données contre tout risque de fuite ou d'accès frauduleux, ou autre faille de sécurité. Les mesures de sécurité doivent être à la fois physiques (protection des serveurs, accès aux locaux, etc.) et logiques (politiques de gestion des accès et mots de passe, pare-feu, maintenance évolutive des systèmes), et peuvent notamment passer par des certifications du type de la famille

ISO 27000. Dans tous les cas, les mesures de sécurité doivent être définies avec soin au vu des types de données traitées, des finalités du traitement, des risques afférents aux conditions de mise en œuvre du traitement, etc. Le troisième axe principal en matière de prévention des risques de cybersécurité porte sur la sensibilisation et la formation des personnels de l'entreprise, à titre préventif mais aussi afin de communiquer sur les réponses à adopter en cas de faille de sécurité.

Si malgré ces efforts l'entreprise est victime d'une faille de sécurité exposant des données personnelles, elle doit réagir conformément à une procédure spécifique prédéfinie. En particulier, cette procédure doit prendre en compte (i) les obligations de notifications applicables (destinataires, contenu, délais, etc.), (ii) la nécessité de faire intervenir dès que possible juristes et avocats, afin de s'assurer du respect de l'ensemble des obligations légales, réglementaires et contractuelles applicables dans ce cas, et de protéger l'enquête interne du sceau de la confidentialité, et (iii) la nécessité de faire intervenir rapidement des équipes spécialisées (ingénieurs, commerciaux, communication externe) afin de stopper la faille, d'en limiter les effets sur les plans technologiques, réglementaires, commerciaux et réputationnels, et d'adopter une véritable stratégie de gestion de crise vis-à-vis des clients, usagers, partenaires commerciaux et autorités de contrôle, voire des gouvernements.

**RÉGLEMENTAIRES**

---

**THÈME 8**

**Politique de concurrence  
&  
transformation numérique :**

**LA QUESTION DE LA DATA**

# Le point de vue...



**Frédéric Jenny, professeur d'économie à l'ESSEC et co-directeur du Centre Européen de Droit et d'Économie de l'ESSEC (CEDE), Président du Comité de la concurrence de l'OCDE**

**Le numérique biaise le jeu de la concurrence en créant des marchés dans lesquels entreprises, indépendants et particuliers sont en capacité d'offrir des services similaires (UBER, BLABLACAR, AirBNB...) sans être cependant soucis aux mêmes règles. Comment peut-on restaurer une concurrence non biaisée ? Est ce souhaitable ?**

Le numérique transforme la concurrence. Les plates-formes multi-faces permettent à des indépendants offreurs potentiels de service de satisfaire les demandes des consommateurs en dehors du cadre classique d'une entreprise hiérarchique. Le service ainsi offert, par le biais de la coopération, s'il n'est pas exactement le même que celui offert par les entreprises classiques est voisin et le concurrence.

Le cadre juridique qui s'applique aux plates-formes numériques et à la coopération entre leurs utilisateurs peut être différent de celui qui s'applique aux entreprises classiques (le droit du travail peut ne pas s'appliquer aux plates-formes) tant parce que l'organisation de l'activité n'est pas la même que parce que l'activité des entreprises classiques est soumise à des réglementations sectorielles qui ne s'appliquent pas facilement à des plates-formes numériques ou à des indépendants mettant à disposition certains de leurs actifs.

Le cadre juridique doit être neutre entre les formes de production d'un même type de service tant pour faciliter une meilleure utilisation des ressources que pour promouvoir la concurrence et l'innovation. Il faut revoir le cadre juridique de l'activité économique trop étroitement centré sur la notion de société, éliminer les réglementations sectorielles là où elles sont abusivement restrictives de concurrence et, ne gardant que celles qui ont

une véritable rationalité économique, les rendre applicables aux différentes formes de production d'un service.

**Comment appréhender de manière plus efficace les enjeux liés à la concentration dans le secteur du numérique ?**

La concentration dans le numérique n'est pas néfaste si elle résulte d'une concurrence effective portant sur l'innovation et la productivité et si elle préserve la possibilité d'émergence de concurrents. Mais elle peut aussi résulter de pratiques ou de transactions anticoncurrentielles (l'absorption par une entreprise dominante de start-up afin d'empêcher l'éclosion de concurrents potentiels), d'effets de réseaux ou de taille qui donnent à certaines entreprises un avantage impossible à rattraper pour les concurrents (Amazon) ou, encore, d'un accès privilégié à des données personnelles permettant d'exploiter les consommateurs à leur insu ou de mettre en œuvre des stratégies d'exclusion de concurrents (Facebook ou Google). La vigilance s'impose car la domination du numérique peut se faire au détriment de l'efficacité économique et de l'innovation mais également avoir des effets délétères au-delà du strict domaine économique. Il faut adapter le droit de la concurrence à la spécificité du secteur numérique, par exemple en baissant les seuils de contrôle des concentrations externes ou en modifiant leur base, en se montrant plus vigilant sur les abus d'exploitation des consommateurs ou d'exclusion des concurrents par les entreprises dominantes, en développant des instruments appropriés pour les marchés ou les faces de marché sur lesquels les prix sont nuls. Mais limiter par principe la taille des entreprises du numérique pourrait porter atteinte à la diffusion d'innovation ou à l'efficacité économique.



Par **Edouard Sarrazin** et **Clara Deveau**

**S**elon certaines études, la quantité de données numériques devrait atteindre 44 zetaoctets d'ici 2020<sup>1</sup>, pour une valeur créée d'environ 260 milliards d'euros par an d'ici 2022<sup>2</sup>. Ce phénomène est essentiellement alimenté par les consommateurs, qui génèrent environ deux tiers de ces données, le tiers restant étant produit par les entreprises et les pouvoirs publics. Ces informations, généralement désignées par le terme « *data* », sont en outre produites à un rythme exponentiel puisqu'on estime généralement que 90 % des données actuellement existantes ont été générées au cours des deux dernières années<sup>3</sup>.

Si les inquiétudes du point de vue de la protection individuelle de ces données sont grandes, la collecte massive de données combinée à l'essor des nouvelles technologies et des techniques d'analyses dont font partie les algorithmes, offre des perspectives de développement exceptionnelles pour les entreprises. Il est ainsi fréquent de voir qualifier les données personnelles de « *newel or noir* » du XXI<sup>e</sup> siècle<sup>4</sup>. Les entreprises, que leur activité appartienne à la sphère de l'économie numérique ou soit impactée par la digitalisation de l'économie, l'ont bien compris puisque la grande tendance du secteur est à la concentration du marché. Bien conscientes de l'intérêt de faire main basse sur une base de données massive, sur une technologie ou sur un algorithme, les entreprises établies ont tendance à racheter de plus ou moins petites start-ups au modèle disrupteur afin de cumuler données et technologies d'analyse. Il en va ainsi notamment du leader des réseaux sociaux Facebook qui a racheté Whatsapp, l'application mobile de messagerie, de Microsoft qui a racheté LinkedIn ou encore de l'application Shazam rachetée par Apple.

Une telle concentration génère cependant inmanquablement de vives inquiétudes quant à la préservation du jeu concurrentiel et ne

peut que renforcer l'attention portée aux avantages économiques et concurrentiels que la collecte et la possession de données sont susceptibles de procurer sur un marché. En effet, si de nombreux acteurs de l'économie numérique mettent en avant l'innovation considérable au service des consommateurs que constitue l'utilisation des données, d'autres voient la collecte et la détention d'une quantité colossale de données comme un avantage concurrentiel leur barrant définitivement la route lorsqu'ils souhaitent entrer sur le marché. Le dynamisme du secteur risquerait alors de ne bénéficier qu'à certains acteurs au détriment de la concurrence, de l'innovation et *in fine* du consommateur. On le voit, l'analyse n'est pas aisée et a donné lieu à de nombreux travaux tant à l'échelle nationale qu'européenne. La difficulté que les autorités de concurrence semblent avoir à appréhender le pouvoir de marché que les données sont susceptibles de conférer, pose également la question de l'adaptation des règles actuelles du droit de la concurrence au défi posé par la complexité du secteur, son évolution toujours plus rapide et sa très forte sensibilité à l'innovation.

## 1. L'explosion du numérique : la collecte massive de données

1. Etude conduite par l'International Data Corporation (IDC) et EMC<sup>2</sup>, *The Digital Universe of Opportunities : Rich Data and the Increasing Value of the Internet of Things*, avril 2014

2. Etude conduite par l'IDC, *Worldwide Semiannual Big Data and Analytics Spending Guide*, août 2018

3. Intervention d'Oliver Bäte, Président-Directeur Général d'Allianz SE, conférence «*Shaping competition policy in the era of digitisation*», 17 janvier 2019, Commission Européenne, Bruxelles

4. Autorité de la concurrence, Avis n°18-A-03, 6 mars 2018 portant sur l'exploitation des données dans le secteur de la publicité sur internet, p.2

La collecte et l'exploitation de ces données participent à l'émergence de nouveaux acteurs et permettent de nombreuses innovations (1.1), mais soulèvent de vraies problématiques en droit de la concurrence (1.2).

### 1.1. Données et entreprises, de quoi parle-t-on?

Du point de vue des entreprises, les données peuvent être tout à la fois un bien (elles sont non rivales, parfois complémentaires), un investissement ou un intrant (à ce titre, elles affectent les coûts des opérateurs qui les utilisent, constituent d'éventuelles barrières à l'entrée, peuvent faire l'objet d'économies d'échelle...), une monnaie (la contrepartie des services proposés, dont la valeur peut varier considérablement). Elles sont en outre particulièrement importantes sur les marchés multifaces, dont l'évolution est très rapide<sup>5</sup>.

#### 1.1.1. Des données au «big data» : l'expansion des données dans tous les secteurs

Dans une étude conjointe relative au droit de la concurrence et aux données publiée en mai 2016, les autorités de concurrence française et allemande (le Bundeskartellamt), estiment qu'il n'existe pas de définition unique du mot « données ». L'étude retient toutefois que ce terme peut être « employé pour faire référence à une information ou sa représentation, souvent en association avec son stockage sur un ordinateur »<sup>6</sup>. La notion de « big data », qui ne fait pas non plus l'objet d'une définition aboutie, présente selon les deux autorités des caractéristiques qui « ont trait à l'importance, en termes de volume et de variété, des données, à leur mode de collecte, ainsi qu'à la puissance informatique et algorithmique requise pour leur traitement et leur analyse »<sup>7</sup>. Le big data est ainsi caractérisé par la combinaison de trois « V » : Volume, Vitesse et Variété, desquels découle généralement la Valeur. Afin de mieux appréhender cette masse d'informations, les données sont traditionnellement différenciées en fonction de différents facteurs qui influent

sur leur disponibilité pour les entreprises et donc leur utilité dans le jeu concurrentiel<sup>8</sup> :

- La nature de leur émetteur et le type d'information qu'elles fournissent sur ce dernier ;
  - Leur caractère ou non de données personnelles<sup>9</sup>, dont la collecte et le traitement font l'objet d'un encadrement réglementaire ;
  - Leur degré de structuration, les rendant plus ou moins faciles à interpréter et exploiter ;
  - Leur méthode de collecte, selon qu'elles sont fournies volontairement ou collectées via différentes technologies telles que notamment les cookies, les pixels et les tags<sup>10</sup>, ou encore dans un environnement « logué » qui nécessite une authentification pour accéder au service.
- Ces données sont manipulées par différents types d'acteurs - les plus exposés étant naturellement les entreprises numériques, dont le cœur de métier réside dans leur captation et leur exploitation. La problématique des

5. Intervention de David Sevy, économiste Compass Lexecon, conférence Concurrences, *Big data et concurrence : quelle importance pour le secteur de la publicité en ligne?*, 24 mai 2018

6. Étude conjointe de l'Autorité de la concurrence et du Bundeskartellamt, *Droit de la concurrence et données*, 10 mai 2016, p.4

7. Étude conjointe de l'Autorité de la Concurrence et du Bundeskartellamt, op. cit., p.4-5

8. Voir notamment Étude conjointe de l'Autorité de la Concurrence et du Bundeskartellamt, op. cit., p.5-8

9. Les données personnelles sont définies comme toutes les informations concernant une personne physique identifiée ou identifiable, aux termes de l'article 4 du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, 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

10. Autorité de la concurrence, Avis n°18-A-03, 6 mars 2018, op. cit. p.30-31

11. Notamment le secteur de l'assurance, voir l'intervention d'Oliver Bäte, PDG d'Allianz SE, conférence «*Shaping competition policy in the era of digitisation*» op. cit.

12. Les Echos, *Les banques hésitent encore sur l'exploitation des 'data' clients*, 19 mai 2016

13. Les Echos, *Aux États-Unis, le business juteux des données bancaires*, 19 mai 2016. Ce marché est aujourd'hui estimé à 1,7 milliard de dollars.

données intéresse toutefois tous les secteurs, y compris ceux n'appartenant pas à la sphère numérique et considérés comme les secteurs traditionnels<sup>11</sup>. Dans le secteur financier, les banques européennes commencent à développer des partenariats avec des start-ups agrégeant des données<sup>12</sup>, à l'instar de leurs consœurs américaines qui monétisent depuis plusieurs années les données relatives aux comportements d'achat de leurs clients auprès des grands magasins<sup>13</sup>. Une illustration pratique du rôle des données dans le secteur bancaire a d'ailleurs été récemment apportée par la Commission européenne, qui a annoncé en octobre 2017 la tenue d'opérations de visites et saisies concernant de potentielles restrictions à l'accès en ligne aux informations bancaires d'utilisateurs pour des fournisseurs de services financiers concurrents des banques traditionnelles<sup>14</sup>. De même, le secteur des télécoms utilise et croise historiquement les données de ses clients afin de prévoir leur comportement, et notamment leur fidélité<sup>15</sup>.

Les plateformes, dont l'activité repose sur le « *classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers; ou 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 service* »<sup>16</sup>, restent parmi les plus grosses consommatrices de données afin de proposer à leurs utilisateurs les services les plus appropriés à leurs besoins. C'est par exemple le cas d'Uber, qui fournit aux consommateurs une application leur permettant d'accéder à un service de transport rapide et fiable, en échange de données que ces derniers ou leurs téléphones lui envoient, et qu'elle peut ensuite céder aux VTC. De même, Google fournit un service gratuit aux internautes (moteur de recherche<sup>17</sup>, messagerie etc.) en échange de leurs données, qu'il revend ensuite à différents annonceurs. C'est enfin également le cas des réseaux sociaux, au premier rang desquels Facebook, qui fournit de nombreux services gratuits à ses utilisateurs en échange

de la collecte d'un certain nombre d'informations personnelles les concernant<sup>18</sup>. Ces entreprises sont ainsi situées sur des marchés bifaces : sur la première face, elles collectent des données fournies par leurs utilisateurs en échange d'un service, souvent gratuit ; sur la seconde, elle exploitent ces données auprès de clients professionnels, le plus souvent publicitaires. Le secteur de la publicité en ligne constitue ainsi l'un des secteurs dans lequel le rôle des données est particulièrement fondamental, justifiant ainsi la conduite d'une enquête sectorielle par l'Autorité.

### 1.1.2. L'utilisation des données dans l'économie

Si les données numériques ont toujours été utilisées par les entreprises dans le cadre de leurs activités commerciales, les évolutions technologiques de l'économie numérique ont eu pour conséquence une augmentation exponentielle des possibilités de collecte, traitement et utilisation commerciale de ces dernières dans tous les secteurs de l'économie. Dès lors, d'avantage que l'utilisation de données par les acteurs économiques, c'est la quantité d'informations utilisables et l'accès qu'y ont les différents acteurs qui

.....  
**14.** Communiqué de presse de la Commission européenne, 6 octobre 2017, « *Antitrust: Commission confirms unannounced inspections concerning online access to bank account information by competing services* ».  
 .....

**15.** Les Echos, *Les données, nouvel eldorado pour l'entreprise connectée*, 18 mai 2015: « *dans les telecom, c'est bluffant. Il se dit que le traitement croisé des données clients et des réseaux sociaux permet d'être sûr qu'un client va se désabonner dans les quinze jours* ».  
 .....

**16.** Loi pour une République Numérique, article 49, modifiant l'article L. 111-7 du code de la consommation.  
 .....

**17.** La Commission européenne a par ailleurs reconnu que Google occupait une position dominante sur les marchés de la recherche générale sur internet dans l'ensemble de l'Espace économique européen, Commission européenne, décision AT.39740, Google Search (Shopping), 27 juin 2017  
 .....

**18.** Autorité de la concurrence, Avis n°18-A-03, op. cit.  
 .....

**19.** Etude conjointe de l'Autorité de la Concurrence et du Bundeskartellamt, op. cit., p.10-12

suscitent aujourd’hui l’enthousiasme comme les interrogations.

Enthousiasme, car l’utilisation des données constitue un facteur d’innovation considérable pour les entreprises<sup>19</sup> :

- Amélioration des produits et services proposés : on peut évoquer le cas des moteurs de recherche sur Internet. L’augmentation du nombre de recherches, couplée à la possibilité d’observer les résultats sur lesquels l’utilisateur clique, permet au moteur de recherche utilisé d’améliorer et d’affiner ses résultats et le fonctionnement de son algorithme. Il effectue ainsi des recherches plus pointues, ce qui incite davantage de consommateurs à l’utiliser<sup>20</sup>.

- Exploitation de nouvelles opportunités commerciales : les données peuvent permettre le développement de marchés encore embryonnaires. Bruno Lasserre cite « *BlaBlaCar qui fait décoller le covoiturage, parce qu’Internet est un outil unique pour savoir qui va de telle ville à telle autre à quel moment* »<sup>21</sup>. Les entreprises peuvent également réemployer les données collectées à l’occasion de la fourniture d’un service en vue de proposer un autre service. C’est ainsi que les données de mobilité générées par les téléphones et GPS des automobilistes peuvent notamment être utilisées afin d’améliorer l’information sur le trafic et d’orienter les utilisateurs en fonction de l’encombrement.

- Amélioration des modèles économiques en fonction de leur cible : les données peuvent par exemple être exploitées pour mieux cibler les clients potentiels et leur fournir des messages publicitaires, services ou produits personnalisés. Les entreprises peuvent ainsi adapter leur stratégie publicitaire au public qu’elles ciblent réellement. De même, les données permettent de contrôler et de suivre le déroulement des campagnes publicitaires afin d’en apprécier l’efficacité en temps réel et d’en tirer les enseignements utiles pour les campagnes ultérieures. Enfin, les données peuvent permettre aux entreprises d’effectuer une meilleure discrimination par les prix, c’est-à-dire de moduler le prix de leurs biens ou services en fonction des caractéristiques connues de la demande et

d’atteindre une plus grande efficacité.

Comme le souligne la Commissaire européenne à la concurrence Margrethe Vestager, « *nous obtenons des avantages considérables lorsque nous partageons nos données, des outils incroyablement puissants (...) qui sont disponibles gratuitement (...) parce que nous, en tant que consommateurs, disposons d’une nouvelle monnaie que nous pouvons utiliser pour payer : nos données* »<sup>22</sup>. Certains économistes estiment ainsi que la valeur créée par l’identité personnelle constituerait près du quart de la croissance annuelle en Europe d’ici 2020.

S’il convient pour les autorités de ne pas freiner l’innovation, les données en tant que nouvel actif et donc possible vecteur de pouvoir de marché pour les entreprises qui les détiennent, soulèvent toutefois de nombreuses interrogations en matière de droit de la concurrence.

## 1.2. Les problématiques concurrentielles soulevées par la détention de données

La détention d’un grand volume de données peut-elle alors représenter un avantage concurrentiel durable pour les entreprises qui innovent en analysant les données ? Autrement dit, leur utilisation est-elle susceptible de constituer un privilège pour les premières entreprises qui les détiendraient, ou est-elle plutôt un vecteur de développement pour l’ensemble du marché ?

<sup>20</sup>. Communiqué de presse de la Commission européenne, « *Google has come up with many innovative products and services that have made a difference to our lives. That’s a good thing* », 27 juin 2017.

<sup>21</sup>. Entretien de Bruno Lasserre dans l’Opinion, 16 mars 2015

<sup>22</sup>. Discours de Margrethe Vestager, *Competition in a Big Data World*, 18 janvier 2016: « *we get major benefits from sharing our data (...) Incredibly powerful tools, like search engines and social media, are available for free. In many cases, that’s because we consumers have a new currency we can use to pay for them - our data* »

### 1.2.1. L'ampleur des données : une source d'inquiétude pour les autorités de régulation

La collecte des données personnelles fait l'objet d'une attention particulière, tant du point de vue de leur protection que de l'avantage concurrentiel et du pouvoir de marché qu'elles sont susceptibles de procurer. La frontière entre les règles relatives à la protection des données et le droit de la concurrence n'est à cet égard, pas toujours aisée à tracer. Du fait de l'inquiétude qu'elle suscite auprès des autorités, cette problématique a donné lieu à de nombreux travaux.

Concernant la question de la protection de la vie privée que soulève la collecte d'un nombre toujours croissant de données personnelles, l'Europe a choisi la voie d'un renforcement des règles avec l'adoption du Règlement général sur la protection des données le 27 avril 2016, entré en vigueur le 25 mai 2018<sup>23</sup>, et le projet de règlement dit « *e-privacy* » (pour la vie privée sur internet). Cette réglementation s'inscrit dans le prolongement de l'avis rendu par le Contrôleur Européen de la Protection des Données en septembre 2016, relatif à l'application des droits fondamentaux à l'ère des données massives (*Big Data*)<sup>24</sup> qui plaidait déjà pour un renforcement des mesures de protection des données devant aller de pair avec les possibilités qu'offrent ces dernières de stimuler la productivité.

Dans le cadre plus global de la stratégie du marché unique numérique, la Commission européenne a également lancé une enquête sur le commerce électronique le 6 mai 2015, dont le rapport final a été publié le 10 mai 2017<sup>25</sup>. Un règlement relatif aux pratiques de blocage géographique et aux plateformes numériques a également été adopté le 28 février 2018<sup>26</sup>.

Les autorités de concurrence nationales se sont également saisies de la problématique. La Competition and Markets Authority (CMA) anglaise a la première publié des rapports portant sur l'utilisation commerciale des données des consommateurs<sup>27</sup> ou les plateformes de comparaison de prix en ligne<sup>28</sup>. Suivant le mouvement, les autorités française

et allemande ont publié en mai 2016 l'étude conjointe précitée sur les données et leurs enjeux pour l'application du droit de la concurrence, concomitamment en France avec le lancement d'une enquête sectorielle sur l'exploitation des données dans le secteur de la publicité en ligne, dont les conclusions ont été publiées en mars 2018<sup>29</sup>. L'autorité allemande a par ailleurs lancé une enquête sur les pratiques de Facebook en mars 2016<sup>30</sup>, dont les conclusions viennent d'être publiées<sup>31</sup>, selon lesquelles Facebook a abusé de sa position dominante sur le marché des réseaux sociaux allemand en imposant à ses utilisateurs des conditions d'utilisation excessives liées à la collecte de données personnelles sur des sites tiers. L'autorité allemande a également publié plusieurs rapports ayant traités à la problématique des données<sup>32</sup>, et s'est engagée dans une réflexion plus globale portant sur la place de

.....  
23. Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

.....  
24. Avis 8/2016 du Contrôleur Européen de la protection des données sur *une application cohérente des droits fondamentaux à l'ère des données massives (Big Data)*, 23 septembre 2016

.....  
25. Commission européenne, *Final report on the e-commerce sector inquiry*, 10 mai 2017

.....  
26. Règlement (EU) n°2018/302 du 28 février 2018 visant à contrer le blocage géographique injustifié et d'autres formes de discrimination fondée sur la nationalité, le lieu de résidence ou le lieu d'établissement des clients dans le marché intérieur

.....  
27. Rapport de la Competition & Markets Authority, *The commercial use of consumer data*, juin 2015

.....  
28. Rapport de la Competition & Markets Authority, *Digital comparison tools market study*, 26 septembre 2017

.....  
29. Autorité de la concurrence, Avis n°18-A-03 op. cit.

