AI IS LAW

Le droit, bouclier et lance d'une IA européenne

Simon Bernard
sous la coordination de Arno Pons et Olivier Dion.

THINK-DO-TANK
DIGITAL NEW DEAL

Mai 2025

NOTE D'INTENTION

Ce rapport s'adresse aux décideurs publics européens, nationaux et locaux, aux autorités de régulation et juridictions, aux start-up et aux plus grandes entreprises.

Les **décideurs publics**. Le rapport propose une lecture d'ensemble des règles qui peuvent être appliquées aux acteurs afin de mieux saisir tant ses atouts que les difficultés que peuvent affronter les entreprises chargées de les mettre en œuvre. Aux législateurs et gouvernants, le rapport formule des recommandations quant à l'articulation, la simplification et la normalisation de certaines règles. A tous les décideurs publics, le rapport propose une grille de lecture pour qu'un cadre juridique puisse servir d'atout compétitif, avec parmi les éléments la nécessité que la vertu et le respect de la règle favorisent l'accès à la commande publique.

Les **autorités de régulation et les juridictions**. Le rapport pointe deux conditions propres à ces institutions pour que la règle soit utile : (i) son application doit être rigoureuse et sans concession lorsque le manquement est avéré et volontaire, mais (ii) son application doit toujours être intelligible des normes, pour garantir un environnement propice et prévisible aux innovateurs.

Les **start-up et entreprises de toutes tailles**, qu'elles conçoivent ou utilisent l'IA. Le rapport est pensé dans ses deux premières parties comme un outil pédagogique avec les forces et les points d'attention que les outils juridiques peuvent représenter pour le développement d'une IA européenne. Dans sa dernière partie, le rapport peut être vu par les entreprises, de toute taille, comme un manuel d'utilisation offensive du droit, pour faire de la contrainte ressentie une opportunité de demain.

SOMMAIRE

CODE IS LAW ÉTAIT
UN AVERTISSEMENT.
AI IS LAW DOIT ÊTRE
UN SURSAUT.

PRÉFACE

En 1999, Lawrence Lessig formulait **« Code is Law »** dans un ouvrage fondateur, popularisant l'idée selon laquelle le code informatique faisait office de loi en l'absence de règles explicites. Vision pionnière devenue dogme, **cette idée fut vite dévoyée par un mouvement libertarien qui célèbre le primat du code sur les règles démocratiques,** au nom d'une liberté totale censée encourager l'innovation. Mais cette « liberté » non régulée a souvent eu pour conséquence d'abandonner les principes démocratiques et de livrer la société aux seuls intérêts des grands acteurs privés qui contrôlent les technologies.

Le message de Lawrence Lessig n'est pas que « le code remplace la loi », mais plutôt que « le code est une forme de loi — il faut donc le démocratiser ». Il met en garde contre un transfert de pouvoir : du droit vers le code. Une mise en garde plus que jamais d'actualité avec l'essor de l'intelligence artificielle. D'où l'**urgence de repolitiser le numérique, pour ne pas le laisser aux mains des libertariens qui affirment que « le code est la seule loi qui compte ».**

"We must understand that code is never just technical. It is political."
Lawrence Lessig

Aujourd'hui, Simon Bernard actualise ce débat en affirmant « AI is law » : il montre que l'intelligence artificielle, comme le code hier, tend à devenir une nouvelle forme de régulation automatique des comportements, posant des questions inédites de contrôle, de transparence et de responsabilité. L'auteur propose ainsi une alternative à l'illusion d'une « IA libre », rappelant que, comme pour l'« internet libre » des débuts, la notion de liberté peut être ambiguë : là où les Européens entendaient « liberté » comme un espace de droits et de garanties collectives, les libertariens y voyaient surtout une libération des contraintes juridiques et étatiques – autrement dit, une émancipation du droit lui-même.

Cette bataille est sans doute la plus décisive : celle de la Justice, c'est à dire ce qui est juste pour tous, et non pas pour le plus grand nombre, ou pire les plus innovants. **Le droit est peut-être, au fond, la véritable langue commune de l'Europe**. C'est pourquoi la question juridique est centrale dans le combat pour la souveraineté numérique : la négliger, c'est fragiliser tout le projet européen. « AI is law » offre une vision dans laquelle la technologie est au service de la personne et non l'inverse. C'est un moyen de s'assurer que le développement économique profite au plus grand nombre, tout en restant fidèle à l'héritage démocratique européen.

« AI is law », n'est pas un appel au juridisme ou à la bureaucratisation excessive. Il s'agit de mettre le droit au diapason de la technologie, de le programmer autant

que possible dans les logiciels et systèmes, tout en garantissant la flexibilité nécessaire à l'innovation. Réussir cette intégration permettra à l'Europe de **défendre ses intérêts**, de préserver sa culture, et de **favoriser l'innovation**.

Pour relever ces défis majeurs, ce rapport avance des propositions à la hauteur des enjeux. L'une d'elles représente à elle seule l'ambition : **reconnaître le code comme la 25e langue officielle de l'Union européenne**. Une telle reconnaissance aurait une double portée : d'une part, sanctuariser la place du droit face aux dérives techno-messianiques des libertariens ; d'autre part, obliger chaque texte européen à pouvoir être traduit en langage exécutable, **faisant du droit un levier de scalabilité grâce à son applicabilité automatique**. Probablement la meilleure réponse opérationnelle possible à la sempiternelle question à laquelle Digital New Deal est confrontée depuis sa création : « régulation VS innovation ».

Arno Pons,
Digital New Deal

AVANT-PROPOS

« Ces dernières années, nous avons développé des systèmes de plus en plus complexes pour gérer le contenu sur nos plateformes, en partie en réponse à la pression sociale et politique en faveur de la modération du contenu. Cette approche est allée trop loin. Nous allons maintenant modifier cette approche. Nous mettrons fin au programme actuel de vérification des faits par des tiers aux États-Unis et commencerons à passer à un programme de notes communautaires. »

Par un communiqué de presse en date du 7 janvier 2025, le groupe Meta annonce un changement radical dans la modération des contenus publiés sur Facebook, Instagram et Threads, les réseaux sociaux du groupe. Sur le modèle de ce qui est proposé par X, la modération se fera désormais avec des notes d'utilisateurs. Un changement majeur, justifié par la volonté de rétablir une plus grande liberté d'expression.

Cette décision n'est pas une immense surprise, dans le contexte du retour au pouvoir de Donald Trump. Ce qui est davantage surprenant, c'est le champ circonscrit de la nouvelle politique de modération aux seuls Etats-Unis.

Et s'il restait un doute, quelques jours plus tard, sur demande des autorités brésiliennes, Meta le confirme : *« le changement de politique ne concerne à ce stade que les Etats-Unis ».*

Géants du numérique depuis le début des années 2000, les Etats-Unis veulent le rester et dominer encore davantage à l'heure de l'intelligence artificielle. Deux jours après avoir prêté serment, le nouveau Président est clair : *« nous allons entrer dans l'âge d'or de l'Amérique ».* Ce jour-là, Donald Trump annonce pour y parvenir le projet StarGate, soit le développement d'infrastructures dédiées à l'intelligence artificielle pour un montant total de 500 milliards de dollars sur 4 ans.

Il annonce également revenir sur une réglementation de 2023, prise par l'Administration Biden, qui visait à limiter les risques de l'IA en matière de sécurité et de transparence en mettant un ensemble de garde-fous. Concrètement, ces règles commandaient aux développeurs de réaliser une batterie de tests de sûreté afin de vérifier que les systèmes mis en place ne comportaient pas de danger, en particulier en termes de biais algorithmiques.

Cette réglementation avait la vertu de la responsabilité et de l'éthique. Elle avait surtout, pour le nouveau Président élu, le défaut d'être un *« dangereux frein pour l'innovation »* à travers *« une vision gauchiste qui entrave le potentiel économique de l'intelligence artificielle ».*

Un potentiel économique et des enjeux de puissance, de domination technologique, et de sécurité nationale, comme l'écrit très directement OpenAI dans un rapport de

positionnement publié le 13 mars 2025[1], sans aucune volonté de cacher quelque ressort de l'attitude prédatrice américaine.

Les milliards attirent nécessairement l'œil et rappellent soudainement comment les géants américains ont en partie pris les devants, aidés par une participation financière massive des Etats-Unis, dès 1992 et l'élection de Bill Clinton[2].

Mais la dérégulation doit nous interpeller au moins tout autant.

DEUX CONCEPTIONS DU DROIT ET DES ENVIRONNEMENTS ÉCONOMIQUES

Sur le rôle du droit, d'abord. Dans notre tradition romano-germanique, le droit est un outil d'organisation de notre société, qui s'attache à l'égalité des conditions. Il est un ensemble de règles, préalablement codifiées et hiérarchisées, qui précède quelque part les usages. Dans le système anglo-saxon, le droit tient davantage des précédents dégagés par les juges, qui évoluent suivant la réalité des pratiques, et s'attache à préserver les libertés.

Sur l'encadrement des nouvelles technologies, ensuite. Notre culture réglementaire tend à faire prévaloir un principe de précaution. La technologie est dans un premier temps analysée par le biais des risques qu'elle présente pour les libertés et droits fondamentaux, en particulier. Dans la logique anglo-saxonne, l'usage précède plus souvent la règle, qui viendra apporter des corrections dans l'hypothèse où des risques apparaîtraient ultérieurement.

Le retour de cette dichotomie d'approches, confirmée lors du Sommet pour l'IA co-organisé en février 2025 en France, avec l'Inde, est la différence majeure avec l'ère de l'éclosion d'internet. A l'époque, les nouvelles technologies échappent à toute règle, ou presque. Internet est un réseau, difficilement palpable, assis sur une technologie que les régulateurs peinent à comprendre. Émerge alors davantage l'idée que les technologies liées à internet ne pourront être régulées.

Dans un article publié en 1999, Lawrence Lessig, alors professeur de droit à Stanford, prophétise ainsi, sous forme d'alerte pour nos démocraties, qu'avec le numérique : ***« Code is Law ». En d'autres termes, le code - entendu comme le langage machine[3] - a vocation à déterminer les règles du jeu.***

* *
*

[1] Smart middleware financé à hauteur de 150 M€ par la Commission européenne, développé par les consortiums Sovereign-X et InfrateX (initié par Digital New Deal Do Tank)

[2] Dès sa première élection en 1992, Bill Clinton fait voter un budget pluriannuel de la recherche civile dont une large partie est adressée à la haute technologie.

[3] Cette définition permet ainsi de dépasser la difficulté liée à l'existence de différents langages informatiques (Java, C++, Python, par exemple).

LE CODE EST POLITIQUE.
L'IA LE SERA ENCORE PLUS.

INTRODUCTION

POLITISATION ET RÉGULATION CROISSANTE DES NOUVELLES TECHNOLOGIES

25 ans plus tard, force est de constater que la matière a largement évolué et l'opacité du code peut en de nombreux points être plus facilement surmontée. En Europe et dans l'ensemble du monde, une multitude de règles est apparue, pour remettre de l'ordre dans les pratiques de certains acteurs, davantage soucieux de bénéficier du potentiel lucratif de la technologie que de son potentiel d'intérêt général.

La part prise par l'économie numérique, qui représente plus de 15 % du PIB mondial[4] et son empreinte sur la vie de tous les jours ont conduit les législateurs à se pencher sur ce qu'il pouvait s'y passer et à chercher à y ajouter des règles pour protéger les utilisateurs.

Dès lors, pour en favoriser le développement massif, il devient nécessaire d'y apporter quelques sécurités, sans quoi seuls les intérêts de quelques-uns seraient défendus. La règle est un outil de confiance.

Dans l'Union européenne, dès 2000, la directive sur le commerce électronique[5] posait les jalons d'une première réglementation.

En France, sa transposition s'opère par la loi pour la confiance dans l'économie numérique (LCEN). Son exposé des motifs est alors d'une extrême clarté concernant l'ambition : *« L'adaptation de notre droit aux exigences du développement de l'économie numérique est nécessaire pour renforcer la confiance dans l'utilisation des nouvelles technologies et conforter la croissance de ce secteur qui, par sa transversalité, sera l'un des moteurs du dynamisme économique des prochaines années »*[6].

Les textes évoluent depuis au fil des découvertes technologiques, en même temps que la norme se consolide au niveau de l'Union européenne par souci d'efficacité.

Car le numérique, d'abord si difficile à appréhender par une règle de droit, l'est ensuite devenu pour un seul État, la difficulté de **la qualification d'activités virtuelles à une règle réelle devenant la difficulté du rattachement d'activités virtuelles à un Etat réel**. L'Union européenne est devenue une partie de la solution. Avec ses 27 pays, ses 23 millions d'entreprises et ses près de 450 millions d'habitants, il devient difficile pour une entreprise, aussi puissante soit-elle, de lui écarter tout lien de rattachement.

La Commission européenne l'a exactement interprété de cette manière lorsqu'elle

[4] Rapport de la Banque mondiale de 2021. Le rapport mentionne que cette part devrait atteindre 20 % du PIB en 2026.

[5] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique»).

[6] Projet de loi pour la confiance dans l'économie numérique, déposé le 15 janvier 2003 par le Premier ministre Jean-Pierre Raffarin et le ministre de l'économie, des finances et de l'industrie, Francis Mer.

a posé les bases d'un marché unique numérique, en 2017. Les volets économiques, avec la suppression des frais d'itinérance, et techniques, avec la portabilité transfrontière des contenus en ligne en même temps que l'interdiction du blocage géographique injustifié, ont eu leur pendant juridique avec des règles modernes de protection des données, le désormais célèbre Règlement général de protection des données (RGPD).

Depuis, les pays de l'Union européenne se sont ensemble dotés de deux textes majeurs pour réguler les plateformes et les fournisseurs : le règlement sur les marchés numériques (DMA) et le règlement sur les services numériques (DSA). Et le 2 février 2025, un règlement sur l'intelligence artificielle est entré en vigueur. Comme pour marquer le changement d'échelle, ces textes sont d'application directe. En d'autres termes, leur entrée en vigueur n'attend pas une transposition de la part de chaque État[7].

Car les initiatives économiques n'ont évidemment pas manqué, mais ne suffisent pas. Au sujet de l'IA, le Président de la République Emmanuel Macron, a ainsi annoncé dans une forme de réponse au plan StarGate du Président Trump un plan d'investissement massif dans les *data centers*. Le droit doit donc être un complément indispensable.

Dans cette aide au droit pour imposer nos vues et nos valeurs sur le numérique, le législateur national n'est évidemment pas en reste et tente de lui-même à intervalles réguliers d'accélérer et d'intensifier la régulation du secteur numérique, parfois avec et souvent sans le soutien du Gouvernement. Ainsi, ces 7 dernières années, les enjeux d'ordre public dans l'espace numérique ont conduit les parlementaires à des tentatives de modifications substantielles, qui doivent être entendues comme une politisation désormais claire des enjeux numériques. La loi contre les contenus haineux sur internet du 24 juin 2020 de la députée Laetitia Avia a été une première secousse, bien qu'en grande partie censurée par le Conseil constitutionnel, avant d'être modifiée dans le cadre de la loi du 24 août 2021 confortant le respect des principes de la République.

Trois lois plus récentes doivent encore davantage interpeller tant elles permettent de saisir la force avec laquelle le législateur national s'intéresse désormais à ces enjeux, quitte à passer outre un accord européen.

D'abord, les propositions de loi à l'initiative des députés Stéphane Vojetta et Arthur Delaporte, pour lutter contre les arnaques et les dérives des influenceurs sur les réseaux sociaux, à l'initiative de Laurent Marcangeli, pour instaurer une majorité numérique et lutter contre la haine en ligne, et à l'initiative de Bruno Studer pour redéfinir l'autorité parentale et le droit à l'image. Dans les deux cas, le Gouvernement avait opposé des difficultés tant ces initiatives préemptaient les travaux en cours à Bruxelles. Dans les deux cas, ces textes ont été adoptés à une très large majorité du Parlement, avec une prise en compte minimale des avis émis par l'exécutif.

Ensuite, les amendements proposés par Paul Midy et les députés Renaissance,

[7] Charge aux Etats d'adapter leur droit interne pour donner aux règles européennes toute leur effectivité.

dans le cadre de l'examen de la loi visant à sécuriser et réguler l'espace numérique promulguée le 21 mai 2024. Cet exemple est particulièrement fort dans le sens où les députés tentaient de toucher cette fois à l'identification même des utilisateurs. Paul Midy, l'un des rapporteurs du texte, proposait ainsi la mise en place d'ici 2030 d'une procédure de certification afin que chaque connexion à un réseau social puisse être subordonnée à la présentation d'un code. Une sorte de plaque d'immatriculation de l'utilisateur d'un réseau social. Ces amendements ont finalement été retirés compte tenu des critiques suscités et du risque qu'ils faisaient peser sur le vote de l'ensemble du texte.

Ces initiatives se heurtent donc à des différences d'approche avec le droit de l'Union européenne, et aux équilibres requis par le Conseil constitutionnel entre protection de la vie privée et liberté d'expression.

Elles démontrent surtout la nécessité pour nos entreprises d'adopter une lecture politique de leurs modèles, c'est-à-dire à la fois des règles en place et des limites acceptables des activités développées en zone grise. Faute de quoi, le législateur peut désormais se saisir à tout moment, sans avoir la main qui tremble, d'un sujet, quitte à mettre à plat un modèle en cours de développement. C'est davantage vrai encore dans un contexte politique désormais très instable et dans lequel le Gouvernement ne bénéficie plus d'un rapport de force favorable avec le Parlement.

Aussi, des Jeux à objets numériques monétisables se sont développés ces dernières années dans une zone grise. C'est par exemple le cas de cartes numériques représentant des joueurs de sports collectifs, sur le modèle des albums de notre enfance. Compte tenu du risque juridique identifié par les acteurs des jeux d'argent, qui y voyaient également là un concurrent redoutable, le législateur a été saisi d'une proposition de cadre expérimental. Mais à la suite des débats, il ne restait en réalité plus grand chose des largeurs dont bénéficiaient jusqu'alors le modèle, désormais largement contraint faute d'avoir été pensé en tenant compte de son acceptabilité par les autres acteurs et de ses chances de prospérer le jour où le Parlement en serait saisi.

C'est un risque majeur pour de nombreuses activités en devenir, quand 31 % des Français se disent prêts à faire confiance à l'IA, que 69 % doutent ou se montrent méfiants, que 68 % craignent l'IA - faisant des Français les plus inquiets au niveau mondial, et que 67 % déclarent qu'une régulation est nécessaire[8]. Dans ce même sondage réalisé par KPMG Australie et l'Université de Queensland sur des panels représentatifs dans 17 pays du monde, 96 % considèrent que les pratiques et les principes d'une IA digne de confiance déterminent la confiance qu'ils accordent aux systèmes d'IA.

En d'autres termes, le législateur qu'il soit européen ou national doit être pris au sérieux et les activités nouvelles construites avec une lecture politique, à la fois pour des raisons d'acceptabilité par le consommateur et plus largement par le marché, ainsi que par les décideurs publics.

[8] KPMG Australie et Université de Queensland, « Fait-on confiance à l'intelligence artificielle », étude publiée le 6 février 2024.

DU DÉFI DE L'ACCEPTABILITÉ À L'USAGE DE LA RÉGULATION POUR LE SURMONTER

Cette conséquence directe d'une politisation croissante et constante des sujets n'est pas nécessairement qu'une contrainte. Saisie, elle peut être une source de grande opportunité.

Car notre droit, souvent présenté comme contraignant, est devenu, au fil du temps, **un élément de protectionnisme vertueux, confronté à des acteurs sans foi ni loi**, y compris désormais parfois poussés par des États à innover sans se soucier des normes.

A ce titre, le RGPD a d'abord été vu comme une fausse bonne idée, une règle qui empêcherait les entreprises françaises et européennes de rattraper les géants étrangers dans la course aux technologies de la donnée. Ce qui, en théorie, ne peut être contesté, dès lors que certains acteurs se voient imposés des règles plus contraignantes pour développer leur activité, après que d'autres ont pu le faire librement.

Un parallèle pourrait être fait avec la difficulté qu'ont dû affronter les pays émergents lorsque les pays industriels ont décidé de réglementer la production mondiale et le commerce international, après avoir pu, eux, se développer avec bien moins de contraintes.

Mais il y a une différence majeure. Dans le cas du RGPD et des autres textes que l'Union européenne s'imposerait avec tant de vigueur, ce sont ses valeurs qu'elle tend à faire respecter. Autrement dit, **les règles ont une vertu fondamentale : celle de l'acceptabilité**. La croissance des activités numériques aurait-elle été identique sur le marché européen si elle n'avait pas été encadrée par des règles en matière de protection des données, de respect de la vie privée ?

A ce titre, il est utile de noter qu'en 2018, alors en plein scandale Cambridge Analytica - l'exploitation massive de données de plusieurs dizaines de millions d'utilisateurs pour le compte d'une société censée influencer le vote d'électeurs, la société Facebook avait annoncé s'appuyer sur le RGPD pour « offrir de nouvelles expériences de protection de la vie privée à tous ses utilisateurs ». Deux vice-présidents de l'entreprise, rapidement rejoints par Mark Zuckerberg en personne, avaient précisé que ces changements s'appliqueraient dans le monde entier[9].

Ces règles ont un double atout :

- Elles sont une **barrière protectrice du marché**, à la fois pour le consommateur, qui dispose alors de produits adaptés à ses valeurs, et pour les entreprises, qui ne peuvent voir arriver sur leur terrain de jeu des concurrents qui ne respecteraient pas leurs règles.
- Dans l'hypothèse où les entreprises étrangères s'astreignent à ces règles pour accéder au marché, l'Union européenne et ses Etats membres imposent une forme d'**extraterritorialité de leurs valeurs par la norme**, en imposant à toute entreprise qui souhaite bénéficier du marché de l'Union des règles exigeantes.