.....  
30. Bundeskartellamt, *Preliminary Assessment in Facebook proceeding*, 19 décembre 2017

.....  
31. Bundeskartellamt, *Bundeskartellamt prohibits Facebook from combining user data from different sources*, 7 février 2019

.....  
32. Rapport du Bundeskartellamt, *The Market Power of Platforms and Networks*, 9 juin 2016 et Rapport du Bundeskartellamt, *Big data and Competition*, 6 octobre 2017

la concurrence et de la protection du consommateur dans l'économie digitale.

Au niveau européen enfin, le rapport des conseillers spéciaux au digital nommés en avril dernier par la Commissaire à la Concurrence, Margrethe Vestager, sur les futurs enjeux de la digitalisation pour le droit de la concurrence est attendu pour le 31 mars 2019. Dans la même lignée, la commissaire a organisé au mois de janvier 2019 une conférence spéciale pour débattre des principaux enjeux posés par la digitalisation, en amont de laquelle une consultation publique ayant recueilli près de 130 participations de la part de tous les acteurs du secteur a été organisée<sup>33</sup>.

Si les angles d'approche et les champs d'études sont parfois différents, c'est la même réalité que les autorités cherchent à appréhender : le pouvoir que peut conférer à certains leaders du marché la collecte massive de données.

### 1.2.2. La collecte massive de données, facteur d'une transparence accrue du marché

La collecte et l'utilisation des données augmentent la transparence du marché, ce qui permet aux consommateurs de comparer efficacement les prix et de faire jouer à plein la concurrence. Elle pourrait toutefois avoir pour corollaire de favoriser les collusions entre concurrents, qu'elles soient tacites (alignement spontané des acteurs sur les mêmes tarifs) et dans ce cas licites, ou explicites (mise en place de la politique de fixation des prix) et donc prohibées.

L'intérêt de la question est renforcé par le développement des algorithmes. Si la numérisation du commerce permet d'avoir accès en temps réel aux tarifs de tous les acteurs d'un marché, les algorithmes permettent quant à eux d'anticiper les comportements des concurrents face à une politique tarifaire et ainsi de mettre en place une politique « supra-concurrentielle ». La mise en place de politique de fixation tarifaire illicite n'en est que plus difficile à déceler, dans la mesure où les concurrents ne se rencontrent plus, mais utilisent parfois simplement les mêmes

algorithmes. Ces derniers pourraient ainsi servir de support à la réalisation d'ententes sans que l'on soit en présence d'une forme de collusion entre entreprises. La frontière entre l'alignement spontané et l'accord anticoncurrentiel illicite risque donc d'être de plus en plus difficile à établir pour les autorités de concurrence.

Cette question n'est pas théorique et a d'ores et déjà fait l'objet d'une affaire devant le Department of Justice américain, qui s'est saisi d'une entente sur les prix mise en œuvre par le biais d'algorithmes sur la marketplace d'Amazon. Selon le DOJ, « *afin de mettre en œuvre cet accord, Topkins et ses co-conspirateurs ont adopté des algorithmes tarifaires spécifiques pour la vente de certains posters afin de coordonner les évolutions de leurs prix respectifs et ont écrit un code informatique du logiciel basé sur l'algorithme afin qu'il fixe les prix conformément à cet accord* »<sup>34</sup>.

L'enjeu est donc de distinguer les effets bénéfiques de la transparence du marché pour les consommateurs, qui sont plus à même de comparer efficacement les offres, des effets néfastes que la transparence, lorsqu'elle est le résultat d'accords illicites, peut induire sur le comportement des concurrents, ces accords illicites étant désormais de plus en plus difficiles à identifier. À la lumière de ce débat, l'Autorité de la concurrence et le Bundeskartellamt ont lancé récemment un projet conjoint sur les algorithmes afin d'analyser les risques et les enjeux de l'utilisation de ces derniers au regard du droit de la concurrence<sup>35</sup>.

33. [http://ec.europa.eu/competition/scp19/media\\_en.html](http://ec.europa.eu/competition/scp19/media_en.html)

34. Le jugement du DoJ est accessible sur [www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/04/06/topkins\\_information.pdf](http://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/04/06/topkins_information.pdf)

35. Communiqué de presse de l'Autorité de la concurrence, l'Autorité de la concurrence française et le Bundeskartellamt allemand lancent un projet conjoint sur les algorithmes et leurs enjeux pour l'application du droit de la concurrence, 19 juin 2018

### 1.2.3. Des problématiques déjà partiellement abordées par les autorités de concurrence

Plusieurs décisions impliquant la problématique des données ont déjà été rendues par des autorités de concurrence, que ce soit dans le cas d'anciens monopoles historiques pour lesquels les bases de données ont pu être considérées comme des facilités essentielles<sup>36</sup>, ou dans le cas d'entreprises actives dans le secteur numérique. Il s'agit dans ce dernier cas essentiellement de décisions d'autorisation de concentrations rendues par la Commission européenne relatives par exemple au rachat de Skype par Microsoft<sup>37</sup>, de Whatsapp par Facebook<sup>38</sup> ou encore de DoubleClick par Google<sup>39</sup>.

Jusqu'à récemment, ces décisions n'avaient abordé que partiellement, et de manière superficielle, la question du pouvoir de marché que de larges bases de données sont susceptibles de conférer à des acteurs jouissant pourtant déjà de fortes parts de marché. En effet, en l'absence de chevauchement évident entre les activités de l'une et l'autre des parties à la concentration, l'analyse du risque anticoncurrentiel et du renforcement des parts de marché pouvait être moins aboutie qu'en présence de concurrents immédiats. À ce titre, la question du marché pertinent des données n'a jamais été examinée en tant que telle par les autorités de concurrence.

Néanmoins, l'autorisation sous conditions par la Commission européenne de l'opération de rachat de LinkedIn par Microsoft a été l'occasion pour cette dernière d'exprimer ses préoccupations quant aux effets potentiels sur la concurrence de la combinaison des données des deux acteurs, bien que les chevauchements d'activité soient mineurs<sup>40</sup>. La Commission y distingue deux situations, celle où les bases de données des parties ne peuvent être combinées, qui ne pose a priori aucune préoccupation de concurrence, et celle où cette combinaison est techniquement et commercialement possible. L'importance des données et leur lien avec un potentiel pouvoir de marché a par la suite de nouveau été pris

en compte par la Commission dans le cadre de son examen de l'acquisition de Shazam par Apple<sup>41</sup>.

La Commission européenne a par ailleurs rappelé en mai 2017 l'importance des données dans l'analyse concurrentielle en infligeant une amende à Facebook pour avoir fourni des informations inexactes ou dénaturées concernant les capacités de mise en correspondance automatisée entre les comptes utilisateurs Facebook et Whatsapp<sup>42</sup>. Comme l'a souligné la Commissaire Vestager, « *les données sont des éléments essentiels de l'économie numérique. C'est pourquoi nous devons soigneusement examiner les opérations qui débouchent sur l'acquisition de jeux de données importants, notamment de données potentiellement commercialement sensibles, afin de veiller à ce qu'elles ne restreignent pas la concurrence* »<sup>43</sup>. Au niveau français, l'Autorité de la concurrence tient également compte de manière croissante du rôle exercé par les données sur la concurrence au sein des marchés de services numériques. Dans la décision récente relative à l'acquisition de Concept Multimédia, éditrice du site Logic-Immo, par le groupe Axel Springer, l'Autorité a ainsi analysé les

.....  
**36.** Par exemple : Autorité de la concurrence, décisions n°14-MC-02 dans le secteur de l'énergie ou n°14-D-06 dans le secteur des bases de données médicales  
 .....

**37.** Commission européenne, décision COMP/M.6281, Microsoft/Skype, 7 octobre 2011  
 .....

**38.** Commission européenne, décision COMP/M.7217, Facebook/Whatsapp, 3 octobre 2014  
 .....

**39.** Commission européenne, décision COMP/M.4731, Google/DoubleClick, 11 mars 2008  
 .....

**40.** Commission européenne, décision COMP/M.8214, Microsoft/LinkedIn, 6 décembre 2016  
 .....

**41.** Commission européenne, décision COMP/M.8788, Apple/Shazam, 6 septembre 2018  
 .....

**42.** [http://europa.eu/rapid/press-release\\_IP-17-1369\\_en.htm](http://europa.eu/rapid/press-release_IP-17-1369_en.htm)  
 .....

**43.** [http://europa.eu/rapid/press-release\\_IP-18-5662\\_fr.htm](http://europa.eu/rapid/press-release_IP-18-5662_fr.htm)  
 .....

**44.** Autorité de la concurrence, décision n°18-DCC-18 du 1<sup>er</sup> février 2018 relative à la prise de contrôle exclusif de la société Concept Multimédia par le groupe Axel Springer.

risques d'éviction des concurrents sur les marchés des petites annonces en ligne liés à l'acquisition des données<sup>44</sup>.

Enfin, l'approfondissement de la place des données dans l'analyse concurrentielle se manifeste également dans le traitement des affaires contentieuses dans le secteur numérique. Ainsi, dans l'affaire Google Shopping de 2017, la Commission a tenu compte du rôle des données dans la définition des marchés pertinents ainsi que dans l'appréciation des barrières à l'entrée et à l'expansion sur le marché des services de recherche générale<sup>45</sup>. De même, l'Autorité française de la concurrence a annoncé suite à la publication de son avis sur le fonctionnement du marché de la publicité en ligne avoir ouvert plusieurs enquêtes contentieuses relatives notamment à l'utilisation des données dans le secteur de la publicité en ligne<sup>46</sup>. La décision récente du Bundeskartellamt sanctionnant un abus de position dominante de Facebook sur le marché allemand des réseaux sociaux du fait de l'utilisation des données personnelles de ses utilisateurs illustre également bien le dynamisme des autorités sur ces nouveaux sujets et leur intérêt quant au traitement des données, y compris en matière contentieuse.

#### 1.2.4. La collecte massive de données confère-t-elle un avantage concurrentiel durable ?

Certaines théories économiques ont pour leur part tendance à répondre par la négative. Selon une étude menée par deux professeurs de la London Business School et de la Sloan School of Management du MIT<sup>47</sup>, les données ne sont pas en tant que telles susceptibles de conférer un avantage concurrentiel durable. En effet, pour que leur collecte massive constitue un tel avantage, il faudrait selon l'analyse concurrentielle classique qu'elle soit inimitable, rare, profitable et non-substituable.

Or, une quantité extrêmement importante de données est constamment produite par des acteurs variés, au point que le volume de données double en moyenne tous les deux ans<sup>48</sup>. Les consommateurs laissent en permanence

de multiples empreintes de leurs besoins, comportements et préférences.

Les données sont de plus des biens non-rivaux, qui peuvent être collectés et utilisés par plusieurs acteurs à la fois, et dont la consommation ne réduit ni la disponibilité ni la valeur auprès des autres acteurs. Elles pourraient, selon les économistes précitées, être collectées par de nouveaux entrants sur les marchés du numérique, de la même façon que les acteurs aujourd'hui dominants l'ont fait lors de leur création. Ainsi, Uber, AirBnB ou encore Tinder ont construit progressivement leur base de données. Les acteurs qui n'en détiennent pas pourraient en outre acquérir des « *third party data* » auprès de data brokers spécialisés dans cette activité. L'Autorité de la concurrence définit ainsi dans son avis récemment publié sur la publicité en ligne les *data providers* comme des fournisseurs de données tierces qui vendent des données collectées sur des sites tiers telles que des données fondées sur des centres d'intérêt, des données géographiques ou sociodémographiques. Axiom, Exelate (Nielsen) ou Datalgix, par exemple, rassemblent et vendent des sets de données collectées sur des centaines de milliers d'utilisateurs. Les données constitueraient donc des biens reproductibles, ni rares ni inimitables. La question de l'intérêt et de la nécessité des données mérite par ailleurs d'être posée. Il ne suffit pas toujours de détenir une large base de données pour en tirer un avantage concurrentiel sur les autres entreprises du secteur. Dans son dernier rapport publié en octobre 2017, l'autorité allemande de concurrence (FCO) considère ainsi clairement que la possession d'une grande quantité de données ne soulève pas en

44. Commission européenne, décision AT. 39740 op. cit.

45. Autorité de la concurrence, Communiqué de presse du 11 janvier 2019, « l'Autorité de la concurrence annonce ses priorités pour l'année 2019 ».

46. Etude de Anja Lambrecht and Catherine E. Tucker, *Can big data protect a firm from competition?*, 18 décembre 2015

47. Rapport de BSA The Software Alliance, *What's the Big Deal with Data ?*, novembre 2015

48. Rapport du Bundeskartellamt, 6 octobre 2017, op. cit.

soi de problèmes de concurrence, sauf à démontrer non seulement que les données en cause ne sont pas accessibles aux concurrents, mais aussi que l'accès à ces données est nécessaire pour prospérer sur le marché<sup>49</sup>. Il s'agit, avant tout, de collecter les données utiles en provenance d'une grande variété de sources, de les agréger dans des bases exploitables et d'en tirer de justes conclusions quant à ses clients ou ses partenaires. Le principal défi rencontré par les entreprises du numérique pourrait ainsi ne pas être la détention de données en soi, mais la possibilité de les exploiter de façon productive : « *the more data you have, the more vital it is to ask smart questions* »<sup>50</sup>, dans la mesure où plus la base de données exploitée est importante, plus elle est susceptible de conforter n'importe quelle théorie<sup>51</sup>. Selon le Directeur des analyses économiques de Google<sup>52</sup>, la théorie selon laquelle les acteurs collectant le plus de données sont ceux qui réussissent le mieux est assez fautive. En effet, selon lui, d'une part les données collectées dans le cadre d'une analyse ont une valeur dégressive en ce qu'elles sont de moins en moins utiles à l'analyse. Google n'utiliserait ainsi, en réalité, jamais plus de 1% des données sur une recherche. D'autre part, il relève que les données ont une date de péremption, et que celles collectées il y a trois ans sont désormais quasi-inutiles.

Il existe ainsi de multiples exemples d'entreprises ayant émergé sans avoir accès aux données, dans des secteurs où les données ont historiquement une forte valeur ou dans des secteurs où elles sont moins utilisées. Ainsi, dans le secteur des télécommunications qui utilise depuis toujours de larges bases de données, un acteur comme WhatsApp a réussi à devenir un concurrent sérieux de Skype ou Facebook en offrant un produit susceptible de satisfaire les besoins des utilisateurs de réseaux sociaux. Dans un secteur historiquement peu consommateur de données, Uber a réussi à s'imposer de la même manière en améliorant la manière dont le produit était proposé aux consommateurs. De même, Tinder, l'application de rencontre en ligne dont le fonctionnement repose sur l'accès aux données de géolocalisation et

qui n'est efficace que si le nombre de ses utilisateurs est suffisamment important, ne s'est pas servi de bases de données massives, mais a préféré cibler des personnes clés au sein de groupes d'étudiants afin de développer son système au sein de ces groupes, puis de l'étendre. À l'inverse Google+, pourtant fort des données récoltées par la firme, n'a pas réussi à s'imposer comme un acteur robuste du secteur des réseaux sociaux. L'émergence de disrupteurs souvent rapidement considérés comme leaders sur leur marché dépendrait ainsi plus de la création de services innovants et d'une meilleure capacité à satisfaire la demande que de la détention de données.

L'Autorité de la concurrence nuance toutefois cette opinion : si toute entreprise peut en théorie acquérir des données auprès de data brokers, intermédiaires qui collectent, stockent et analysent des données pour le compte de tiers, cela peut s'avérer compliqué en pratique, notamment dans certains secteurs qui requièrent une quantité et une variété de données extrêmement élevées, pouvant constituer de véritables barrières à l'entrée pour de nouveaux concurrents<sup>53</sup>. La qualité des données collectées, qu'elles soient volontairement transmises par les utilisateurs dans des environnements «logués» ou déduites des comportements de ces derniers, peut également constituer un avantage concurrentiel significatif sur certains marchés, en particulier ceux liés à la publicité en ligne, entravant potentiellement l'émergence de nouveaux acteurs. Certaines entreprises cristallisent ainsi les craintes des autorités nationales et européenne : Google ou Facebook, par exemple, génèrent un volume, une qualité et une diversité de données

.....  
 50. Article de Julian Birkinshaw, *Drowning in numbers*, Deloitte institute of innovation and entrepreneurship, 2 novembre 2015  
 .....

51. Etude de Anja Lambrecht and Catherine E. Tucker, op. cit., p.10  
 .....

52. Intervention de Fabien Curtot Millet, Directeur des analyses économiques de Google, lors de la conférence «les données et la concurrence dans l'économie numérique» Paris, 8 mars 2016.  
 .....

53. Etude conjointe de l'Autorité de la Concurrence et du Bundeskartellamt, op. cit., p.12

difficilement reproductibles par leurs concurrents. En outre, ces deux entreprises disposent d'une taille unique d'inventaires publicitaires liée à leur forte popularité. Or, la combinaison de ces données et inventaires leur permet de disposer d'avantages concurrentiels uniques leur conférant la place de leaders sur de nombreux marchés liés à la publicité en ligne et utilisant les données<sup>54</sup>. Les régulateurs se veulent donc attentifs à ce que ces avantages ne leur permettent pas de restreindre l'accès à certaines données, de conclure des contrats d'exclusivité avec des tiers ou d'abuser de leur position dominante sur des marchés connexes. Bruno Lasserre observait à ce propos que « *désormais, nous sommes confrontés à des monopoles non pas nés du pouvoir des États, mais de l'agilité, de l'innovation, avec des investissements considérables et permanents, et qui bien souvent se revendiquent libertaires contre les États* »<sup>55</sup>.

Il est également patent de constater que dans la pratique, l'accès aux données détenues par les principaux géants du numérique constitue aujourd'hui l'une des préoccupations principales des différents acteurs du secteur<sup>56</sup>. La question de la qualification de certains jeux de données en tant que « *facilités essentielles* » apparaît dès lors de plus en plus présente au sein des débats. L'une des pistes de réponse envisagée par de nombreux experts du secteur consisterait en une analyse au cas par cas des comportements, en fonction notamment d'un ensemble de critères tels que les moyens de collecte des données, la propriété des données, le degré d'innovation sur le marché etc<sup>57</sup>.

Ainsi, l'analyse de la place des données en tant qu'avantage concurrentiel constitue à plusieurs titres, comme en témoignent le foisonnement de travaux sur le sujet, un défi plus que jamais d'actualité pour les autorités de concurrence.

## 2. Analyse de l'effet des données : les défis des autorités de concurrence

La définition du marché pertinent, pierre angulaire de l'analyse concurrentielle est la première difficulté à laquelle les autorités

de concurrence font face dans le secteur du numérique tant celui-ci présente des particularités (2.1). Ces spécificités posent ensuite la question de l'adaptation des outils et méthodes actuels à ces nouvelles problématiques (2.2).

### 2.1. La définition de marché

En matière contentieuse, la question du Big data est principalement appréhendée sous l'angle de l'abus de position dominante. Rappelons que la détention d'une position dominante, telle celle que semble posséder les entreprises visées par les enquêtes des autorités européennes, ne constitue pas *per se* une infraction au droit de la concurrence. Seul l'abus d'une telle position est en effet prohibé. L'abus de position dominante se caractérisant par la démonstration de pratiques abusives, liées ou permises par la détention d'une position dominante sur un marché défini, les autorités devront dans un premier temps s'atteler à la définition d'un marché pertinent. Or, l'économie numérique peut de ce point de vue donner du fil à retordre aux autorités.

Afin de tenter d'en donner une définition, il est nécessaire de distinguer les *data brokers*, pour lesquels les données constituent un bien offert, des entreprises pour lesquelles les données sont une ressource. Le marché de collecte des données n'est, en effet, un marché en soi que lorsque les données sont le bien qui s'échange entre offreurs et demandeurs. Cette situation ne concerne pas nécessairement des acteurs comme Google et Facebook, pour lesquels la donnée est plutôt un actif ou un avantage, dont le caractère essentiel ou non doit être démontré.

L'Autorité de la concurrence distingue en effet

<sup>54</sup>. Autorité de la concurrence, Avis n°18-A-03 op. cit.

<sup>55</sup>. Entretien de Bruno Lasserre dans l'Opinion, op. cit.

<sup>56</sup>. Contributions publiques dans le cadre de la Conférence «*Shaping competition policy in the era of digitisation*» op. cit.

<sup>57</sup>. Intervention d'Ariel Ezrachi, professeur de droit de la concurrence Université d'Oxford, conférence «*Shaping competition policy in the era of digitisation*» op. cit.

selon que l'entreprise tire ses données de son activité économique, auquel cas il s'agit d'autoconsommation, ou que les bénéfices sont directement tirés de la collecte des données et dans ce cas il est possible de définir un marché des données.

Si le marché des données numériques en tant que tel n'a encore jamais été défini par les autorités de concurrence, leur utilisation par différents secteurs a cependant été abordée de manière indirecte à de nombreuses reprises, notamment en dernier lieu dans l'avis rendu par l'Autorité de la concurrence concernant le secteur de la publicité en ligne. Dans cet avis, l'Autorité distingue ainsi certains services d'exploitation de données (*Data Analytics*), qu'il convient de différencier des services rendus par les plateformes aux internautes, permettant de collecter des données en échange d'un service rendu à titre gratuit dans différents secteurs, et des services publicitaires, utilisant les données collectées sans qu'il s'agisse pour autant du seul intrant créateur de valeur.

La définition du marché pertinent revêt en droit de la concurrence une importance particulière. En effet, une autorité de concurrence ne vient sanctionner une pratique que pour autant qu'elle a lieu sur un marché. L'Autorité doit ainsi définir le marché sur lequel le comportement intervient et appréhender l'état de la concurrence qui y règne.

De ce point de vue, certaines spécificités des marchés marqués par le numérique ont pu être identifiées. De nombreuses études relèvent notamment que les marchés en ligne sont généralement :

- des marchés bifaces voire multifaces : les entreprises opérant sur ce marché s'adressent à plusieurs groupes d'utilisateurs ou de consommateurs. Le caractère biface du marché est notamment présent dans le secteur des plateformes qui s'appuient sur deux marchés distincts. Ce secteur est également marqué par le fait que les entreprises fournissent très souvent un service apparemment gratuit aux utilisateurs sur une partie du marché. C'est par exemple le cas des moteurs de recherche

qui offrent gratuitement cette fonction aux utilisateurs, et sont financés par la publicité. Néanmoins, l'Autorité de la concurrence a rappelé dans son avis sur la publicité en ligne que le droit de la concurrence s'applique à l'ensemble des services fournis aux internautes, y compris lorsqu'ils apparaissent gratuits, dans la mesure où ces services sont offerts à titre gratuit aux internautes parce que leur fréquentation constitue un support de commercialisation auprès de professionnels ou d'annonceurs.

- Ces marchés sont caractérisés par les effets de réseau : la valeur du service fourni augmente plus que proportionnellement au nombre d'utilisateurs. Cet effet « *boule de neige* » n'est pas propre à l'économie numérique, mais il est particulièrement puissant lorsqu'il s'appuie sur une nouvelle technologie et contribue à la concentration du marché.