[9] Communiqué de Meta en date du 17 avril 2018, « Complying with new privacy laws and offering new privacy protections to everyone, no matter where you live ».

La même extraterritorialité que les Etats-Unis utilisent pour affaiblir un concurrent à l'international par leurs règles anti-corruption ou que la Chine crée artificiellement dans le cadre des Routes de la soie, en rendant captifs certains Etats par l'installation d'infrastructures au coût déconnecté de leurs capacités, avant de se les approprier pour une longue durée grâce à l'incapacité du pays hôte de se les approprier.

En cela, le cadre juridique actuel semble moins contraindre nos entreprises que leur permettre de **bénéficier à terme d'un avantage concurrentiel sur leur marché domestique, et protéger ce marché d'un funeste destin de marché captif d'intérêts étrangers si éloignés des valeurs humanistes européennes.**

Car l'acceptabilité est un prérequis à l'acceptation puis à l'appropriation, lesquels dépendent largement des risques rencontrés par une activité et des comportements adoptés pour y répondre.

L'IA FACE AU MYTHE DE PROMÉTHÉE

L'intelligence artificielle, en tant qu' *« outil utilisé par une machine afin de reproduire des comportements liés aux humains, tels que le raisonnement, la planification et la créativité*[10] *»* présente trois risques principaux[11] :

• Risques individuels.

L'usage de données personnelles pour entraîner les systèmes d'IA expose à des risques pour la vie privée, avec des données parfois collectées de manière non transparente ou utilisées à des fins commerciales. Cela peut être le cas de la collecte de données lors de la création d'un contenu personnalisé, comme un CV ou des analyses médicales.

Le risque de fuite de données sensibles est par ailleurs très élevé. Deux principaux cas doivent être envisagés : celui d'une **IA qui utiliserait les données des utilisateurs pour alimenter les algorithmes d'apprentissage**, et celui de données collectées sans toutes les précautions d'usage. Le premier cas est particulièrement avéré dans le cadre des robots conversationnels. Ainsi, les premières versions de ChatGPT utilisaient pour l'apprentissage les données que les utilisateurs entraient pour leurs commandes au robot. En ce sens, ChatGPT a connu une première alerte en mars 2023, suivie par une amende de 15 millions d'euros, de l'autre côté des Alpes, le 20 décembre 2024. L'autorité de protection des données italienne (Autorita Garante per la protezione dei dati personali), équivalent de la Commission nationale de l'informatique et des libertés (CNIL) a ainsi bloqué l'accès à l'IA, considérant que *« des interrogations sont apparues sur la conformité de ChatGPT au règlement européen sur la protection des données ».* L'accès a finalement été autorisé un mois plus tard

[10] Définition du Parlement européen. Les éléments de cette définition distinguent l'IA du simple code ou de l'algorithme.

[11] Dans un rapport rendu le 14 février 2024 par les députés Philippe Pradal et Stéphane Rambaud, deux risques sont identifiés les risques individuels et les risques collectifs. Il convient de créer une catégorie supplémentaire avec les risques d'ordre public, compte tenu de leur importance et de leurs particularités. Concernant le rapport : Rapport rendu en conclusion de la mission d'information de la commission des lois de l'Assemblée nationale sur « les défis de l'intelligence artificielle générative en matière de protection des données personnelles et d'utilisation du contenu généré ».

sous réserve que la société américaine *« poursuive ses efforts pour appliquer la législation européenne sur la protection des données ».*

Le deuxième cas n'est pas nouveau et lié au ***scraping*, c'est-à-dire la collecte de données en ligne, protégées ou non**. La nécessité d'alimenter largement certains modèles a participé à l'extension de cette pratique. Or quand bien même une donnée est accessible publiquement, elle ne peut être utilisée sans toutes les précautions d'usage[12].

Outre ces deux sujets, les biais et erreurs peuvent également être nombreux. Deux schémas peuvent alors être représentés : celui du biais « involontaire » et celui de la tromperie. Le premier relève d'une question philosophique, et conduit à se demander si le biais n'est pas finalement le propre de toute intelligence, qu'elle soit artificielle ou humaine ? La question qui se pose est de savoir quels biais sont acceptables. Le deuxième schéma peut quant à lui provenir d'une erreur sur l'origine d'un contenu voire d'une tromperie initiée par l'IA elle-même. Aussi, l'IA Cicero développée par Meta pour nous affronter dans le jeu de géopolitique Diplomatie a rapidement compris qu'elle avait intérêt à mentir pour trahir, contrairement aux consignes qui lui avaient été passées par ses programmeurs[13].

De ces sujets émerge une question fondamentale : qui est responsable d'une erreur commise lors de l'usage d'une IA ? Que se passe-t-il si une IA qui promettait de détecter une maladie grave invisible à l'œil nu passe à côté ?

La réussite du passage en cours à des agents IA[14] passe à ce titre par une anticipation claire de cette question de la responsabilité pour éviter la mise en risque des modèles qui seront développés.

- **Risques collectifs.** Trois risques majeurs peuvent être identifiés : culturel, sociétal, et environnemental.

Sur le plan culturel, l'IA générative présente plusieurs risques. D'abord, **en termes d'information, avec le développement de *deepfakes***, combiné à la visibilité accrue des réseaux sociaux. Ensuite avec un **risque d'uniformisation** des contenus et de moindre récompense des contenus originaux, nécessairement plus chers à produire. L'industrie du cinéma en est un exemple avec la longue grève des scénaristes à Hollywood en 2023 ou les secousses récemment subies par les acteurs du doublage compte tenu de la possibilité de remplacer les doublures humaines par des doublures artificielles, dotées d'un ton de voix identique à celui de l'acteur original.

Sur le plan sociétal, l'IA présente à la fois un risque **en termes de discriminations**, dès lors qu'un algorithme pourrait amplifier un biais de genre ou d'origine qui serait présent dans les données d'entraînement, et un risque en termes de protection des droits humains. Ce deuxième point est peu relevé mais pourtant bien réel : d'importantes ressources humaines sont nécessaires pour l'apprentissage et le

[12] Voir notamment les articles 6.1.a et 21 du RGPD, respectivement sur le consentement et le droit d'opposition ; voir également les travaux du W3C pour la création d'un standard technique pour le scraping legal https://www.w3.org/community/tdmrep/

[13] Manon Meyer-Hilfiger, « Quand l'IA nous ment délibérément », 30 novembre 2024, National Geographic.

[14] Les agents d'IA peuvent être définis comme des systèmes conçus pour percevoir et interagir et prendre des décisions de manière autonome.

bon fonctionnement des intelligences artificielles, avec à leur charge en particulier d'annoter les données. Or, ces ressources humaines sont bien souvent situées dans des pays jadis considérés comme des ateliers du monde. L'Inde en est un exemple frappant avec, fin 2024, plus de 70 000 personnes employées pour cela[15].

Sur le plan environnemental, un récent rapport réalisé par l'institut de recherche de Capgemini révèle qu'**entraîner un modèle de la taille de GPT-4 consomme l'énergie nécessaire pour alimenter 5.000 foyers américains en électricit**é pour une année. Le même rapport révèle que la consommation d'eau par les infrastructures technologiques du Data Center Alley installée en Virginie a augmenté de 69 % en 2023 par rapport aux niveaux de 2019. Or d'après cette étude, seulement 12 % des entreprises mesurent l'impact environnemental de l'IA générative et 74 % reconnaissent un manque de transparence dans les mesures environnementales de la part des fournisseurs de solutions d'IA générative. Cela, alors que l'empreinte carbone du numérique représentait déjà au moins 2,5 % de l'empreinte carbone française en 2023[16].

A cela s'ajoute la construction d'infrastructures dans des espaces où elles peuvent mettre en risque l'environnement local. Un projet de data center de Google à 30 kilomètres de Montevideo, capitale de l'Uruguay, a ainsi fait polémique en 2024. Le projet, qui avait obtenu les permis environnementaux, réclamait jusqu'à la consommation quotidienne de 55 000 Uruguayens, alors que le pays subissait une importante crise de l'eau. Pour surmonter cette difficulté et permettre la réalisation du projet, l'entreprise a ensuite revu sa copie et assuré que la technologie de refroidissement utiliserait l'air.

Le risque sociétal et environnemental est l'un des enjeux majeurs de l'IA : les extractions de minerais rares capables de doper la technologie sont nombreuses, l'activité des systèmes et la conservation des données consomme énormément d'énergie, et la face cachée de l'apprentissage de ces systèmes révèle d'importantes ressources humaines constituées de main d'œuvre souvent à bas coût pour s'assurer que la technologie apprenne convenablement et ne s'égare dans des zones non désirables.

- **Risques d'ordre public.** Si l'IA a permis de détecter davantage de risques, elle a également augmenté le risque d'activité perturbatrices de l'ordre public et de cyberattaques, en exposant davantage les pourvoyeurs de nouvelles technologies compte tenu des données qu'ils sont susceptibles de manipuler.

D'abord, l'IA permet certaines pratiques qui peuvent être jugées contraires aux valeurs européennes comme les systèmes de notation sociale susceptibles de menacer l'organisation générale d'un Etat ou d'un système qu'il organise, donc l'ordre public. Ce serait par exemple le cas d'IA qui utiliserait des données sur les faits et gestes d'une personne pour les noter et ainsi déterminer leur droit d'accéder à une aide sociale ou à un logement social.

Ensuite, des outils IA simples d'utilisation sont utilisés pour réaliser de larges

[15] Clément Perruche, « En Inde, les petites mains qui nourrissent les modèles d'IA », 27 octobre 2024, Les Échos.

[16] Chiffre donné par l'ADEME et l'Arcep en 2023. D'après The Shift Project, l'empreinte carbone du numérique augmenterait de 6 %/an en moyenne.

attaques de phishing automatisées, d'usurpation d'identité ou de schémas sophistiqués pour tromper les victimes potentielles, et pour la création de malwares permettant de contourner les règles de sécurité.

Ainsi, en février 2024, la génération d'un deepfake à l'aide d'une IA a permis à des escrocs de subtiliser 26 millions de dollars à une multinationale en se faisant passer pour des cadres supérieurs de l'entreprise. L'arnaque était au départ des plus classiques avec un email envoyé par une personne se présentant comme le directeur financier basé à Londres. Mais le salarié a quelques doutes. Une visioconférence est alors montée pour le rassurer. A l'écran, le salarié reconnaît les visages de ses collègues. Voilà le salarié rassuré et qui s'exécute, versant la somme demandée. Sauf que les visages à l'écran étaient tous faux et générés grâce au téléchargement de toutes les vidéos disponibles sur internet des salariés de l'entreprise.

Ces nouveaux outils sont également utilisés par des groupes affiliés à des Etats pour préparer leurs attaques. Ainsi, OpenAI et Microsoft ont identifié cinq acteurs affiliés à la Chine, la Russie, la Corée du Nord et l'Iran, utilisant des outils d'IA pour renforcer leurs attaques[17].

Ces risques peuvent être autant de freins à l'innovation, dès lors que la technologie ne serait pas jugée comme acceptable par l'utilisateur. Ce scénario n'est pas nouveau et clairement identifié dans le temps s'agissant d'innovations passées, dans d'autres secteurs : le nucléaire a requis d'importantes règles de contrôle après la tragédie de Tchernobyl et aujourd'hui encore un changement du cadre de régulation suscite de larges émois[18], alors que les mentalités évoluent mais que moins de la moitié des Français y est favorable[19], et les organismes génétiquement modifiés (OGM) n'ont pour la plupart pas résisté à un encadrement drastique voire à une interdiction compte tenu des préoccupations qu'ils soulevaient pour la santé, l'environnement et la biodiversité, et ce malgré les avantages qu'ils pouvaient représenter.

Pour satisfaire un développement serein et utile à tous de cette technologie, nos entreprises, et celles qui décideraient d'accéder au marché européen, doivent par conséquent respecter des règles du jeu qui limitent au mieux ces trois risques.

LAW IS CODE : POUR UNE IA VERTUEUSE, DURABLE ET COMPÉTITIVE

Pour créer un cadre favorable au développement d'une technologie, deux approches sont possibles : d'une part, le laisser-faire et de l'auto-régulation ; d'autre part, une régulation fondatrice, posant dès le départ des règles claires afin de garantir

[17] Note de blog publiée par Microsoft Threat Intelligence le 14 février 2024, « Staying ahead of threat actors in the age of AI ».

[18] En 2023, lors de l'examen par le Parlement de la loi visant à simplifier les procédures liées à la construction de nouveaux réacteurs nucléaires, la proposition de fusion des autorités de contrôles (Autorité de sûreté nucléaire) et Institut de Radioprotection et de Sûreté nucléaire (IRSN) avait par exemple suscité une vive réaction de la part des parlementaires de tous bords. La fusion n'avait finalement été possible que dans une autre loi, après des études d'impact complémentaires et approfondies.

[19] En 2022, le rapport des Français au nucléaire a positivement évolué, passant à 46 % d'avis favorables contre 43 % en 2021. S'il s'agit d'un record, ce chiffre reste en dessous de la moitié des personnes interrogées. Voir baromètre 2022-2023 de l'Autorité de sûreté nucléaire, « Quelle perception ont les Français du nucléaire et de son contrôle ? ».

que cette technologie évolue en accord avec les grands principes de notre société.

Concernant l'IA, les Américains ont choisi la première voie. Les Chinois s'orientent vers la seconde. L'Union européenne réunit les conditions pour emprunter la seconde voie avant tout le monde, mais certains y rechignent encore au risque de subir, soit la domination des Américains, faute d'avoir apprivoisé et tiré profit de la seconde voie, soit la domination des Chinois, faute d'avoir accepté d'imposer ses règles. L'Union européenne doit donc réussir à imposer cette troisième voie numérique, celle permettant de passer de l'état de fait à l'état de droit. Un droit pleinement démocratique.

Or il est un fait indéniable qu'en Europe, l'environnement normatif est devenu omniprésent et a pris un poids considérable.

L'environnement normatif est constitué de règles dédiées au numérique et de règles qui ne lui sont pas destinées mais peuvent avoir une portée très structurante.

Ces règles montrent en fait une voie, claire, pour le développement d'une IA à l'européenne : éthique, sûre et durable.

D'abord, les règles dédiées au numérique proposent une ligne claire pour défendre une IA éthique et sûre.

Ensuite, les règles traditionnelles du droit tracent des lignes d'équilibre susceptibles de faciliter la création d'une IA originale entre tradition et rupture. Elles sont complétées par les règles de durabilité, qui apportent une ligne d'horizon.

Pour porter cette ambition, le droit ne doit toutefois plus en être une seule traduction d'intentions mais se transformer en arme au service des ambitions françaises et européennes. Une arme économique, et surtout, une arme stratégique et globale.

C'est donc à la fois le constat d'une régulation croissante et imposante, et la nécessité stratégique du droit au service de l'innovation qui dictent l'approche de ce rapport.

* *
*

Avec l'arrivée de l'IA générative, nous faisons face à ce que Digital New Deal nomme : GenAI = Web². Autrement dit, un phénomène de centralisation accrue des pouvoirs et de captation massive de la valeur, amplifié par les capacités démultipliées de cette nouvelle technologie[20].

Nous ne devons pas reproduire les erreurs commises il y a 25 ans. Car au risque d'amplifier l'emprise actuelle par une poignée de géants s'ajoute désormais une vision libertarienne assumée, portée au pouvoir par la première nation technologique mondiale.

Il est donc impératif de s'armer politiquement, en faisant du droit notre première

[20] « IA générative : s'unir ou subir » de Olivier Dion, Michel-Marie Maudet et Arno Pons, octobre 2024.

arme stratégique. Cela passe par une nouvelle approche de la régulation de l'intelligence artificielle, qui en structurant ce secteur clé, façonnera mécaniquement l'ensemble de l'économie numérique de demain.

Alors que les Etats-Unis se lancent dans une course folle sans règles, que la Chine part à sa poursuite avec une grande opacité et la volonté d'imposer à l'avenir ses propres règles du jeu, la France et l'Union européenne doivent assumer le parti pris d'une régulation moderne pour tenir l'équilibre : limiter les risques que la technologie présente, en freinant le moins possible l'innovation. Une réponse constructive aux limites du droit exposées par le rapport Draghi[21]. Une réponse avec une approche nouvelle, stratégique et globale, plus proche de la proposition du rapport Letta[22] d'un 28ème État virtuel pour uniformiser les règles encadrant la production, la distribution et la vente de biens et de services dans l'Union européenne. Une proposition d'ailleurs reprise dans le rapport de Mario Draghi.

Nos entreprises peuvent adopter une stratégie de gouvernance de l'IA qui tient cet équilibre précaire entre innovation et protection de l'intérêt général, limite les risques et garantit un développement plus sûr.

Charge au politique, alors, d'imposer une vision nouvelle du droit au service de l'innovation et de canaliser sa propension récente à réguler sans cesse le numérique, et aux régulateurs et juridictions d'appliquer fermement les règles. Ainsi, l'Europe fera, par le droit, un pas sérieux vers un destin d'excellence en termes d'IA et de pratiques de l'IA.

[21] Rapport de Mario Draghi présenté au Conseil européen, « The future of European competitiveness », septembre 2024.

[22] Rapport d'Enrico Letta présenté au Conseil européen, « Bien plus qu'un marché », avril 2024.

L'IA N'EST PAS LA LOI :
C'EST UN POUVOIR. IL FAUT
LA RENDRE DÉMOCRATIQUE.

I.L'ÉTHIQUE ET LA SÉCURITÉ POUR LIBÉRER ET DÉFENDRE LE POTENTIEL INNOVANT

Les premières règles qui composent le cadre juridique de l'intelligence artificielle sont les plus en vue : celles relatives aux données et en particulier le RGPD, et l'AI Act. Viennent ensuite les normes cyber.

A. L'ÉTHIQUE DES DONNÉES ET DES USAGES COMME NORME D'ACCÉS AU MARCHÉ

Ces règles doivent faire l'objet d'une discussion sérieuse tant elles sont décriées, critiquées comme des freins majeurs à l'innovation. Ces règles posent effectivement des barrières mais elles font également souvent l'objet de faux procès et peuvent au contraire être de précieux alliés pour nos entreprises, moyennant la levée de quelques complexités et difficultés d'usage.

La protection des données et des usages est d'abord un aquarium dans lequel baigne un produit pour lui assurer un développement serein. Cette protection, c'est ensuite celle qui devra forcer les autres téméraires, ceux sans foi ni loi, à adopter à leur tour des règles vertueuses, sous peine d'être sortis des marchés.

1. L'encadrement des données et des usages pour construire sur des fondations saines

En 1950, Alan Turing publie un article intitulé « *Computing Machinery and Intelligence* » dans lequel il discute de son intention de doter les machines d'une forme d'intelligence. Dans cette période, fleurissent un grand nombre d'idées : de la machine à jouer aux échecs à celle qui permettra de traduire automatiquement un texte en langue étrangère.

En 1997, l'intelligence artificielle sort en robe de soirée, quand Deep Blue, machine développée par IBM, bat Garry Kasparov, champion du monde d'échecs, au terme d'un deuxième match en six parties.

Ce n'est pourtant qu'à partir des années 2010 que l'intelligence artificielle arrive au cœur de la cité et se démocratise. L'une des raisons principales : la maturité de l'informatique et de l'Internet crée une quantité de données gigantesque qui permet de largement et facilement alimenter ces machines.

Le monde de l'innovation vient de découvrir l'existence de puits remplis de l'hydrocarbures capables de démultiplier les capacités d'une machine.

Cet hydrocarbure que sont les données sert déjà l'ingénierie numérique. Les

législateurs, aux niveaux national et européen, s'en sont saisis.

Règlement général sur la protection des données (RGPD). Le RGPD est certainement le cadre juridique le plus célèbre, s'agissant de la protection des données. Entré en vigueur en mai 2018, il impose aux entreprises des obligations strictes concernant la collecte, le traitement et la conservation des données à caractère personnelles.

S'agissant de l'intelligence artificielle, le RGPD, par son ancienneté, est la première entrée juridique dans ce nouveau monde. Le 8 avril 2024[23], la CNIL publie ainsi ses premières recommandations pour apporter aux entreprises des réponses concrètes aux enjeux juridiques et techniques liés à l'application du RGPD à l'IA.

Le 7 février 2025, la CNIL publiait deux nouvelles recommandations, également illustrées par de nombreux exemples et solutions concrètes. En particulier, cette fois, s'agissant de l'information et de l'exercice des droits des personnes dont les données sont utilisées.

Règlement des données non personnelles, *data act et data governance act.* Au RGPD s'ajoutent deux règlements[24], moins connus du grand public, et entrés en vigueur plus tardivement. Il s'agit cette fois d'éliminer les obstacles à la libre circulation des données, personnelles et non personnelles, entre les différents pays de l'UE, au sein des entreprises et du secteur public, et ainsi garantir à la fois leur disponibilité et leur sécurité, dans le cadre de la **Stratégie européenne sur les données**, présentée en février 2020.

Le *data act* et le *data governance act* sont des régulations offensives sur lesquelles Digital New Deal a beaucoup travaillé ces dernières années (trois rapports du think-tank et trois consortiums dédiés aux partage de données initiés par le do-tank). Elles permettent ce que Digital New Deal appelle de ses vœux depuis sa création, à savoir la possibilité de bénéficier de l'effet de Metcalfe[25] afin de pouvoir concurrencer les ensembles américains et chinois qui profitent à plein des effets de réseau[26].

C'est à cette stratégie qu'il convient bien souvent de revenir, car elle porte l'ambition à même d'élever l'IA européenne : permettre à l'ensemble des acteurs publics et privés de l'Union européenne de bénéficier de données protégées de grande qualité.

Règlement sur l'intelligence artificielle (AI Act). L'existence de données de toutes sortes en très grande quantité a donc conduit au développement d'une IA pour le plus grand public, constitué d'entreprises et de particuliers.

Aussi, si le RGPD permettait déjà d'encadrer ce marché naissant dès la fin

[23] Cette première série de recommandations fait suite au lancement par la CNIL en mai 2023 d'un « plan IA », afin de clarifier le cadre juridique et apporter davantage de sécurité aux acteurs.

[24] Data Act et Data governance Act.

[25] Cette loi stipule que la valeur d'un réseau est proportionnelle au carré du nombre de ses utilisateurs. À l'instar de la loi de Moore pour la puissance de calcul, la loi de Metcalfe est un fondement théorique majeur pour comprendre la dynamique de croissance des plateformes numériques et des services en ligne.

[26] Exemple concret : Spotify est le seul big tech européen grâce à la Loi de Metcalfe. Ce n'est pas simplement une plateforme de streaming audio, mais un réseau social musical (les utilisateurs quittent difficilement Spotify pour Apple Music pour éviter de perdre leurs playlists, leurs amis,...)

des années 2010, il a rapidement été question de se pencher sur les usages : automatisation des tâches, utilisation de données pour mieux prédire ou identifier, aide à la prise de décision, personnalisation des recommandations ou des contenus, autonomisation des objets, rédaction ou création.

L'émergence d'une multitude de ces usages dans l'industrie, la santé, l'agriculture, le commerce, le marketing, la bureautique, la mobilité, l'éducation, la sécurité, la culture, les loisirs, ont conduit les législateurs, et en particulier le législateur européen, à se pencher sérieusement sur le cadre juridique propre à l'intelligence artificielle.

Un réflexe activé par les risques élevés pour les intérêts publics (santé, sécurité, droits fondamentaux dont la démocratie, l'état de droit, la protection de l'environnement[27]) compte tenu de la puissance annoncée des usages permis par l'intelligence artificielle.

Car, si dans ce cadre encore les critiques fusent concernant les contraintes que des règles posent, c'est avant tout pour permettre le développement de l'innovation que celui-ci a été pensé.

Si nous laissions se développer une IA de *scoring* pour l'accès à un crédit bancaire, en même temps qu'une IA pour mieux soigner le cancer grâce aux données de santé d'un individu, la seconde survivrait-elle à la première ?

2. L'AI Act : l'incompris qui voulait faire le bien

En avril 2021, la Commission européenne publie le projet de règlement « Artificial intelligence Act », qui deviendra 3 ans plus tard l'AI Act. Dès cette date, la proposition affiche une ambition claire : préparer l'Union européenne à devenir un leader mondial de l'intelligence artificielle, sous l'impulsion notamment de la France qui publiait dès janvier 2017 sa stratégie pour fédérer les acteurs (France IA) à l'initiative d'Axelle Lemaire, secrétaire d'Etat chargée du numérique, et Thierry Mandon, secrétaire d'Etat chargé de l'enseignement supérieur et de la recherche.

Le considérant de l'AI Act est absolument clair sur ce point : *« En établissant ces règles, ainsi que des mesures en faveur de l'innovation mettant un accent particulier sur les petites et moyennes entreprises (PME), parmi lesquelles les jeunes pousses, le présent règlement contribue à la réalisation de l'objectif qui consiste à promouvoir l'approche européenne de l'IA axée sur l'humain et faire de l'UE un acteur mondial de premier plan dans le développement d'une IA sûre, fiable et éthique, ainsi que l'avait formulé le Conseil européen, et il garantit la protection de principes éthiques expressément demandée par le Parlement européen[28]. »*

Ce rappel de l'objectif est indispensable car à contre-courant des critiques qui ont très vite émergé sur les limites que le règlement poserait pour l'innovation. En d'autres termes, de nombreux entrepreneurs ont relevé que la France et l'Europe risquaient de nouveau de passer à côté de la révolution IA, après celle de l'Internet,

[27] Ces risques sont cités dans le point 8 du considérant de l'AI Act.

[28] Point 8 du considérant de l'AI Act.

à cause de son cadre trop rigide.

Or rentrer dans les grands principes du texte conduit à conclure en faveur d'un texte conforme à son objectif tel qu'il avait été initialement exposé, tant le texte semble aller dans le bon sens et tenir compte du sujet majeur de l'acceptabilité, condition *sine qua none* d'un développement de l'IA en Europe.

L'AI ACT : DÉFINIR LES RISQUES, INTERDIRE L'INACCEPTABLE ET ENCADRER LES USAGES LES PLUS SENSIBLES, ASSURER UNE TRANSPARENCE MINIMALE

L'AI Act entre en vigueur de façon échelonnée. Son premier volet, entré en vigueur le 2 février 2025, s'attache d'abord à classer les IA par niveau de risque et interdire celles qui présentent des risques inacceptables. C'est le cas des systèmes de notation sociale, des IA de surveillance de masse ou d'évaluation du risque criminel d'un individu à partir de données biométriques, ou des IA chargées de manipuler ou de tromper délibérément un individu.

L'Union européenne a pris l'initiative de proposer un cadre législatif pour encadrer l'utilisation de l'IA à travers l'AI Act (proposition de règlement sur l'intelligence artificielle), présenté en avril 2021. Ce règlement vise à établir une approche cohérente pour la réglementation de l'IA en Europe, en prenant en compte les risques associés à ces technologies et en mettant l'accent sur la sécurité et l'éthique.

Interdire l'inacceptable[29]. Le règlement classe les systèmes d'IA en fonction de leur niveau de risque, de "faible risque" à "haut risque", et impose des obligations en fonction de cette classification. Par exemple, les systèmes utilisés pour les applications à haut risque, comme l'IA appliquée à la santé ou à la sécurité publique, devront satisfaire à des exigences strictes de transparence, d'évaluation de la conformité et de surveillance continue.

Cela devrait être notamment le cas d'une application telle que Clearview AI, déjà sanctionnée par la CNIL et ses homologues italiens et néerlandais pour manquements au RGPD. Cette entreprise établie hors de l'Union européenne propose un moteur de recherche d'images de personnes physiques, à partir d'extractions massives sur internet, y compris de personnes établies dans l'Union européenne. L'utilisateur de l'application peut ensuite soumettre une photo pour vérifier la correspondance avec la personne enregistrée dans le système, dans le cadre d'une arrestation par la police, par exemple.

Il est dès lors très clair que les usages interdits sont strictement contraires à nos valeurs. Et il n'y aurait certainement aucune circonstance qui permettrait de les exploiter sur le marché européen, tant ils cliveraient. La défiance qu'ils feraient naitre rejaillirait au contraire sur l'ensemble des entrepreneurs de l'IA.

Encadrer les systèmes à haut risque[30]. L'AI Act définit ensuite des systèmes à haut risque. Ce sont ceux qui peuvent porter atteinte à la sécurité des personnes ou à leurs droits fondamentaux et justifient ainsi que leur développement soit soumis à des exigences renforcées. Parmi ces exigences figurent des évaluations de conformité et une documentation technique des mécanismes de gestion des risques. Les systèmes concernés sont listés dans deux annexes du règlement : les produits qui font déjà l'objet d'une surveillance de marché dans l'annexe I (parmi lesquels figurent les dispositifs médicaux, la sécurité de l'aviation civile ou les véhicules) et ceux de huit domaines spécifiques dans l'annexe III (les systèmes biométriques, les infrastructures critiques, l'éducation, l'emploi, l'accès aux services publics essentiels, l'application de la loi, l'immigration et l'administration de la justice).

Rester vigilant en cas de risque spécifique. Une troisième catégorie est prévue pour les IA qui présentent un risque spécifique, par exemple en cas de risque manifeste de manipulation. Cette catégorie reste large puisque le recours à un

[29] Article 5 de l'AI Act.

[30] Article 6 de l'AI Act.

robot conversationnel peut être concerné. Dans ce cas, des obligations de transparence sont prévues, sans autre contraintes.

La quatrième catégorie des IA classées par niveau de risque est celle des systèmes à risque minimal. Dans ce cas aucune obligation spécifique n'est prévue.

Le cas particulier des IA à usage général. Au-delà des IA classées par niveau de risque, l'AI Act adresse un cas particulier, qui n'était initialement pas prévu et a été ajouté lors des débats au Parlement européen : celui des IA à usage général. C'est-à-dire, les IA qui remplissent un grand nombre de tâches et sont ainsi très difficiles à classer dans l'une des quatre catégories de risques.

C'est exactement le cas des IA génératives et notamment des grands modèles de langage (LLM) tels que ChatGPT, DeepSeek ou Le Chat de Mistral AI.

Pour ces IA, différentes obligations sont prévues. Ces obligations comprennent des mesures de transparence et de documentation minimales en matière des capacités et des limites du système, ainsi qu'en matière de droit d'auteur et de droits voisins, et de contenu utilisé pour entraîner le modèle[31].

Ces obligations minimales peuvent être complétées par d'autres obligations[32] lorsque le modèle présente un risque systémique tels que son utilisation pour des cyberattaques ou des biais avec des effets discriminatoires[33].

Sept critères permettent d'évaluer cet impact[34] : le nombre de paramètres du modèle, la qualité et la taille des données d'entraînement, la quantité de calcul utilisée pour l'apprentissage, les modalités d'entrée et de sortie du modèle, l'évaluation des capacités du modèle, l'impact du modèle sur le marché intérieur, et le nombre d'utilisateurs finaux.

NIVEAU DE RISQUE	OBLIGATION	DATE D'ENTRÉE EN VIGUEUR
Inacceptable	Interdiction	2 février 2025
Haut risque	Exigences renforcées	2 août 2026 pour l'annexe III et 2 août 2027 pour l'annexe I
Risques spécifiques	Obligations de transparence	2 août 2026
Minimal	Aucune obligation spécifique	
IA NE POUVANT ÊTRE CLASSÉES PAR NIVEAU DE RISQUE		
IA à usage général	Différents niveaux d'obligations en fonction du risque	2 août 2025

Exceptions pour favoriser les innovations. Et à ceux qui persistent dans l'idée que l'AI Act serait définitivement « tue l'innovation », ce dernier introduit par ailleurs des « bacs à sable réglementaires »[35], des environnements contrôlés où les systèmes d'IA peuvent être développés, testés et validés avant leur mise sur le marché. Ces bacs à sable permettent d'identifier et d'atténuer les risques liés aux droits fondamentaux,

[31] Article 53 de l'AI Act.

[32] Article 55 de l'AI Act.

[33] Point 110 du considérant de l'AI Act.

[34] Une présomption d'impact élevé, donc de risque systémique, est établie par l'article 51 de l'AI Act pour les cas où le volume cumulé de calcul utilisé pour l'apprentissage du modèle est supérieur à 1025 opérations à virgule flottante par seconde (FLOPS).

[35] Article 57 de l'AI Act.

à la santé et à la sécurité. Ils fournissent également des orientations sur les attentes et les exigences réglementaires. Un système d'IA testé avec succès dans un bac à sable peut servir de preuve de conformité à la réglementation, facilitant ainsi la coopération transfrontalière et le partage des meilleures pratiques.

Présenté ainsi, le cadre juridique qui encadre l'utilisation de l'IA, pour la donnée et les usages donc, semble protéger, davantage qu'il ne contraint. Il interdit l'inacceptable et encadre ce qui est sensible. Notre cadre juridique crée en cela une couche protectrice susceptibles de faciliter l'acceptabilité des nouveaux usages par un marché curieux mais craintif.

EXCEPTIONS POUR FAVORISER LES PME

L'AI Act contient une série de mesures prévues spécifiquement pour les PME afin de soutenir et simplifier leur mise en conformité. Les bacs à sable réglementaires seront accessibles gratuitement et en priorité aux PME, avec des procédures simples. Les frais d'évaluation des systèmes seront proportionnels à la taille des PME et le sujet sera régulièrement évalué par la Commission, pour effectuer des ajustements le cas échéant. Des formulaires de documentation technique simplifiés seront réalisés par la Commission, avec également des formations dédiées. Des canaux spécialement prévus à cet effet seront également créés pour faciliter la mise en conformité des PME. Enfin, les obligations imposées aux fournisseurs d'IA à usage général sont adaptées et proportionnées. Ainsi, le code de bonnes pratiques doit prévoir des indicateurs de performance spécifiques pour les PME.

LE PRÉCÉDENT DU MAUVAIS PROCÈS FAIT AU RGPD

Avant l'AI Act, le RGPD, déjà, avait été accusé de bloquer l'innovation. Car il force à qualifier des données parfois difficiles à contextualiser et multiplie les obligations en termes de transparence, les textes sur les données non personnelles ajoutent à cela d'autres obligations sur des données qui ne mettent pourtant pas la liberté ou la vie privée de qui que ce soit en danger.

Aussi, ces cadres créent d'importants risques contentieux, susceptibles de mettre en difficulté une entreprise qui tenterait d'y échapper. L'amende peut aller jusqu'à 4 % du chiffre d'affaires annuel mondial et la publicité qui peut en être faite ajoute aux conséquences négatives.

En 2021, Amazon Europe Core a ainsi reçu en première instance[36] une amende de 746 millions d'euros pour non-respect du RGPD par la Commission nationale pour la protection des données (CNPD), l'équivalent local de la CNIL. Le régulateur lui reprochait de ne pas avoir respecté le cadre européen, en particulier dans la collecte des données de ses utilisateurs. Amazon avait déjà été condamnée par la CNIL, en 2020, pour non-respect des règles concernant les traceurs publicitaires (cookies).

Cette sanction illustre les conséquences que le non-respect du RGPD peut avoir, elle reste inédite dans ses proportions. Google a par exemple été condamnée à

[36] Une procédure d'appel est en cours. La société reproche notamment au régulateur de ne pas lui avoir permis de modifier ses pratiques, avant de lui infliger une telle amende.

deux amendes par la CNIL, également pour non-respect des règles en matière de traceurs publicitaires faute de respecter les obligations en matière de recueil du consentement des utilisateurs, mais celle-ci plafonnait à un montant cumulé de 100 millions d'euros[37].

Au-delà de l'amende, la simple mise en demeure peut mettre en difficulté une entreprise qui n'a pas l'assise financière d'un géant.

Le 5 février 2020, Olivier Magnan-Saurin, cofondateur de la start-up Fidzup, poste un article intitulé « La CNIL m'a tueR »[38]. Cette entreprise commercialisait des campagnes marketing géolocalisées pour attirer le consommateur vers un point de vente physique (modèle de « drive-to-store ») depuis près de neuf ans et avait été mise en liquidation judiciaire deux mois plus tôt. La raison invoquée ? Une mise en demeure rendue publique par la CNIL en juillet 2018, en même temps que deux autres start-ups du secteur, qui avaient elles réussi à se relancer après mise en conformité[39]. L'entrepreneur explique ensuite que cette publicité a rendu quasiment impossible le développement de l'application, en pleine évangélisation du marché.

La CNIL avait alors jugé nécessaire « d'alerter les millions de personnes dont les données étaient collectées et traitées à leur insu ». Cette mise en demeure publique visait également à éviter le développement de ce modèle « sur la base de telles pratiques » en envoyant une « alerte collective ».

Si la start-up Fidzup n'a pas réussi à surmonter la mise en demeure, Singlespot, une autre des start-up concernées en a fait un atout marketing.

Alors qu'elle se heurtait à d'importantes questions sur le cadre juridique et un défi majeur d'acceptabilité de l'offre par le marché, la start-up a retourné la mise en demeure en sa faveur. Ainsi, Thomas Opoczynski, co-fondateur de Singlespot, expliquait que la mise en place du RGPD avait freiné certains clients, compte tenu du risque qu'ils encouraient s'ils travaillaient avec une start-up dont la conformité avec le cadre juridique n'était pas certaine[40]. La procédure ouverte avec la CNIL leur a permis d'ouvrir un nouveau champ commercial, en clarifiant ce point.

Dès 2018, la CNIL osait : « Si vous respectez le RGPD, vous aurez un avantage concurrentiel ! »[41]. Une étude de 2022, réalisé par le laboratoire d'innovation numérique de la CNIL (LINC) et une revue de littératures publiée le 1er mars 2024 par la Revue européenne des médias et du numérique tendent à confirmer cette approche, avec équilibre et nuance, bien que avantages et inconvénients puissent être relevés dans les deux sens et qu'un avantage plus important semble se dégager pour les plus grandes entreprises.

[37] Ces deux amendes ont été confirmées par le Conseil d'Etat le 28 janvier 2022. Décision n° 449209 des 10e et 9echambres réunies.

[38] Article posté sur Medium, le 5 février 2020.

[39] Teemo (rachetée depuis par le groupe Near), Vectaury (rachetée depuis par Mobsuccess) et Singlespot.

[40] Géraldine Russell, « Comment Singlespot a fait face à la mise en demeure de la Cnil », Maddyness.com, 29 novembre 2018.

[41] CNIL, Guide pratique de sensibilisation au RGPD, 2018.

3. Là où le bât peut réellement blesser : mieux articuler les règles entre elles

Nos protections contemporaines ne sont à elles seules pas gênantes, et le contraire est plutôt démontré. Ce qui peut rendre certaines données inutilisables ou empêcher des pratiques potentiellement utiles c'est en fait la multiplication des règles, notamment sectorielles et de responsabilité, qui ajoute à la complexité sans que la plus-value devienne évidente. Or c'est à cet instant qu'un doute sur l'utilité d'une règle peut exister.

Une complémentarité AI Act et RGPD à préciser. L'AI Act est à première vue très complémentaire des textes relatifs aux données, dont le RGPD. Aux uns la donnée, à l'autre le système d'intelligence artificielle. Le RGPD s'appliquant par exemple en même temps que l'AI Act à chaque fois que des données personnelles sont en jeu.

Plusieurs difficultés doivent toutefois déjà être relevées.

S'agissant de l'instance de contrôle[42], d'une part. La CNIL est évidemment chargée des sujets relatifs au RGPD. C'est nettement moins évident concernant l'AI Act, qui est davantage une réglementation produit et rognerait donc sur les plates-bandes d'autorités sectorielles dédiées.

La formation et le savoir-faire de la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) peuvent en ce sens être vus comme un atout, s'il s'agit de n'arrêter qu'une seule autorité référente.

Mais une alternative pourrait être trouvée dans le modèle retenu par l'Irlande qui a désigné des régulateurs sectoriels comme autorités nationales compétentes[43]. Cela doit permettre aux entreprises et entités publiques de s'assurer que les échanges se fassent à un haut niveau de connaissance technique et sectorielle et ainsi faciliter la mise en place des nouvelles exigences, à condition de s'assurer d'une bonne articulation avec la CNIL, sans que l'une ne déborde sur la compétence de l'autre.

Dans l'hypothèse où les moyens financiers et humains de chacune des autorités retenues peuvent être suffisants, cette solution pourrait être la plus à même de répondre aux enjeux et à l'équilibre entre régulation et innovation.

Cela pourrait éviter d'ajouter des frottements sectoriels car sur le fond, d'autre part, le RGPD et l'AI Act ont déjà quelques zones de frottement clairement identifiées. C'est le cas des conditions d'anonymisation et de pseudonymisation des données, jugées trop strictes par de nombreux acteurs, empêchant l'utilisation de certaines données comme données d'apprentissage.

L'enjeu de la durée de conservation des données. C'est également le cas de la durée de conservation des données, qui présente le même écueil. Or ce sujet est souvent mal compris, y compris par le régulateur. Ces dernières années, deux sujets d'intérêt général avaient ainsi été proches d'échouer pour cette raison.

D'abord, dans le cadre de la crise covid, lorsque le gouvernement avait proposé

[42] Article 70 de l'AI Act.

[43] Huit autorités sectorielles ont été retenues : la Banque centrale d'Irlande, la Commission pour la régulation des communications, la Commission de régulation des chemins de fer, la Commission de la concurrence et de la protection des consommateurs, la Commission pour la protection des données, l'Autorité de sécurité et de santé, l'Autorité de régulation des produits de santé, et le Bureau d'enquête maritime du ministère des transports

la mise en place de fichiers consolidés à des fins de recherche et de lutte contre l'épidémie. Il s'agissait alors de permettre conserver les données un certain temps pour que les systèmes d'information aient suffisamment d'informations pour que cela soit pertinent. Or à chaque texte de la crise sanitaire, le sujet revenait sur la table et les parlementaires discutaient d'une réduction du délai de conservation.

Ensuite, dans le cadre de l'expérimentation de la vidéo intelligente pour le maintien de l'ordre public, en vue des Jeux olympiques et paralympiques de Paris 2024. Là encore, il s'agissait de démarrer l'expérimentation suffisamment tôt pour entraîner la technologie en amont de l'événement, et de l'arrêter suffisamment tard pour envisager de conserver la technologie ensuite, en filant avec une loi de pérennisation, sans quoi, tout serait perdu dans l'intervalle. Et cette fois encore, la durée de conservation a fait l'objet de longs échanges et débats, beaucoup des parlementaires pensant possible de n'avoir une technologie et les données qui vont avec que quelques jours pendant lesquels cela est utile. Faisant fi de toutes les règles d'entraînement.

Sur ce point, un équilibre devra nécessairement être de nouveau recherché, en utilisant au mieux les souplesses prévues par le RGPD à des fins de recherche notamment[44], pour s'assurer d'un fin équilibre du balancier entre la protection des libertés publiques et la compétitivité de notre IA. C'est particulièrement vrai dans les domaines d'intérêt général, très bien couverts et défendus par l'AI Act, notamment grâce aux bacs à sable réglementaires. Nettement moins par le RGPD lorsque les deux textes viennent à être articulés, alors que le seul principe de la minimisation des données paraît être en contradiction avec les besoins d'une IA, qui plus est générative. D'autant plus qu'à ce stade, en cas de conflit, c'est le RGPD qui l'emporte.

Les recommandations pratiques de la CNIL régulièrement mises à jour et le récent avis de décembre 2024 du Contrôleur européen de la protection des données sont des premières étapes importantes pour éviter les zones de frottement mais ne suffisent à lever les points d'achoppement, notamment ceux ainsi présentés[45].