- Ces marchés fortement marqués par l'innovation font la part belle aux premiers arrivants, ce qu'on appelle également l'effet de « *winner takes all* ». L'évolution très rapide de l'innovation sur les marchés numériques implique qu'un « nouveau » marché est créé à chaque nouvelle vague d'innovation. Il a pu être constaté que bien souvent sur ces marchés le premier arrivé « *rafle la mise* » et bloque généralement l'arrivée de nouveaux entrants.

Comme le constate cependant l'étude franco-allemande précitée, le marché du numérique est également de plus en plus marqué par le phénomène du multi-homing (ou multi-hébergement) lorsque les consommateurs utilisent plusieurs prestataires pour obtenir un même type de service, notamment dans l'hypothèse où le service est fourni gratuitement, ce qui incite les consommateurs à multiplier les fournisseurs de services. Une telle situation est de nature à réduire le pouvoir de marché. Les autorités relèvent toutefois que la situation dans laquelle chaque utilisateur fait appel à plusieurs offreurs est en réalité plutôt rare, en raison des coûts de transferts liés par exemple à l'effet de réseau et au fait que le prestataire le plus utilisé est le plus à même de satisfaire le consommateur en personnalisant

son offre. Cependant, sur le marché des plateformes d'annonces immobilières, le rôle du multi-homing a été reconnu comme fondamental par l'Autorité de la concurrence dans le bilan concurrentiel de l'opération de rachat de Logic-immo par Seloger.com et a grandement contribué à son autorisation.

- Ces marchés se caractérisent enfin par une dynamique particulière en raison de la rapidité de gains à laquelle peut donner lieu l'innovation technologique.

## 2.2. L'adaptation des outils et des méthodes

### 2.2.1. Vers une évolution des règles de concurrence applicables ?

Les autorités françaises, allemande et européenne se sont longtemps accordées à dire que les règles gouvernant le droit de la concurrence étaient tout à fait adaptées dans leur principe au secteur des données numériques. Les notions d'abus de position dominante et d'entente anticoncurrentielle semblaient en effet suffisamment flexibles et malléables pour s'adapter à différents secteurs.

La commissaire européenne Margrethe Vestager considérait ainsi qu'il fallait remettre les marchés technologiques dans un contexte économique plus large, et que ces marchés n'étaient pas différents des autres, mais que ce qui différait était le rythme du changement<sup>58</sup>.

Or, à l'occasion de la conférence menée en janvier 2019 sur le secteur du digital, la commissaire européenne à la concurrence a semblé-t-il nuancé son propos en considérant que les préoccupations relatives aux données, aux plateformes en ligne et aux stratégies d'acquisition des grandes entreprises technologiques pourraient justifier l'introduction de nouvelles règles de concurrence. Dans son discours introductif, la Commissaire Vestager a ainsi souligné que le secteur de l'économie digitale pourrait nécessiter une adaptation des règles du droit de la concurrence via la réinterprétation des règles européennes actuelles, ou voire même par l'ajout de nouvelles règles dans le respect des traités et de l'innovation<sup>59</sup>.

Le directeur général de la Direction Générale de la Concurrence, Johannes Laitenberger, est également venu appuyer ce propos en considérant lors de son discours de clôture que l'application de certaines des théories, tests juridiques, méthodes d'analyse et procédures d'enquête existantes en droit européen de la concurrence devait être reconsidérée pour répondre au mieux aux nouveaux phénomènes constatés. Le directeur général a également envisagé un possible élargissement des pratiques entrant dans le champ du contrôle de la Commission européenne, voire la définition de nouveaux comportements prohibés. Tout en soulignant que le droit de la concurrence européen restait pertinent pour l'appréhension de tels phénomènes, il a néanmoins été reconnu que l'application de ce dernier à un tel secteur différait nécessairement de son application usuelle.

Cette évolution semble en cohérence avec les particularités des marchés du numérique et notamment leur rapidité d'évolution, leur technicité, et leur très forte sensibilité à l'innovation, qui justifient une adaptation des outils utilisés. En effet, la longueur des procédures contentieuses devant les autorités de concurrence est tout d'abord aujourd'hui en décalage avec l'évolution extrêmement rapide de ces secteurs. En effet, une procédure au fond devant l'autorité française dure en moyenne deux à trois ans. Devant la Commission européenne, la même procédure est susceptible d'être significativement plus longue, notamment dans certains dossiers complexes. Ainsi, plus de cinq ans d'enquête ont été nécessaires dans le cadre des pratiques d'abus de position dominante reprochées à Google. Or, sur des marchés qui évoluent rapidement, il est nécessaire pour préserver les conditions de concurrence d'agir au plus vite. L'ancien président de

58. Discours de Margrethe Vestager, *Competition in a Big Data World*, op. cit.

59. Discours d'ouverture de Margrethe Vestager : "We don't know if we should just reinterpret the rules we have already, or to what degree we should add new rules", Conférence "Shaping competition policy in the era of digitisation" op. cit.

l'Autorité française considérerait ainsi que cette dernière devait privilégier des modes d'intervention rapides et tournés vers les remèdes, car les interventions de fond risquaient d'arriver trop tard. Les mesures conservatoires et la mise en œuvre de procédure d'engagements permettent à ce titre de répondre plus rapidement aux préoccupations de concurrence. L'affaire Google Ads constitue à ce titre une excellente illustration de l'utilisation concrète par l'Autorité de la concurrence de mesures conservatoires dans le secteur du numérique<sup>60</sup>. Cette faculté devrait en outre être renforcée à la suite de l'adoption de la directive ECN+ permettant à l'Autorité d'imposer des mesures provisoires d'urgence d'office, y compris en l'absence de saisine par une entreprise.

En outre, il existe un décalage de compétences entre les autorités et les acteurs : les autorités de concurrence sont constituées de juristes et d'économistes. Cependant, elle doivent désormais traiter des dossiers dans lesquels il est question de produits d'une très grande complexité, conçus par des ingénieurs. À l'exception des cas de clémence, dans le cadre desquels une partie à un accord dénonce elle-même des pratiques anticoncurrentielles et fournit des éléments et explications techniques aux autorités, ces dernières doivent comprendre seules les enjeux des acteurs sur lesquels elles enquêtent. Les autorités de concurrence sont donc face à un défi technique qui justifie également une adaptation éventuelle des outils mis en œuvre.

L'intervention des autorités de concurrence dans ce secteur s'avère donc délicate, d'une part parce que le droit de la concurrence ne doit pas être instrumentalisé et utilisé à tort pour défendre la position des acteurs en place, dont la situation est remise en question par ces nouveaux modèles qui génèrent incontestablement des bénéfices économiques, et d'autre part car une intervention mal maîtrisée ou trop hâtive pourrait décourager l'innovation.

Cependant, un déficit d'intervention pourrait avoir des conséquences néfastes, non seulement parce que certains comportements

anticoncurrentiels resteraient impunis, mais également parce que le vide laissé par l'absence de régulation des autorités sectorielles pourrait conduire à une intervention législative accrue. Or, la régulation ex ante, à l'inverse de l'intervention au cas par cas des autorités de concurrence, place tous les acteurs d'un même secteur, petit ou gros face à la même réglementation. Une telle similitude de traitement dans un secteur où cohabitent des géants comme Facebook ou Google et de petites start-ups nationales pourrait avoir l'effet inverse de celui recherché.

Il est notable qu'alors que les autorités de concurrence sont restées pendant longtemps relativement prudentes sur le sujet, comme en témoigne la rareté des décisions et le foisonnement d'études sectorielles, une nouvelle dynamique semble s'instaurer avec notamment l'ouverture de procédures contentieuses par les autorités nationales françaises et allemandes.

### 2.2.2. Contrôle des concentrations : des seuils inadaptés

En dehors des procédures contentieuses visant à sanctionner des abus, le contrôle des concentrations est également un moyen de contrôle et de régulation des marchés. Les décisions de l'Autorité de concurrence relatives à des opérations de concentration sont en effet l'occasion pour cette dernière de définir les marchés en cause et d'apprécier les positions des acteurs.

Or, si l'OCDE relève que dans les secteurs liés aux données, « *le nombre des fusions et acquisitions (M&A) a rapidement augmenté de 55 opérations en 2008 à près de 164 en 2012* »<sup>61</sup>, seule une décision française est intervenue à ce jour dans le secteur digital<sup>62</sup>.

60. Autorité de la concurrence, décision 19-MC-01 du 31 janvier 2019 relative à une demande de mesures conservatoires de la société Amadeus.

61. Etude de l'OCDE, *Data-Driven Innovation: Big Data for Growth and Well-Being*, OECD Publishing, Paris (2015), p.94

62. La décision de l'Autorité de la concurrence n°18-DCC-18, *op. cit.*, a été l'occasion pour l'Autorité de se prononcer pour la première fois sur une concentration impliquant deux plateformes en ligne

L'explication tient notamment au fait que le secteur est fortement composé de start-ups à fort potentiel mais dont le chiffre d'affaires n'est pas toujours significatif. Les opérations de prise de contrôle de ces entreprises, dans la mesure où elles ne dépassent pas les seuils français relatifs au contrôle des concentrations, ne donnent pas lieu à examen par l'Autorité alors même que la valorisation de ces start-ups peut être particulièrement élevée malgré la faiblesse de leur chiffre d'affaires, comme l'illustre notamment le rachat par Facebook de Whatsapp pour 19 milliards de dollars.

Les seuils apparaissent donc de ce point de vue inadaptés au secteur comme le relevaient tant l'autorité française que l'autorité allemande dans leur étude conjointe, alors même que les seuils de chiffre d'affaires allemands sont beaucoup plus bas que les seuils français.

En Allemagne, le législateur a donc réagi à cette situation en introduisant dans la loi allemande contre les restrictions de concurrence (GWB) un nouveau critère alternatif et indépendant du chiffre d'affaires lié à la valeur de la transaction. Ainsi, à compter du 9 juin 2017, les concentrations sont devenues obligatoirement notifiables en Allemagne lorsque la valeur de la contrepartie obtenue par le vendeur dépasse 400 millions d'euros et que la cible exerce des activités significatives sur le territoire national<sup>63</sup>. Cette réforme est destinée à élargir le contrôle des concentrations allemand aux opérations mises en œuvre dans des secteurs innovants et pour lesquelles les chiffres d'affaires peuvent être faibles, tel qu'en particulier le secteur de l'économie numérique.

En France et en Europe, des consultations publiques ont également été lancées concernant les modalités du contrôle des concentrations, respectivement en octobre 2017 et 2016, et qui interrogeaient notamment sur l'opportunité d'introduire de nouveaux critères de contrôle non uniquement basés sur le chiffre d'affaires. Si l'instauration d'un nouveau seuil alternatif fondé sur la valeur de la transaction

a été envisagé, cette solution a définitivement été écartée par l'Autorité française<sup>64</sup> et semble peu probable au niveau européen au regard des réponses collectées lors de la consultation et publiées par la Commission<sup>65</sup>. En revanche, l'Autorité française n'écarte pas la possibilité d'un nouveau contrôle *ex-post* qui permettrait à l'Autorité de contrôler, à son initiative, un nombre limité d'opérations qui pourraient s'avérer problématiques, en particulier dans le secteur numérique.

Des modifications législatives sont donc vraisemblablement à prévoir afin de prendre en compte les spécificités de ce secteur. Reste à savoir quelle méthodologie sera appliquée, et si celle-ci passera par la création d'une exception sectorielle et ainsi de seuils spécifiques au secteur du numérique. Une telle option pourrait cependant s'avérer vite obsolète dans la mesure où désormais beaucoup de secteurs dont le cœur d'activité n'est pas digital sont impactés par la numérisation de l'économie.

.....  
 63. § 37, 1, de la loi allemande contre les restrictions de concurrence (GWB) tel qu'issu de la réforme du 31 mars 2017  
 .....

64. Communiqué de presse de l'Autorité de la concurrence, *Modernisation et simplification du contrôle des concentrations*, 7 juin 2018  
 .....

65. Summary of replies to the Public Consultation on Evaluation of procedural and jurisdictional aspects of EU merger control, juillet 2017

RÉGLEMENTAIRES

---

THÈME 9

# Jetons numériques : les ICO au Luxembourg

PRÉSENTATION GÉNÉRALE  
ET ENJEUX JURIDIQUES

# Le point de vue...



**Laurent Marochini,**  
**Président Groupe ALFI Digital/Fintech**  
**Blockchain & Crypto-currency - Association**  
**Luxembourgeoise de fonds d'investissement**

## Comment le Luxembourg se positionne sur les levées de fonds par ICOs?

L'innovation a toujours été un facteur clé de succès et de différenciation au sein de notre place financière. Avec plus de 4200 milliards d'euros d'actifs administrés (Nov 2018 - Alfi), le Luxembourg se positionne comme le premier centre d'investissement en Europe et le deuxième au monde derrière les États Unis. Le Luxembourg s'est rapidement positionné en 2014 sur les plateformes d'échange, et en a accueilli dans la foulée (Bitstamp et BitFlyer). La multiplication des cryptos actifs et le développement des ICO en 2016-17 comme levée de fonds alternatifs a suscité de nombreux questionnements dans l'industrie. Au sein de l'ALFI, nous avons créé dès 2016 un groupe dédié à la Blockchain – Crypto en charge de développer le niveau de connaissance de notre centre et d'initier des projets sur des technologies ciblées. Le LHoFT (Luxembourg House of Financial Technology) en collaboration avec Stellar a publié un rapport détaillé sur les risques et les opportunités des ICO. Alors que certains pays prônaient un nombre de règles visant à développer leur compétitivité sur ce sujet comme la France ou la Suisse, notre régulateur, la CSSF a plutôt adopté en Mars 2018 une attitude de mise en garde. Dans la lignée des avertissements émis par l'ESMA en Novembre 2017, la CSSF recommande aux investisseurs d'être prudents en décrivant les principaux risques sans remettre en cause le potentiel de la technologie sous-jacente – la blockchain.

## Quelles garanties offrent ces ICOs ? Quels sont leurs points forts mais également sur quels points les investisseurs doivent-ils être vigilant ?

Il faut reconnaître que les ICOs ont créé un écosystème permettant aux porteurs de projets de lever

des fonds, et ce, avec une rapidité sans précédent. C'est aujourd'hui tout un nouvel écosystème qui s'est créé avec de nouveaux risques qu'il convient d'apprivoiser.

Les ICO ont soufferts d'une mauvaise presse. Selon une étude du groupe Statist, cabinet de conseil américain, 80 % des ICO réalisées en 2017 ont été identifiées comme des scams. Le marché s'adresse donc à un public averti. Les risques sont nombreux comme celui du vol ou de la perte totale de la valeur. L'année 2018 a vu le record du nombre de hacks sur les plateformes. Le Luxembourg, ne fermant pas les portes, souhaite privilégier la qualité en s'assurant du respect des règles de protection en vigueur. La sécurité des investisseurs reste la priorité. Il ne faut pas confondre vitesse et précipitation.

## Les levées de fonds par ICO sont-ils davantage l'apanage des venture capitalists ?

Au cours des deux dernières années, les montants investis à travers les ICOs et celui des fonds de venture capitalists (VC) ont atteint des records sans précédents. À mon sens, les VC et les ICOs ne sont pas toujours en concurrence mais complémentaires. Alors que les ICOs visent un public large avec une documentation plus accessible et sans restriction géographiques, les fonds VC apportent souvent leur expertise dans les projets qu'ils financent et contribuent à leur développement. Les fonds VC ou même les crypto fonds investissent également dans les ICOs, dans le cadre d'une diversification ou d'une croyance sur un secteur ou une entreprise à haute valeur ajoutée.



Par **Laurent Massinon** et **Christina Nickel**

**E**n tant que praticiens du droit, nous observons l'omniprésence des levées de fonds en jetons numériques (*initial coin offerings* ou « **ICO** ») dans notre quotidien, lesquelles font l'objet d'intenses débats entre investisseurs, avocats et autorités de régulation. Toutefois, en l'absence d'un cadre juridique clair et précis qui y serait dédié au Luxembourg, l'ensemble des acteurs du marché doivent s'en remettre au régime juridique existant<sup>1</sup>.

Suite à la publication par l'Autorité européenne des marchés financiers (« **AEMF** ») d'un avertissement adressé aux investisseurs le 13 novembre 2017<sup>2</sup>, et d'une communication par l'Organisation internationale des commissions de valeurs (« **OICV** ») faisant état de certaines préoccupations liées aux ICO le 18 janvier 2018<sup>3</sup>, la Commission de surveillance du secteur financier luxembourgeoise (« **CSSF** ») a publié un « avertissement sur les ICO et *tokens* » le 14 mars 2018<sup>4</sup>.

Outre les autorités susvisées, l'Autorité fédérale de surveillance des marchés financiers suisse (« **FINMA** ») a publié un guide pratique sur les ICO, aussi intéressant qu'utile, pouvant servir de base à la création éventuelle d'un cadre juridique applicable aux ICO. Il convient également de remarquer qu'un certain nombre d'initiatives ont été prises en France et en Lituanie.

Après avoir pris connaissance des différents avertissements et avis traitant des ICO qui ont été publiés, la question du statut actuel des ICO au Luxembourg se pose clairement. Il convient également d'examiner les enjeux juridiques pertinents dans ce cadre.

Dans le présent article, nous nous efforçons de tracer les contours du concept d'ICO, notamment à travers sa définition (1) et les catégories de jetons (2). Il convient ensuite d'exposer la position des différentes autorités

de régulation susvisées en la matière (3) et enfin de relever les enjeux juridiques qui s'y rapportent (4).

### 1. Définition des ICO

Il convient de noter en premier lieu qu'une ICO est une forme de levée de fonds par appel au public destinée à financer le lancement de nouvelles monnaies virtuelles ou de nouveaux projets de toutes sortes. En contrepartie de sa contribution au financement, le participant reçoit des jetons numériques, communément appelés « *tokens* », émis par l'initiateur et qui peuvent, le cas échéant, attribuer certains droits à leurs détenteurs. Ces droits sont définis librement par l'initiateur et peuvent prendre différentes formes<sup>5 6</sup>. Cette nouvelle forme d'investissement échappe à tout cadre juridique dans la mesure où il faudrait reconnaître légalement des jetons (les *tokens*) et des monnaies qui n'ont pas d'existence juridique (1.1). Le projet d'ICO fait l'objet d'un processus de création spécifique mis en place dans un livre blanc (« *white paper* ») (1.2).

1. Veuillez noter que le projet de loi (7363) modifiant la loi du 1<sup>er</sup> août 2001 concernant la circulation des titres et autres instruments financiers a été votée le 14 février 2019 par la chambre des députés, modification législative qui entrera en vigueur 4 jours après sa publication au Mémorial. Nous n'aborderons pas cette modification législative qui irait au-delà de matière spécifique qui est traitée dans cette contribution. Néanmoins, le but de cette loi modificative est de prévoir que les titres pourront désormais être inscrits en compte et être transférés en ayant recours à des mécanismes d'enregistrement électroniques sécurisés, notamment fondés sur la technologie des registres ou grands livres distribués du type blockchain.

2. [https://www.esma.europa.eu/sites/default/files/library/esma50-157-829\\_ico\\_statement\\_investors.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf)

### 1.1. Fondements juridiques

Il n'existe à l'heure actuelle aucune réglementation spécifique et exhaustive applicable aux ICO, ni au niveau national, ni au niveau européen. Chaque ICO doit être envisagée et analysée au cas par cas<sup>7</sup>.

### 1.2. Mécanisme

Afin de réaliser une ICO, un livre blanc (ou « *white paper* ») doit être élaboré pour servir de document de base devant être publié par l'émetteur (l'« **Émetteur** »). Ce livre blanc peut, le cas échéant, être accompagné d'une synthèse ou « *executive summary* ». Le livre blanc décrit les informations pertinentes relatives à l'ICO, telles que les conditions générales de l'offre, le projet donnant lieu à la levée de fonds, la durée de l'offre, le mécanisme de souscription et d'émission des jetons, ainsi que les droits et obligations attachés aux jetons émis. Dans certains cas, le livre blanc est susceptible d'être qualifié, sur le plan juridique, de prospectus en vue d'une offre au public de valeurs mobilières<sup>8</sup>.

À l'expiration de la durée de l'offre, les jetons sont créés et distribués aux participants. Ces jetons peuvent être conservés dans des porte-monnaie électroniques (« *electronic wallets* ») et être structurés de manière à permettre leur négociation sur des plateformes spécialisées. Certains jetons donnent droit à une prestation de service, tandis que d'autres sont structurés de manière à créer des droits proches de ceux attachés à des actions de sociétés<sup>9</sup>.

## 2. Catégories de jetons

Il existe plusieurs catégories de jetons, dont les caractéristiques sont les suivantes :

- *les jetons de paiement/crypto-monnaies* ont vocation à être utilisés, aujourd'hui ou à l'avenir, comme moyen de paiement pour l'achat de marchandises ou de services, ou pour servir à la transmission de fonds et de valeurs, ne conférant aucun droit à l'égard de leur Émetteur ;
- *les jetons d'utilité* ont vocation à fournir un accès numérique à une application ou à un

service et s'appuient sur l'utilisation d'une infrastructure de type blockchain ;

- *les jetons d'investissement* représentent des valeurs patrimoniales telles que des créances ou droits patrimoniaux détenus à l'encontre de l'Émetteur ou la promesse, par exemple, d'une part des revenus futurs d'une entreprise ou des flux de capitaux futurs. Ils sont comparables à des titres de participation, à des titres de créances ou à des produits financiers dérivés et permettent la négociation d'actifs corporels sur la blockchain ;
- *les jetons hybrides* sont à la fois des valeurs mobilières et des moyens de paiement<sup>10</sup>.

## 3. Avis des autorités de régulation

Ces dernières années, les autorités en charge de la régulation des activités financières dans différents pays réagissent au développement du phénomène des *initial coin offerings* (ICO) et analysent, de concert avec les autorités politiques desdits pays, des pistes de régulation de ces levées de fonds en jetons numériques. Différents acteurs de la sphère financière tentent progressivement d'appréhender les ICO : AEMF (3.1), OICV (3.2), CSSF (3.3), FINMA (3.4), AMF (3.5) et ministre des Finances lituanien (3.6)

### 3.1. AEMF

Le 13 novembre 2017, l'AEMF a publié une déclaration à l'intention des investisseurs

3. <http://www.iosco.org/news/pdf/IOSCONEWS485.pdf>.

4. [http://www.cssf.lu/fileadmin/files/Protection\\_consommateurs/Avertissements/A\\_ICOS\\_140318.pdf](http://www.cssf.lu/fileadmin/files/Protection_consommateurs/Avertissements/A_ICOS_140318.pdf)

5. CSSF – Avertissement sur les ICO et tokens [Warning on ICOs and tokens], 14 mars 2018, p. 1.

6. G. Kolifraith et Jérôme Blanchet, Blockchain : Les enjeux en droit suisse, *Revue internationale des services financiers/International Journal for Financial Services*, p. 27.

7. CSSF – Avertissement sur les ICO et tokens, 14 mars 2018, p. 1.

rappelant que les ICO constituent des placements à haut risque, soulignant le risque lié à l'existence d'un vide juridique, propice à la fraude et aux activités illégales, le risque de perdre la totalité du capital investi, les opportunités de revente réduites, la volatilité extrême des prix, l'opacité et les carences technologiques<sup>11</sup>.

Suite à la déclaration susmentionnée de novembre 2017, l'AEMF a publié le 9 janvier 2019 son avis sur les ICO et les crypto-actifs, résumant ses observations sur l'évolution des ICO et ses évaluations de la pertinence du cadre réglementaire actuel à cet égard<sup>12</sup>. Tout en rappelant que les ICO pourraient fournir des alternatives utiles à la source de financement pour les start-ups et autres entreprises innovantes et que les ICO fournissent des moyens rapides et efficaces de lever des fonds auprès d'une base d'investisseurs diversifiée si les garanties pertinentes sont en place, elle rappelle néanmoins qu'il est important de surveiller les risques macro-financiers potentiels qui peuvent être liés aux crypto-actifs. En outre, l'AEMF examine la qualification juridique des crypto-actifs au regard des implications réglementaires lorsque ils sont qualifiés d'instruments financiers.

### 3.2. OICV

Le 18 janvier 2018, l'OICV a publié une communication détaillant certaines préoccupations liées aux ICO, rappelant aux investisseurs que les ICO constituent des investissements hautement spéculatifs dans lesquels ces derniers risquent la totalité de leur capital investi sans bénéficier de toute la protection qui leur est due, et qu'ils s'exposent à des cas de fraude<sup>13</sup>.

### 3.3. CSSF

#### 3.3.1. « Avertissement sur les ICO et tokens » publié par la CSSF<sup>14</sup>

Le 14 mars 2018, la CSSF a publié un « avertissement sur les ICO et *tokens* ». Elle indique que les ICO ne sont soumises à aucune réglementation spécifique et ne procurent aucune garantie

ou autre forme de protection des investisseurs. La CSSF estime que ces caractéristiques sont susceptibles d'attirer des criminels souhaitant utiliser les ICO comme instruments dans le cadre d'opérations de blanchiment d'argent ou de financement du terrorisme, ou afin de contourner la réglementation existante.

Elle rappelle aux investisseurs que les ICO sont liées à des investissements hautement spéculatifs comportant un certain nombre de risques, y compris la perte totale de l'investissement. La CSSF souligne que la technologie sous-jacente à ces ICO, la blockchain, peut présenter certains avantages lorsqu'elle est utilisée dans le cadre d'activités du secteur financier, et que cet avertissement porte sur les levées de fonds

.....  
8. *Ibid.*

.....  
9. *Id.*, p. 2.

.....  
10. Guide pratique pour les questions d'assujettissement concernant les levées de fonds en crypto-monnaies (ICO) [*Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICO)*] – FINMA, p. 3 ; Comprendre les levées de fonds en crypto-monnaies : technologies, avantages, risques et réglementations [*Understanding Initial Coin Offerings : Technology, Benefits, Risks and Regulations*], Stellar Development Foundation & The Luxembourg House of Financial Technology, White paper, p. 29 (<https://www.stellar.org/blog/understanding-initial-coin-offerings/>).

.....  
11. Déclaration – Avertissement de l'AEMF à l'intention des investisseurs sur les risques élevés liés aux levées de fonds en crypto-monnaies (ICO) [*Statement – ESMA alerts investors to the high risks of Initial Coin Offerings (ICOs)*], p. 1-2 ([https://www.esma.europa.eu/sites/default/files/library/esma50-157-829\\_ico\\_statement\\_investors.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-829_ico_statement_investors.pdf)).

.....  
12. Avis de l'AEMF [Advice - Initial Coin Offerings and Crypto-Assets], p. 7, 17, 18. ([https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391\\_crypto\\_advice.pdf](https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf)).

.....  
13. Communication de l'OICV sur les préoccupations relatives aux levées de fonds en crypto-monnaies (ICO) [*IOSCO Board Communication on Concerns related to Initial Coin Offerings (ICOS)*], p. 1 (<https://www.iosco.org/news/pdf/IOSCONEWS485.pdf>).

.....  
14. CSSF – Avertissement sur les ICO et *tokens*, 14 mars 2018, p. 2-3.

.....  
15. CSSF – Avertissement sur les ICO et *tokens*, 14 mars 2018, p. 4.

réalisées par le biais des ICO qui utilisent cette technologie sans pour autant remettre en question la technologie elle-même.

Il s'avère néanmoins que les technologies permettant la création, le transfert et la conservation des jetons sont à la fois innovantes et exposées aux tentatives de piratages et autres problèmes informatiques. En conséquence, les investisseurs sont exposés à des risques d'indisponibilité, de vol, de saisie ou de confiscation des jetons.

La CSSF indique en outre que les projets financés par les ICO sont généralement à un stade précoce de développement, de sorte qu'il n'existe aucune garantie que les projets pourront être réalisés ou connaître le succès espéré et ainsi générer une valeur quelconque.

Elle rappelle également aux investisseurs que le capital investi dans le financement lui-même ou dans les jetons générés à travers des marchés secondaires n'est pas garanti. Par conséquent, le capital investi peut être partiellement ou totalement perdu, selon l'évolution des marchés, et les droits attachés aux jetons pourront se révéler sans valeur ultérieure si l'Émetteur n'a pas été en mesure de remplir ses obligations contractuelles à la suite de la levée de fonds.

Les récents importants mouvements à la hausse des cours d'un certain nombre de monnaies virtuelles ont pu laisser penser à certains investisseurs que la valeur de leur portefeuille pourrait de nouveau connaître une croissance exponentielle, tout en oubliant les risques qui y étaient liés.

La CSSF indique enfin que le manque de transparence et de réglementation peut entraîner un risque de manipulation des prix.

### 3.3.2. Recommandation de la CSSF<sup>15</sup>

La CSSF conseille aux investisseurs de s'assurer qu'ils ont entièrement compris les risques liés aux ICO, et notamment aux différents projets sous-jacents, ainsi que les rendements de leur investissement, avant d'effectuer un investissement quelconque. Elle leur conseille en outre de vérifier la fiabilité des informations

fournies au sujet de l'Émetteur, ainsi que de tout agrément prétendument accordé au Luxembourg ou à l'étranger. Toutefois, dans certains cas, l'Émetteur peut être soumis à certaines dispositions légales luxembourgeoises de la loi du 10 juillet 2005 relative au prospectus pour valeurs mobilières, dans sa dernière version (la « **loi Prospectus** ») ou de la loi du 5 avril 1993 relative au secteur financier, dans sa dernière version (la « **LSF** »).

### 3.4. FINMA

Le 16 février 2018, la FINMA a publié un guide pratique pour les questions concernant le cadre réglementaire des ICO<sup>16</sup>.

La FINMA souligne le fait que de nombreux acteurs du marché ont besoin de réponses à leurs questions relatives à l'applicabilité du droit régissant les marchés financiers aux ICO et à l'existence d'obligations d'autorisation. La FINMA explique ainsi que, lorsque l'Émetteur et l'investisseur ont défini le type de jetons qu'ils souhaitent émettre ou dans lesquels ils souhaitent investir, il convient ensuite de vérifier si les jetons peuvent être qualifiés de valeurs mobilières<sup>17</sup>.

Par ailleurs, la FINMA opère une distinction entre les différents types de jetons, comme indiqué plus haut, avant d'aller plus loin et d'envisager les cas où les jetons doivent être considérés comme des valeurs mobilières.

La FINMA considère que les jetons de paiement, ne présentant aucune analogie avec les valeurs mobilières traditionnelles dans leur fonctionnement, ne doivent pas être aveuglément qualifiés dans leur ensemble de valeurs mobilières, à moins que la jurisprudence et

<sup>16</sup>. <https://www.finma.ch/fr/news/2018/02/20180216-mm-icowegleitung/>

<sup>17</sup>. Guide pratique pour les questions d'assujettissement concernant les *initial coin offerings* (ICO) – FINMA, p. 1.

<sup>18</sup>. La FINMA adapterait sa pratique si la jurisprudence ou le législateur prévoyaient notamment à l'avenir une qualification de jetons de paiement comme valeurs mobilières. *Id.*, p. 4.

la législation ne se rangent à cet avis<sup>18</sup>. En ce qui concerne les jetons d'utilité, la FINMA ne les qualifie pas de valeurs mobilières s'ils ont pour seul objet de conférer un droit d'accès à une application ou à un service numérique, et si le jeton d'utilité est utilisable de la sorte à sa date d'émission. La fonction sous-jacente est de conférer ce droit d'accès et le lien avec les marchés de capitaux fait défaut, alors qu'il s'agit d'une caractéristique essentielle des valeurs mobilières. Les jetons d'investissement sont traités par la FINMA comme des valeurs mobilières s'ils représentent un droit-valeur et si les jetons sont standardisés et susceptibles d'être diffusés en grand nombre sur le marché<sup>19</sup>. Si des jetons sont qualifiés de valeurs mobilières, la réglementation relative aux valeurs mobilières pourra leur être applicable, tandis que s'ils sont considérés semblables à des titres de capitaux propres ou à des obligations, les exigences relatives au prospectus pourront leur être applicables.

La FINMA indique en outre que les jetons peuvent être qualifiés de dépôts. L'émission de jetons n'est habituellement pas associée à des demandes de remboursement envers l'organisateur de l'ICO et ces jetons n'entrent donc pas dans la définition du dépôt. En ce sens, il n'y a donc pas besoin d'obtenir un agrément bancaire. S'il existe en revanche des engagements ayant un caractère de capital d'emprunt, les fonds collectés sont traités comme des dépôts et il est alors nécessaire d'obtenir un agrément bancaire.

### 3.5. Autorité des marchés financiers (« AMF »)

Du fait que les ICO ne se rattachent à aucune qualification juridique française, l'Autorité des marchés financiers est dans l'obligation d'en trouver une nouvelle, sans pour autant risquer une surprotection des investisseurs et un effondrement du marché.

La France envisage d'ajouter une nouvelle disposition intitulée « Intermédiaires en biens divers et émetteurs de jetons »<sup>20</sup> à son Code monétaire et financier. Un nouveau Chapitre 2

(« Émetteur de jetons ») détaillera les règles applicables aux ICO. L'approche française diffère de l'approche suisse décrite ci-dessus en ce qu'elle crée de nouvelles dispositions spécifiques aux ICO alors que la Suisse tente de rendre son arsenal existant applicable aux ICO.

### 3.6. Ministre des Finances lituanien

Le ministre des Finances lituanien a fait publier, le 6 juin 2018, des principes directeurs concernant les ICO<sup>21</sup>. Cette publication précise les conditions dans lesquelles des jetons cryptographiques peuvent être considérés comme des valeurs mobilières et les lois nationales applicables à la vente de jetons. L'objectif de cette réglementation est d'atteindre une plus grande transparence ainsi qu'une plus grande sécurité juridique. Elle tient compte des enjeux fiscaux et comptables et prévoit des dispositions relatives au blanchiment d'argent.

## 4. Enjeux juridiques

Le Luxembourg n'ayant publié aucun principe directeur ni formulé de proposition visant à encadrer les ICO, il est éminemment important de s'attarder sur une multitude d'enjeux juridiques. Les considérations juridiques pertinentes s'apprécient au cas par cas pour chaque ICO, ce qui peut poser problème. C'est la raison pour laquelle il faut faire preuve d'une grande vigilance, au plan juridique. Les sujets listés ci-dessous pourraient constituer les jalons d'une analyse réglementaire des jetons sous-jacents à une ICO au Luxembourg. Nous recommandons, en particulier, de débiter l'analyse en déterminant si un jeton peut être considéré comme un jeton « ordinaire » ou plutôt comme un jeton « valeur mobilière » (4.1). Nous devons

19. Guide pratique pour les questions d'assujettissement concernant les *initial coin offerings* (ICO) – FINMA, p. 3.

20. [http://www2.assemblee-nationale.fr/documents/notice/15/projets/pl1088/\(index\)/projets-loi](http://www2.assemblee-nationale.fr/documents/notice/15/projets/pl1088/(index)/projets-loi)

21. <http://finmin.lrv.lt/uploads/finmin/documents/files/ICO%20Guidelines%20Lithuania.pdf>

ici également garder à l'esprit tout projet éventuel d'établir des plateformes dédiées aux ICO, dans la mesure où un tel projet peut impliquer que d'autres obligations légales soient étudiées. Après l'analyse du régime prospectus, il convient de déterminer les autorisations requises (4.2). En outre, les opérations doivent être menées conformément aux dispositifs d'anti-blanchiment (4.3), de la protection des données (4.4) et du droit de la consommation (4.5). Afin de procéder à l'analyse juridique, il convient notamment de suivre les étapes décrites ci-dessous.

#### 4.1. Régime prospectus

Eu égard au régime prospectus, il faut tenir compte du fait que le mécanisme de participation et la transférabilité par voie de cession de jeton sans le consentement de l'Émetteur ou de tout détenteur de jeton pourraient être perçus comme caractéristiques des valeurs mobilières<sup>22</sup>. Lorsque la préparation de l'ICO se fait sur plusieurs territoires, certaines des autorités de régulation de ces pays peuvent ne pas qualifier l'instrument de valeur mobilière. Néanmoins, du point de vue du droit luxembourgeois et lorsque le jeton n'entre dans aucune catégorie juridique connue, il ne peut être exclu qu'il puisse être qualifié de valeur mobilière après une analyse minutieuse et approfondie. À ce stade de l'analyse, il est déconseillé d'adopter une position trop générale ou trop hâtive, dans la mesure où, s'il existe une possibilité que le jeton soit considéré comme une valeur mobilière, une offre publique de valeurs mobilières pourrait être déclenchée et un prospectus devrait être approuvé par la CSSF ou transmis vers le Luxembourg *via* le mécanisme du « pas-seport » en l'absence d'exemption applicable.

#### 4.2. Autorisations requises

Il convient également de déterminer si l'Émetteur doit obtenir certaines autorisations au titre de l'ICO et du jeton sous-jacent. Les autorisations suivantes doivent être envisagées afin d'être certain que ce n'est pas le cas. Les mécanismes d'autorisation diffèrent selon le

statut de l'Émetteur, c'est-à-dire selon qu'il est un établissement de crédit (4.2.1), un établissement de paiement (4.2.2), une entreprise d'investissement (4.2.3), un gestionnaire de fonds d'investissement (4.2.4) ou un professionnel du secteur financier (4.2.5). Les règles diffèrent également selon le type d'instrument, comme nous le verrons avec ceux constituant une obligation perpétuelle (4.2.6).

##### 4.2.1. Établissement de crédit

En vertu de la LSF, un établissement de crédit désigne une personne juridique dont l'activité consiste à recevoir du public des dépôts ou d'autres fonds remboursables et à octroyer des crédits pour son propre compte<sup>23</sup>. Aucune personne de droit luxembourgeois ne peut exercer l'activité d'établissement de crédit sans être en possession d'un agrément écrit du ministre des Finances<sup>24</sup>.

En outre, seul un établissement de crédit, dont l'activité comprend l'octroi de crédits pour son propre compte, peut exercer l'activité de réception de dépôts ou d'autres fonds remboursables du public<sup>25</sup>. Il existe donc un fort monopole bancaire. Avant l'entrée en vigueur de la directive 2013/36/UE<sup>26</sup> du Parlement européen et du Conseil du 26 juin 2013

22. Veuillez noter qu'en vertu de l'article 2 (1) (w) de la loi Prospectus, les « valeurs mobilières » sont définies comme des catégories de titres négociables sur le marché des capitaux (à l'exception des instruments de paiement), telles que : (I) les actions de sociétés et tous autres titres équivalents à des actions de sociétés de capitaux, de sociétés de personnes ou d'autres entités, ainsi que les certificats représentatifs d'actions ; (II) les obligations et les autres titres de créance, y compris les certificats représentatifs de tels titres ; (III) toute autre valeur donnant le droit d'acquiescer ou de vendre de telles valeurs ou donnant lieu à un règlement en espèces, fixé par référence à des valeurs mobilières, à une monnaie, à un taux d'intérêt ou rendement, aux matières premières ou à d'autres indices ou mesures.

23. Article 1 (12) de la LSF.

24. Article 2 (1) de la LSF.

25. Article 2 (3) de la LSF.

26. <https://eur-lex.europa.eu/legal-content/EN-FR/TXT/?uri=CELEX:32013L0036&from=EN>

concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement (« **CRD IV** »), les directives européennes précédentes ne prohibaient l'activité de réception de dépôts ou d'autres fonds remboursables du public que dans un cadre professionnel. Suite à la CRD IV, une seule opération de réception de dépôts ou d'autres fonds remboursables du public tombe à présent dans le périmètre du monopole bancaire. Au vu de ce qui précède, il convient d'évaluer la portée des notions de « réception de dépôts » et « d'autres fonds remboursables ».

### A. (1) Réception de dépôts<sup>27</sup>

L'avis du 27 novembre 2014 de l'Autorité bancaire européenne (« **ABE** ») sur les questions relatives au périmètre des établissements de crédit (« **Avis de l'ABE** »)<sup>28</sup> apporte des lumières quant à l'expression « réception de dépôts » et précise qu'elle comprend les éléments essentiels suivants :

- une somme d'argent ;
- remboursable sur demande ou à une date convenue contractuellement (sinon, le remboursement du principal n'est soumis à aucune condition) avec ou sans intérêts ou primes ;
- reçue de la part de personnes morales ou physiques tierces ; et
- reçue au cours de l'exercice de l'activité à des fins professionnelles, et soumise à un certain nombre d'exclusions (par exemple, les sommes d'argent se rapportant à la fourniture de biens ou services<sup>29</sup> ou la constitution de sûretés pourraient être exclues du champ de la définition).

Lorsqu'il n'y a pas lieu de considérer l'instrument comme un dépôt, l'analyse se poursuit par l'examen de la notion d'autres fonds remboursables.

### B. (2) Autres fonds remboursables<sup>30</sup>

Selon l'Avis de l'ABE, la notion d'« autres fonds remboursables » pourrait être définie comme désignant notamment les obligations et autres valeurs mobilières comparables, dont les certificats de dépôt négociables, à condition qu'ils

soient émis continuellement par l'entité concernée. Dans son rapport du 27 novembre 2014 à la Commission européenne sur le périmètre des établissements de crédit établis dans des États membres (« Rapport de l'ABE »)<sup>31</sup>, l'ABE fait clairement référence aux conclusions de la Cour de justice en date du 11 février 1999 dans l'affaire C-366/97 (arrêt Romanelli) dans lesquelles la Cour a estimé que l'expression « autres fonds remboursables » vise non seulement les instruments financiers possédant la caractéristique intrinsèque d'être remboursables, mais également ceux qui, bien que ne possédant pas cette caractéristique, font l'objet d'un accord contractuel prévoyant le remboursement des fonds versés<sup>32</sup>. En l'espèce, il est possible que l'instrument entre dans le champ de la définition de la notion « autres fonds remboursables » si cet instrument ne relève d'aucune qualification juridique existante en soi et s'il prévoit un mécanisme contractuel de remboursement des fonds.

### 4.2.2. Établissement de paiement

Pour l'étape suivante, il convient d'examiner s'il existe un quelconque problème éventuel susceptible de découler de l'obtention d'une autorisation requise pour exercer en qualité d'établissement de paiement. Dans un tel cas, il faudra respecter toutes les exigences légales en rapport avec la directive (UE) 2015/2366 concernant les services de paiement et avec la loi du 10 novembre 2009

27. Avis de l'ABE, p. 3.

28. [https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-12+\(Opinion+on+perimeter+of+credit+institution\).pdf](https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-12+(Opinion+on+perimeter+of+credit+institution).pdf) [traduction libre en français]

29. Par exemple, les avances versées en vertu d'un contrat de vente, de location ou d'une autre forme de fourniture de biens ou de services qui ne sont remboursables que dans le cas où la vente, la location ou l'autre forme de fourniture du bien ou service concerné n'a pas lieu.

30. Avis de l'ABE, p. 3.

31. <https://www.eba.europa.eu/documents/10180/534414/2014+11+27+-+EBA+Report+-+Credit+institutions.pdf>

32. Rapport de l'ABE, p. 10.

relative aux services de paiement, dans sa dernière version. Néanmoins, du moment qu'aucun service de paiement n'est fourni au Luxembourg, cette étape ne devrait soulever aucun problème pour l'Émetteur.

#### 4.2.3. Entreprise d'investissement

Lorsque l'instrument devant être émis peut être considéré comme une valeur mobilière ou, plus généralement, comme un instrument financier, son processus de création, de distribution et de négociation pourrait impliquer des activités/services relatifs à la directive 2014/65/UE du Parlement européen et du Conseil du 15 mai 2014 concernant les marchés d'instruments financiers (« MiFID II »), telle que mise en œuvre au Luxembourg par le biais de la loi du 30 mai 2018 relative aux marchés d'instruments financiers, c'est-à-dire le placement, la négociation ou le conseil en matière d'instruments financiers. Lorsque l'Émetteur envisage de mettre en place une plateforme dédiée aux ICO, une vérification du périmètre des services devant être fournie en vertu des contrats respectifs devra être effectuée.

#### 4.2.4. Fonds d'investissement : AIFM

Il convient également de vérifier si un quelconque problème pourrait survenir du point de vue des fonds d'investissement, eu égard à la directive 2011/61/UE du Parlement européen et du Conseil du 8 juin 2011 sur les gestionnaires de fonds d'investissement alternatifs (« AIFM ») telle que transposée en droit luxembourgeois par la loi du 12 juillet 2013 sur les gestionnaires de fonds d'investissement alternatifs, telle que modifiée. Le résultat de cette analyse pourrait (I) dans le meilleur des cas, n'entraîner aucune conséquence, (II) conduire à une simple déclaration auprès de la CSSF en fonction de certains seuils, ou (III) aboutir à l'obligation d'obtenir une autorisation en tant que gestionnaire de fonds d'investissement alternatifs.

#### 4.2.5. Professionnels du secteur financier accordant des prêts

Enfin, il convient de vérifier si l'obtention d'une autorisation pour agir en qualité de professionnel du secteur financier accordant des prêts

doit être envisagée et en particulier d'analyser l'utilisation des produits, c'est-à-dire si des prêts sont accordés à titre professionnel.

#### 4.2.6. Instrument constituant une obligation perpétuelle<sup>33</sup>

Lorsque les principales caractéristiques de l'instrument indiquent que l'instrument peut être émis pour une période indéfinie, il convient de noter que cet instrument constituant une obligation perpétuelle peut ne pas être valable en application du droit luxembourgeois, dans la mesure où il peut être considéré comme contraire à l'ordre public international luxembourgeois. Afin de lever toute ambiguïté, ce point doit être clarifié et, par conséquent, l'octroi à chaque partie (Émetteur et investisseurs) d'un droit de résiliation/rachat doit être envisagé. La clause prévoyant les cas admis (« *good cause* ») dans les conditions générales d'émission de l'instrument doit être clairement définie.

#### 4.3. Blanchiment d'argent et lutte contre le terrorisme

Compte tenu du fait qu'il n'existe pas de disposition légale expresse couvrant les ICO, il n'est pas surprenant que de nombreux doutes surgissent au sujet de la lutte contre le blanchiment d'argent et la lutte contre le financement du terrorisme. L'Émetteur devra le plus souvent recourir aux services d'un agent de domiciliation qui, en tant que professionnel du secteur financier, est soumis aux « *obligations de vigilance à l'égard de la clientèle* » découlant de la loi du 12 novembre 2014 relative à la lutte contre le blanchiment et le financement du terrorisme, dans sa dernière version (la « loi LBC »). Les mêmes obligations s'appliquent à la banque de l'Émetteur du lieu où le compte en banque est détenu. D'autres

<sup>33</sup>. Philippe-Emmanuel Partsch, *Droit bancaire et financier européen*, 2<sup>e</sup> édition, tome 1 – Cadre général – Les établissements de crédit, chapitre I, section V – Monopole de principe sur l'activité de réception des dépôts et d'autres fonds remboursables du public, paragraphe 651, p. 401.

prestataires travaillant pour l'Émetteur seront également confrontés aux obligations découlant de la loi LBC (à savoir avocats, notaires, etc.). À cet égard, selon les caractéristiques des jetons, cela peut créer des difficultés supplémentaires pour ces personnes quant à leurs obligations en vertu de la loi LBC.