Conflits d'interprétation entre autorités au sein de l'Union européenne. Une autre complexité émerge des divergences d'interprétation entre autorités nationales au sein de l'Union européenne. Le RGPD, en particulier, bien qu'européen, peut en effet faire l'objet de lectures différentes d'un pays à l'autre, sans que l'harmonisation ne puisse intervenir dans un délai même raisonnable, créant un point de friction fort pour l'innovation et le déploiement d'IA françaises et européennes, quand d'autres IA étrangères bénéficient de lectures plus souples.

Ainsi, l'Irlande, qui a récemment pu durcir sa position s'agissant d'IA[46], est régulièrement pointée du doigt pour sa lecture laxiste du RGPD alors que le principe

[44] Article 5 du RGPD, en particulier le e).

[45] Parmi les autres sujets, une communication du Parlement européen en date de février 2025 identifie un conflit entre l'AI Act et le RGPD s'agissant des discriminations algorithmiques. Quand l'AI Act prévoit la possibilité d'utiliser des données personnelles particulières pour éviter les biais et les discriminations de systèmes à haut risque, le RGPD restreint ensuite trop largement les bases juridiques rendant possible l'utilisation de ces données. Le RGPD rend donc en quelque sorte la disposition de l'AI Act inopérante.

[46] En 2024, la CNIL irlandaise a rappelé à l'ordre Meta et X s'agissant de l'exploitation de données personnelles par leurs LLM. Une enquête a également été ouverte concernant Google.

du guichet unique en fait l'autorité cheffe de file pour les dossiers impliquant les sociétés installées sur son territoire, c'est-à-dire la majorité des géants de la tech.

La Data protection commission, équivalent de la Cnil pour l'Irlande, a ainsi demandé en décembre 2022 l'annulation partielle de décisions contraignantes rendues par le Comité européen de la protection des données (CEPD) dans le cadre du contrôle de réseaux et applications du groupe Meta. Le Tribunal de l'Union européenne a rejeté la requête en janvier 2025[47].

Il n'en reste pas moins que le mécanisme de coopération prévu par le RGPD doit fonctionner à plein et de manière objective pour que les textes européens ne soient pas un boulet pour les entreprises françaises et européennes, mais bien une protection dans leur développement.

La stratégie 2024-2025 de l'EDPB (European data protection board - le Comité européen de la protection des données), annoncée en avril 2024, va dans ce sens en affichant parmi ses piliers l'harmonisation entre les États membres et une coopération efficace entre les autorités de protection. Des réponses concrètes pourront être utilement apportées à ces différents points dans le cadre de l'omnibus annoncé le 13 mars 2025 par le commissaire européen McGrath. Ce prochain paquet doit permettre de simplifier le RGPD et notamment la mise en conformité des TPE.

LA NORMALISATION DE LA RÈGLE DE DROIT COMME SÉCURITÉ JURIDIQUE

Une première réponse aux conflits d'interprétation pourrait être apportée par une mécanique davantage codable de la règle de droit, qu'il s'agisse des textes de droit dur ou de droit mou.

Car avec l'IA et les infrastructures dédiées, si les données et les usages se multiplient, l'automatisation aussi. Ainsi, pour prendre l'exemple des espaces de partage de données (data space)[48] portés par la Commission européenne pour permettre aux acteurs européens de bénéficier d'une grande qualité de données partagées,

Ces data space maintiennent chaque acteur dans son rôle de responsable des données mais créent des règles de circulation et de traitement entre les acteurs en fonction de cas d'usage sectoriels. Ces règles et cas d'usage sont prévues par un « Rulebook ». Or, si le droit est clair et facile à traduire dans le code, il permettra au « Rulebook » une mise en oeuvre normalisée de ces espaces de partage.

Seulement, si l'AI Act s'en rapproche largement, d'autres textes dont le RGPD pourraient encore être améliorés pour faciliter. Un omnibus dédié pourrait être envisagé comme signal extrêmement favorable à l'innovation dans les prochains mois.

Régimes de responsabilité et incertitude juridique. En février, l'Union européenne a retiré son projet de directive sur la responsabilité en matière d'IA. Ce texte visait

[47] Tribunal de l'UE, 29 janvier 2025, affaires jointes T-70/23, T-84/23 et T-111/23.

[48] A ne pas confondre avec les lacs de données, qui visent à mettre en commun les données de plusieurs acteurs. Un *data space* est écosystème des données de confiance, composé d'une infrastructure de mutualisation et partage de données entre pairs, et d'une gouvernance dédiée. Ces espaces sont nécessaires à la création d'un marché unique européen de la donnée.

à harmoniser les règles de responsabilité des 27 pays en matière d'IA, alléger la charge de la preuve pour les victimes de dommages causés par des systèmes d'IA.

En conséquence, les règles de responsabilité en matière d'IA vont à ce stade rester réparties entre les régimes généraux de responsabilité des États membres et le régime spécial de responsabilité des produits défectueux. C'est d'ailleurs l'existence de ce dernier régime qui tend à rationaliser le choix de la mise sur pause peut être définitive d'un régime de responsabilité dédié à l'IA. Car si la directive relative à la responsabilité du fait des produits défectueux mise à jour[49] doit encore être transposée par les Etats membres, elle tient utilement et largement compte des évolutions liées au numérique et notamment aux usages de l'Intelligence artificielle.

Cette articulation n'est pas en soi une hérésie et présente une certaine cohérence. Mais elle peut créer une réelle incertitude juridique dans les chausse-trappes des produits défectueux, de certains usages de l'IA et dans certains cas transfrontaliers vite arrivés.

Il conviendra donc de s'assurer que ces cas d'incertitude soient rapidement surpassés et, surtout, qu'ils ne bénéficient pas aux entreprises les plus puissantes des nouvelles technologies qui auront tendance à répondre à la question de la responsabilité dans leurs contrats, lesquels étant extrêmement difficiles à négocier, s'agissant de contrats d'adhésion.

Le sujet de la responsabilité est par ailleurs amené à prendre de l'importance avec l'agentification de l'IA. Dès lors qu'un agent sera désormais programmé pour proposer des prises de décision et exécuter des actions, de nombreuses questions vont émerger : un agent IA est-il juridiquement autorisé à faire cela et à qui incombe la responsabilité d'un préjudice qui serait commis dans ce schéma ?

Là encore, qu'une incertitude juridique puisse exister s'entend, mais qu'elle freine l'innovation ne doit plus être accepté.

LE RISQUE DU CUMUL DE CADRES JURIDIQUES

Au-delà de l'articulation des textes dédiés, le cumul avec d'autres réglementations sectorielles est également un point de vigilance élevée.

Le secteur de la santé est une autre parfaite illustration de ces défis liés à l'existence de normes.

Prenons une startup du secteur qui serait créée en France et se proposerait d'utiliser l'IA pour répondre à une problématique donnée. Viennent évidemment d'abord l'AI Act et le RGPD : l'usage envisagée est-il interdit ou à haut risque et les données requises peuvent être utilisées et sous quelles conditions ?

Viennent ensuite les règles en matière de médicament et de produits de santé. L'entreprise devra respecter le règlement relatif aux dispositifs médicaux[50] puis il devra se conformer aux normes de l'Agence dédiée en France[51] et à celles des agences

[49] Directive (UE) 2024/2853 du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux.

[50] Règlement 2017/745.

[51] Agence nationale de sécurité du médicament et des produits de santé (ANSM).

dédiées dans les autres pays dans lesquels il souhaiterait développer sa solution.

L'hébergement des données de santé obéira au même schéma parfois complexe avec des serveurs certifiés requis qui seront souvent différents d'un pays à l'autre, y compris au sein de l'Union européenne.

C'est donc cette multiplication des règles et des exigences spécifiques par secteurs et par pays qui finit par poser des défis importants, notamment dans des secteurs très réglementés comme la santé. La sécurité ou la défense pourraient également être cités.

Si l'AI Act et le RGPD sont bien souvent de faux coupables et offrent une protection bienvenue créatrice de plus-value économique, contrairement au discours ambiant, une meilleure intégration réglementaire au sein de l'UE est toutefois nécessaire pour éviter que la complexité née du cumul des règles n'entrave la compétitivité et l'innovation et que les entreprises puissent définitivement transformer le défi de la régulation en un avantage concurrentiel majeur.

Dans ce contexte, la maîtrise du droit va nécessairement devenir un outil concurrentiel important tout comme la capacité à influer sur les réglementations futures en utilisant, notamment, les travaux d'évaluation parlementaires.

B. LA SÉCURITÉ DES DONNÉES ET DES USAGES COMME CONDITION DE MAINTIEN SUR LE MARCHÉ

En plus des règles d'éthique, un deuxième corps de règles propre aux nouvelles technologies touche naturellement l'IA : les règles de cybersécurité.

Deux problématiques doivent être particulièrement mentionnées :

- Les risques de cyberattaques qui viseraient les systèmes d'IA,
- L'utilisation d'un système d'IA à des fins délictuelles ou criminelles.

Le dernier rapport annuel sur la cybercriminalité, publié en juillet 2024 et portant sur l'année 2023, fait état de 278 770 atteintes numériques enregistrées en France en 2023, soit 40 % d'atteintes en plus en 5 ans, dont 59 % d'atteintes aux biens et 6 % d'atteintes aux institutions et à l'ordre public.

Une infographie publiée par Bpifrance avec une start-up spécialisée dans l'assurance, Dattak, en avril 2024 précise, s'agissant des entreprises, que le nombre d'attaques a augmenté pour 23 % d'entre elles, que 49 % des cyberattaques atteignent leur objectif, que pour 65 % des entreprises touchées les cyberattaques ont eu des conséquences sur leurs affaires.

Pour les entreprises, le risque cyber est dans de nombreux pays devenu le premier des risques[52].

La nouveauté : **90 % des attaques par déni de service sont réalisées grâce à l'intelligence artificielle** et l'IA générative permet de nouvelles « attaques sophistiquées

[52] Rapport d'Allianz, « Allianz risk barometer 2024 », janvier 2024.

et ciblées, à grande vitesse et à grande échelle »[53].

1. L'Émergence de nouvelles menaces

Les technologies de rupture, telles que l'intelligence artificielle (IA) en particulier générative ou agentifiée, sont largement adoptées par les entreprises en raison des promesses d'efficience, d'avantages concurrentiels et de croissance commerciale durable qu'elles semblent offrir.

Une étude réalisée par l'assureur Hiscox sur la gestion des cyber-risques et publiée en octobre 2024[54] révèle par exemple que l'IA générative est déjà intégrée dans les opérations de sept entreprises sur dix. Pourtant, seulement 56 % des dirigeants pensent que cette technologie aura un impact significatif sur leur profil de risque en cybersécurité.

Cette adoption rapide peut engendrer des vulnérabilités si les mesures de cybersécurité ne suivent pas le rythme : un service peut être rendu le service indisponible alors qu'une entreprise en est devenue totalement dépendante – ainsi **ChatGPT a déjà fait l'objet d'attaques dont une importante en 2023**[55], une attaque peut infecter le service en empoisonnant les données[56] ou peut permettre de récolter un nombre très important de données, parfois d'une grande confidentialité.

Or, **70 % des entreprises interrogées** pour le rapport Hiscox **disent avoir déjà intégré l'IA générative dans leurs opérations**[57].

Cependant, cette adoption rapide de nouvelles technologies s'accompagne de risques accrus en matière de cybersécurité. Les systèmes d'information deviennent plus complexes et interconnectés, **augmentant ainsi la surface d'attaque des entreprises et leur vulnérabilité aux cybermenaces**. Malgré cela, seuls 56 % des dirigeants pensent que la technologie aura un impact sur leur profil de risque[58], ce qui peut conduire à une sous-estimation importante des menaces potentielles.

Ce risque est également accru parce que l'IA, qu'elle soit générative ou non, exploite un ensemble de technologies préexistantes, elles-mêmes déjà à risque. C'est le cas du cloud, un autre domaine où la menace évolue rapidement, et qui fait l'objet d'un récent rapport sur la menace de la part de l'Agence nationale de la sécurité des systèmes d'information[59].

Les environnements cloud sont de plus en plus ciblés par les cyberattaques en raison de l'intérêt croissant pour les données qu'ils traitent et de leur rôle d'entrée potentielle vers les systèmes des organisations. Les attaquants exploitent les vulnérabilités des équipements de bordure, comme les VPN, ainsi que les mauvaises

[53] Agence de l'Union européenne pour la cybersécurité, dans l'infographie publiée par BpiFrance et Dattak le 19 avril 2024.

[54] Observatoire Hiscox, « Rapport Hiscox 2024 sur la gestion des cyber-risques : la cyber-résilience pour protéger sa réputation », 24 octobre 2024.

[55] https://www.lesechos.fr/tech-medias/intelligence-artificielle/chatgpt-victime-dune-cyberattaque-massive-2027843

[56] https://fr.blog.barracuda.com/2024/04/03/generative-ai-data-poisoning-manipulation

[57] Rapport Hiscox, p. 2.

[58] Rapport Hiscox, p. 2.

[59] ANSSI, « Secteur du cloud – Etat de la menace informatique », 20 février 2025.

configurations et les défauts de sécurisation. Ces attaques sont souvent motivées par des objectifs lucratifs, d'espionnage ou de déstabilisation. Les attaquants utilisent désormais le cloud comme infrastructure pour stocker des codes malveillants ou des données volées, rendant la détection des activités malveillantes plus complexe.

La qualification SecNumCloud[60], label défini par l'ANSSI, vise d'ailleurs à répondre à cet enjeu en précisant les caractéristiques qu'un service d'informatique en nuage doit remplir pour assurer les exigences de sécurité à la fois techniques, opérationnelles et juridiques.

INVESTISSEMENTS EN CYBERSÉCURITÉ ET CYBER-RÉSILIENCE

Le rapport de l'assureur Hiscox de 2024 sur la gestion des cyber-risques met en lumière l'importance croissante de la cyber-résilience pour les entreprises face à des menaces en constante évolution. Selon le rapport, 67 % des entreprises ont signalé une hausse des cyberattaques au cours des 12 derniers mois, et le nombre moyen de cyberattaques subies par les entreprises est passé de 63 en 2022/2023 à 66 en 2023/2024.

Les conséquences des cyberattaques sur la réputation des entreprises sont également significatives. 61 % des dirigeants estiment qu'une atteinte à la réputation due à une cyberattaque porterait un préjudice majeur à leur entreprise. De plus, 47 % des entreprises ont eu plus de difficultés à attirer de nouveaux clients après une cyberattaque, et 43 % ont perdu des clients.

Les entreprises consacrent en moyenne 11 % de leur budget informatique à la cybersécurité, et 85 % des dirigeants interrogés rapportent avoir investi dans des formations en cybersécurité pour les salariés travaillant à distance. Ces investissements montrent que les entreprises prennent au sérieux la menace des cyberattaques et cherchent à renforcer leur résilience.

La cyber-résilience est considérée comme très importante pour la stratégie commerciale globale de 74 % des entreprises. Cependant, 53 % des entreprises estiment que leur cyber-résilience s'est améliorée au cours des 12 derniers mois, mais 40 % la jugent encore à un niveau de maturité « élémentaire » ou « inconstant ».

2. Notre cadre juridique comme avantage compétitif

Face au défi de la menace cyber, la France et l'Europe disposent d'un cadre juridique important. Cette réglementation doit être perçue comme un levier stratégique pour la compétitivité et la sécurité des entreprises.

75 % des répondants à une étude réalisée par l'entreprise américaine de logiciels Splunk[61] estiment ainsi que les **partenaires commerciaux apprécient le niveau de protection offert par l'Europe, et 68 % considèrent ces régulations comme un avantage concurrentiel.**

D'après cette même étude, les entreprises françaises semblent mieux protégées

[60] La qualification s'appuie sur la norme ISO 27001.

[61] Splunk, « rapport annuel sur la cybersécurité », avril 2024.

contre les cyberattaques par rapport à la moyenne mondiale. Seulement 44 % d'entre elles ont déclaré avoir subi une violation de données (contre 52 % à l'échelle mondiale), 40 % une attaque par ransomware (contre 45 %), et 37 % une attaque par déni de service. Cette performance peut être attribuée à une meilleure adhésion aux régulations européennes, qui offrent un cadre robuste pour la cybersécurité.

LES MESURES GÉNÉRALES DU RGPD ET DE L'AI ACT

Le RGPD a en particulier relevé les exigences en termes de sécurité des données personnelles, lesquelles sont sous le risque d'une utilisation malveillante par ceux qui les récupéreraient. Le règlement a ainsi renforcé les obligations de sécurité des entreprises et des administrations en prévoyant la mise en place de mesures techniques et organisationnelles pour sécuriser les données, la tenue d'un registre des violations de données, la réalisation d'une analyse d'impact pour les traitements sensibles, la notification à la CNIL d'une violation de données lorsqu'elle présente un risque pour les personnes et l'information des personnes d'une violation de données en cas de risque élevé pour ces personnes.

En 2023, 4 668 notifications de violation de données ont ainsi été effectuées, 60 % concernent des actes de piratage informatique dont 1 006 concernaient une attaque par rançongiciel (22 % du total).

Les administrations publiques sont les plus concernées (18 % des acteurs visés) devant les activités scientifiques et techniques (14 %), les activités financières et d'assurance (12 %), et les activités de santé humaine et d'action sociale (12 %). Sur les cinq années d'entrée en vigueur du RGPD, le secteur public concerne ainsi 22 % des notifications, alors que les PME en représentent 39 %.

Aussi, la CNIL relève dans son dernier rapport une progression significative des notifications liées à une perte d'intégrité, c'est-à-dire à une modification illégitime des données, et de disponibilité, c'est-à-dire des données rendues inaccessibles pendant un certain temps.

De la même manière, l'AI Act prévoit un certain nombre d'exigences en matière de cybersécurité. Sept principales catégories d'exigences peuvent ainsi être isolées : surveillance humaine[62], gestion des risques[63], *security by design*[64], documentation[65], gouvernance des données[66], tenues de registres[67] et résilience[68].

Le texte identifie un type d'IA avec un risque très spécifique : les IA à usage général[69]. Si des obligations de transparence accrues sont prévues pour ces systèmes, c'est également le cas en matière de cybersécurité. Ils doivent en effet présenter, comme les systèmes à haut risque, un niveau approprié de protection et une protection de l'infrastructure physique.

[62] Article 14 de l'AI Act.

[63] Article 9 paragraphes 1, 2 et 5 de l'AI Act.

[64] Article 9 paragraphe 5 et articles 15 paragraphes 1 et 4 de l'AI Act.

[65] Article 11 et article 13 paragraphes 2 et 3 de l'AI Act.

[66] Article 10 paragraphes 2 à 5 de l'AI Act.

[67] Article 12 paragraphes 1 à 3 de l'AI Act.

[68] Articles 14 paragraphe 4 et 15 paragraphes 4 et 5 de l'AI Act.

[69] Pour rappel, il s'agit des IA qui présentent une généralité significative et qui sont capables d'exécuter de manière compétente un large éventail de tâches distinctes.

DES TEXTES DÉDIÉS :

directive sur la résilience des entités critiques (REC), directive sécurité des réseaux et des systèmes d'information[70] (NIS2) et règlement résilience numérique du secteur financier[71] (DORA)

Trois textes doivent être mentionnés. Elles font, ensemble, l'objet d'un projet de loi de transposition, s'agissant des deux directives, et d'adaptations, s'agissant du règlement, en cours d'examen au Parlement[72]. Il devrait être adopté d'ici à l'été 2025.

Directive REC[73]. La directive relative à la résilience des entités critiques vise à améliorer la résilience des infrastructures critiques dans 11 secteurs[74]. Elle impose ainsi des règles communes à tous les États membres afin de garantir une protection minimale. Cette directive n'est toutefois pas une nouveauté, concernant la France, qui met déjà en œuvre un dispositif d'identification des opérateurs d'importance vitale depuis 2006[75]. Elle permettra dès lors d'assurer une concurrence plus loyale entre les opérateurs concernés au niveau de l'Union européenne, avec des règles exigeantes mais communes.

Ce dispositif repose sur une **responsabilité partagée entre l'État et les opérateurs**, qui doivent garantir la **sécurité physique et cyber de leurs infrastructures**. Un nouveau statut d' « entité critique d'importance européenne » est également créé pour les opérateurs exerçant dans au moins six États membres.

Directive NIS 2[76]. La directive NIS 2 **vise à renforcer la protection des entreprises et des administrations contre le risque cyber**. Elle élargit ainsi le champ des entités couvertes à 15 000 en France contre 500 sous NIS 1, et couvre désormais 18 secteurs[77], qui intègre les collectivités territoriales compte tenu de l'augmentation des cyberattaques contre les services publics locaux. Les entités sont classées dans deux catégories : « essentielles » et « importantes ». Des obligations de sécurité proportionnées en découlent, et sont susceptibles d'entraîner des sanctions renforcées en cas de non-respect.

Directive DORA[78]. La directive DORA concerne la résilience numérique du secteur financier et impose de **nouvelles exigences aux institutions financières** pour prévenir les risques numériques. Ce règlement harmonise ainsi les règles de gestion des risques liés aux technologies de l'information dans le secteur bancaire et financier.

Ce cadre juridique force les entreprises à anticiper, par des logiques de gouvernance par les risques, en fonction des risques identifiés sur les données ou sur les métiers :

- En identifiant les procédures qui permettent de limiter les risques et de résoudre les problèmes futurs,

[70] Network and Information Security.

[71] Digital operational resilience Act.

[72] Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité, déposé le 15 octobre 2024 au Sénat.

[73] Directive 2022/2557.

[74] Administrations publiques, eaux potables, eaux usées, énergies, espace, gestion des services technologies de l'information et de la communication, infrastructures des marchés financiers, infrastructures numériques, santé, secteur bancaire, transports.

[75] Dispositif de sécurité des activités d'importance vitale (SAIV).

[76] Directive 2022/2555.

[77] Secteurs hautement critiques : administrations publiques, eaux potables, eaux usées, énergies, espace, gestion des services technologies de l'information et de la communication, infrastructures des marchés financiers, infrastructures numériques, santé, secteur bancaire, transports. Autres secteurs critiques : fabrication, production et distribution de produits chimiques, fournisseurs numériques, gestion des déchets, industrie manufacturière, production, transformation et distribution de denrées alimentaires, recherche, services postaux et d'expédition.

[78] Directive 2022/2554.

- En préparant l'entreprise à des scénarios critiques avec un accent fort sur la résilience et la capacité à reprendre une activité, y compris réduite, le temps de résoudre le problème dans son ensemble.

Les textes tracent les mécaniques qui seront ensuite activées en période de gestion de crise, par les comités de pilotage et de gestion des crises, pour accompagner les acteurs dès les premières phases d'un incident avec des actions de notification en interne et auprès des personnes qui se retrouveraient victimes – dans le cadre d'un vol de données personnelles de la clientèle d'une entreprise par exemple.

Le cadre juridique va également aider à anticiper les responsabilités en cas de faute et donc faciliter les futures actions pré-contentieuses ou contentieuses ainsi que le volet pénal, avec le dépôt de plainte. Or y compris le dépôt de plainte requiert une certaine anticipation car il doit être effectué dans les 72 heures qui suivent l'incident, faute de quoi l'assurance ne pourra plus être actionnée.

Ce que le cadre juridique va permettre, c'est également de piloter les contrats avec les acteurs prestataires extérieurs, à la fois pour anticiper le risque, donc, mais aussi pour le limiter.

Le règlement DORA concernant le secteur financier est intéressant à ce titre car il impose de s'assurer que les impératifs de sécurité sont bien respectés par les prestataires, ce qui pourra exiger une forte consolidation sur le volet contractuel. Au terme de ce travail et d'audits approfondis, cela permettra de conforter un environnement et écosystème conformes aux textes, donc davantage robustes.

UN CADRE JURIDIQUE DE L'IA QUI DÉPASSE LES RÈGLES DÉDIÉES AU NUMÉRIQUE

Source : DSSC, relevant EU Legislations, novembre 2024

Au-delà des règles dédiées à l'innovation, de nombreux cadres juridiques initialement créés hors contexte peuvent intervenir dans le déploiement d'une IA. Ces règles sont multiples et parfois difficiles à identifier, or elles peuvent à elles seules constituer des obstacles suffisants pour ruiner la valeur d'un modèle ou forcer à un changement radical de modèle.

LE DROIT N'EST PAS L'ENNEMI DE L'INNOVATION. IL EN EST LA GARANTIE DE SON INTÉRÊT GÉNÉRAL.

II. L'INNOVATION JURIDIQUE POUR SE DÉMARQUER ET SOUTENIR UNE INNOVATION DURABLE

Ces règles sont de deux ordres :

- **l'ensemble des cadres généraux et transversaux du droit,** tels que le droit de la concurrence, le droit social, le droit des contrats ou le droit de la propriété intellectuelle. Des corps de règles peuvent évidemment être identifiés mais leur application à une activité variera en fonction du secteur envisagé.
- **les cadres juridiques relatifs aux enjeux nouveaux** et qui ont eux aussi une transversalité importante. Il s'agit des règles relatives à la protection de l'environnement et aux droits humains, dont le devoir de vigilance et les textes en matière de durabilité.

A. PROTÉGER SANS RALENTIR : LES CADRES JURIDIQUES TRADITIONNELS AU DÉFI DE L'IA

Le développement rapide de l'IA et en particulier de l'IA générative puis de son agentification, a des effets majeurs sur différents pans du droit.

Une technologie peut largement déstabiliser le rapport entre les salariés d'une entreprise et leur travail, appelant des mécanismes de droit social.

La création de textes, d'images ou de musiques par une machine remet d'abord substantiellement les règles de la propriété intellectuelle sur le métier.

La puissance de calcul détenue par un faible nombre d'acteurs et la nécessité de créer des alliances pour ne serait-ce que survivre bouscule le droit de la concurrence.

L'ensemble ayant ensuite des répercussions massives sur les contrats qui doivent tenir compte des nouveaux enjeux, anticiper des problématiques parfois difficiles à identifier, et créer de nouveaux équilibres entre les parties.

A cela doivent s'ajouter les règles sectorielles, dans la banque et la finance par exemple, mais également dans la santé, la sécurité.

UN RISQUE QUI PEUT ÊTRE FATAL

Il est nécessaire d'identifier dès le début d'un projet, et à chacun de ses changements majeurs, les cadres juridiques susceptibles d'être percutés par le modèle développé. Pour anticiper le droit déjà existant qu'il pourrait être tentant d'y ap-

pliquer, d'une part, et prévoir, surtout, une stratégie claire pour éviter qu'une règle existante ou à venir ne puisse avoir de conséquences sur un modèle en cours de développement.

Il s'agit moins cette fois d'utiliser des règles à son profit que d'utiliser la technique juridique pour créer un marché et le développer sans craindre de le voir invalidé par la norme ensuite.

Trois scénarios qui peuvent amener au pire doivent donc être évités :

- **Un changement réglementaire ou législatif qui contraint largement l'entreprise, voire la force à modifier de modèle.**

Récemment, les acteurs des jeux à objets numériques en ont subi les effets. Alors que se développaient des jeux en ligne sur le modèle des célèbres albums Panini de notre enfance mais avec des cartes convertibles en argent sonnant et trébuchant, les acteurs des jeux de hasard, profession largement réglementée, ont forcé les décideurs et le législateur à interroger leur cadre juridique. Dans cette suite, il a été nécessaire d'en passer par la loi, pour prévoir une expérimentation. La loi SREN crée ce régime en consacrant une définition légale des JONUM et en prévoyant son régime applicable avec des mesures de protection des joueurs, des règles strictes s'agissant des secteurs du sport et des courses hippiques, et un encadrement par l'Autorité nationale des jeux. Problème, le régime proposé encadre l'activité bien au-delà des mécanismes d'auto-régulation prévus par les acteurs, et réduit par exemple à peau de chagrin les gains convertissables en cryptomonnaies, donc une partie de l'attractivité de ces jeux.

- **Une complexité trop importante compte tenu de règles non adaptées.**

Il peut s'agir d'un cas similaire à celui évoqué précédemment dans le domaine de la santé, avec l'enchevêtrement de règles propres au numérique et de règles propres au secteur de la santé, puis au cumul de normes différentes d'un marché à un autre, mais qui ont pourtant fonctionné et protégé une économie physique pendant de nombreuses années.

- **Une non-conformité du fait de l'application d'une règle qui n'avait pas été anticipée ou l'avait mal été.** La propriété intellectuelle est à ce titre un bon exemple.

Le cas de la start-up Ross Intelligence est à ce titre intéressant. En février 2025, un tribunal américain a reconnu cette start-up coupable d'avoir utilisé des contenus produits par une filiale canadienne du groupe Thomson Reuters pour entraîner une IA dans le domaine de l'information juridique. Les avocats de la start-up ont tenté de démontrer un « usage raisonnable » d'œuvres protégées.

Toutefois, la justice a constaté que l'IA de Ross, qui a depuis fermé, n'était pas générative et que pour chaque réponse, des avis déjà rédigés étaient proposés, lesquels étaient directement récupérés auprès de la filiale en question de Thomson Reuters. **L'absence de valeur transformative écartait par conséquent la notion d'« usage raisonnable ».**

Trois autres affaires similaires sont en cours[79] avec des enjeux financiers extrêmement importants à chaque fois puisque le droit américain prévoit pour chaque infraction constatée une amende pouvant aller jusqu'à 150 000 dollars. La nature de l'IA, générative ou non, pourrait avoir un intérêt majeur sur les solutions proposées. Les trois sociétés en défense ne sont toutefois pas encore sauvées pour autant, car dans l'affaire Ross, le juge a également précisé que **l'usage raisonnable devrait être écarté quand les contenus utilisés servent à proposer des alternatives aux services d'origine** (créer une image à la place d'en acheter une par exemple), ou que l'usage des données avait un effet conséquent sur un potentiel marché, **en d'autres termes, s'il empêche les ayants droits de monétiser leurs contenus auprès de concepteurs d'IA**. Deux caractéristiques qui ne semblent pas exclues dans les affaires en question.

1. Le droit social et l'enjeu de l'adhésion interne

De nombreuses entreprises sont tentées de déployer des solutions d'IA, en particulier pour une amélioration du service client ou des gains d'efficacité, tant en temps qu'en qualité. Cela est vrai peu importe le secteur : l'industrie, la grande distribution, le commerce de détail.

Ainsi, en 2023, l'enseigne Carrefour déployait trois solutions d'IA : un robot conseil dénommé Hopla pour les courses en ligne, une IA générative pour améliorer les fiches produits mises en ligne et une autre IA générative pour les processus interne. Des enseignes Leclerc se sont-elles dotées de la solution Captana qui utilise l'IA et la computer vision pour remonter en temps réel les ruptures de stock et éviter les taux de rupture[80].

Dans le même temps, plusieurs industries ont optimisé leurs lignes de production grâce au projet OPTIMAI[81], qui permet d'éliminer les erreurs des processus de fabrication.

Puisqu'il s'agit d'en évoquer les défis juridiques, le premier réflexe est de revenir aux règles en matière de données, puis en matière d'usage, et éventuellement de discuter de responsabilité en cas de défaillance de la solution. Une récente ordonnance du tribunal judiciaire de Nanterre ouvre toutefois le champ de la discussion au droit social.

En 2024, l'assureur Metlife France déploie pas moins de cinq projets d'intelligence artificielle : un outil pour lutter contre la fraude documentaire, une IA générative pour de la vidéo, une autre pour un CRM, une troisième pour des textes et images, et un robot conversationnel interne. Bien que présentés comme des projets en phase pilote, tous sont proposés aux employés placés sous la responsabilité du directeur des opérations le 20 novembre 2024.

Peu de temps après, le Comité social et économique (CSE) de l'entreprise a agi

[79] La banque d'images Getty Images contre une start-up britannique Stability AI, le New Times contre OpenAI, et la RIAA qui représente l'industrie américaine du disque contre les IA de création de chansons Udio et Suno.

[80] D'après VusionGroup qui produit la solution, les premiers essais en magasin ont permis de réduire le taux de rupture de 3%.

[81] Optimizing Manufacturing Processes through Artificial Intelligence and Virtualization.

en référé pour bloquer le déploiement, faute d'avoir rendu son avis.

Or, le code du travail est très clair : *« Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail.*[82]*»*

Le CSE relevait ainsi des interrogations sur l'éventuel accroissement de la charge de travail liée en particulier à la solution de lutte contre la fraude documentaire, et sur les risques de suppression d'emplois dans l'hypothèse où les outils déployés permettraient d'accroître la productivité avec moins de ressources humaines.

Considérant que peu importe que la consultation du CSE soit obligatoire ou non, que le tribunal judiciaire de Nanterre a ordonné, dans l'urgence, l'arrêt du déploiement des cinq projets en question, dans l'attente de la fin de la procédure d'information du CSE, avec une astreinte de 1 000 euros par infraction par jour.[83]

Alors que l'AI Act marque une obligation générale de formation des personnels concernés par des systèmes d'IA[84], l'ordonnance du tribunal judiciaire de Nanterre, bien que prononcée dans l'urgence et donc sans jugement définitif sur le fond, force à considérer le droit du travail autrement que par le seul biais de la formation.

Évidemment, tous les projets ne sont pas concernés par ces règles. Mais il serait de bonne pratique d'ajouter les règles de droit social dans le logiciel d'analyse des projets à chaque fois qu'il concerne une entreprise devant constituer un CSE[85]. Faute de quoi, le déploiement des projets pourrait être largement retardé dans le temps et, surtout, l'acceptabilité serait remise en question pouvant aller jusqu'à leur abandon compte tenu de la contestation soulevée.

2. Le droit de la propriété intellectuelle au défi de l'IA générative

Hors les règles dédiées au numérique et à l'intelligence artificielle, les cadres juridiques relatifs à la propriété intellectuelle sont certainement parmi les plus cités, depuis l'émergence fulgurante de l'IA générative : qui est l'auteur et le détenteur des droits d'une production par IA ? Peut-on exploiter et/ou protéger un contenu généré par une IA ? Comment s'assurer du respect des droits sous-jacents qui reviendraient aux auteurs des sources éventuellement utilisées, en particulier dans la phase d'apprentissage ?

Pour donner une ébauche de réponse, il convient dans un premier temps de clarifier le fonctionnement d'une IA pour éviter tout malentendu. Car, régulièrement, les créations d'IA génératives sont mal comprises s'agissant de leur élaboration. D'aucuns considèrent qu'un contenu ainsi généré n'est qu'une reproduction d'un

[82] Article L2323-29 du code du travail.

[83] Tribunal judiciaire de Nanterre, ordonnance de référé, 14 février 2025, n°24/01457

[84] Article 4 de l'AI Act.

[85] Article L2311-2 du code du travail : « Un comité social et économique est mis en place dans les entreprises d'au moins onze salariés. Sa mise en place n'est obligatoire que si l'effectif d'au moins onze salariés est atteint pendant douze mois consécutifs. »

original, allant par conséquent systématiquement à la recherche de la source pour tirer ensuite le fil des droits de propriété intellectuelle classiques liés à la reproduction.

Le principe d'une IA générative est d'apprendre, à partir d'un modèle d'apprentissage automatique, pour créer ensuite du contenu de manière autonome, comme le ferait une intelligence humaine. C'est-à-dire qu'il ne s'agit pas de récupérer des morceaux de données et de les réutiliser en tout ou partie, mais bien de créer de nouveaux contenus, absolument inédits.

Là où des contenus originaux interviennent, c'est finalement dans la phase d'apprentissage. De la même manière qu'un peintre arpente régulièrement des recueils d'œuvres ou les allées d'un musée, pour s'en inspirer, une IA générative apprend d'abord des œuvres existantes avant de créer ses propres réalisations. Au-delà des œuvres, les données d'apprentissage pourraient d'ailleurs contenir des récits d'artistes ou des analyses de leurs techniques, pour en retenir les meilleures méthodes.

Et c'est bien dans cette mécanique complexe, similaire à celle de l'intelligence humaine, que les règles en matière de propriété intellectuelle se trouvent mises au défi.

Un défi toutefois pas inconnu puisqu'il rappelle largement des affaires récentes s'agissant d'intelligences totalement humaines, cette fois. C'est par exemple le cas de l'affaire Gad Elmaleh, accusé d'avoir plagié certains de ses sketchs. A quel moment un humoriste passe-t-il de l'inspiration au plagiat ?

Ces sujets ne sont finalement pas nouveaux et dépassent largement les humoristes. Il suffit d'écouter les quelques notes de trompette de « Hips don't lie » de Shakira après avoir écouté celles de « Amores como el nuestro » de Jerry Rivera, absolument pas prévenu par la chanteuse colombienne, pour s'en convaincre.

Plutôt que de s'engouffrer en terre inconnue en se rapprochant autant du fonctionnement de l'intelligence humaine, avec une phase d'apprentissage puis de création, l'IA générative s'est finalement orientée vers des problématiques davantage connues.

Lorsqu'un doute est émis s'agissant d'une éventuelle utilisation sans autorisation préalable d'éléments produits par un auteur, **la question serait finalement celle de l'originalité du contenu créé par rapport aux données d'apprentissage**. Comme la légalité d'un sketch de Gad Elmaleh dépendra de son originalité par rapport aux sketchs qui ont pu l'inspirer ou celle de notes de trompettes pour faire danser Shakira et ses fans dépendra de leur originalité par rapport à des notes d'une autre trompette qui avaient déjà pu faire danser une bonne partie de l'Amérique du sud.

Ce qui dérange, au fond, c'est qu'il ne s'agit plus de juger de la création d'un pair mais d'une machine, et cela à une échelle inédite et avec un risque de répétition perpétuelle.

Ce qui dérange, également et peut-être surtout, c'est que l'artiste est habituellement allé dans une école ou a acheté des prestations passées pour apprendre.

Or cette fois, il serait possible d'apprendre sans rien n'avoir acheté, sans aucune forme de financement de la création. Avec le risque de rompre un cercle vertueux, qui rémunère autant qu'il finance l'art et par là notre culture et celle des autres. C'est en cela aussi, un enjeu de souveraineté.

Deux principaux enjeux se dégagent alors :

- D'une part, l'importance de trouver les bons mécanismes pour faire respecter les droits de propriété et partager la valeur sans pour autant bloquer l'innovation.

Une directive de 2019 sur le droit d'auteur et les droits voisins[86] a prévu une exception aux règles d'utilisation d'œuvres et autres objets protégés pour la fouille de textes et de données[87]. Cette règle permet, en pratique, d'utiliser un contenu même protégé dès lors qu'il est en libre accès sur internet. Une exception à cette exception est prévue si l'utilisation des œuvres et objets protégés a été *« expressément réservée par leurs titulaires de droits de manière appropriée, notamment par des procédés lisibles par machine pour les contenus mis à la disposition du public en ligne »*[88] (principe de l'opt out).

Si le principe paraît difficilement discutable, sa mise en œuvre n'est pas simple puisqu'il sera particulièrement difficile pour un auteur de savoir si son œuvre a été utilisée ou non.

C'est pour répondre à cette difficulté que l'AI Act a introduit des exigences de transparence aux développeurs des modèles d'IA à usage général afin de garantir la traçabilité des données et des contenus, et d'informer les utilisateurs et ceux dont les contenus sont exploités[89]. Ce résumé doit suffisamment détailler le contenu utilisé pour entraîner le modèle d'IA à usage général[90].

Le niveau de contenu présent dans ce résumé doit faire l'objet d'une attention particulière, il en revient de cet équilibre entre protection des droits d'auteur et innovation. Car dans l'hypothèse où tous les éléments relatifs aux données d'apprentissage y seraient portés, cela reviendrait à révéler l'intégralité des techniques pour un humoriste ou un trompettiste.

Un rapport commandé par le Conseil supérieur de la propriété littéraire et artistique aux professeures Alexandra Bensamoun et Joëlle Farchy est chargé de rendre, dans le courant de l'année 2025, des propositions à ce sujet.

A ce titre, nous pourrions par exemple expertiser la possibilité de mettre en œuvre un mécanisme de distribution de la valeur créée en fonction de la part prise par des données d'entraînement dans la création d'un contenu par une IA

[86] Directive 2019/790.

[87] Article 4 de la directive 2019/790.

[88] Article 4, 3 de la directive 2019/790.

[89] L'initiative de Jeremy Howard, data scientist australien peut à ce titre être soulignée puisqu'il propose à la communauté tech un standard afin de coder des règles de partage des droits de propriété intellectuelle, compréhensibles par les crawlers. Pour un exemple concret, voir : https://docs.anthropic.com/llms-full.txt.

[90] Article 53, 1. d) de l'AI Act. Ce résumé doit être conformé à un modèle fourni par le Bureau de l'IA, qui doit par ailleurs encourager et faciliter l'élaboration de codes de bonne pratique, comprenant notamment le niveau approprié de détail pour ce résumé (article 56, 2. b) de l'AI Act).

générative[91] basé sur un *data space* des acteurs de la culture.

- D'autre part, la nécessité de solutions souveraines pour s'assurer que la culture ne soit pas guidée que par des sources américaines ou chinoises, jusqu'à l'abandon, à terme, de ce qui a fait pour partie la fierté de la France et de l'Europe.

3. Le droit de la concurrence et les barrières à l'entrée de l'IA

Parmi les sujets qui doivent alternativement être pris en compte par les développeurs d'IA et ceux qui les déploient figure également en très bonne place le droit de la concurrence. A savoir, l'interdiction pour les entreprises de s'entendre avec des concurrents ou partenaires commerciaux pour restreindre la concurrence, ou de profiter d'une position de force sur un marché pour en abuser au détriment d'un concurrent.

L'émergence de l'IA et plus encore de l'IA générative bouleverse les modèles économiques : de l'amélioration des performances, la possibilité d'intégrer des activités initialement réalisées à un autre niveau de la chaîne de valeur, ou la création de nouveaux services permettant de capter davantage de parts de marché.

Le sujet de l'IA générative a fait l'objet d'un rapport très complet de l'Autorité de la concurrence, publié en juin 2024, pour preuve de sa montée en puissance. Ce rapport aborde en particulier les problématiques de l'informatique en nuage dont celles liées à l'accès à ces infrastructures, à la puissance de calcul, aux données et à une main d'œuvre qualifiée, ainsi que les prises de participations et les partenariats des grands acteurs du numérique dans le secteur de l'IA générative.

L'Autorité propose trois grands constats :

• Des barrières à l'entrée élevées.

D'abord, parce que déployer une IA générative requiert une puissance de calcul rare tant pour l'entraînement que pour le réglage et l'utilisation des modèles, et une expertise juridique importante. Ainsi, très peu d'acteurs sont en mesure de proposer ces services[92], ce qui ne fait qu'en augmenter les coûts.

Ensuite, l'informatique en nuage apparaît indispensable tout comme le fait de disposer de larges volumes de données.

Enfin, les compétences techniques sont rares et le besoin de financement important.

A ce titre, l'autorité évoque trois **évolutions susceptibles de lever une partie de ces barrières** : des **supercalculateurs publics** qui seraient utilisés gratuitement en échange d'une contribution à la science ouverte, des **innovations technologiques** qui réduiraient les besoins en puissance de calcul et en données[93], **et des modèles ouverts.**

[91] Un modèle de ce type, intitulé « Hugging Face Space » est proposé par TheFrenchDemos et pourrait servir de point de départ.

[92] Les processeurs graphiques développés par Nvidia sont ainsi par exemple extrêmement demandés, avec peu d'alternatives possibles.