Il est à noter que la Directive (UE) 2018/843 du Parlement Européen et du Conseil du 30 mai 2018 modifiant la Directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme ainsi que les directives 2009/138/CE et 2013/36/UE qui devra être transposée au plus tard pour le 10 janvier 2020 par les États membres de l'UE couvre les monnaies virtuelles<sup>34</sup>. Comme indiqué dans son cinquième considérant, cette directive devrait permettre d'adopter une approche équilibrée et proportionnelle, préservant les progrès techniques et le haut degré de transparence atteints dans le domaine de la finance de substitution et de l'entrepreneuriat social.

#### 4.4. Protection des données

Dans la mesure où les ICO ciblent fréquemment des personnes physiques, certaines règles relatives à la protection des données doivent être respectées par l'Émetteur (à savoir, celles prévues par le règlement dénommé règlement général sur la protection des données (RGPD) (UE) 2016/679).

#### 4.5. Code de la consommation

Il convient de garder à l'esprit, en outre, qu'il faudra tenir compte de certaines dispositions du Code de la consommation, le livre blanc devant aborder ce point ainsi que les termes et conditions applicables aux jetons.

### 5. Conclusion

Compte tenu de ce qui précède, il apparaît que les ICO soulèvent un certain nombre de questions, notamment en ce qui concerne l'évaluation des risques y afférents, tels que, notamment :

- le risque que l'instrument soit qualifié de valeur mobilière, déclenchant l'obligation d'établir un prospectus soumis à l'approbation de la CSSF ou transmis au Luxembourg *via* le mécanisme du passeport, à défaut d'exemption ;
- le risque que l'instrument puisse être qualifié d'instrument financier, ce qui pourrait impliquer certaines obligations en vertu de MiFID II ;
- le risque d'enfreindre le monopole des établissements de crédit de recevoir du public des fonds remboursables ;
- le risque d'enfreindre la LSF, la loi LBC, l'AIFM, le Code de la consommation, etc.

Au vu des risques susmentionnés et compte tenu du risque élevé des opérations liées aux jetons, il est conseillé de réaliser une analyse de l'ICO envisagée et du jeton sous-jacent à un stade très précoce, puis de préférence d'obtenir l'avis de la CSSF, s'il y a lieu, avant d'aller plus loin. La CSSF recommande le respect d'un tel *modus operandi*, lequel est conforme au comportement habituel de la CSSF s'agissant de nouvelles technologies et d'innovation. À la suite des avertissements formulés par certaines autorités et des projets de réglementation des ICO dans plusieurs pays européens, d'autres principes directeurs pourraient bientôt être fournis par les autorités de régulation, suivant l'approche de la FINMA visant à apporter davantage de sécurité juridique dans ce secteur, et à tenter d'établir un cadre réglementaire pour les ICO et davantage de stabilité dans ce secteur d'activité.

Les principes directeurs déjà disponibles peuvent certainement servir de base à l'élaboration d'un cadre juridique pour les ICO. Ce cadre juridique apporterait davantage de sécurité juridique pour l'ensemble des investisseurs et des Émetteurs. Dans certains cas, cela peut clairement constituer une voie alternative aux introductions en bourse (IPO) si l'opération est correctement structurée.

<sup>34</sup>. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843>

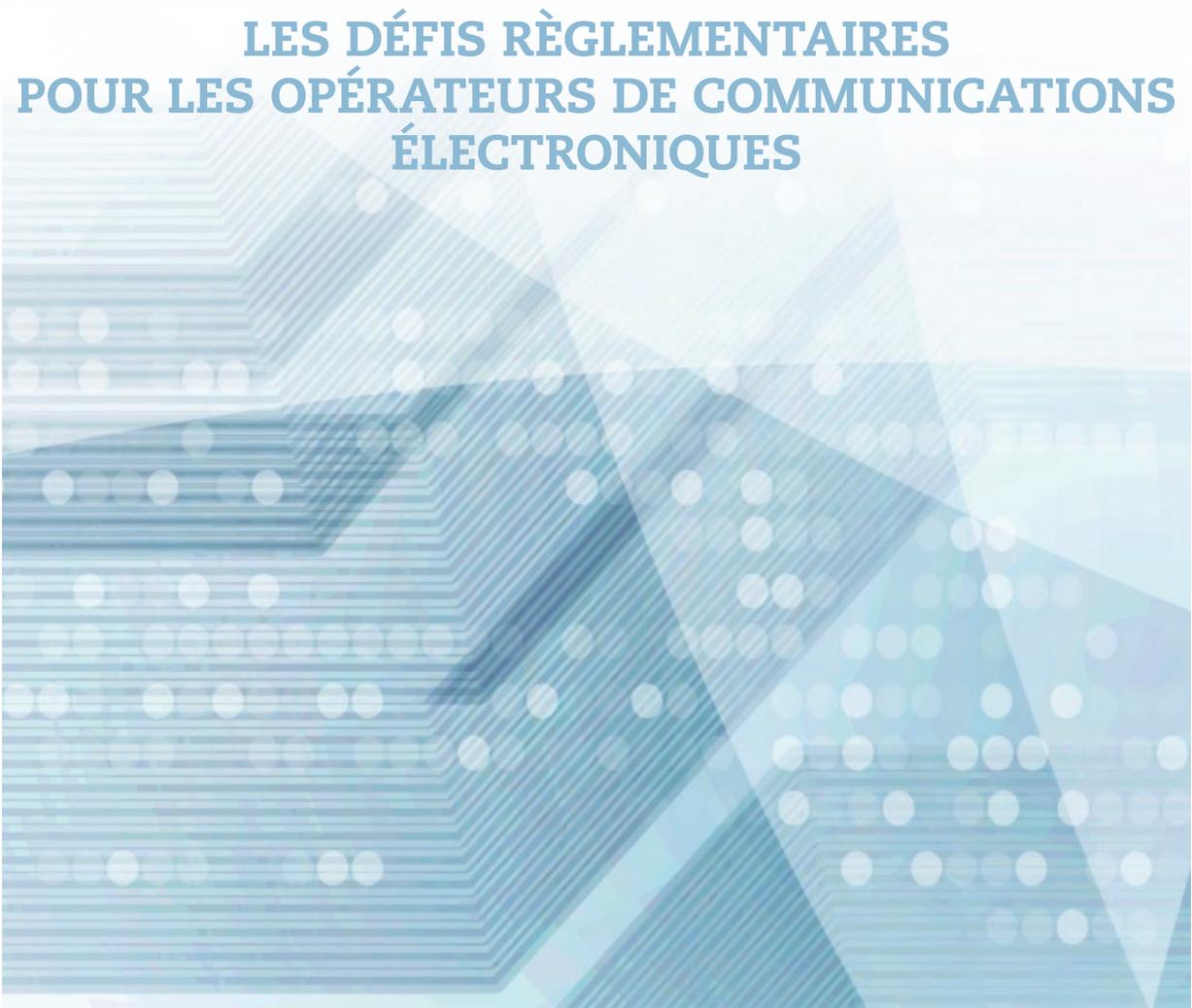
RÉGLEMENTAIRES

---

THÈME 10

# Objets connectés & transformation numérique :

LES DÉFIS RÉGLEMENTAIRES  
POUR LES OPÉRATEURS DE COMMUNICATIONS  
ÉLECTRONIQUES



# Le point de vue...



**Michel Combot,**  
Directeur général,  
Fédération Française des Télécoms

## Qu'est-ce que le « New Deal » mobile ?

Le New Deal mobile est un accord unique signé entre les opérateurs télécoms, le Gouvernement et l'Arcep. Il vise à :

- **Généraliser la 4G sur le territoire** (d'ici fin 2020, l'ensemble des sites mobile devront migrer vers la 4G et d'ici 2022 pour les sites mobiles « zones blanches »).
- **Couvrir les axes de transport**. En tout, ce sont 55 000 km d'axes prioritaires routiers qui devront être couverts en 4G d'ici fin 2020. Les 23 000 km d'axes ferroviaires devront être couverts d'ici fin 2025.
- **Mettre en œuvre un dispositif de couverture ciblée**. Ce dispositif est novateur car il donne aux collectivités le pouvoir de choisir leurs sites, de les identifier en amont et de transmettre leurs souhaits de couverture aux services de l'État qui arbitrera, par la voie d'un arrêté, les sites qui devront être construits et financés par les opérateurs.
- **Améliorer la couverture dite « indoor »**, c'est-à-dire, à l'intérieur des bâtiments.

## Quelles sont les innovations notamment digitales qui bousculent l'industrie ? Comment le numérique a-t-il rebattu les cartes de l'industrie des télécoms ?

La 3G et la 4G ont introduit la variable « data » dans l'équation, ce qui a permis aux pratiques digitales de se développer. Depuis plusieurs années, l'utilisation de la data sur smartphone a explosé, ce qui a permis le développement de nouveaux usages. À chaque fois, l'industrie des télécoms a dû s'adapter pour prendre en considération l'évolution des pratiques digitales en proposant de nouveaux services, le tout en investissant massivement dans le redimensionnement et la densification des réseaux mobiles.

Aujourd'hui, le secteur se prépare à l'arrivée de la 5G qui amènera de nouveaux usages et de nouvelles

pratiques numériques. Sans nul doute cette technologie rebattra une nouvelle fois les cartes du secteur. Cependant, les opérateurs et les industries concernées par ces nouveaux usages doivent d'abord identifier les business models qui en découleront pour rationaliser leurs investissements.

## Quels sont selon vous les défis juridiques de demain en matière d'innovation dans les télécoms ?

Dans un premier temps, il sera nécessaire de simplifier les procédures administratives pour faciliter les déploiements. Il n'y aura pas d'innovation digitale sans infrastructures.

Aussi, avec l'arrivée prochaine de la 5G, il semblerait que les fréquences 5G puissent être attribuées à des industriels pour qu'eux-mêmes puissent déployer leurs réseaux. Attribuer des fréquences aux industriels reviendrait à miter le spectre de fréquences, et cela, sans prendre en considération les fonctionnalités permises par la 5G (notamment le « network slicing »).

Il sera également nécessaire d'assouplir le cadre législatif pour les nouveaux usages (véhicules autonomes notamment) pour faciliter les différentes phases de tests qui sont un préalable essentiel avant la mise sur le marché.

Le maintien de la confiance du public dans les réseaux mobiles avec les autorités publiques est essentiel. Il faut convaincre les métropoles de l'intérêt de la 5G, alors que de nombreuses villes sont réticentes face à l'installation de nouvelles antennes. Enfin, l'un des grands enjeux du futur est la question de l'adéquation entre les données personnelles et la capacité d'innovation des opérateurs. La privacy, au cœur de l'actualité législative, d'abord avec le RGPD, et aujourd'hui avec le projet de règlement e-Privacy, soulève en effet d'importantes questions sur les traitements de données, ainsi que sur la manière de continuer à innover.

# Le point de vue...



**Jean-Pierre Bienaimé, Secrétaire General de la 5G Infrastructure Association (5G-IA), et Président de l'IREST (Institut de Recherches Economiques et Sociales sur les Télécommunications)**

*« Le numérique questionne beaucoup les relations sociales dans les entreprises »*

## Comment le numérique a-t-il transformé le secteur des télécommunications ?

Dans le secteur des télécoms, cela fait plusieurs années que le numérique a bouleversé les pratiques au sein des entreprises, notamment au sein de mon ex-entreprise, Orange. La nécessité de se transformer s'est très vite fait ressentir et il y a eu énormément de formations. Les collaborateurs ont ainsi été sensibilisés, non seulement aux nouveaux outils, mais à la transversalité, à l'interactivité, à l'horizontalité permise par le numérique. En réalité, la transformation numérique donne beaucoup l'occasion de parler de l'organisation du travail et des relations dans les entreprises. Elle permet aussi d'organiser autrement les relations sociales, de passer du vertical à l'horizontal, au collaboratif etc. A l'IREST, nous avons organisé en décembre 2016 un colloque intitulé : « Révolution numérique : le management sens dessus-dessous », cela résume la situation.

## Quelles conséquences l'utilisation des outils numériques et la transformation en interne a-t-elle eues sur les pratiques du secteur ?

Le développement des outils numériques a permis, par exemple, d'avoir moins recours à des réunions physiques, et davantage à la visioconférence et au télétravail. Il a également fallu poser des règles afin que les outils soient utilisés à bon escient. L'arrivée de nouvelles entreprises dans le secteur, plus collaboratives et plus agiles, a défié les anciennes. Évidemment lorsqu'on a le poids du passé, on va moins vite. Mais Orange, qui est partie d'un statut d'administration publique, a très bien réussi sa transformation complète par rapport à des entreprises comme EDF ou la SNCF, qui sont restées sur leurs anciens quasi-monopoles. Ensuite les grosses structures, si elles réussissent leur mutation, sont en capacité d'aller plus loin que les autres, car elles ont un réservoir de talents plus important. Ainsi chez Orange Wholesale Francenous avons mis en

place des outils d'e-learning qui fonctionnaient avec des avatars, rendant ainsi les formations ludiques et interactives. Nous avions, au départ, sous-traité l'outil puis nous l'avons adapté et finalement nous l'avons fait évoluer en interne.

## Comment innover grâce au numérique dans un environnement où les contraintes se font de plus en plus prégnantes ?

On constate que dans le secteur des télécoms, l'hyperconcurrence encouragée par les instances européennes devient de moins en moins compatible avec les investissements lourds que nécessite la progression du secteur, en particulier pour déployer la 4G, puis la 5G, et la fibre optique. Il est nécessaire que les opérateurs gagnent de l'argent pour pouvoir investir. Dans ce cadre, le mythe du « tout gratuit », auquel le consommateur s'est habitué, avec un business model de type publicitaire peut devenir un anti-business model... Les opérateurs, avec la réglementation RGPD, n'ont plus accès aux données personnelles et les questions de sécurité deviennent de plus en plus importantes. En outre pour favoriser l'innovation, il est nécessaire d'avoir un paysage réglementaire prédictible et harmonisé. Concernant les questions de spectre et de fréquences, cela a permis de généraliser l'itinérance, avec des conséquences sur les prix. En octobre 2019, lors de la prochaine conférence mondiale des radio-communications (CMR19), qui aura pour thèmes principaux les hautes fréquences (ondes millimétriques) et la 5G, il s'agira d'aboutir à des normes et bandes de fréquences harmonisées. Dans le domaine des réseaux, on se rend finalement compte que, davantage que la neutralité de l'Internet (« Net neutrality »), ce qui est intéressant, c'est plutôt d'avoir un Internet « ouvert », permettant d'offrir un service de base satisfaisant à tous les utilisateurs, auquel s'ajoutent des services sur-mesure et adaptés en fonction des besoins plus spécifiques de certaines catégories d'utilisateurs.



Par **Florence Guthfreund-Roland, Aurelia Pons**  
et **Mathilde Hallé**

**L**a croissance du marché des objets connectés atteint de nouveaux records tous les ans, impliquant à la fois des distributeurs et les fournisseurs de services (1). Le développement de ces objets implique l'itinérance internationale et la réglementation qui va avec (2). Dans la même lignée, nous sommes amenés à nous interroger sur l'application du RGPD puisque les objets connectés produisent et transmettent constamment des données (3). Or le règlement ePrivacy pourrait trouver à s'appliquer en sus, rendant nécessaire une organisation entre ce dernier et le RGPD (4).

## **1. Un marché en plein essor avec une demande croissante en capacité**

Le marché mondial de l'Internet des objets (IdO) a atteint 598,2 milliards de dollars en 2015 et devrait poursuivre sa croissance pour atteindre plus de 724,2 milliards de dollars d'ici 2023. Le nombre d'objets connectés, de capteurs et autres, devrait se situer entre 26 et 46 milliards en 2021. Derrière ces chiffres impressionnants, l'éventail des utilisations et des applications potentielles de l'internet des objets s'est considérablement élargi et couvre désormais tous les secteurs industriels et sociaux, tels que le secteur de la santé, les maisons connectées, les villes intelligentes, les chaînes d'assemblage et de fabrication, les solutions de livraison, ou encore la sécurité publique, entre autres. Les objets connectés peuvent être mobiles (tels que les montres ou voitures connectées) ou fixes (par exemple, une machine à laver ou un robot). Dans tous les cas, il s'agit d'équipements « intelligents », qui génèrent et transmettent des données en temps réel, pour communiquer avec le monde qui les entoure.

Plusieurs catégories d'acteurs sont essentielles au marché des objets connectés. Outre les distributeurs d'objets connectés et les fournisseurs de solutions de gestion de flotte, les fournisseurs de

services de connectivité sont essentiels, dans la mesure où ils conditionnent directement la possibilité d'offrir des dispositifs ou des solutions d'IdO aux utilisateurs finaux en fournissant des capacités de communications. Selon les estimations, le marché de la connectivité devrait passer de 2,9 milliards de dollars en 2016 à 17,67 milliards de dollars d'ici 2021, ce qui va offrir aux opérateurs de communications électroniques mobiles en place l'opportunité de commercialiser des services de connectivité et leur capacité disponible aux fournisseurs et utilisateurs d'objets connectés. Néanmoins, et même si les opérateurs de communications électroniques ont déjà par définition une bonne connaissance de l'environnement réglementaire applicable à leurs services « traditionnels », l'offre de services de connectivité IdO est soumise à des contraintes réglementaires complémentaires, de nature à affecter leur modèle d'exploitation.

## **2. Itinérance internationale : dans l'attente de clarifications au niveau européen, l'itinérance intra-communautaire des objets connectés est soumise à la réglementation tarifaire *ex ante***

Le développement de produits et services IdO nécessite le recours à des solutions de connectivité transfrontalière capables d'accompagner la circulation et la portabilité des objets connectés d'un pays à l'autre et d'un réseau à l'autre. Alors que l'itinérance est habituellement conçue comme un service répondant à une demande ponctuelle de consommateurs dans le contexte des communications mobiles 2G/3G traditionnelles, l'itinérance est au contraire inhérente à l'utilisation normale et au fonctionnement envisagé d'un nombre important d'objets connectés. Dans l'Union européenne, l'itinérance est très régulée. Pour autant, la question de savoir si

cette réglementation est généralement applicable à l'itinérance des objets connectés n'a pas encore été tranchée. Malgré un libellé peu clair, le règlement (UE) n° 531/2012, tel qu'ultérieurement modifié, prévoit que les services d'itinérance pour les objets connectés doivent se conformer à l'ensemble des obligations applicables de manière générale aux services d'itinérance, y compris notamment la méthodologie de fixation des tarifs, les obligations de publication ou encore le contrôle des autorités de régulation, à l'exception de certaines obligations spécifiquement prévues. Toutefois, le périmètre des technologies et catégories d'objets connectés soumis aux obligations relatives à l'itinérance n'est pas encore totalement clair. Selon l'Organe des régulateurs européens des communications électroniques (ORECE), la réglementation de l'Union européenne en matière d'itinérance devrait à ce stade être applicable uniquement aux prestations d'itinérance fournies dans le cadre de services de connectivité reposant sur les technologies 2G/3G/4G (ou GSM/UMTS/LTE), qui correspondent aux standards de marché les plus répandus et les plus connus des autorités de régulation. Inversement, l'ORECE considère que la réglementation applicable à l'itinérance ne devrait pas trouver à s'appliquer aux services de connectivité utilisant la technologie LPWA (*low power, wide area*), c'est-à-dire les technologies généralement utilisées dans le cadre de service de connectivité pour l'internet des objets, dans la mesure où ce marché n'est pas encore assez mûr pour mettre en place une quelconque régulation de manière efficace. L'ORECE considère également que les services de connectivité pour les appareils en situation d'itinérance permanente devraient être exemptés et préconise plus généralement une approche au cas par cas de tous les scénarios et technologies d'itinérance possibles. Dans ces circonstances, les fournisseurs de services de connectivité pour objets connectés devront être attentifs à toute initiative réglementaire de la part des institutions européennes au cours des mois à venir, en particulier dans le prolongement du vote par le Parlement européen le 14 novembre dernier en faveur de l'établissement d'un Code des communications électroniques

européen. De telles initiatives pourraient entraîner un remodelage en profondeur de l'environnement réglementaire en matière d'itinérance des objets connectés, avec toutes les conséquences commerciales et techniques potentielles.

### 3. Protection des données personnelles : quelles que soient les données traitées, quelle que soit la qualification retenue pour le fournisseur, les obligations du RGPD seront désormais incontournables

La question de la protection des données personnelles constitue un autre défi réglementaire substantiel pour les fournisseurs de services de connectivité de l'internet des objets. En effet, selon le type d'appareil et de services utilisés, des données à caractère personnel peuvent être collectées et traitées concernant les communications échangées. Alors que des communications entre machines contenant des informations purement techniques, ou des informations excluant toute donnée relative à une personne physique identifiée ou identifiable ne seront pas considérées comme des données à caractère personnel, il ne peut être exclu que les communications émises ou reçues par des objets connectés contiennent des données personnelles. Ainsi, si le contenu des communications transmises sur les réseaux comprend certaines données relatives à une personne physique comme son âge, son nom ou sa localisation ou si l'appareil est connecté à une personne physique (par l'intermédiaire de sa voiture, de ses vêtements, de ses appareils domestiques, ou d'équipements de santé par exemple), alors ces communications seront considérées comme un traitement de données à caractère personnel conformément au règlement (CE) n° 2016/679 relatif à la protection des données à caractère personnel (RGPD). Dans ce cas, le respect du RGPD devra en principe être assuré dans le cadre de la fourniture de ces services. Dans la mesure où il existe un grand nombre d'acteurs et d'intermédiaires impliqués dans l'écosystème de l'internet des objets, la question de la conformité au RGPD soulève des questions juridiques et pratiques complexes. Tout d'abord,

la qualification des fournisseurs de services de connectivité comme responsables du traitement des données ou sous-traitants conformément au RGPD peut varier selon que le traitement recouvre les données à caractère personnel contenues dans les communications électroniques acheminées (c'est-à-dire des données transportées) ou bien les données relatives au trafic (c'est-à-dire des métadonnées, dont l'emplacement de l'objet connecté, la date, l'heure, la durée de la communication, etc.). Bien qu'ils soient habituellement considérés comme des sous-traitants s'agissant du traitement des données à caractère personnel contenues dans les communications électroniques acheminées (et même si l'on peut s'interroger sur la qualification du transport de données en traitement de données personnelles), une qualification de responsable de traitement pourrait être retenue s'agissant du traitement des données personnelles contenues dans les données de trafic. Dans tous les cas, assurer le respect du RGPD implique des conséquences pratiques, contractuelles et financières majeures pour les fournisseurs de services de connectivité de l'internet des objets. Par exemple, lorsqu'ils agissent en tant que sous-traitants pour le compte d'un fournisseur de solutions IoT, les fournisseurs de services de connectivité auront l'obligation légale de s'assurer que leurs sous-traitants ultérieurs (y compris leurs partenaires opérateurs de téléphonie mobile) ont bien été autorisés par le responsable de traitement et respectent les mêmes obligations que celles qui lui sont applicables (telles que les obligations en matière de sécurité et confidentialité, les restrictions sur les transferts en dehors de l'Espace économique européen, le strict respect des instructions émanant du responsable de traitement, etc.). S'ils agissent en tant que responsables de traitement concernant les données relatives au trafic, les fournisseurs de services de connectivité pour les objets connectés auront notamment l'obligation de procéder à des évaluations de sécurité afin de déterminer les mesures de sécurité appropriées à mettre en œuvre pour protéger les données traitées. Les coûts – potentiellement importants – résultant des mesures à mettre en place pour se conformer au RGPD pourront potentiellement être compensés

*via* des opportunités de monétisation des données traitées. Toutefois, les fournisseurs de services de connectivité pour objets connectés ne sont à ce jour habilités à traiter les données relatives au trafic que pour certaines finalités définies et limitées (par exemple pour la facturation, ou pour la fourniture de services à valeur ajoutée sous réserve néanmoins du consentement préalable des utilisateurs finaux et pour une durée déterminée).

#### 4. Le projet de règlement ePrivacy : des obligations complémentaires à prendre en compte ?

L'issue des discussions en cours à Bruxelles concernant le projet de règlement relatif à la protection de la vie privée dans le secteur de l'électronique (règlement dit « ePrivacy ») aura également un impact important sur les fournisseurs de services de connectivité pour objets connectés. Une fois adopté, le règlement ePrivacy remplacera la directive n° 2002/58/CE dite « vie privée et communications électroniques », telle que modifiée par la directive n° 2009/136/CE. Selon le calendrier initialement prévu par la Commission européenne, le règlement ePrivacy devait s'appliquer dès le 25 mai 2018, à la même date que le RGPD. Toutefois, le processus législatif européen est loin d'être achevé en raison des nombreuses discussions que soulève l'adoption du règlement. La teneur de ces discussions témoigne de la complexité de l'articulation des règles du RGPD avec les règles spécifiquement applicables aux traitements mis en œuvre par les fournisseurs de services de communications électroniques. S'agissant plus spécifiquement des objets connectés, les discussions en cours illustrent également les difficultés rencontrées par le législateur européen pour assurer la protection de la vie privée des utilisateurs et la confidentialité des communications, tout en favorisant l'essor de l'IdO.

##### 4.1. Articulation entre RGPD et règlement ePrivacy

Le RGPD prévoit expressément qu'il n'impose pas d'obligations supplémentaires pour les

traitements de données à caractère personnel dans le cadre de la fourniture de services de communications électroniques ouverts au public, en ce qui concerne les aspects régulés par la directive n° 2002/58/CE<sup>1</sup> (soit par le futur règlement ePrivacy). La proposition de règlement ePrivacy<sup>2</sup> prévoit quant à elle que le règlement précise et complète la réglementation relative au traitement des données personnelles tel que défini dans le RGPD en établissant des règles spécifiques<sup>3</sup>.

En ce qui concerne les traitements de données à caractère personnel, le règlement ePrivacy se positionne donc en *lex specialis* vis-à-vis du RGPD. Autrement dit, il traduit les principes établis dans le RGPD en règles spécifiquement applicables dans le cadre des communications électroniques<sup>4</sup>. S'agissant par exemple de la licéité du traitement, l'article 6 du projet de règlement vient préciser les bases légales sur lesquelles les données de communications électroniques peuvent être traitées par les fournisseurs de services<sup>5</sup>.

Toutefois, le règlement ePrivacy n'aura pas seulement vocation à encadrer les traitements de données à caractère personnel mis en œuvre dans le cadre des communications électroniques. En effet, tout comme la directive 2002/58/CE<sup>6</sup>, le règlement ePrivacy aura vocation à protéger la confidentialité de toutes les données de communications, y compris lorsqu'elles ne contiennent aucune donnée à caractère personnel ou aucune donnée relative à la vie privée. Dans ce cas de figure, le RGPD n'aura pour sa part pas vocation à s'appliquer.

En synthèse, les fournisseurs de services soumis au règlement ePrivacy devront donc veiller à respecter les règles du RGPD et celles du règlement lorsque le service fourni implique des données à caractère personnel, alors que seul le règlement ePrivacy s'appliquera en l'absence de données à caractère personnel. En pratique, la distinction risque toutefois d'être ardue pour les fournisseurs de services. S'agissant plus spécifiquement des objets connectés, de nombreuses interrogations demeurent quant aux modalités d'application du règlement ePrivacy.

## 4.2. Modalités d'application du règlement ePrivacy à l'IdO

En l'état du processus législatif, le projet de règlement ePrivacy s'applique au premier chef au traitement des métadonnées et des données transportées dans le cadre de la fourniture et l'utilisation des services de communications électroniques. Or, les services de transmission entre objets connectés sont des services de communications électroniques au sens de la Directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen<sup>7</sup>. Le règlement ePrivacy a donc *a priori* vocation à s'appliquer à l'IdO. Le législateur européen entend ainsi protéger la vie privée des utilisateurs, la confidentialité des échanges, et favoriser l'émergence d'un IdO sécurisé et fiable<sup>8</sup>. Toutefois, l'application de règles inadaptées à la nature des communications de machine à machine (M2M) aurait pour conséquence de

1. Article 95 du RGPD.

2. La première proposition de règlement ePrivacy a été émise par la Commission européenne le 10 janvier 2017.

3. Article 1(3) de la proposition de règlement ePrivacy de la Commission européenne du 10 janvier 2017 (COM(2017)10 final).

4. Voir la proposition de considérant (2a) dans la proposition de règlement ePrivacy du Conseil en date du 19 octobre 2018 (DOC 13256/18, p. 5).

5. Le RGPD dispose qu'un traitement de données à caractère personnel n'est licite que si, et dans la mesure où, il repose sur l'une des bases légales limitativement énumérées à l'article 6 du RGPD.

6. Articles 1(1) et 1(2) de la directive 2002/58/CE telle que modifiée.

7. L'article 2(4) de la Directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen définit le service de communication électronique comme « le service fourni normalement contre rémunération via des réseaux de communications électroniques qui comprend le "service d'accès à l'internet" défini à l'article 2, paragraphe 2, du règlement (UE) 2015/2120 ; et/ou un "service de communications interpersonnelles" ; et/ou des services consistant entièrement ou principalement en la transmission de signaux tels que les services de transmission utilisés pour la fourniture de services de machine à machine et pour la radiodiffusion..

freiner le développement de l'IdO. La question se pose en particulier pour les traitements de données de communication M2M n'impliquant ni donnée relative à la vie privée, ni donnée confidentielle. En effet, le projet de règlement ePrivacy prévoit comme base légale du traitement des données de communication le consentement de l'utilisateur, sauf application de l'une des exceptions au consentement limitativement énumérées<sup>9</sup>. Or certaines hypothèses de traitement de données M2M sont susceptibles de n'être couvertes par aucune de ces exceptions. Le fournisseur de service de connectivité M2M devrait donc aller rechercher un consentement, sans savoir auprès de qui l'obtenir, ni comment. Malgré son orientation généralement très protectrice de la vie privée, le groupe de travail article 29 (G29)<sup>10</sup> a lui-même pointé cet écueil dans son avis sur la proposition de règlement ePrivacy<sup>11</sup> en prenant pour exemple le monitoring de données échangées entre des voitures sans conducteur pour le maintien d'une distance de sécurité. Comme le souligne le G29, le consentement de l'utilisateur ne constitue pas une base légale adéquate pour ce traitement, et aucune des exceptions au consentement prévues dans le projet de règlement ne lui serait par ailleurs applicable. Cet exemple démontre la nécessité de prévoir une exception spécifique pour les traitements des données de communication M2M afin de ne pas freiner le développement de l'IdO. Mais toute la difficulté réside dans la définition des contours de cette exception. Faut-il prendre le parti d'exclure totalement les communications M2M du périmètre d'application du règlement ePrivacy ? Cette solution faciliterait sans nul doute la mise en conformité pour les fournisseurs de services de connectivité M2M. Dans cette hypothèse, les données de communication M2M également données personnelles resteraient soumises au régime du RGPD. Les données de communication M2M non personnelles ne bénéficieraient pour leur part d'aucune protection au titre de la confidentialité des échanges. Cette solution pourrait donc également présenter des risques, en particulier pour les entreprises mettant en œuvre des projets avec une forte valeur ajoutée associée aux données collectées à travers un réseau d'objets connectés.

Faut-il donc prévoir la possibilité d'un consentement donné une seule fois, lors de la signature du contrat avec le fournisseur de services de connectivité M2M ? Faut-il prévoir des modalités de consentement différenciées selon que les données de communication sont relatives à des personnes physiques ou à des personnes morales ? Et dans cette hypothèse, comment avoir la certitude des catégories de données qui seront effectivement traitées dans le cadre des services fournis ? Les réponses que le législateur choisira d'apporter à ces questions auront un impact majeur sur les contraintes réglementaires s'imposant aux fournisseurs de services de connectivité M2M, ainsi que sur leur capacité à monétiser les données collectées à travers les objets connectés.

### 4.3. Pour conclure

Les défis réglementaires pour les opérateurs de communications électroniques offrant des services de connectivité pour objets connectés sont nombreux. Cette situation induit un nombre important de risques (amendes administratives, notamment) et impose par conséquent de suivre de manière attentive les évolutions du paysage réglementaire applicable à ce secteur en constante innovation. Ce suivi est indispensable pour permettre d'accompagner de manière proactive le développement des utilisations et des applications de l'internet des objets tout en assurant une totale sécurité juridique pour les opérateurs concernés. Cette expertise est également essentielle afin de pouvoir saisir pleinement les opportunités de monétisation des données collectées lors de la fourniture de services de connectivité.

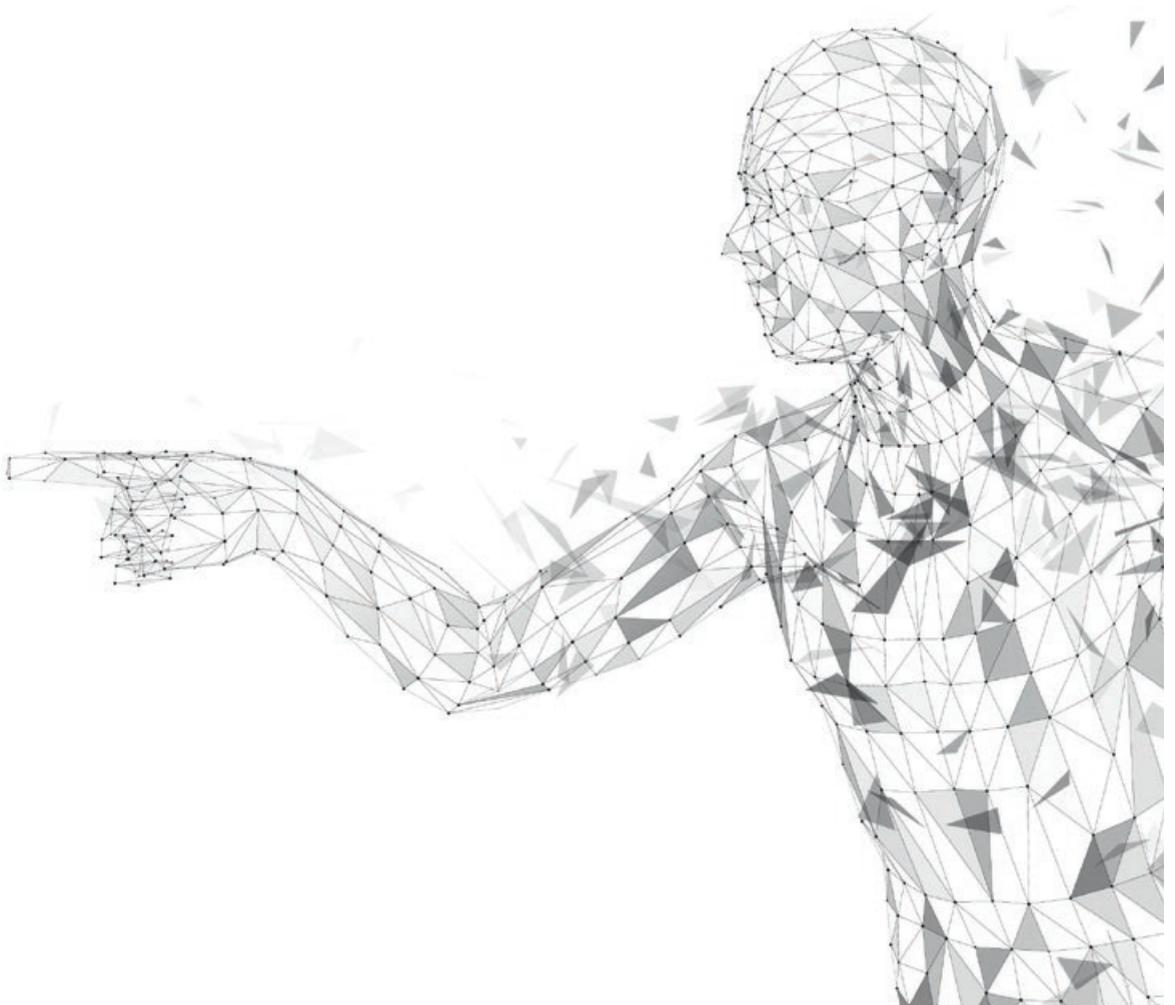
8. Voir la proposition de considérant (12) dans la proposition de règlement ePrivacy du Conseil en date du 19 octobre 2018 (DOC 13256/18, p. 12)

9. Article 6 du projet de règlement ePrivacy

10. Le G29 regroupe au niveau européen les autorités nationales de protection des données à caractère personnel des États membres de l'Union européenne.

11. Avis du G29 n° 01/2017 en date du 4 avril 2017 sur la proposition de règlement ePrivacy, point 40(h), p. 14

# Intelligence artificielle : quel encadrement ?



# Le point de vue...

**Gaspard Koenig, Philosophe, écrivain et Président  
du laboratoire d'idées GenerationLibre**

**A-t-on raison de se poser la question de l'éthique de l'intelligence artificielle alors qu'en l'état actuel de la technique, nous sommes encore loin d'être parvenus au stade de l'autonomie des machines ?**

Les discours qui annoncent l'IA forte ou la « singularité » sont en réalité très minoritaires et me paraissent assez rocambolesques. Les seuls qui en font sérieusement la promotion sont, en fait, des physiciens comme Bostrom ou Tegmark, qui ont l'habitude de disserter sur des sujets certes intéressants, mais théoriques et lointains. Nous voyons bien par exemple, sur un sujet tel que la reconnaissance du langage naturel, que l'on se heurte rapidement à des limites techniques. Les chatbots, tellement à la mode, sont perdus au bout d'une conversation de six phrases. L'intelligence artificielle ne peut pas imiter la pensée humaine, parce que l'intelligence humaine n'est pas seulement le résultat de connexions neuronales, mais de nombreux autres paramètres biologiques. C'est pour cette raison que je n'ai pas d'inquiétude concernant la fin du travail, car l'IA ne pourra jamais avoir ce que l'on appelle le « sens commun », c'est-à-dire la notion de représentation du monde telle que l'ont les humains. L'humain sera toujours nécessaire et une IA ne pourra jamais remplacer, par exemple, un serveur dans un restaurant. Sur ce sujet, il me semble que nous sommes plutôt dans un mouvement classique de destruction créatrice et il n'y a pas, à mon sens, de menace réelle. En revanche, la question de l'abandon de notre libre-arbitre par la délégation de nos décisions à une machine me semble plus inquiétante. Ce n'est pas le problème de l'acquisition de l'autonomie par la machine qui devrait nous préoccuper, mais davantage celui de la perte de notre autonomie à nous, les humains. N'allons-nous pas perdre notre responsabilité ? Le mouvement de rejet du libre-arbitre et le développement de techniques qui nous permettent de déléguer notre capacité de décision, que ce soit pour des questions anodines, comme le GPS qui nous dit où nous diriger, jusqu'à des décisions qui affectent profondément notre existence comme le choix d'une profession, ou d'un amoureux. Cela envahit des champs

importants du quotidien et remet profondément en cause le sous-bassement libéral de notre société. Il y a un troisième aspect à l'éthique de l'intelligence artificielle, qui est celui des biais et des discriminations. Ce point est assez souvent exploré et il appelle des solutions techniques assez simples dans leur principe. Il apparaît donc que l'on se préoccupe, en la matière soit de sujets trop importants théoriques et un peu farfelus, soit d'aspects très techniques. La question centrale, et la plus importante de la perte de notre libre arbitre n'est malheureusement pas assez évoquée.

**Que pensez-vous de la réflexion mise en place au sein de l'Union européenne et de la réglementation relative aux données personnelles ?**

Cette réflexion et ces réglementations sont conformes au principe européen de protection de l'individu, et conforme à la philosophie des Lumières à laquelle j'adhère. Mais c'est de la part de l'Europe, une forme de suicide stoïcien. Car l'Europe, en entravant la mise en place de systèmes d'IA performants, va perdre la bataille économique et géostratégique face aux autres pays, et en particulier la Chine, qui par sa culture de l'intérêt collectif, très confucéenne, est tout à fait disposée, elle, à mettre en place des systèmes de traitement de données holistiques. Je souhaite que la réflexion au sein de l'UE sur la portabilité ouvre la voie à la patrimonialité des données, qui permettrait à l'Europe de rester dans une logique économique, mais qui permettrait aussi à l'individu de préserver la maîtrise de ses données. En réalité, l'IA questionne la question de la propriété telle que nous la concevons dans les pays occidentaux. Les systèmes d'IA qui reposent sur un partage sans limite des données, à travers des secteurs différents et dans le but utilitariste de procurer le maximum de bien-être à un maximum d'individus, sont contraires à nos valeurs. C'est l'inverse en Chine où l'on fait prévaloir la gestion collective des intérêts sur tout le reste, dans une logique, au fond, très communiste. Nous sommes dans une position très inconfortable.





Par **Denise Lebeau-Marianna** et **Yaël Hirsch**

**L**a transformation digitale est aujourd'hui présente dans tous les secteurs, de l'aéronautique jusqu'à l'hôtellerie. Le développement et l'exploitation de l'intelligence artificielle (IA) constituent l'étape suivante. Cette technologie atteint un périmètre vaste, touchant à la fois les particuliers et les entreprises de tous les secteurs. Elle a la capacité d'accompagner des professionnels de toutes les industries pour améliorer leurs pratiques et gagner en productivité et en compétitivité. Face à cet outil puissant, il convient de s'interroger sur les risques et comment les limiter.

L'apport du règlement général sur la protection des données (RGPD) était nécessaire pour dépoussiérer une directive adoptée il y a 23 ans. Pourtant, les nouveaux défis technologiques tels que le développement de l'IA, indissociable de l'utilisation massive de données avec l'utilisation d'algorithmes d'apprentissage profond, soulèvent déjà des questions quant à la compatibilité de l'IA avec ce nouveau texte qu'est le RGPD. Si les principes du RGPD restent applicables et trouvent toute leur place dans le contexte d'une utilisation de l'IA centrée sur l'individu, l'IA soulève de nouveaux enjeux qui ne peuvent seulement être appréhendés par la protection des données personnelles telle que régulé par le RGPD (1). En effet, les algorithmes de l'IA peuvent comporter des biais pour produire des résultats, lesquels peuvent donner lieu à des discriminations et avoir des impacts collectifs et non seulement individuels. Ces nouveaux enjeux nécessitent donc d'envisager d'autres mesures pour encadrer son utilisation (2).

## 1. Encadrement de l'intelligence artificielle dans une perspective « individualiste »

En tant que moyen d'automatisation de tâches complexes, l'IA peut être un outil prometteur

pour aider les entreprises à se conformer au RGPD dans le cadre de leurs traitements de données usuels se rapportant à des individus. Par ailleurs, dans la mesure où les algorithmes d'IA ont recours à des traitements de données personnelles générant des résultats s'appliquant directement aux personnes concernées, le RGPD et la loi du 6 janvier 1978<sup>1</sup> sont applicables. Ce sera notamment le cas des traitements de données donnant lieu à un « scoring » de risque (par exemple en matière d'octroi de crédit ou dans le domaine de l'assurance) ou encore les traitements de données de patients (par exemple pour assurer le suivi de leur santé par leurs médecins) ou les traitements de données des voitures autonomes.

### 1.1. L'intelligence artificielle, un moyen de mise en conformité de l'entreprise au RGPD

Le RGPD est un texte structurant pour les entreprises en ce qu'il instaure des règles précises pour mettre en place une gouvernance des données. Cette gouvernance repose notamment sur des processus d'identification et de classification des données et des procédures pouvant être standardisées. Une telle standardisation peut reposer sur l'IA. Sans prétendre à l'exhaustivité, nous pouvons ainsi envisager que :

- l'IA permette de dresser une cartographie précise des données personnelles en classant les données par degré de sensibilité en appliquant une approche basée sur les risques, conforme au RGPD. L'automatisation de l'établissement de la cartographie des traitements par le recours à l'IA permettrait ainsi de gagner en précision et en rigueur là où un recensement

<sup>1</sup>. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

manuel peut s'avérer fastidieux et approximatif ; et

- l'IA puisse également être un outil d'accompagnement dans la mise en œuvre du principe de proportionnalité, principe clé du RGPD, en aidant l'entreprise (i) à identifier les données pouvant faire l'objet d'un processus d'anonymisation ou de pseudonymisation, (ii) à interdire ou contrôler le renseignement de champs libres dans des applications comportant de tels champs, ou encore (iii) à conduire une évaluation d'impact sur la base d'une procédure standardisée.

L'IA peut donc devenir un outil précieux pour accompagner les entreprises dans leur programme de mise en conformité RGPD tant dans sa mise en œuvre initiale que dans sa continuité et sa mise à jour régulière.

---

## 1.2. Le RGPD, un moyen d'encadrer les projets basés sur l'intelligence artificielle

---

Comme l'indique la CNIL, autorité de contrôle française de la protection des données, dans son document de synthèse<sup>2</sup>, suite à la concertation citoyenne initiée en 2017 sur le thème des enjeux éthiques liés à la place des algorithmes dans notre vie quotidienne, « *les algorithmes et leurs usages sont déjà encadrés par de nombreuses règles juridiques* ».

Dans le domaine des données personnelles, la loi du 6 janvier 1978 et le RGPD prévoient ainsi des règles fondamentales pour éviter des déviations :

(i) **un encadrement strict de l'utilisation des données personnelles** de manière générale, lequel s'applique aux données nécessaires au fonctionnement des algorithmes (au niveau des conditions de la collecte, de la conservation et des droits des personnes). Les principes de minimisation des données, de protection de la vie privée dès la conception ou par défaut, de limitation des finalités et d'analyse d'impact pourront ainsi utilement être mis en œuvre pour apporter des garanties appropriées aux personnes concernées dans le cadre de la collecte de grandes masses de données sans

finalités préétablies. Il va de soi que les autres exigences, notamment les obligations de sécurité, d'information préalable et de protection des transferts en dehors de l'Union européenne, restent également applicables ;

(ii) **une interdiction que des décisions soient prises sur la seule base d'un traitement entièrement automatisé** (sans intervention humaine). Il est toutefois admis que cette intervention humaine vienne en complément d'une décision entièrement automatisée pour en atténuer les conséquences, une pratique qu'il conviendra sans doute de réviser pour apporter plus de garanties aux personnes concernées ;

(iii) **le droit des personnes concernées d'être informées de la logique suivie par l'algorithme** sur lequel repose le traitement. Ce droit induit un principe de loyauté tant dans la détermination des critères de fonctionnement de l'algorithme que dans l'information des personnes concernées sur ce que fait l'algorithme et sur son objectif.

En outre, l'IA doit pouvoir capitaliser sur les règles strictes du RGPD en matière de transferts internationaux des données et de sécurité.

Toutefois, l'IA peut également reposer sur des données non personnelles. Dans une telle hypothèse, il importe de rester vigilant car les conséquences de ces traitements peuvent avoir des impacts collectifs non négligeables.