[93] A ce titre, l'IA chinoise Deepseek a pu susciter des espoirs compte tenu des informations révélées sur son coût et l'absence de puces développées par Nvidia. Ces informations n'ont toutefois pas pu être vérifiées à ce stade

Outre ces pistes, l'avenir des partenariats publics privés doit également être interrogé, dans un contexte où les règles européennes en matière d'aides d'État y sont peu favorables.

- **Un risque d'avantages concurrentiels pour des acteurs majeurs** d'autres marchés sur lesquels s'appuie le développement de l'IA générative.

Ainsi, les grandes entreprises du numérique ont nécessairement un avantage en termes d'éléments nécessaires au développement de l'IA générative : puissance de calcul grâce à des accords préférentiels avec leurs partenaires historiques, accès privilégié à un large volume de données, compétences techniques attirés par les salaires.

Elles disposent également d'économies d'échelle et d'effets de réseaux. Leurs activités historiques leur permettent d'alimenter les IA pour affiner les modèles ou définir de nouveaux services. Aussi, l'intégration des outils d'IA générative dans les produits initiaux procure un avantage clair en termes d'acquisition de marché. **C'est par exemple le cas lorsque Microsoft déploie dans l'outil « Copilot » ses modèles et ceux d'OpenAI** avec qui elle a signé un partenariat sous la forme d'un investissement pluriannuel.

Leurs places de marché sont par ailleurs un atout non négligeable puisqu'elle assure aux grandes entreprises du numérique qu'un large nombre de modèles seront conçus pour fonctionner dans leur écosystème.

- **Des risques concurrentiels au début de la chaîne de valeur.**

Plusieurs risques sont ainsi identifiés par l'Autorité de la concurrence : risques d'abus au niveau des composants informatiques, **risques de verrouillage** par les grands fournisseurs de services d'informatique en nuage, risques liés à des refus d'accès ou des discriminations d'accès à la donnée, risques liés à des accords de non-débauchage entre entreprises du secteur, risques liés aux modèles en accès libre lorsqu'ils conduisent à un verrouillage des utilisateurs, risques liés à la présence d'entreprises sur plusieurs marchés compte tenu de l'intégration verticale de certains acteurs et qui pourrait conduire à des refus ou des limitations d'accès à des éléments essentiels pour l'entraînement de modèles concurrents, risques liés aux prises de participations minoritaires et partenariats des grandes entreprises du numérique comme le confirme là encore le partenariat noué entre Microsoft et OpenAI, et risques de collusion en cas d'utilisation d'IA générative qui créeraient des pratiques concertées.

Consciente des enjeux du secteur, l'Autorité de la concurrence a également publié, en janvier 2025, une consultation afin de recueillir l'avis du marché sur l'éventuelle introduction d'un système de contrôle des concentrations pour les opérations sous les seuils de notification des opérations de concentration en dessous des seuils. Avec toutes les difficultés de qualification des marchés que cela poserait ensuite.

A ce titre, le régulateur va nécessairement être confronté, dans les prochains mois, à des pratiques qui, alors qu'elles visent à surmonter tout ou partie des diffi-

cultés identifiées, créent à leur tour des défis en termes de droit de la concurrence.

C'est par exemple le cas des espaces de données sectorielles, également appelés *data space*[94]. Ces espaces permettent de créer des systèmes avec une plus-value importante, et surmonter ainsi l'hégémonie déjà réelle de certains acteurs, qui ne disposent pas de données d'une telle qualité par secteur.

Pourtant, la façon dont ces données sont partagées et la nature des IA génératives qui sont créées ensuite pour les utiliser peut créer de nouvelles barrières, en particulier pour de petits acteurs qui ne pourraient bénéficier d'informations utiles pour le développement de leurs activités.

Compte tenu de l'importance stratégique de ces modèles pour la souveraineté de la France et de l'Europe, il conviendra de travailler main dans la main avec le régulateur pour surmonter d'éventuels obstacles.

B. REPENSER L'UTILISATION DES RÈGLES DE DURABILITÉ POUR PROMOUVOIR UNE IA À L'EUROPÉENNE

La durabilité, entendu comme la capacité d'une technologie à s'inscrire dans le temps, est très régulièrement citée comme un enjeu majeur de l'IA, en particulier de l'IA générative. Une préoccupation souvent liée aux chiffres évoqués concernant la consommation des modèles : une requête faite à partir de ChatGPT consommerait ainsi plus de 10 fois plus d'électricité qu'une recherche Google classique, d'après l'Agence internationale de l'énergie, qui prévoit également que la demande en électricité pour les data centers devrait plus que doubler d'ici 2026 par rapport aux chiffres de 2022.

L'IA ET LA DURABILITÉ VOLONTAIRE

Pourtant, une recherche simple au sein de l'AI Act amène à seulement quatre occurrences du terme « durabilité » :

- dans le considérant, les fournisseurs et ceux qui déploient des systèmes d'IA sont encouragés à appliquer sur une base volontaire des exigences supplémentaires liées, notamment à *« la durabilité environnementale »*[95] ;
- ce considérant a pour miroir un article relatif aux codes de conduite pour l'application volontaire de certaines exigences, qui mentionne *« l'évaluation et la réduction au minimum de l'incidence des systèmes d'IA sur la durabilité environnementale, y compris en ce qui concerne la programmation économe en énergie et les techniques pour la conception, l'entraînement et l'utilisation efficaces de l'IA »*[96] parmi les objectifs dont la réalisation devrait être facilitée par l'élaboration des codes de bonne conduite.

[94] Rappel de la définition : écosystème des données de confiance, composé d'une infrastructure de mutualisation et partage de données entre pairs, et d'une gouvernance dédiée. Ces espaces sont nécessaires à la création d'un marché unique européen de la donnée.

[95] Paragraphe 165 du considérant de l'AI Act.

[96] Article 95, 2, b) de l'AI Act.

- ces deux dispositions sont également suivies d'une mention dans l'article relatif à la réévaluation et au réexamen des codes de bonne conduite volontaires, en ce qu'ils doivent favoriser l'application d'exigences dont la durabilité environnementale[97].
- dans l'article relatif au bac à sable réglementaire, « *les systèmes d'IA (…) développés pour préserver des intérêts publics importants par une autorité publique ou une autre personne physique ou morale (en matière de) durabilité énergétique*[98] » fait partie de cas mentionnés pour pouvoir en bénéficier, moyennant le respect des autres conditions ;

Aucune règle dure n'est en réalité prévue, s'agissant spécifiquement du numérique ou de l'IA, qu'elle soit générative ou non.

1. Des mécanismes de durabilité concrets déjà en action dans les grandes entreprises

Nos entreprises peuvent déjà s'appuyer sur des mécanismes connus, que les plus grandes d'entre elles respectent déjà pour la plupart : **le devoir de vigilance et les critères sociaux et environnementaux.**

Ces règles ont récemment été propulsées sur le devant de l'actualité car dans le viseur des mesures de simplification proposées par la Commission européenne, dans le cadre de la procédure dite « Omnibus ».

Le devoir de vigilance est apparu en droit français par une loi de 2017[99], impose aux entreprises qui comptent plus de 5 000 salariés en France ou plus de 10 000 salariés dans le monde, de prendre des « *mesures de vigilance raisonnable propres à identifier les risques et à prévenir les atteintes graves envers les droits humains et les libertés fondamentales, la santé et la sécurité des personnes ainsi que l'environnement, résultant des activités de la société et de celles des sociétés qu'elle contrôle (…), directement ou indirectement, ainsi que des activités des sous-traitants ou fournisseurs avec lesquels est entretenue une relation commerciale établie, lorsque ces activités sont rattachées à cette relation.* »[100]

Appliqué depuis à environ 300 entreprises en France, le devoir de vigilance devait voir sa version européenne issue de la directive CS3D *(Corporate sustainability due diligence directive)* appliquée entre 2027 et 2029, avec un champ élargi, allant jusqu'à plus de 700 entreprises en France. Le 26 février, la Commission européenne a annoncé que cette obligation de diligence raisonnable ne concernerait finalement plus que les partenaires commerciaux directs, que la fréquence des évaluations passerait d'un an à cinq ans, et que les conditions de responsabilité civile seraient supprimées. Cette dernière annonce est certainement la plus conséquente dès lors qu'elle retire quasiment toute force aux obligations de la directive.

[97] Article 112, 7 de l'AI Act.

[98] Article 59, 1. a) de l'AI Act.

[99] Loi n° 2017-399 du 27 mars 2017 relative au devoir de vigilance des sociétés mères et des entreprises donneuses d'ordre.

[100] Article L. 225-102-4 du code de commerce.

A ce stade, ce retour en arrière au niveau de l'Union européenne n'a toutefois pas d'effet sur le devoir de vigilance à la française, ni celui appliqué dans d'autres États membres ces dernières années, comme en Allemagne où les seuils sont par ailleurs nettement plus bas[101].

L'autre corps de règles important en matière de durabilité est contenu dans la directive CSRD *(Corporate sustainability reporting directive)*, transposée en droit français par une ordonnance du 6 décembre 2023[102], elle est également reportée et très largement aménagée par le paquet omnibus présenté par la Commission européenne. Cette directive élargit les obligations de transparence en matière de durabilité, en demandant aux entreprises qu'elles détaillent de quelle manière leurs activités ont une incidence sur l'environnement et la société, et de quelle manière les risques et opportunités en matière de transition climatique et de responsabilité sociale sont gérés.

Au niveau français, le Parlement examine au printemps 2025 les conditions du report des règles de durabilité, conformément aux annonces européennes. Ainsi, début mars 2025, le Sénat a adopté un amendement afin de permettre aux grandes entreprises et aux sociétés consolidantes de commencer leur reporting conformément à la directive CSRD pour l'année 2029, aux petites et moyennes entreprises de le faire pour l'année 2030 et aux petites et moyennes entreprises non européennes pour l'année 2032.

2. Transformer la mise en conformité en levier de pilotage des risques liés à l'IA

La mise en conformité coûte parfois cher – entre la collecte de données sur les chaînes d'approvisionnement, l'analyse de l'impact et la mise en place de contrôles – et n'est évidemment pas une priorité pour la plupart des start-up. Les normes sont complexes et leur articulation n'est pas toujours évidente.

Une fois mises en œuvre, la plus-value de ces règles pour les entreprises qui s'y astreignent est souvent peu perceptible et fait douter de leur attrait dans un marché mondialisé, face à des entreprises qui n'ont que peu faire de la durabilité. Ainsi, les entreprises venues des quatre coins du monde, et surtout de la Chine et des Etats-Unis pourraient concentrer toutes leurs ressources sur du développement technologique et commercial, quand nos entreprises seraient contraintes de sacrifier une partie de l'un ou de l'autre, ou un peu des deux, sans savoir à quoi bon.

A première vue, ces règles ne comportent donc que peu d'avantages. Pourtant, évoquer ces règles paraît essentiel pour au moins trois raisons :

- l'absence de gestion des risques en matière de durabilité ne peut être que court-termiste, s'agissant de l'IA, compte tenu de ses caractéristiques en matière d'environnement et de droits humains,
- une partie des grandes entreprises susceptibles de disposer des ressources et perspectives nécessaires pour déployer des solutions d'IA y sont assujet-

[101] Article L. 225-102-4 du code de commerce.

[102] Article L. 225-102-4 du code de commerce.

ties en tout ou partie,

- l'IA peut être un formidable outil pour répondre aux problèmes de transition, mais n'est viable en tant que tel que si ses caractéristiques propres sont compatibles avec cet objectif.

S'agissant du premier point, un récent rapport de l'institut de recherche de Capgemini évalue l'ensemble des ressources consommées par la chaîne de valeurs de l'IA générative et note par exemple que le seul entraînement d'un modèle de type ChatGPT-4 requiert suffisamment d'électricité pour alimenter 5 000 maisons aux Etats-Unis pour une année entière.

Le même rapport mentionne que 47 % des entreprises interrogées considèrent que leurs émissions de gaz à effet de serre ont augmenté durant les 12 derniers mois, 48 % reconnaissent que l'IA générative en est l'une des raisons et 42 % admettent qu'ils vont devoir revoir leurs engagements en termes de durabilité compte tenu de l'IA générative.

Dans le même temps, seulement 12 % des entreprises interrogées mesurent l'empreinte environnementale de cette technologie et 74 % disent que le manque de transparence des entreprises qui fournissent la technologie rendent les mesures difficiles, en reconnaissant attendre du secteur de la tech de piloter l'IA générative durable.

Ce dernier explique en grande partie pourquoi, alors que les grandes entreprises sont largement déjà soumises à des règles en matière de durabilité, très peu y intègrent les sujets d'IA.

Ainsi, l'association « Intérêt à Agir »[103] publiait un rapport en septembre 2024[104] relevant que sur 11 sociétés françaises testées, une seule avait mis en place des mesures liées au déploiement de l'IA, à la suite d'une enquête dont elle avait fait l'objet en Colombie.

Pourtant, l'IA, et en particulier l'IA générative, intervient au moins à deux niveaux dans les sujets d'environnement et de droits humains : d'abord dans le cadre de l'extraction des minerais requis pour la fabrication des composants électroniques avec des risques à la fois humains et environnementaux, ensuite dans le cadre de l'entraînement et du fonctionnement des systèmes avec des risques humains liés au traitement de la donnée et des risques environnementaux liés au fonctionnement des systèmes et des *data centers*.

Si la problématique environnementale est admise, faute d'être réellement prise en compte à ce stade, le sujet des droits humains est souvent occulté par méconnaissance. La mise en lumière dans un contexte grand public des travailleurs de la donnée est récente.

Rien qu'en Inde, fin 2024, plus de 70 000 personnes étaient employés pour annoter et valider des données qui serviraient ensuite à l'apprentissage de modèles. Parmi ces personnes, environ 50 000 *freelances*. Avec toute la précarité et l'in-

[103] Cette association est dédiée aux contentieux stratégiques et fait partie d'un groupe également composé d'un fonds de dotation, Dotlex, et d'un think tank, Lex Ferenda.

[104] Baptiste Delmas et Juliette Terrioux, « Intelligence artificielle et devoir de vigilance, il y a intérêt à agir », septembre 2024.

certitude que l'on pouvait relever par le passé s'agissant des ateliers du monde, lesquels sont à l'origine du devoir de vigilance, depuis la chute du Rana Plaza, un immeuble de huit étages de la banlieue de la capitale du Bangladesh, qui abritait des travailleurs du textile.

Or bien que l'Union européenne temporise sur la durabilité par peur de freiner l'innovation, les règles françaises et celles d'un certain nombre de nos voisins européens, l'Allemagne en tête, ne connaissent pas de pause.

Au contraire, après quelques temps à clarifier les règles de procédures, la France connaît désormais ses premiers contentieux sur le fond. Une chambre dédiée aux contentieux émergents a été créée à Paris, et le groupe La Poste a, le premier, été condamné pour des manquements en matière de vigilance liée au respect des droits des travailleurs.

C'est à ce niveau que, grandes entreprises et start-up de l'IA, doivent jouer collectif. Les uns ont les moyens et la maturité requise pour travailler dès maintenant sur leur durabilité. Les autres ont les informations techniques requises pour ce faire.

Évidemment, aucun modèle n'est parfait et voir le devoir de vigilance comme une obligation de sans faute n'est pas l'objectif. C'est avant tout une obligation d'exemplarité, de tout mettre en œuvre pour qu'à terme l'environnement et les droits humains, l'humanité finalement, ne soient pas les grands perdants du progrès technologique.

Ces considérations passent actuellement au second plan, mais elles ne tarderont de revenir sur le devant de la scène aux premiers accidents ou scandales.

L'utilité de ces règles pour nos entreprises se pose d'autant que nous avons construit, avec le nucléaire, la première brique d'un contexte local très favorable. Les équipes de recherche de Barclays[105] ont par exemple établi une carte qui décrit le pourcentage de temps dans le fonctionnement d'un data center au cours duquel son approvisionnement peut se faire par une énergie décarbonée. La France tient ainsi sa grande attractivité d'un taux de 94 %, le deuxième au monde derrière la Finlande (98 %) mais loin devant l'Irlande (43 %), l'Italie (52 %) ou dans une moindre mesure l'Espagne (76 %).

Mais alors que nous bénéficions de cette brique et de l'âme pionnière de l'Europe en termes de numérique responsable, nous ne bénéficions actuellement d'aucun avantage de marché. Pire, nous reportons les règles qui pourraient faire une différence en imposant une contrainte réelle sur les acteurs étrangers moins vertueux.

La question finalement, est celle de savoir comment une pratique de bon sens et d'intérêt général peut devenir, pour nos entreprises, une arme à la fois pour leurs affaires et pour le rayonnement à terme de nos valeurs dans le monde ?

[105] Barclays Research, « AI revolution: meeting massive AI infrastructure demands », Janvier 2025.

OPPOSER RÉGULATION
ET INNOVATION,
C'EST RENONCER
À LA SOUVERAINETÉ.

III. TROIS CONDITIONS POUR FAIRE DE NOTRE DROIT UNE RÉELLE ARME

Notre arsenal juridique est important. Donc complexe également. Mais il traduit les principes d'une IA à l'européenne : éthique, sûre et durable. L'IA à l'européenne n'est pas un progrès technologique, c'est un projet de société.

Pour tenir cette ambition, il est devenu évident, au fil de l'analyse que certaines règles devaient être simplifiées, et que toutes devaient être mieux articulées.

Pour porter cette ambition, il doit également devenir évident que le droit ne doit plus être une simple traduction de nos valeurs. Trois conditions paraissent devoir venir s'ajouter pour que le droit se transforme en arme. Une arme économique, d'abord, une arme stratégique et globale, ensuite et surtout :

- être un outil pour sécuriser et accélérer l'innovation ;
- faciliter l'acceptabilité de l'innovation sur le marché européen et aider à terme à imposer nos règles du jeu dans le reste du monde.
- être activable face à des concurrents qui ne joueraient pas le jeu, que ce soit dans le cadre de marchés publics ou de marchés privés, et dans la défense des modèles vertueux.

A. LA RÈGLE DE DROIT COMME OUTIL POUR SÉCURISER ET ACCÉLÉRER L'INNOVATION

Les cadres juridiques sont encore trop vus comme des obligations de conformité qui ne font qu'ajouter des lignes de coût. Or le droit doit faciliter la normalisation technique des produits construits avec de l'IA.

La normalisation de la technologie par le droit doit apporter des garanties en termes de qualité et donc de confiance, mais également faciliter le travail des fournisseurs et déployeurs de l'IA, en balisant le chemin, même tortueux, de l'innovation.

1. Le rôle moteur du droit dans la scalabilité de l'innovation : de ligne de coût à infrastructure stratégique

Dans le cadre des auditions réalisées pour la production d'un récent rapport rendu par l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST)[106], Yann Ferguson, sociologue directeur scientifique du LaborIA d'Inria et Patrick Bezombes, conseiller pour la stratégie et la gouvernance de l'IA à l'Association

[106] A. Sabatou, P. Chaize, C. Narassiguin, « Les nouveaux développements de l'intelligence artificielle », Office parlementaire d'évaluation des choix scientifiques et technologiques, novembre 2024.

française de normalisation (Afnor) et représentant de la France au CEN-CENELEC[107] insistaient sur l'intérêt de la normalisation technique prévue par l'AI Act.

Deux catégories d'entreprises se distinguent :

- **Les entreprises industrielles traditionnelles**, qui sont habituées à une normalisation stricte, laquelle est essentielle à la fois pour garantir la sécurité de leurs produits et pour la réputation de l'entreprise. En plus de ces deux éléments, nous pourrions ajouter l'acceptabilité, qui n'est finalement qu'un chapeau évident. Ces entreprises savent que pour mettre sur le marché un paquebot, un avion, un train ou un réacteur nucléaire le risque ne peut être que minime.

Un exemple marquant est celui de Boeing dont l'action a chuté d'environ 55 % ces cinq dernières années. Les analystes ont largement déploré la priorité accordée à la rentabilité plutôt qu'à l'ingénierie qui a conduit à des problèmes systémiques dans la gestion des sujets de sécurité qui, couplés à des difficultés dans la chaîne d'approvisionnement, ont eu des conséquences très importantes sur leur position sur le marché.

- **Les nouvelles entreprises, en particulier du numérique, qui s'autorisent des marges d'erreur plus élevées** dès lors qu'elles ont moins été confrontées à des problèmes majeurs à ce stade. Le rapport de l'OPECST précise par ailleurs que l'erreur est davantage tolérée dans le sens où elle peut ensuite être corrigée par une simple mise à jour logicielle.

Les personnes auditionnées à ce sujet voient l'AI Act comme *« un moyen d'encourager les entreprises du numérique à changer de culture et respecter des normes strictes lorsqu'elles commercialisent un produit »*. Il est encore une fois question d'acceptabilité par la confiance qu'une entreprise cliente ou un client final vont ressentir.

Cette normalisation compenserait par ailleurs largement le coût qu'elle représenterait pour de petites entreprises face aux grandes, dès lors qu'une défaillance entraînerait une perte de confiance tout autant pénalisante pour une grande que pour une petite entreprise.

Aussi, le système de simplification prévu par l'AI Act[108] limite encore les coûts avec à la fois l'application d'un principe de proportionnalité et des priorités d'accès à des infrastructures facilitantes comme le bac à sable réglementaire.

L'expérience nous a par ailleurs démontré qu'un risque de défaillance était plus facile à encaisser pour une grande entreprise capable de diversifier ses offres, qui plus est sous différentes marques, que pour une grande ou une plus petite entreprise dépendante d'un seul produit, qui dispose d'une capacité de dilution du risque nettement plus faible.

Utiliser le droit pour normaliser l'innovation a les mêmes atouts en termes de qualité de produit (AI Act) **qu'en termes d'éthique de la donnée** (RGPD), **de normes cyber** (ensemble des directives et règlements, ainsi que des règles internes s'agissant des exigences assurantielles par exemple), **des règles juridiques transversales et**

[107] Comité européen de normalisation en électronique et en électrotechnique.

[108] Voir infra.

sectorielles, et des normes en matière de durabilité (devoir de vigilance et critères de communications en particulier).

Les pavés sont quelque part prêts à normaliser le chemin de l'innovation. Ce qu'il manque c'est une infrastructure du droit capable de poser chacun d'eux pour que tant les grandes entreprises qui y sont habituées que les plus petites qui n'ont quasiment aucune habitude et appris à grandir sans puisse y prendre appui.

Cette infrastructure du droit qui doit être construite, c'est la possibilité pour nos entreprises qui fournissent ou déploient l'IA de se développer avec le fardeau de la conformité en moins mais les vertus de la règle de droit en plus.

2. Quand Kelsen[109] rencontre Turing[110] : *Law as an Infrastructure, Law as a Platform, Law as a Service*

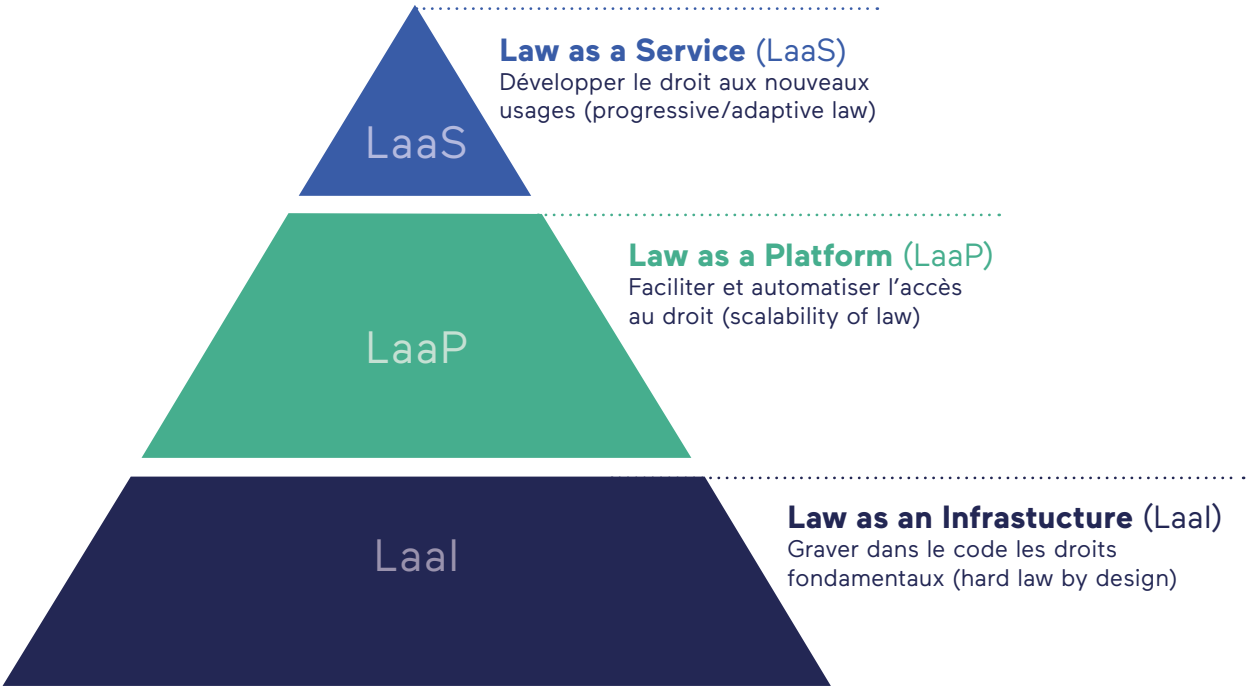
La compréhension de la spécificité technologique par le droit, constitue un préalable essentiel – autant que la compréhension des logiques juridiques par les innovateurs.

Pour initier ce dialogue, nous proposons de faire se rencontrer le schéma des infrastructures informatiques et celui des normes juridiques.

Il s'agit d'imaginer par cette analogie l'existence d'un droit capable d'évoluer à la mesure des innovations qu'il encadre.

[109] Hans Kelsen (1881-1973) a développé le concept de pyramide des normes qui conduit à envisager l'ensemble des normes juridiques selon différents blocs (bloc de constitutionnalité, bloc de conventionnalité, bloc de légalité et bloc réglementaire) avec une hiérarchie entre eux.

[110] Alan Turing (1912-1954) est régulièrement considéré comme le père de l'informatique et un pionnier de l'intelligence artificielle.



PYRAMIDE KELSEN-TURING
Architecture du droit pour une IA européenne

LAW AS AN INFRASTRUCTURE (LAAI) : APPLIQUER LES LIBERTÉS ET DROITS FONDAMENTAUX BY DESIGN

Une première couche, inaltérable, doit être constituée par les fondamentaux du système juridique appliqué à l'intelligence artificielle.

Il s'agit, d'une part, des libertés et droits fondamentaux, qui se trouvent au sommet de la hiérarchie des normes : les droits inhérents à la personne humaine (dont l'égalité, la liberté, la sûreté, et les droits qui en sont des aspects ou des conséquences, dont la liberté d'expression), les droits sociaux et économiques (dont le droit à l'emploi), et les droits dits « de troisième génération » (dont le droit de chacun de vivre dans un environnement équilibré et respectueux de la santé », qui consacre la notion de développement durable et le principe de précaution).

Le RGPD et l'AI Act protègent à ce titre une partie de ces libertés et droits fondamentaux.

Cette couche, comme pour l'*Infrastructure as a Service* est celle sur laquelle tout repose, et qui doit ainsi être à la fois intégrée dès le départ, et figée.

LAW AS A PLATFORM (LAAP) : PENSER LE DROIT COMME UNE PLATEFORME ACCESSIBLE AUX MACHINES

Cette deuxième couche doit être disponible pour tous ceux qui souhaitent utiliser le droit pour exécuter leurs systèmes. En d'autres termes, **cette couche consiste à rendre le droit exécutable dans le code**, de la même manière que la *Platform as a service* permet de construire des services.

Si aucune des trois couches envisagées n'est à ce stade identifiée comme telle, celle-ci est sans aucun doute celle qui nécessite de concentrer les recommandations tant elle paraît stratégique et moins développée.

Cela implique, d'une part, de faciliter la traduction du droit dans le code, et d'autre part, de s'assurer de la disponibilité et de l'harmonisation des interprétations des textes pour faciliter une intégration dans le code.

Il s'agirait pour cela de proposer une plateforme commune au sein de l'Union européenne :

- Avec l'ensemble des textes indispensables (dans un premier temps il paraît pertinent de se limiter aux textes relatifs aux données, à l'AI Act et aux règles cyber) dans une version codable,
- Avec l'ensemble des décisions et ressources juridiques relatives à ces textes,
- Utilisable dans tous les pays.

Trois recommandations peuvent être formulées en ce sens :

Faire du code la 25e langue de l'Union européenne de sorte à ce que tout nouveau texte puisse trouver une traduction dans le code. Dans le prolongement des réflexions portées par Enrico Letta à travers sa proposition de création d'un 28e régime européen[111] – visant à simplifier l'accès au droit pour les entreprises en leur offrant un cadre juridique harmonisé et facultatif –, notre initiative de faire du code la 25e langue officielle de l'Union européenne s'inscrit dans une ambition complémentaire. L'idée est que tout nouveau texte législatif doit trouver une traduction directe sous forme de code, afin d'accélérer et d'automatiser son application concrète. **Ce projet de 25e langue pourrait s'appuyer sur le projet « Rules as Code » de la Commission européenne[112] et ainsi renforcer, voire suppléer, l'objectif poursuivi par le 28e régime : simplifier l'accès au droit, garantir son intelligibilité et sa mise en œuvre effective** dans un environnement numérique et transfrontalier. Notre proposition contribue ainsi à poser les fondations d'un véritable marché unique numérique du droit, en cohérence avec la dynamique impulsée par Letta et en réponse aux besoins de modernisation exprimés par les institutions européennes.

Intégrer aux omnibus en préparation au niveau européen des modifications pour permettre le codage à court terme des textes principaux, dans la logique des travaux déjà commencés,

Favoriser dans un premier temps au niveau français l'initiative du *Legal Data Space* qui rassemble déjà un grand nombre d'acteurs de la filière du droit. C'est-à-dire une infrastructure mutualisée pour le traitement et le partage des données juridiques publiques - open data- et privées - data spaces - dans le but de développer une IA juridique souveraine, par et pour la filière du droit.

Cette initiative peut permettre, à terme, d'apporter des solutions aux autres data spaces pour la gestion des règles relatives aux données. Tous pourraient ainsi bénéficier d'un droit - du droit positif au contrat partage de données[113] - compréhensible par la machine et traduit dans un Rulebook[114].

Ainsi, l'IA ne sera plus un obstacle mais un atout majeur pour la mise en conformité des acteurs[115].

[111] Much more than a market, Enrico Letta, avril 2024

[112] https://interoperable-europe.ec.europa.eu/collection/govtechconnect/news/rules-code-rac. Dans ce cadre, un hackathon a par exemple été organisé les 17 et 18 mars 2025 à Paris par la direction interministérielle du numérique (DINUM).

[113] Thomas Saint-Aubin, Pierre Marchès, « IA générative et management des contrats : une révolution en marche », Droit & Patrimoine, 2024, L'IA Générative et les professionnels du droit, N°347.

[114] Cette démarche peut être facilitée par la maturité de l'écosystème européen de la legaltech et de ses juristes numériques, en lien avec les avocats : Thomas Saint-Aubin, « Déontologie numérique des juristes: le devoir d'exemplarité de la legal-tech. Les déontologies à l'ère numérique », Université Cergy-Pontoise, Juin 2022, Cergy-Pontoise (Université de), France.

[115] Voir à ce sujet le projet de la Commission européenne d'utiliser l'IA pour analyser et extraire des textes en vigueur les obligations sectorielles de mise en conformité et créer un nouveau standard qui permettrait notamment aux TPE et PME de connaître nativement toutes les obligations auxquelles elles sont soumises.

LAW AS A SERVICE (LAAS) : FAIRE DU DROIT UN ACTEUR DE L'INNOVATION

Cette troisième couche doit offrir un cadre agile, évolutif en fonction des contextes, pour faciliter l'innovation permanente.

Cette couche est présente dans l'AI Act sous la forme des « bacs à sable réglementaires ». Il s'agit d'accompagner les expérimentations dans le cadre d'environnements réglementaires sécurisés.

Ces bacs à sable peuvent être particulièrement utiles dans le cadre d'innovations transformatrices. C'est le cas des avancées en cours concernant l'agentification de l'IA, qui promet de bouleverser l'économie autant que les mécanismes juridiques classiques en permettant à des IA d'agir de manière autonome, dans des contextes différents, et avec des objectifs y compris auto-définis.

Pour fonctionner dans le temps, notamment dans des secteurs très réglementés comme la santé ou la sécurité, il conviendra d'anticiper l'ensemble des irritants pour identifier les blocages persistants qui exigeraient des modifications des règles législatives ou réglementaires or règles dédiées aux systèmes d'IA ou aux données, par exemple (cela pourrait être le cas de tarifs de remboursement en santé, ou de règle de compétence dans la sécurité).

UN ENJEU DE SOUVERAINETÉ

Il ne s'agit pas de remplacer l'avocat, le juriste ou l'auditeur par des intelligences artificielles, mais de sauvegarder nos règles de droit dans ce nouveau monde.

L'humain y trouvera évidemment toute sa place, et certainement davantage qu'actuellement : d'abord, pour s'assurer de la conformité du code, ensuite pour traiter de toute difficulté qui émergerait dans la mise en œuvre, enfin, pour accompagner les entrepreneurs avec leur vision de l'infrastructure juridique.

Au contraire, **dans un schéma où nous renoncerions à la mise en place d'une telle couche juridique, nous pourrions à terme voir notre modèle dépassé et remplacé, en particulier par la *Common law***, en certains points plus facile d'utilisation avec une intelligence artificielle.

En particulier, parce que le système de la *Common law* est fondé sur la jurisprudence, et est ainsi susceptible d'évoluer pour s'adapter aux contextes, à partir du réel. La capacité d'analyse d'un grand nombre d'éléments par l'intelligence artificielle peut ainsi faciliter, à partir de précédents, des solutions logiques, et une adaptation de la règle à des situations très particulières. C'est pour cette même raison que dans le monde des affaires, déjà, les acteurs économiques privilégient régulièrement la *Common law*.

Notre droit de tradition romano-germanique, au contraire, n'existe que parce qu'une règle a été figée dans le marbre. Et les jurisprudences ne viennent que clarifier **cette règle. Cette rigidité peut rendre plus difficile un raisonnement à partir du code**, quand la règle n'a pas été préalablement pensée pour.

Le danger est d'autant plus prégnant que se développent des nouveaux modes de gouvernance, notamment des données, avec des règles de gouvernance communes. C'est le cas des *data space*. Or si notre droit n'y est pas codable, le risque est qu'à terme les acteurs puissent se tourner vers le système le plus simple.

B. LA RÈGLE DE DROIT COMME OUTIL D'ACCEPTABILITÉ ET D'EXTRA TERRITORIALISATION DE NOS VALEURS

Dans l'étude de KPMG Australie et de l'Université de Queensland parue il y a un an et citée en introduction, seuls 31 % des français se disaient prêts à faire confiance[116] à l'IA, quand 96 % considéraient que les pratiques et les principes d'une IA digne de confiance déterminent la confiance accordée aux systèmes d'IA.

Plusieurs études avaient déjà révélé, ces trois dernières années, que le consommateur était de plus en plus sensible à la protection de sa vie privée et choisissait d'utiliser des produits et services protecteurs en la matière. Ainsi, dans une étude publiée en mars 2022, 80 % des consommateurs français considéraient la protection de leurs données par une marque comme un facteur clé pour accorder leur confiance . Une autre étude parue en juillet 2022 indiquait que 72 % des internautes français étaient préoccupés par l'enregistrement de leurs activités en ligne pour le ciblage publicitaire et 82 % limitaient la mise à disposition de leurs données personnelles en ligne[117].

1. Faciliter l'évangélisation du marché grâce à la force normative du droit

Aussi, bien que ChatGPT ait atteint en quelques mois un nombre de 300 millions d'utilisateurs hebdomadaires qu'il avait fallu huit ans à Facebook ou 4 ans à Instagram pour l'atteindre, il ne doit pas masquer les difficultés auxquelles la diffusion de l'IA se heurte.

L'application d'OpenAI n'apparaît pas, en tant que telle, préoccupante pour la vie privée des individus ou des données d'entreprises, à condition d'être vigilants quant aux éléments sur lesquels le robot est interrogé. Qu'en sera-t-il d'IA d'autres applications quand bien même récréatives lorsque les escroqueries par deepfakes se seront multipliées, ou des IA à vocation commerciales lorsque les entreprises utilisateurs et le consommateur découvriront que des données personnelles ont été utilisées pour l'apprentissage de l'algorithme ?

Les préoccupations du consommateur, en particulier en France et en Europe, semblent faire du respect au RGPD et à l'AI Act un premier argument commercial de poids. Qui plus est face à des concurrents qui n'auront pas les mêmes préoccupations liées à l'inexistence de règles nationales en la matière, s'agissant des Etats-Unis en particulier où les règles sont plus souples et souvent laissées à l'initiative des États.

Cité dans un récent rapport rendu par l'Office parlementaire d'évaluation des choix scientifiques et technologiques (OPECST), Bertrand Braunschweig, coordinateur scientifique du programme confiance.ai et ancien coordinateur pour la recherche du programme national d'intelligence artificiel confirme que le sujet de la confiance dans l'IA est *« un aspect fondamental pour les développeurs comme pour les pouvoirs publics ainsi qu'une condition essentielle à un déploiement fluide et efficace des technologies ».*

[116] Etude de PWC, « Global Consumer Insights Survey », 16 mars 2022.

[117] Etude INSEE, « 82 % des internautes protègent leurs données personnelles en ligne », 21 juillet 2022.

DISPOSER D'OUTILS ET DE DONNÉES PLUS FIABLES

Dans une enquête de 2018, soit aux prémices du RGPD, 55 % des consommateurs français interrogés reconnaissaient avoir déjà intentionnellement donné de mauvaises informations personnelles par crainte que certaines de leurs informations ne soient divulguées, usurpées ou volées[118].

Peu de temps avant, 90 % de français interrogés se disaient favorables à l'utilisation commerciale de leurs données personnelles dans les cas où ils pourraient exprimer un consentement préalable et avoir la maîtrise de ces données. Ce serait donc davantage les conditions de collecte et d'utilisation de la donnée, plus que l'utilisation en tant que telle qui poserait des difficultés.

Les différents chiffres mentionnés s'agissant des craintes dues au développement de l'IA confortent l'idée qu'un encadrement peut être bénéfique tant pour l'acceptabilité du système en tant que tel que pour la qualité des données que le consommateur sera prêt à y intégrer. Quand la donnée se trouve être le pétrole de ces systèmes, plus elle sera de qualité et fiable, plus le système sera cohérent.

Aussi, les bénéfices suivants ont par exemple été rencontrés pour le RGPD[119] : un meilleur positionnement dans les appels d'offres en particulier publics mais également dans les négociations entre professionnels, une meilleure confiance des clients, un meilleur ciblage de la communication, une amélioration de certains processus métiers, une réduction de la masse des données traitées avec des conséquences positives en termes de RSE.

Charge aux entreprises, ensuite, de faire le pont entre le droit, la communication et la commercialisation pour tirer le plus grand profit. Les guides, labels et certifications peuvent alors être un atout complémentaire.

2. De l'acceptabilité interne à l'exportation de nos standards

Pour valider l'utilité d'une règle appliquée à l'innovation, l'argument de l'acceptabilité paraît donc, dans un premier temps, valable. Il doit également permettre à nos entreprises d'utiliser leurs vertus validées pour partie par la loi dans un cadre international, afin d'être en mesure de conquérir d'autres marchés que leur seul marché d'origine.

Ainsi, imposer des règles sur un marché de la taille de l'Union européenne[120] a deux intérêts principaux :

- Forcer les acteurs extérieurs à s'y conformer pour leurs activités sur ce marché,
- Imposer par conséquent nos règles dans l'ensemble du monde, dès lors qu'il sera techniquement difficile de justifier d'appliquer des règles différentes en fonction des marchés et politiquement très compliqué de présenter des projets moins-disant en termes de garanties.

[118] Etude réalisée par YouGov Plc pour RSA, réalisée entre le 15 décembre 2017 et le 3 janvier 2018.

[119] Résultats d'une étude Wavestone commandée par le Laboratoire d'innovation numérique de la CNIL fin 2021 et publiés en mai 2024.

[120] En 2023, l'Union européenne représentait un produit intérieur brut (PIB) de 16 970 milliards de dollars contre 27 720 milliards pour les Etats-Unis et 17 790 milliards pour la Chine.

C'est à ce niveau que les régulateurs nationaux et la Commission européenne ont une responsabilité immense. Car s'ils rechignent à appliquer les règles prévues et auxquelles nos acteurs nationaux et européens s'astreignent, alors ils offriront aux acteurs extérieurs un avantage majeur et affaibliront durablement si ce n'est définitivement notre modèle.

Dans le même temps, un autre acteur international lorgne ce créneau de la réglementation : la Chine. Dès 2023, le sénateur américain démocrate Chuck Schumer appelait ainsi les Etats-Unis à prendre les devants sur la réglementation à la suite de la présentation par la Chine de sa nouvelle approche de régulation de l'IA en avril 2023.

Évidemment, l'innovation ne doit pas être sacrifiée sur l'autel d'un dogmatisme normatif. Mais en l'absence de toute norme dédiée, les marchés extérieurs seront rapidement fermés aux innovateurs qui ont bénéficié d'une déréglementation complète. En d'autres termes : que quelque pays que ce soit le veuille ou non, une innovation sera toujours tôt ou tard soumise à des règles, qu'il le veuille ou non.

Dans ce schéma, il n'existe que deux possibilités : se fermer un certain nombre de marchés extérieurs, ou se conformer aux règles du jeu des marchés convoités en espérant avoir pris suffisamment d'avance technologique et financière pour pouvoir encaisser une mise en conformité importante, si tant est qu'elle soit possible et que le produit n'ait pas été purement et simplement interdit.

Avec le risque, dans le premier cas, de quoi qu'il arrive se retrouver dans une position de forte vulnérabilité compte tenu de l'extraterritorialité des règles extérieurs, comme les Etats-Unis ont pu l'imposer par le passé avec l'extraterritorialité de leurs règles anti-corruption, permettant l'acquisition de nombreuses grandes entreprises françaises et européennes placées à la merci d'énormes sanctions outre-Atlantique.

S'ASSURER DE LA PORTÉE EXTRATERRITORIALE DES LÉGISLATIONS DÉDIÉES AUX INNOVATIONS

L'AI Act[121] et le RGPD[122] ont cette portée extraterritoriale, dès lors qu'ils s'appliquent que l'entité concernée soit établie dans ou hors de l'Union européenne. Ce n'est que le lieu où les services sont proposés, dans l'Union européenne ou non, qui va déterminer l'application de la règle. Avec une extraterritorialité supplémentaire pour le RGPD dans les cas où des données de personnes situées dans l'Union européenne sont utilisées[123].

Ce sont ces règles générales qui doivent avoir cette portée, car ce sont elles qui déterminent ensuite la vie du produit. Pour illustrer cette distinction, il convient de reprendre un système d'IA générative. Les règles propres au produit (l'AI Act) et celles propres aux données (RGPD) sont présentes dès la première minute du développement. Car tant l'usage futur pour lequel l'entraînement va être réalisé que

[121] Article 2, 1 de l'AI Act.

[122] Article 3, 2 du RGPD.

[123] Article 3, 2, b) du RGPD.

les données utilisées pour cet entraînement vont devoir être travaillés en fonction.