---

## 2. Encadrement de l'intelligence artificielle dans une perspective « collectiviste »

---

Le rapport de Cedric Villani<sup>3</sup> part du constat que

---

2. *Comment permettre à l'homme de garder la main ?* Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, CNIL, décembre 2017 [https://www.cnil.fr/sites/default/files/atoms/files/cnil\\_rapport\\_garder\\_la\\_main\\_web.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf).

3. *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne*, mars 2018, <https://www.ladocumentationfrançaise.fr/rapports-publics/184000159-donner-un-sens-a-l-intelligence-artificielle-pour-une-strategie-nationale-et>.

l'intelligence artificielle ne mobilise pas systématiquement des données personnelles, laissant ainsi sans cadre juridique véritable certains traitements qui en résultent et qui pourtant peuvent avoir des effets significatifs sur les personnes concernées, à un niveau non plus individuel mais collectif.

En effet, lorsque les individus interagissent avec des plateformes numériques (réseaux sociaux, moteurs de recherche, plateforme d'e-commerce, de streaming, etc.), ils laissent des traces qui sont collectées avec pour objectif officiel la personnalisation des services, l'optimisation des déplacements ou la création des playlists. Or la mise en œuvre de ces traitements donne lieu de manière officieuse à du profilage aboutissant, après un traitement dans une « *boîte noire* », à un classement produisant des effets juridiques ou économiques conformes au profil correspondant.

Il a ainsi été observé dans le cadre des applications de justice prédictive visant à produire un score de risque de récidive de détenus libérés, qu'un score élevé apparaissait (pourtant sans récidive effective observée) pour les anciens détenus afro-américains et qu'il était plus fort que pour les blancs.

Cet effet pervers vient du fait que les systèmes d'IA ayant donné le plus de résultats aujourd'hui s'appuient sur des algorithmes d'« *apprentissage profond* » (*deep learning*) qui se fondent essentiellement sur la donnée d'expériences passées (ou plus précisément le *big data*) sans s'appuyer sur des règles établies à l'avance, comme c'est le cas en programmation classique.

La partialité de ces algorithmes crée des inégalités entre les individus qui peuvent par la suite être victimes de biais, discriminations ou exclusions.

La réglementation des données personnelles essentiellement centrée sur la protection d'un individu (perspective « *individualiste* ») ne permet pas d'apporter une protection suffisante contre ces dérives. En effet, ces technologies reposent sur l'analyse d'une masse importante de données visant à identifier des tendances et comportements sur des groupes d'individus

et non sur les données précises d'un individu. Ce changement de paradigme nécessite donc d'entamer une réflexion autour de nouveaux droits ou de droits existants revisités.

Le rapport de Cédric Villani<sup>4</sup> préconise notamment (i) de veiller à intégrer l'éthique dès la conception, le développement et la commercialisation de systèmes d'IA ; (ii) de mettre en place une reconnaissance de « *droits collectifs sur les données* » qui seraient protégés par le législateur, qui encadrerait les motifs en fonction desquels peut être refusé l'accès à une offre de services ; (iii) de renforcer l'action de groupe déjà prévue par le RGPD, afin de permettre la réparation du préjudice établi ; et (iv) de repenser le « *droit à la portabilité* » « *dans une perspective citoyenne en permettant aux [consommateurs] de récupérer leurs données pour les mettre à la disposition d'un acteur public ou de la recherche scientifique au profit de missions d'intérêt général* » (exemples : données de patients au service d'instituts de recherche afin d'améliorer la détection ou le traitement de pathologies ; optimisation de la circulation d'une commune sur la base des données collectées dans une application de transport auprès des administrés). Il s'agirait ainsi de développer des nouvelles bases de données à usage de service public.

La CNIL<sup>5</sup> quant à elle appelle (i) à un renforcement de l'obligation de transparence et de loyauté nécessitant d'explicitier la finalité du traitement envisagé par l'algorithme d'IA et ses conséquences d'une manière accessible, c'est-à-dire claire et compréhensible ; (ii) à la vigilance collective face aux impacts possibles de l'IA ; et (iii) à une intervention sur la conception même des algorithmes pour lutter

4. Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne, mars 2018, <https://www.ladocumentationfrancaise.fr/rapports-publics/184000159-donner-un-sens-a-l-intelligence-artificielle-pour-une-strategie-nationale-et>

5. Comment permettre à l'homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle, CNIL, décembre 2017 [https://www.cnil.fr/sites/default/files/atoms/files/cnil\\_rapport\\_garder\\_la\\_main\\_web.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf)

contre leur opacité par la mise en place d'outils de visualisation permettant à la personne concernée de mieux contrôler les critères qui détermineront la décision finale.

Il est également prévu de procéder à un audit régulier des algorithmes afin de contrôler leur conformité à la loi et leur loyauté. Une labellisation des algorithmes vertueux pourrait également être envisagée.

Enfin, les entreprises déployant des algorithmes susceptibles d'avoir des impacts significatifs doivent penser à la mise en place d'une gouvernance, dont les composantes pourraient être un comité éthique et un déontologue, pour contrôler les projets d'IA et s'assurer de leur éthique.

L'IA étant une technologie en perpétuelle mutation, elle ne peut être régie par un régime juridique figé. Il conviendra donc d'être particulièrement vigilant afin de permettre son utilisation dans un environnement juridique capable de s'adapter aux caractéristiques évolutives de cette technologie.

PROPOS CONCLUSIF

---

# Quelle vision pour le digital en France ?

LORSQUE L'ÉTHIQUE ACCOMPAGNE  
LA TRANSFORMATION DIGITALE





Par Isabelle Eid

**L**e président de la République a appelé en mai 2018, lors du salon Vivatech, à la définition d'un nouveau cadre de régulation numérique international, et le Premier ministre a précisé, dans son discours à l'Université de Tsinghua en juin 2018, que « *cette régulation du numérique n'a de sens qu'à l'échelle mondiale. La France lancera une consultation internationale pour réfléchir à ces régulations intelligentes* ». C'est dans ce contexte que le 30 janvier 2019 une première consultation en ligne grand public, dans le cadre des États généraux, était mise en place<sup>1</sup>.

Depuis le début de l'ère informatique, le monde ne cesse de changer et provoque dans tous les domaines, que cela soit économique, juridique ou social un bouleversement des normes et des standards qui affecte considérablement la vie économique des entreprises et qui oblige jusqu'au niveau étatique, le législateur à s'adapter à cette nouvelle révolution : la révolution numérique<sup>2</sup>. Cette dernière correspond à l'intégration de nouveaux outils technologiques et méthodes de travail au sein des entreprises entraînant ainsi une nouvelle organisation interne afin de gagner en productivité. Ainsi, reconsidérer efficacement la transformation numérique est l'un des principaux leviers de croissance actuels.

La numérisation des méthodes de travail implique la mise en place d'un environnement numérique plus respectueux des utilisateurs, partenaires et clients et de leurs intérêts légitimes. Ainsi, l'éthique semble particulièrement adaptée aux nouveaux défis de la révolution numérique. En effet, elle a comme vertu première de servir de vecteur aux technologies afin qu'elles soient jugées fiables par les individus et la société dans son ensemble. Il s'agit avant tout d'agir avec la conscience d'une action sociétale responsable puisque l'éthique se situe à la réception des avancées technologiques et digitales. En outre, l'action éthique apparaît comme « *éclairceuse du*

*droit, la norme éthique perçue comme une préfiguration de la norme juridique* »<sup>3</sup>. En conséquence, il est opportun de considérer l'éthique numérique comme une éthique des données et gouvernance morale, encadrant les mesures prises sur la base d'une analyse d'informations. Au regard des défis éthiques en présence et de la multiplication des impacts de la transformation digitale, l'alignement des intérêts des acteurs en présence est nécessaire, tout en garantissant une sécurité digitale puis juridique en réponse à une évolution technologique exponentielle (1). En effet, la notion d'éthique s'appréhende comme une notion régulatrice fondamentale, permettant à la fois de développer et de renforcer l'arsenal juridique dédié à la transformation digitale. En outre, la régulation pourrait s'implanter au sein des secteurs d'activités irrigués par la transformation digitale, moyennant une intégration par le droit positif des différents principes directeurs éminents, tels que la précaution, la loyauté, la transparence ou la vigilance (2).

## 1. La nécessaire adaptation du modèle français face à la transformation digitale actuelle

L'éthique numérique envisage de s'appuyer efficacement sur les enjeux sécuritaires afin

1. Consultation en ligne, 30 janvier 2019 <http://www.vie-publique.fr/forums/consultation-ligne-cadre-etats-generaux-nouvelles-regulations-numeriques.html>

2. Encadrer la révolution du numérique : lancement des « *états généraux des nouvelles régulations numériques* », 1<sup>er</sup> octobre 2018, Les Echos Executives <https://business.lesechos.fr/directions-juridiques/partenaire/partenaire-1807-etat-des-lieux-sur-la-regulation-du-numerique-323762.php>

3. « *Les enjeux éthiques* », Synthèse du débat public animé par la CNIL, Décembre 2017 [https://www.cnil.fr/sites/default/files/atoms/files/cnil\\_rapport\\_garder\\_la\\_main\\_web.pdf](https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf)

que les entreprises se protègent au mieux des menaces extérieures (atteinte à l'e-reputation, fuites de données, cybercriminalité, etc.). C'est pourquoi, une nécessaire évolution du cadre sécuritaire doit être envisagée (1.1) de façon à, par la suite, mieux encadrer l'éthique algorithmique dans la gestion des risques (1.2).

### 1.1. Vers un modèle français souverain et durable réconciliant innovation et cadre éthique

Lors de son discours devant le Conseil des entreprises franco-chinoises à Pékin le 9 janvier 2018, Emmanuel Macron insistait sur sa volonté de faire reconnaître la France comme une nouvelle puissance numérique aux yeux de la Chine. Tels sont les mots du président de la République : « *Je veux aussi, c'est l'un des objectifs de ma visite, que la France soit mieux identifiée en Chine pour ce qu'elle est aujourd'hui, une puissance du numérique, de la transition énergétique, de la recherche, de l'innovation, de l'industrie du futur et une grande place financière.* »

Actuellement, une vision binaire de *souveraineté numérique et digitale* fait office de modèle sur la scène internationale. En effet, ceux sont les États-Unis et la Chine, deux grandes puissances d'ampleur mondiale qui prédominent en matière de data. Néanmoins, le modèle américain n'est pas régulé et les acteurs privés en place semblent être souverains tant sur le plan de la collecte que sur celui de l'explicitabilité des data à leurs concitoyens. Quant au modèle chinois, il ne représente pas les valeurs françaises et européennes en matière de vie privée ou de droits de l'homme. En conséquence, lesdits modèles sont critiquables à plusieurs égards et démontrent une fois encore, la nécessité pour la France de se doter de sa propre souveraineté numérique et digitale afin de ne pas laisser un État s'emparer d'un quelconque monopole de collecte et gestion de données.

VivaTech 2018 fut l'occasion pour le président de la République Emmanuel Macron d'annoncer sa volonté de réformer en profondeur le

financement de l'innovation et de la recherche en France, par le biais de stratégies ambitieuses dans des domaines technologiques prometteurs comme l'IA ou le véhicule autonome. Afin d'accélérer le déploiement des innovations digitales, les écosystèmes en réseaux sont en train de travailler pour accélérer la création. Le but étant de forger une politique ambitieuse et un écosystème fort afin de déployer encore davantage l'excellence de la recherche française. À ce titre, les grands groupes, tels qu'Orange, Publicis ou Sanofi devront nécessairement s'allier à des start-ups françaises florissantes, afin de contribuer au(x) changement(s) de leur stratégie de développement. Force est de constater qu'en pareil cas, l'éthique s'avère être un vecteur efficace pour assister la transformation digitale des grands groupes à tous les niveaux tant sociaux, financiers, économiques que stratégiques.

Dans son rapport annuel de 2018<sup>4</sup>, la Cour des comptes a encouragé l'État à accélérer le déploiement de la stratégie d'État plateforme, à former massivement l'ensemble des agents publics aux compétences numériques. C'est dans ce contexte que la responsabilité de l'État au sein de ce mouvement de transformation digitale pourrait se traduire par l'ouverture des données publiques, le développement des « start-ups d'État », la mutualisation de plusieurs services, l'efficacité des API créées par l'Etat pour développer des services numériques communs.

### 1.2. La dimension humaine nécessairement impactée par la transformation numérique

Dans son discours à VivaTech 2018, le président de la République Emmanuel Macron énonçait que « *nous sommes en train de vivre une révolution. Partout il y a une peur du changement parce que les acteurs du changement n'ont pas toujours été exemplaires en venant bouleverser les acteurs existants sans*

<sup>4</sup>. Le rapport public annuel 2018 <https://www.ccomptes.fr/fr/publications/le-rapport-public-annuel-2018>.

*pour autant se conformer à leurs règles. La défiance est née parce que ces transformations en profondeur bousculent notre société. Elles changent les modèles d'affaires par la reformation des salariés. La transformation des données bouscule nos repères lorsque le meilleur peut aider le pire* »<sup>5</sup>. En outre, les répercussions de la transformation digitale sur le plan social et humain ne sont pas négligeables et doivent être prises en considération par l'État et tous les acteurs de la société civile.

La transformation digitale représente un atout majeur mais nécessite inéluctablement de reconsidérer les tenants du volet social. En effet, les entreprises doivent repenser et réorganiser leur fonctionnement interne autour de nouveaux métiers. Cette transformation peut susciter des craintes relatives à de potentielles pertes d'emploi en cascade ou de mutation des métiers. Or, sans les femmes et les hommes qui constituent l'entreprise et son écosystème, il ne peut y avoir de projet de transformation numérique réussie. L'objectif principal est d'écarter au maximum la corruption et les abus de pouvoir, en imposant l'application de règles éthiques dont la transparence des décisions et leur motivation.

La transformation digitale ne doit pas négliger la responsabilité des acteurs en présence lorsque l'innovation dévie de manière significative du cadre éthique préétabli. Ainsi, la responsabilité sociale de l'entreprise pourrait être une première manière de réguler certains comportements et modèles de management. La responsabilité des entreprises (grands groupes, PME, start-ups) doit reposer sur une gouvernance lisible, bien comprise et admise par tous, en concertation avec les personnels et leurs représentants.

C'est ainsi que l'allocation du président de la République à VivaTech 2018 démontrait que malgré les mutations de certains secteurs, et l'impact sur les métiers de ces dernières, il doit toujours y avoir une volonté de créer de l'emploi que le secteur technologique peut attirer, car la réussite passe avant tout par ce *leadership*. Le président de la République

poursuivait en considérant à juste titre que « *cette réussite permet la réussite au carré mais aussi plus de justice (créations d'entreprises au sein des quartiers populaires, multiples opportunités à saisir) pour pouvoir ainsi, financer cette redistribution* ».

Par ailleurs, il ne faut pas oublier que les outils technologiques et plus largement, la transformation numérique, se construisent avant tout autour de l'être humain et de ses besoins, que ce dernier soit client ou professionnel<sup>6</sup>.

---

## 2. L'éthique comme notion régulatrice au déploiement de la transformation digitale

---

Selon Stéphane Richard, PDG d'Orange « *nous sommes à un moment décisif de l'histoire en termes de rythme d'innovation et de potentiel disruptif dans tous les secteurs* ». Ainsi, l'évolution du cadre normatif en matière de digitalisation des entreprises est prédisposée à se soumettre à de nouvelles règles déontologiques et juridiques propres à encadrer de manière efficiente les secteurs régulés (2.1). Avec le développement digital, l'éthique devient complémentaire au droit, et pourrait notamment permettre d'envisager les comportements éthiques des acteurs face aux « *boîtes noires* » des algorithmes (2.2).

---

### 2.1. Le foisonnement avéré des usages digitaux dans les secteurs régulés

---

Parallèlement au déploiement des pratiques digitalisées, le secteur bancaire et financier est enclin à une amélioration notable de ses infrastructures informatiques – tout particulièrement dans la gestion des données, afin

---

5. Discours du président de la République à VivaTech 2018, Les Echos <https://videos.lesechos.fr/lesechos/sujet-actus/reecoutez-le-discours-demmanuel-macron-a-vivotech/kusqu3>.

---

6. « *Village de la LegalTech 2018 : ce qu'il faut en retenir* », Village de la justice, n° 86, décembre-février 2019

de faire face à la concurrence des fintechs. La digitalisation et l'automatisation des processus ont pour objectif de faire évoluer les collaborateurs sur des tâches à plus forte valeur ajoutée, moins répétitives et plus adaptées à l'humain. Ainsi, les directeurs financiers sont en charge de la transformation digitale de leur entreprise. Pour ce faire, l'éthique numérique permet d'accompagner cette transformation par la détection d'anomalies au cœur même des opérations de marché, la surveillance des risques de marché, la recommandation de stratégies d'investissement pour les clients ainsi que l'évaluation des profils de risque pour la gestion des portefeuilles. L'investissement éthique ouvre de nouveaux champs de réflexion(s), s'étendant jusqu'à l'impact des activités financées par les banques sur la société.

*In fine*, la transformation digitale devrait accompagner une certaine « culture de l'éthique » et ainsi, se soumettre aux principes éthiques régulièrement appliqués dans le secteur bancaire et financier, tels que le principe de liberté d'expression des intérêts individuels des agents économiques ou encore le principe de préservation de l'intérêt collectif à travers la réglementation du marché par la puissance publique. En outre, le secteur bancaire et financier retient dans l'expérimentation de « *blockchain privée de smart contract* », l'automatisation et l'exécution des programmes automatiques convenus d'avance entre les cocontractants. C'est ainsi que les « *smart contracts* » permettent un échange juste entre deux parties dans une logique programmable<sup>7</sup>.

Par ailleurs, l'investissement éthique est au cœur du débat. En effet, plusieurs secteurs tels que le retail, l'environnement ou l'énergie sont plébiscités pour l'attention qu'ils portent à l'éthique de leur transformation digitale. Les fonds d'investissements prêtent davantage attention à l'éthique des entreprises pour lesquelles ils souhaitent investir. On parle alors de « *placements éthiques* » lorsque les fonds prennent en compte les critères financiers classiques (risque, liquidité, fiscalité...) mais aussi d'autres critères, qualifiés d'extra-financiers.

Ce fut notamment le cas du fonds norvégien « *OSLO Reuters* » qui avait pris soin de vérifier l'éthique de Total au Sahara occidental<sup>8</sup> - ou encore, le fonds « *Éthique et Partage* » du CCFD-Terre Solidaire, premier fonds commun de placement français qui soutient les énergies fossiles.

Ces exemples concrets démontrent ainsi la possibilité d'allier éthique et finance et d'inscrire son épargne dans une démarche innovante<sup>9</sup>. En outre, le projet de loi Pacte s'est penché sur la technologie blockchain puisqu'il prévoit de conférer à l'autorité des marchés Financiers (AMF) un pouvoir de contrôle d'agrément des acteurs de l'ICO (*Initial Coin Offering*). En effet, les ICO représentent une forme nouvelle de levée de fonds s'appuyant tant sur l'usage de crypto-monnaies que sur la technologie blockchain. Par ailleurs, à l'heure actuelle, les ICO ne sont soumis à aucun cadre réglementaire. Tout l'enjeu réside donc dans l'encadrement de ces « *jetons numériques* » et l'amélioration de la confiance et de la transparence auprès de la société civile. L'objectif à terme serait de répertorier sur une liste blanche les acteurs de l'ICO labellisés, destinée à donner toute information utile au public sur l'offre proposée par l'émetteur.<sup>10</sup> De plus, l'existence d'une personne morale pourrait éviter la pseudonymisation des données. Les enjeux en

7. « Les risques des blockchains », n° 164, Juin 2017 <https://cdn.reseau-canope.fr/archivage/valid/feuilleter-les-risques-des-blockchains-N-11271-16257.pdf>.

8. « Le fonds norvégien vérifie l'éthique de Total au Sahara Occidental », 12 mars 2014, Capital <https://www.capital.fr/entreprises-marches/le-fonds-norvegien-verifie-l-ethique-de-total-au-sahara-occidental-917170>.

9. Le fonds « *Éthique et Partage* » reçoit 4 étoiles par Morningstar, 13 mars 2018, CCFD <https://ccfd-terresolidaire.org/infos/economie-solidaire/le-fonds-ethique-et-5675>.

10. « *Le projet de loi Pacte veut encadrer les levées de fonds en ICO* », Les Echos, 5 octobre 2018, <https://business.lesechos.fr/entrepreneurs/patrimoine-dirigeant/12891663-le-projet-de-loi-pacte-veut-encadrer-les-levees-de-fonds-en-ico-323906.php>.

présence pourraient faire émerger les offres les plus vertueuses tout en dissuadant l'émission d'offres frauduleuses<sup>11</sup>.

Selon l'avocat Alain Bensoussan, « *les IA devront être soumises à des règles éthiques, nonobstant l'émergence d'un nouveau cadre juridique. Il faut dès aujourd'hui (...) responsabiliser les créateurs des solutions d'IA* »<sup>12</sup>.

## 2.2. L'interprétabilité du digital, le nouveau challenge éthique des data scientists

Le curseur d'explicabilité est primordial en ce que le digital irrigue plusieurs secteurs matures en matière d'IA à savoir la banque, l'énergie, l'automobile et l'aérien, l'IP&T, le management et la gouvernance des risques - or, on s'aperçoit que tout l'enjeu réside dans la justification et l'explication des prises de décisions. Dès lors, il convient d'apporter des justifications objectives à *posteriori* de la décision prise par les logiciels numériques généralement dotés d'IA. C'est pourquoi, les *data scientists*, tous secteurs confondus, doivent être en mesure d'apporter de la transparence dans les modèles afin de réduire les biais éthiques et moraux, de générer de la confiance et de faire comprendre la prise de décisions. En pratique, il est presque impossible de suivre le cheminement de l'algorithme<sup>13</sup>. Ainsi, le RGDP a pris en compte cette difficulté en retenant qu' « *aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé* ». C'est dans ce contexte particulier que le Conseil constitutionnel s'est prononcé pour la première fois sur la question du recours à des algorithmes auto-apprenants (comme fondement d'une décision administrative individuelle). Par une décision rendue le 12 juin 2018<sup>14</sup>, le Conseil constitutionnel a considéré que « *le responsable du traitement doit s'assurer de la maîtrise du traitement algorithmique et de ses évolutions afin « de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard* ». Ainsi, on constate que la lutte contre

l'opacité des algorithmes de *deep learning* représente un défi majeur pour ces prochaines années.

\*\*\*

Le 20 janvier 2019, Facebook a annoncé la création d'un Centre de recherche consacré à l'éthique de l'IA. L'objectif étant de « *mener des recherches indépendantes et scientifiques pour apporter des connaissances et des conseils à la société, les législateurs et les décisionnaires des secteurs privé et public* »<sup>15</sup>. Notons toutefois que l'éthique se situe à la frontière entre le droit et l'innovation. Faut-il alors que l'éthique se situe en amont des évolutions numériques et technologiques ou, doit-elle avoir une vertu coercitive afin de servir de support à la mise en œuvre d'actions répréhensibles concrètes liées à la transformation digitale ? Telles sont les questionnements qui seront amenés à être traités sous différents aspects durant les années à venir, puisque la transformation digitale ainsi que l'IA au sens large, posent des réflexions économiques et juridiques complexes.

L'adaptation du droit en matière d'éthique numérique représente incontestablement un défi capital afin d'accompagner de la meilleure manière qui soit, la transformation numérique du XXI<sup>e</sup> siècle.

11. « *La Blockchain s'invite dans la loi Pacte* », La Tribune, 29 septembre 2018 <https://www.latribune.fr/economie/france/la-blockchain-s-invite-dans-la-loi-pacte-792154.html>.

12. « *L'IA, une régulation de rupture selon un principe général de neutralité* », Alain Bensoussan, 23 juillet 2018 <https://www.alain-bensoussan.com/avocats/ia-regulation-de-rupture/2018/07/23>.

13. « *L'interprétabilité de l'IA - Le nouveau défi des data scientists* », 22 octobre 2018, ActuIA <https://www.actuia.com/contribution/jean-cupe/linterpretabilite-de-lia-le-nouveau-defi-des-data-scientists>.

14. Décision n° 2018-765 DC, 12 juin 2018 <https://www.conseil-constitutionnel.fr/decision/2018/2018765DC.html>.

15. Facebook lance un centre de recherche consacré à l'éthique de l'intelligence artificielle, 20 janvier 2019, Le Monde [https://www.lemonde.fr/pixels/article/2019/01/20/facebook-lance-un-centre-de-recherche-consacre-a-l-ethique-de-l-intelligence-artificielle\\_5411861\\_4408996.html](https://www.lemonde.fr/pixels/article/2019/01/20/facebook-lance-un-centre-de-recherche-consacre-a-l-ethique-de-l-intelligence-artificielle_5411861_4408996.html).

## Index des abréviations

<b>ABE</b>	Autorité bancaire européenne	<b>IdO</b>	Internet des objets
<b>AEMF</b>	Autorité européenne des marchés financiers	<b>ITU</b>	International Telecommunication Union/Union internationale de télécommunication
<b>AMF</b>	Autorité des marchés financiers	<b>LPWA</b>	Low power, wide area
<b>ASIC</b>	Application Specific Integrated Circuit	<b>LTECV</b>	Loi de transition énergétique pour la croissance verte
<b>CIPA</b>	Circuit intégré propre à une application : circuit électronique spécialisé	<b>MAS</b>	Monetary Authority of Singapour/ Autorité monétaire de Singapour
<b>CCBE</b>	Council of Bars and Law Societies of Europe	<b>M2M</b>	Machine to machine
<b>CEO</b>	Chief Executive Officer/PDG	<b>OICV</b>	Organisation internationale des commissions de valeurs
<b>CFA</b>	Chartered Financial Analyst : diplôme d'analyse financière délivré par l'Institut	<b>ORECE</b>	Organe des régulateurs européens et communications électroniques
<b>CNIL</b>	Commission nationale de l'informatique et des libertés	<b>PCAET</b>	Plan climat air énergie territorial
<b>CMA</b>	Competition and Markets Authority	<b>PGSSI-S</b>	Politique générale de sécurité des systèmes d'information de santé
<b>CRE</b>	Commission de régulation de l'énergie	<b>PME</b>	Petites et moyennes entreprises
<b>CSSF</b>	Commission de surveillance du secteur financier	<b>PPE</b>	Programmation pluriannuelle de l'énergie
<b>FCA</b>	Financial Conduct Authority : instance de régulation du secteur financier britannique	<b>RGPD</b>	Règlement général sur la protection des données
<b>FINMA</b>	Swiss Financial Market Supervisory Authority : Autorité fédérale de surveillance des marchés financiers suisse	<b>SEAS</b>	Sustainable Energy Association of Singapore
<b>FTC</b>	Federal Trade Commission	<b>SNBC</b>	Stratégie nationale bas carbone
<b>GAFA</b>	Google, Amazon, Facebook, Apple	<b>SRCAE</b>	Schémas régionaux climat air énergie
<b>Greentech</b>	Entreprise innovatrice spécialisée dans l'énergie, la modernisation et l'éclairage	<b>STAD</b>	Système de traitement automatisé des données
<b>IAG</b>	International Airlines Group	<b>Techsol</b>	Plateforme pour les besoins de l'industrie médicale comme le développement clinique, les solutions pour les sciences de la vie, les données médicales, la gestion de l'information médicale
<b>ICO</b>	Information Commissioner's Office	<b>TPE</b>	Très petites entreprises
<b>ICT/TIC</b>	Information and Communications Technologies/Technologies de l'information et de la communication	<b>VPPA</b>	Virtual Power Purchase Agreement

## Lexique

- Airbnb** Abréviation de l'anglais « air bed and breakfast » (matelas pneumatique et petit-déjeuner). Cette dénomination a été mise en place par les deux créateurs du concept en 2007, il s'agit d'une plateforme communautaire payante de location et de réservations de logements de particuliers.
- Assurance collaborative** Système collaboratif regroupant les individus pour s'assurer auprès d'autres individus pour des risques qu'ils choisissent.
- Back-office** (En français, service d'appui ou post-marché), l'ensemble des activités liées au support, à l'administration ou au contrôle d'une entreprise.
- Back-office** L'ensemble des activités de support, de contrôle ou d'administration d'une entreprise.
- Beacon** (En français, balise), petit dispositif utilisant la norme Bluetooth 4.0 pour interagir avec le smartphone d'un utilisateur passant à proximité du dispositif, pour lui envoyer particulièrement des promotions (push notifications) lorsqu'il se trouve dans un point de vente.
- Big Data** Ensemble de données numériques produites par l'utilisation des nouvelles technologies à des fins personnelles ou professionnelles.
- Bluetooth** Mode de communication électronique sans fil, permettant à plusieurs appareils de se connecter entre eux
- Blockchain** Technologie de stockage et de transmission d'informations, par blocs, fonctionnant sur le principe d'une base de données contenant l'historique de tous les échanges effectués entre ses utilisateurs depuis sa création et garantissant ainsi l'intégrité desdits échanges, sans recours à un organe central de supervision.
- Booking.com** Site néerlandais de réservation d'hébergement en ligne. Ce site propose de divers types d'hébergement : hôtels, bed and breakfast, auberges, villas, maisons de vacances, etc.
- Cloud Computing** Le Cloud Computing permet aux utilisateurs d'accéder à distance à du matériel et à des logiciels et de les utiliser via Internet. C'est ce qu'on appelle l'informatique dans « les nuages » parce que l'information à laquelle l'utilisateur accède n'exige pas qu'il se trouve à un endroit précis pour y accéder. Ce type de système permet aux employés de travailler à distance. Les entreprises fournissant des services cloud permettent aux utilisateurs de stocker des fichiers et des applications sur des serveurs distants, puis d'accéder à toutes les données via Internet.
- Couchsurfing** Un terme d'origine anglaise, il peut être traduit par le fait de passer d'un canapé à l'autre. Couchsurfing est une plateforme numérique permettant aux locaux d'héberger temporairement et gratuitement des voyageurs chez eux.
- Coworking** (En français, « travailler ensemble ») Nouvelles méthodes de travail qui associe autonomie et collaboration. Des espaces et des infrastructures dédiés au coworking ont été créés pour favoriser ce mode de travail : café aménagé, bureaux en location, wifi, imprimante, ou encore vidéoprojecteur.
- Cybercriminalité** Ensemble des infractions pénales effectuées sur les réseaux de télécommunications, particulièrement Internet.
- Cyber-risques, cyber-menaces** Ensemble de menaces numériques pouvant porter atteinte à l'intégrité d'une organisation et/ou d'un système d'information.
- Cyber-sécurité** Sécurité informatique appliquée au réseau Internet, qui traite de tous les aspects concernant la protection des données transitant par Internet, notamment leur authentification, leur confidentialité et leur intégrité, ainsi que tous les serveurs et tous les systèmes de contrôle reliés à Internet.

- Données personnelles** Ou Donnée à caractère personnel. Selon la loi, il s'agit des informations propres à une personne physique identifiée ou identifiable, directement ou indirectement. Notamment par référence à un numéro d'identification (par exemple : le numéro de sécurité sociale, un identifiant en ligne) ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (nom et prénom, date de naissance, la biométrie des données...).
- Digital natives** Expression américaine employée pour désigner la génération d'individus ayant grandi en même temps que le développement d'Internet. On considère généralement que les « digital natives » sont nés entre 1980 et 2000. Les « digital natives » sont donc les utilisateurs réguliers et habiles d'Internet et des téléphones portables.
- E-commerce** Commerce électronique ou commerce en ligne, vente en ligne ou à distance, parfois cybercommerce. Il évoque la vente par voie électronique. C'est un échange de biens et services ou encore d'informations via le réseau Internet.
- Emailing marketing** (En français, marketing par courriel) Il s'agit d'une action de communication appelée aussi marketing direct. L'objectif est de réaliser la promotion d'un service ou d'un produit en s'adressant directement à la cible par l'intermédiaire de son adresse email.
- FinTech** Contraction entre "Finance" et "Technologie", désigne généralement une start-up qui évolue dans le secteur de la finance entendu au sens large, c'est-à-dire en englobant généralement la finance proprement dite, la banque d'affaires, la banque de détail et le crédit, les nouveaux moyens de paiement et éventuellement des activités d'assurance. Certaines applications mobiles dédiées à la gestion et à la centralisation des comptes sont également considérées comme des FinTechs. Elle est généralement perçue comme une menace pour les acteurs traditionnels de la banque et de la finance.
- GAFAs** Acronyme qui signifie Google, Apple, Facebook et Amazon, les quatre entreprises les plus puissantes du monde de l'Internet. L'utilisation du terme "GAFAs" est de plus en plus courante en Europe. L'acronyme, originaire de France, est utilisé par les médias pour identifier les quatre sociétés en tant que groupe. Ces firmes possèdent un pouvoir économique et financier considérable (parfois supérieur à un État). Ces GAFAs représentent l'économie du XXI<sup>e</sup> siècle et incarnent le passage à l'ère du digital.
- Gamping.com** Ou « Garden camping ». Plateforme numérique permettant aux locaux de louer son jardin ou son terrain aux voyageurs qui camperont chez l'habitant.
- Génération « C »** Ou « Génération connectée ». Elle renvoie à la génération qui a grandi avec les technologies de l'information et de la communication, dont elle se sert pour communiquer échanger au quotidien.
- Greentech** (En français « technologie verte ») Terme qui renvoie à une technologie considérée comme respectueuse de l'environnement en raison de son processus de production ou de sa chaîne d'approvisionnement. Il s'agit d'un moyen de production d'énergie moins nocif pour l'environnement que les méthodes plus traditionnelles de production d'énergie comme la combustion de combustibles fossiles.
- Hackathon** Réunion des termes « hack » et « marathon », il désigne l'événement pendant lequel des équipes composées de développeurs, mais aussi parfois de designers et de chefs de projet doivent développer un projet informatique, en général un logiciel ou une application. Il se déroule sur une période limitée, et généralement courte (une journée, une nuit,...). C'est aussi souvent une compétition créative fréquemment mise en œuvre dans le domaine de l'innovation numérique, à l'issue de laquelle un jury choisit et récompense des gagnants.
- Hydrocarbures** Composé organique contenant seulement du carbone et de l'hydrogène

- ICO** (Initial coin offering) Méthode de levée de fonds fonctionnant via l'émission d'actifs numériques échangeables contre des cryptomonnaies durant la phase de démarrage d'un projet. Ces actifs, appelés "tokens" (jeton numérique), sont émis et échangés grâce à la technologie blockchain.
- InsureTech** Contraction de « insurance » (en français, assurance) et de « technologie ». Catégorie des FinTech ayant vocation à transformer les services d'assurances en y intégrant des développements technologiques pour améliorer et simplifier l'offre aux clients en diminuant notamment son coût.
- Internet of things (IoT)** Internet des objets (IdO)
- Jetons** Token en anglais. Dans l'univers de la cryptomonnaies, un jeton désigne un actif numérique transférable entre deux parties sur Internet sans avoir besoin, pour cela, de l'autorisation d'un tiers. Il s'agit d'un instrument financier utilisé par les entreprises dans le cadre des initial coin offering (ICO).
- Knowledge Management** (En français, Management ou Gestion des connaissances) Il s'agit de l'ensemble des méthodes et des outils logiciels permettant d'identifier, de capitaliser les connaissances d'une organisation afin notamment de les organiser et de les partager.
- Legaltech** (En français, technologie juridique ou technologie au service du droit). Notion issue de l'anglais « Legal Technology » faisant référence à l'usage de la technologie et de logiciels pour offrir des services juridiques.
- Legal Hybrid** (En français, juridique hybride), profession juridique incorporant un autre domaine professionnel (comme le marketing ou la finance) pour en faire une nouvelle profession hybride.
- Legal Knowledge Engineer** (En français, ingénieur des connaissances juridiques), profession juridique participant à la gestion de la connaissance et à l'utilisation d'une famille d'outils, de méthodes et de modes d'organisation pour faciliter la conservation et surtout le partage des connaissances réparties dans l'entreprise.
- Licornes** Le terme « Licorne », ou « unicorn » en anglais, est apparu en 2013. Il désigne les jeunes entreprises ayant une valeur boursière supérieure à un milliard de dollars. Dès lors, figurer dans ce « groupe restreint » est important pour toutes nouvelles start-up, car c'est une énorme opportunité de visibilité auprès des analystes et surtout des éventuels actionnaires.
- LPWA** Ou Low Power Wide Area (en français : zone de faible consommation et de longue portée). Il s'agit des réseaux sans fils basse consommation, bas débit et longue portée, optimisés pour les équipements aux ressources limitées pour lesquels une autonomie de plusieurs années est requise.
- Loi pour une République Numérique** Proposée par la secrétaire d'État au numérique Axelle Lemaire et promulguée le 7 octobre 2016, la Loi n° 2016-1321 a pour ambition d'encourager l'innovation et le développement de l'économie numérique grâce à la circulation des données et du savoir en créant un service public de la donnée, promouvoir une société numérique ouverte, fiable et protectrice des droits des citoyens en affirmant le principe de la neutralité des réseaux et la portabilité des données. Elle vise également à garantir l'accès de tous, dans tous les territoires, aux opportunités liées au numérique avec notamment la couverture mobile, l'accessibilité aux services numériques publics, l'accès des personnes handicapées aux services téléphoniques et aux sites internet.
- Méthodes agiles** Méthodes de gestion de projet dynamiques et réactives
- Multicanal** Le terme multicanal caractérise l'expérience d'un client qui emploie les multiples supports mis à disposition par une entreprise pour effectuer ses achats. Ces différents supports peuvent être par exemple les magasins, catalogues, les sites web et mobiles, les applications, les publicités télévisées, etc. Pour l'entreprise, l'enjeu consiste à adapter ses stratégies à chaque canal afin de les optimiser un maximum et d'améliorer ainsi la relation client.

- Newsletter** (En français, « lettre d'information » ou « infolettre »), contenu publicitaire et/ou d'information envoyé par email à une base de clients ou prospects selon une fréquence régulière ou irrégulière. La newsletter est un outil fréquent de communication. Elle permet de tenir ses clients au courant des dernières nouveautés de l'entreprise. C'est également un outil de fidélisation en matière commerciale.
- Numérisation** Opération technique d'un système informatique qui consiste à transférer le contenu et les caractéristiques formelles d'un document sur support papier vers un support numérique.
- Portefeuilles électroniques** Face au développement des achats sur Internet, des solutions de paiement autres que la carte bancaire ont été créées. C'est le cas du portefeuille électronique (ou numérique) appelé aussi "e-wallet". Il permet ainsi de payer ses achats en ligne, d'effectuer et de recevoir des virements, depuis un ordinateur, un smartphone ou une tablette (Paypal, Paylib...).
- Principe d'accountability** Obligation de rendre compte et d'expliquer, avec une idée de transparence et de traçabilité permettant d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues de la réglementation Informatique et libertés.
- Privacy by design** Le fait de s'assurer que les principes de protection des données à caractère personnel soient intégrés dès la conception des systèmes d'information.
- PropTech** Terme qui résulte de la contraction « property » et « technology », il renvoie à l'ensemble des entreprises qui utilisent la technologie pour améliorer ou réinventer les services dispensés par les acteurs du secteur immobilier (transaction, location, construction...)
- Robo-advisors** (En français robot-conseiller ou robot-géant) Le robo-advisor constitue une plateforme en ligne de conseil. Il s'agit d'une alliance entre technologie et expertise humaine. Les robo-advisors utilisent des algorithmes qui intègrent de nombreuses données afin de réaliser leur conseil.
- Silos internes** Terme illustrant le fait que dans de nombreuses entreprises, les données relatives aux clients ou prospects qui sont obtenues sur différents canaux ne sont pas unifiées.
- Smart city** Ville utilisant les technologies de l'information et de la communication (TIC) pour « améliorer » la qualité des services urbains ou encore réduire ses coûts
- Smart contract** (En français « contrat intelligent ») Concept établi dans le milieu des années 1990. Le smart contract est un contrat programmé et exécuté automatiquement, qui se déclenche lorsque certaines conditions préalablement définies sont remplies. Les smart contracts sont des équivalents informatiques des contrats traditionnels qui s'appuient sur la technologie Blockchain pour rendre infalsifiables leurs termes et les conditions de leurs exécutions.
- Solvency II** Réforme réglementaire de l'Union européenne pour la gestion des risques des compagnies d'assurances.
- Spotted by Locals** Éditeur de guides touristiques disponibles via internet ou applications pour smartphone. Les locaux d'une ville donnée, ou des "Spotters", donnent des conseils et proposent des bons plans aux touristes qui souhaitent expérimenter la ville comme un local.
- Startup disruptive** Jeune entreprise ayant recours aux outils numériques pour transformer certains marchés (Uber, Airbnb, et Netflix par exemple). Ils cassent les systèmes qui paraissent établis des taxis, de l'hôtellerie ou de la location de films, séries, en proposant des services innovants (devenir soi-même chauffeur de sa voiture, proposer la location de son appartement...). Il s'agit donc pour tout entrepreneur de trouver l'idée « disruptive » qui va bouleverser un secteur en particulier.

- Télémédecine** La télémédecine ou médecine à distance consiste à utiliser les technologies de l'information et de la communication afin de permettre ou de faciliter certains actes médicaux, mais aussi améliorer le traitement et le suivi médicaux ainsi que la gestion de la santé et du mode de vie. Ce terme regroupe différentes pratiques médicales, telles que la consultation ou l'échange de données à distance (imagerie médicale, dossier des patients, etc.).
- Tokens** Un token (ou jeton) est un instrument financier utilisé par les entreprises pour lever des fonds dans le cadre d'un ICO (Initial Coin Offering). Ainsi, pour se développer, soutenir un projet ou accélérer sa croissance, une entreprise va mettre sur le marché, en les proposant sur une plateforme dédiée, des tokens (ou jetons) que les investisseurs vont acquérir en les payant avec une crypto-monnaie (le plus fréquemment en ethers ou en bitcoins). En contrepartie de ces jetons, les investisseurs peuvent se voir concéder, soit une forme de propriété (parfois proche d'une action), soit une partie des dividendes générés par l'entreprise émettrice, un bien ou un service produit par l'entreprise...
- TripAdvisor** Site web américain qui propose des avis et des conseils touristiques écrits par des consommateurs sur des hôtels, restaurants et lieux de loisirs. TripAdvisor compare également les prix des hôtels et des billets d'avion pour trouver les meilleurs prix.
- Ubérisation** Néologisme issu du nom de l'entreprise californienne de transport « Uber », qui propose de mettre en relation chauffeurs et clients via une application mobile. Phénomène de rupture et de « disruption », avec le modèle économique classique. Il désigne un nouveau modèle d'économie par lequel les prestataires et la clientèle sont mis en contact directement, voire instantanément, par l'usage des nouvelles technologies numériques. Ce modèle a pour intérêt d'être beaucoup moins cher pour le client par rapport au modèle classique.
- White paper** Livre blanc en français. Dans le domaine des crypto-monnaies, il est généralement publié par l'initiateur d'un projet entre le moment où le projet est annoncé et le lancement de l'ICO (la levée de fonds en crypto-monnaies). Il décrit l'objectif général du projet et les moyens utilisés pour parvenir à sa mise en œuvre. Certains livres blancs mentionnent particulièrement des détails techniques. D'autres, n'expliquent que la démarche à suivre, et les étapes à franchir concernant la mise en œuvre du projet.

# À propos de DLA Piper

**D**LA Piper est un cabinet d'avocats d'affaire international ayant des bureaux en Amérique du Nord et du Sud, en Asie Pacifique, en Europe, en Afrique et au Moyen-Orient, s'imposant ainsi comme un partenaire de premier plan pour accompagner les entreprises partout dans le monde.

Parmi nos clients, nous comptons des multinationales, des entreprises faisant partie du « Global 1 000 » et de « Fortune 500 », mais également des petites et moyennes entreprises. Nous représentons plus de 140 clients appartenant au top du classement de « Fortune 500 » et quasiment la moitié des entreprises et filiales du « FTSE 350 ». DLA Piper, présent dans plus de 40 pays réunit plus de 4 200 avocats dans le monde. À Paris, DLA Piper réunit plus de 175 avocats, dont 40 associés, et conseille les entreprises, banques et fonds d'investissement français et internationaux ainsi que les gouvernements et les autorités de régulation dans leurs opérations stratégiques et pour tous leurs besoins juridiques. Nos domaines d'intervention en France couvrent l'ensemble du droit des affaires : Arbitrage international, Conformité et investigations, Construction, Contentieux, Droit bancaire et financier, Droit de la concurrence, Droit des entreprises en difficulté, Droit des sociétés, Droit fiscal, Droit immobilier, Droit public et administratif, Droit social, Fusions et acquisitions, Marchés de capitaux, Marques et brevets, Outsourcing, Private equity, Propriété intellectuelle, Protection des données, Technologies de l'information, Télécommunications, medias.

Nous avons développé **une approche sectorielle** des domaines juridiques dans lesquels nous intervenons et n'avons cessé de renforcer notre connaissance par secteur d'activité. A cette fin, nous avons identifié 10 secteurs spécifiques constitués d'avocats à travers le monde possédant une expertise particulière et approfondie de ces secteurs, qui constitue pour nous la meilleure

façon d'appréhender les problématiques auxquelles sont confrontés nos clients.

**Nos 10 secteurs clés** : Infrastructure, construction & transports, Industrie, Pharmacie & soins de santé, Média, sport & loisirs, Assurances & réassurances, Immobilier, Technologie, Services financiers & fonds d'investissement, Energie & ressources naturelles, Biens de consommation & distribution.

DLA Piper et ses avocats sont reconnus chaque année pour leur expertise sectorielle par les classements et organismes de référence (Chambers, Legal 500, International Who's Who), notamment en :

**Technologies et télécommunication** : Numéro 1 depuis 2015, avec Stéphane Lemarchand classé band 1 en 2018 - Chambers & Partners.

**Immobilier** : Global international law firm of the year depuis 2005 - 13<sup>e</sup> année consécutive - International Who's Who.

**Aviation** : Numéro 1 en France depuis 2015, avec Vonnick Le Guillou classée band 1 en 2018 - Chambers & Partners.

**Private equity** : Reconnu par les derniers classements MergerMarket et Thomson Reuters. Premier rang en Europe pour le volume total des transactions de PE - 94 Private Equity buyouts et exits en 2018.

DLA Piper est également régulièrement reconnu comme un cabinet à la pointe de l'innovation, notamment par le classement FT Innovative Lawyers, qui met en avant chaque année les initiatives les plus innovantes des cabinets d'avocats et juristes. DLA Piper a été nommé Game changer of the past year (Financial Times - 2015) et un des top 10 des cabinets les plus innovants aux Etats Unis (Financial Times - 2018). Les travaux du bureau de Paris sur la réforme du Code civil en 2016 a obtenu la plus haute distinction du Financial Times (Standout, dans la catégorie Business Development & Sharing Knowledge).