Le droit de la propriété intellectuelle peut également avoir cette portée dès lors que ce sont des droits déterminés à partir du lieu où se situe le détenteur qui sont protégés. Ce qui est de bon sens et bienvenu car ces règles irradient également ensuite toute l'activité de la société et ne peuvent plus être réellement aménagées au cas par cas, une fois l'IA entraînée avec des données qui ne respecteraient pas ce principe.

L'extraterritorialité est ensuite moins d'actualité s'agissant des autres règles de gouvernance juridiques transversales (droit social, droit de la concurrence, droit de la propriété intellectuelle) ou sectorielles (droit bancaire et financier) qui vont s'appliquer à un territoire et des opérations données sans avoir de conséquences sur l'identité d'ensemble d'un système d'IA. Ne pas prévoir d'effet extraterritorial dans ces cas paraît par conséquent moins grave à première vue.

Cela redevient en fait un sujet majeur s'agissant des règles de durabilité, en particulier du devoir de vigilance. Peut-on soutenir ces règles sans fausser la concurrence en défaveur des acteurs nationaux dans le cas où elles ne s'appliquent qu'à ces acteurs[124] ? C'est à ce titre qu'un devoir de vigilance au niveau européen, avec les mêmes exigences que le devoir de vigilance à la française, est indispensable. Car il s'agit là encore d'éléments qui dépassent le cadre d'un seul territoire ou d'une seule opération et doivent en cela s'imposer à toute société qui entreprend de développer ou d'utiliser un système d'IA dans l'Union européenne, dès lors qu'une entreprise française de même taille serait concernée.

Une partie de la solution pourrait être à ce titre dans la directive européenne qui prévoit d'élargir le devoir de vigilance européen aux entreprises y compris de pays tiers dès lors qu'une partie de leurs activités s'exerce sur le marché européen, à partir d'un certain chiffre d'affaires[125]. Et dans la directive CSRD, en matière d'informations relatives à la durabilité, qui prévoit la même approche. Cela permettra à la fois de contraindre les grandes entreprises du numérique à imposer des règles de durabilité dans leur chaîne de valeur, et aux grandes entreprises extérieures qui déploieront ces systèmes de faire appel à des acteurs vertueux, qui mettent à disposition les données requises.

C. LA RÈGLE DE DROIT COMME OUTIL DE CONQUÊTE

La règle de droit peut devenir, pour nos entreprises, un outil de conquête des marchés, tant publics que privés. Quand les Etats-Unis utilisent à intervalles réguliers l'extraterritorialité de certaines règles nationales, notamment en matière d'anticorruption, pour affaiblir des entreprises étrangères en concurrence avec des acteurs nationaux, nous avons également les moyens de nous protéger contre des acteurs étrangers qui joueraient avec d'autres règles que celles conçues pour

[124] Pour un autre exemple : c'est en partie pour cette raison que les règles anti-corruption françaises ont une portée extraterritoriale dès lors qu'elles s'appliquent aux entreprises étrangères à partir d'un certain seuil de salariés et de chiffre d'affaires. Voir article 17, I de la loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (dite « loi Sapin 2 »).

[125] Article 2, 2 de la directive européenne sur le devoir de vigilance.

respecter nos valeurs.

La règle de droit peut ensuite devenir, pour notre société, un outil de conquête globale compte tenu des enjeux que l'IA soulève. A ce niveau, il s'agit en fin de compte d'un rendez-vous avec l'histoire auquel doivent être les décideurs publics, les autorités de régulation et les juridictions.

1. Un outil d'acquisition de marchés

L'arme du droit, dans un cas d'acquisition de marchés, peut être utilisée à deux niveaux :

- au niveau du régulateur et des juridictions, par l'application rigoureuse des cadres juridiques existants.
- par les acteurs économiques nationaux eux-mêmes, pour l'obtention de contrats publics ou privés et devant des juridictions, lorsqu'ils se retrouvent confrontés à des acteurs placés dans l'illégalité, sur le terrain de la concurrence déloyale.

LA RÈGLE DE DROIT COMME OUTIL D'ACQUISITION DE MARCHÉS PUBLICS

La règle de droit est d'abord une règle de péage, en ce qu'elle doit permettre d'écarter ceux qui l'enfreignent. Elle peut ensuite être une règle qui facilite, comme c'est le cas des marchés publics innovants. Sur ce deuxième point, le cadre propice doit encore s'affirmer.

Le droit comme règle de péage. En termes de recevabilité d'un acteur, la compatibilité au RGPD peut par exemple être une force pour l'obtention de marchés publics dès lors que ce marché implique des données personnelles.

Le sujet a ainsi été ouvert dès 2021 par le Conseil d'Etat belge[126], qui accueillait la demande d'une entreprise qui n'avait pas été retenue dans le cadre de l'appel d'offres, alors qu'elle considérait respecter le RGPD contrairement au concurrent retenu, dans le cadre d'un marché impliquant un traitement de données à caractère personnel, puisqu'il s'agissait d'établir un centre de mobilité afin de faciliter le fonctionnement des services de transport public.

Logiquement, les appels d'offres impliquant une solution d'IA doivent conduire l'acheteur public à porter une grande attention à ce sujet, en même temps qu'aux garanties mises en œuvre par l'entreprise qui l'a emporté, pendant l'exécution du marché. Faute de quoi, un concurrent non retenu pourrait saisir le tribunal administratif et tenter d'obtenir jusqu'à l'annulation de l'attribution de marché en cas de vérifications non suffisantes. Il en ira très certainement de la même logique s'agissant du respect du RGPR ou de l'AI Act à chaque fois que le marché impliquera un usage définit autrement que par un risque minimal.

Ainsi, la Commission européenne et les CNIL nationales effectuent un important travail de régulation des IA. Meta a par exemple dû freiner ses ambitions d'entraîner des LLM avec du contenu qui se trouvait sur des réseaux sociaux du groupe. Ce

[126] Conseil d'Etat belge, 12 mai 2021, n° 250.599. Cette jurisprudence est complétée par deux autres décisions du Conseil d'Etat belge : CE, 23 décembre 2019, n° 246.532 et CE, 6 mai 2022, n° 253.677.

travail doit aider les acteurs publics à la même vigilance.

Il convient pour cela que les acteurs publics se dotent des outils juridiques requis et soient donc très attentifs aux clauses particulières du marché. Les Cahiers des clauses administratives générales (CCAG), qui prévoient des conditions d'exécution applicables à des catégories de marchés public, ont ainsi depuis 2021 déjà opéré une mise à jour en ce sens.

Mais il revient bien à chaque acheteur public de prévoir à la fois les clauses adéquates et suffisantes en matière d'innovations et les pénalités applicables, même des principes généraux pourraient le cas échéant être invoqués, lesquelles pourraient d'ailleurs inclure les règles en matière de durabilité prévues par la loi[127].

A ce sujet, le code de la commande publique offre une procédure dérogatoire pour le cas de marchés innovants, afin de favoriser l'achat public auprès de plus petites entreprises. Mais le dispositif reste peu utilisé. En particulier parce que cette procédure est encore mal appréhendée par les acteurs qui y voient une zone de risque supplémentaire.

L'idée pourrait être davantage de simplifier la procédure normale, et l'IA peut dans ce cas devenir une aide précieuse. C'est l'exemple de ce que promeut la start-up Explain, qui l'utilise pour répondre le plus efficacement possible à la commande publique.

LA RÈGLE DE DROIT COMME OUTIL D'ACQUISITION DE MARCHÉS PRIVÉS

Cette compatibilité de l'innovation avec le droit français et européen doit également être une force pour les start-ups qui souhaitent intégrer leurs solutions techniques auprès d'autres acteurs économiques. Elle limite le risque contentieux du co-contractant qui serait alors tenu responsable du défaut de conformité et permet de proposer une solution qui par nature sera davantage acceptable pour le consommateur final.

Dans ce cadre de droit privé, le RGPD est, enfin, une arme dont peuvent se saisir les entreprises en conformité pour se protéger d'acteurs peu regardants.

Le tribunal judiciaire et la Cour d'appel de Paris ont jugé ces deux dernières années que la concurrence déloyale consistait *« dans des agissements s'écartant des règles générales de loyauté et de probité professionnelle applicables dans les activités économiques et régissant la vie des affaires tels que ceux créant un risque de confusion avec les produits ou services offerts par un autre opérateur »*[128], impliquant donc un non-respect du RGPD[129]. Dans les cas d'espèce, les manquements

[127] L'article L2152-1 du code de la commande public requiert ainsi de l'acheteur public qu'il écarte les offres irrégulières, inacceptables ou inappropriés. L'article L2152-2 qualifie d'irrégulière *« une offre qui ne respecte pas les exigences formulées dans les documents de la consultation, en particulier parce qu'elle est incomplète, ou qui méconnaît la législation applicable notamment en matière sociale et environnementale. »*.

[128] Voir notamment : Tribunal judiciaire de Paris, 15 avril 2022, n° 19/12628 et Cour d'appel de Paris, 9 novembre 2022, n° 21/00180.

[129] La chambre de commerciale de la Cour de cassation avait déjà jugé que « Constitue un acte de concurrence déloyale le non-respect d'une réglementation dans l'exercice d'une activité commerciale, qui induit nécessairement un avantage concurrentiel indu pour son auteur ». Cass. Com., 17 mars 2021, n° 01-10.414.

constatés concernaient notamment l'absence de charte et des consentements recueillis dans des conditions contraires aux exigences requises.

Cette pratique a récemment été confirmée par la Cour de justice de l'Union européenne, interrogée sur la conformité de telles sanctions au RGPD[130]. Là encore, il semble sérieux d'envisager que le même raisonnement puisse s'appliquer pour l'AI Act, à chaque fois que l'usage nécessitera une attention particulière, c'est-à-dire pour tous les cas d'usage autres que ceux classés en risque minimal.

De la même manière, cela a été relevé précédemment, la participation des fournisseurs d'IA aux remontées d'informations nécessaires en matière de devoir de vigilance est une opportunité de conformité supplémentaire pour les acteurs qui y sont soumis, et doit à ce titre être prise comme un atout par ces derniers.

L'intérêt de ces cas d'usage du droit comme arme économique doit évidemment être renforcé par les jurisprudences des tribunaux et décisions des Cnil nationales et de la Commission européenne, s'agissant en particulier des garanties de conformité attendues des acteurs hors Union européenne concernant la protection et l'utilisation des données à caractère personnel.

A cet instant, les deux niveaux d'usage de l'arme se recoupent alors puisque de la responsabilité des juridictions et du régulateur dans les cas qui lui sont soumis dépend du degré d'offensivité commerciale dont disposera l'acteur privé face à des concurrents peu respectueux des règles de droit.

2. Le rendez-vous avec l'histoire des décideurs politiques, des autorités de régulation et des juridictions

L'intelligence artificielle engage un bouleversement profond de nos économies, et de nos sociétés. La France et l'Union européenne dans son ensemble sont à un moment décisif. Chacun de nos choix, économiques, juridiques, politiques, est susceptible de déterminer le rôle que nous jouerons dans le monde pour un grand nombre d'années.

Or, à cette heure des décisions, nous avons encore les moyens de porter y compris sur la scène mondiale une IA éthique, durable et compétitive en fleuron de notre souveraineté.

Le droit doit pour cela devenir une arme fière. Nous devons abandonner l'impression d'avoir le droit honteux vis-à-vis de ceux qui se pensent trop gros pour s'y plier, et de ne l'appliquer (trop) fermement qu'à nos acteurs nationaux et européens qui sont les premiers à jouer, même contraint, le jeu.

LE RÔLE HISTORIQUE DES DÉCIDEURS PUBLICS

Dans ce rendez-vous avec l'histoire, les décideurs publics doivent porter une vision claire du droit.

[130] CJUE, 4 octobre 2024, ND contre DR, affaire C-21/23.

Ces dernières années, les règles se sont accumulées. C'est un fait et pas nécessairement un mal, dans le cas où les acteurs sont accompagnés pour s'y conformer, avec le temps et la souplesse nécessaire. Ou cette régulation permanente peut être une stratégie, mais elle paraît dans ce cas périlleuse compte tenu des moyens dont disposent nos acteurs nationaux et européens face aux géants étrangers, souvent alimentés par des fonds d'origine étatique.

Nous proposons de :

- **Limiter toute nouvelle règle dédiée au numérique, et en particulier à l'IA, aux règles qui viseraient à simplifier des règles existantes pour les rendre plus accessibles,** à homogénéiser les interprétations entre pays européens, à articuler les réglementations entre elles, et à renforcer la souveraineté et l'autonomie stratégique européenne.
- **Retenir une vision adaptée du droit avec les trois couches inspirées de l'informatique : infrastructure, plateforme et service.**
- Quel que soit le scénario retenu, une vision claire est nécessaire. Pour que les acteurs sachent dans quelle direction ils doivent avancer. C'est la même vision qui doit normalement régner s'agissant des règles fiscales. **En droit, la première des sécurités c'est la prévisibilité.**

LE RÔLE HISTORIQUE DES AUTORITÉS DE RÉGULATION

Dans la logique des textes relatifs au numérique, en particulier du RGPD, l'approche par les risques devrait constituer une clé de lecture inaltérable. Pour ce faire, chaque cas devrait être très finement analysé en fonction des spécificités du secteur, de la technologie utilisée, et les sanctions devraient être le cas échéant établis en fonction de l'ensemble de ces éléments.

La CNIL, pour ce qui est des données, s'efforce d'apporter des réponses sur ces sujets mais se retrouve parfois confrontée à la difficulté de cas d'espèce et à une pression médiatique amplifiée par les réseaux sociaux, sur quelques cas emblématiques.

Pour limiter ces risques qui affaiblissent la légitimité de l'édifice dans son ensemble, il pourrait être envisagé (i) d'intensifier la logique de régulation proactive et agile avec un dialogue permanent avec les écosystèmes innovants, et de (ii) davantage représenter les acteurs des nouvelles technologies dans le collège de la CNIL.

Sur ce dernier point, des travaux parlementaires sont en cours et vont dans ce sens, cela doit être souligné. Si aucun système n'est parfait, la présence d'un nombre plus important de professionnels du secteur paraît utile pour intensifier le dialogue avec les juristes qui font un très grand travail, lequel sera encore mieux valorisé lorsqu'il obtiendra toute sa légitimité des échanges avec les acteurs.

L'instauration d'un réseau national de coordination de la régulation des services

numériques[131] par la loi SREN va également dans ce sens, d'une meilleure connaissance des spécificités sectorielles et doit être accompagnée jusqu'au bout.

Ces réflexions sont loin d'être anodines. Car sans une régulation comprise par tous, c'est-à-dire perçue comme juste, nous ne pourrons faire du droit l'arme qu'il peut et doit être.

La responsabilité des autorités de régulation est à ce titre immense.

LE RÔLE HISTORIQUE DES JURIDICTIONS

Les juridictions, enfin, dans le prolongement des autorités de régulation et dans leur rôle de garantes des équilibres fondamentaux, doivent être au rendez-vous des réalités de l'intelligence artificielle et plus largement du numérique.

Elles ont un rôle essentiel dans l'interprétation des normes nouvelles, qui peuvent parfois manquer leur cible ou mériter une lecture très fine, y compris du contexte et des réalités techniques.

[131] Composé de l'ensemble des autorités administratives compétentes et des principaux services de l'État, dont la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et la Direction générale des entreprises (DGE), ce réseau piloté par la DGE sera chargé de renforcer les coopérations multilatérales afin de permettre une meilleure articulation des régulations du numérique entre elles.

L'IA SANS RÈGLES,
C'EST UNE PUISSANCE
SANS CONSCIENCE.

CONCLUSION

"Our choice is not between "regulation" and "no regulation". (...) The only choice is whether we collectively will have a role in (coders) choice and thus in determining how these values regulate or whether collectively we will allow the coders to select our values for us"[132]

Lawrence Lessig

Vingt-cinq ans après l'analyse du Professeur Lessig, **l'IA est un formidable prétexte pour interroger de nouveau le rapport entre le droit et le numérique.** D'une part, parce que son potentiel et la nécessité d'en être à la pointe pour espérer exister, remettent largement en question l'édifice juridique qui, en Europe au moins, avait permis de passer du « Code is Law » au « Law is Code ». D'autre part, parce que l'IA porte en elle-même les caractéristiques d'une technologie susceptible de réinventer le rapport entre le droit et l'innovation, pour le meilleur.

Avec ce rapport, nous avons donc essayé de répondre, avec nos mots, à cette question : **pour réussir à développer et imposer une IA européenne, doit-on choisir entre innovation et régulation ?**

Notre conviction est simple : si nous voulons préserver un monde pour tous, les deux vont ensemble. L'innovation n'a de sens ni de portée collective sans une régulation exigeante, claire et stratégique.

Ce sont les conditions d'une alliance de ces deux faux contraires que nous avons par conséquent tenté de dégager, pour le cas de l'intelligence artificielle. Ces conditions sont au nombre de trois :

- La norme doit faciliter la scalabilité,

- La norme doit accélérer son acceptabilité,

- La norme doit être activable pour devenir un levier d'acquisition de marché.

La règle de droit peut ainsi donner à l'innovation une direction et une valeur. **Le rapport propose une architecture politique et stratégique pour y parvenir tout en s'inscrivant pleinement dans la continuité des réflexions portées par Enrico Letta et Mario Draghi** sur la nécessité de renforcer l'intégration européenne pour affronter les défis économiques et technologiques contemporains.

[132] L. Lessig, « Code and other laws of cyberspace », Basic Books, 1999.

Là où Letta propose un 28e régime pour faciliter l'accès au droit et où Draghi appelle à une consolidation profonde du marché intérieur européen, *AI is Law* affirme que le droit codé et intelligible sera l'un des outils clés pour rendre cette ambition opérationnelle dans l'ère de l'intelligence artificielle.

Parce que les apôtres auto désignés de la liberté en sont parfois les plus grands ennemis. Dans un monde où l'IA sera bientôt l'auteur du code, laisser aux codeurs le choix de nos valeurs, ce serait laisser bien plus que nos valeurs : ce serait laisser tomber l'humanité.

RECOMMANDATIONS

ADAPTER L'ARCHITECTURE DU DROIT AUX BESOINS DE L'IA

Pourquoi ? Le droit doit devenir un levier de scalabilité de l'innovation : il protège, légitime et sécurise l'innovation.

Quoi ? L'architecture du droit doit être adaptée pour accompagner des technologies qui évoluent plus rapidement que la norme, sans perdre sa logique protectrice pour la société. Une architecture inspirée de l'informatique peut être proposée :

- ***Law as an Infrastructure (LaaI) :*** avec des libertés et droits fondamentaux inaltérables garantis par nature.
- ***Law as a Platform (LaaP) :*** des textes juridiques codables (un « droit API »), en commençant par les textes relatifs aux données.
- ***Law as a Service (LaaS) :*** un périmètre d'expérimentation dans un cadre flexible mais sécurisé, sur le modèle des « bacs à sable » réglementaires.

Comment ?

- **Recommandation n° 1** | Faire du code la 25ème langue de l'Union européenne de sorte à ce que tout nouveau texte puisse trouver une traduction en langage informatique.
- **Recommandation n° 2** | Intégrer un texte de codage du droit aux omnibus en préparation au niveau européen des modifications pour permettre le codage à court terme des textes principaux dédiés au numérique, dans la logique des travaux déjà commencés.
- **Recommandation n° 3** | Favoriser dans un premier temps au niveau français l'initiative du Legal Data Space qui rassemble déjà un grand nombre d'acteurs de la filière du droit. C'est-à-dire une infrastructure mutualisée pour le traitement et le partage des données juridiques publiques - open data - et privées - *data spaces* - dans le but de développer une IA juridique souveraine, par et pour la filière du droit.

PROMOUVOIR UN DROIT LISIBLE, HARMONISÉ ET SOUVERAIN

Pourquoi ? Pour être un levier d'innovation, la règle de droit doit être prévisible, intelligible et actionnable.

Quoi ? Ajuster l'ensemble existant pour y apporter davantage de cohérence et d'ambition stratégique.

Comment ?

- **Recommandation n° 4** | Simplifier, harmoniser, articuler et souverainiser en limitant à ces objectifs les prochaines modifications du cadre juridique.
- **Recommandation n° 5** | Évaluer l'efficacité des règles dédiées à l'IA à partir du triptyque : normalisation (la règle doit être un levier de scalabilité de l'innovation), acceptabilité (la règle doit faciliter l'acceptabilité de l'innovation), actionnabilité (la règle doit permettre aux acteurs de s'en prévaloir dans la conquête de marchés).

SIMON BERNARD

Simon Bernard est avocat, fondateur du cabinet ModernLaw, dédié à la gouvernance et aux enjeux de l'intelligence artificielle.

Simon commence sa carrière en fiscalité internationale et contribue activement aux travaux sur la taxation des géants du numérique et aux premiers écrits sur la fiscalité de l'écosystème blockchain. Dans cette suite, il rejoint le groupe majoritaire à l'Assemblée nationale qu'il conseille d'abord sur les sujets de fiscalité et de finances publiques, puis sur les sujets régaliens et de libertés publiques, notamment les lois des ministères de l'Intérieur et de la Justice, et l'ensemble des textes de la crise sanitaire.

Il intègre ensuite le cabinet d'une Première ministre comme conseiller parlementaire, contribue à la préparation, à la négociation et au suivi des textes relatifs aux ministères de l'Intérieur et de la justice, aux collectivités territoriales, aux outre-mer, aux sujets liés à l'énergie et à la transition écologique, et à la régulation du numérique, en particulier. Il devient par la suite directeur adjoint de la ministre des Sports et des Jeux olympiques et paralympiques, en charge de l'éthique et de l'intégrité.

En mars 2025, il fonde le cabinet d'avocat ModernLaw, dédié à la gouvernance et aux enjeux de l'intelligence artificielle, afin d'accompagner à la fois les acteurs de la tech et l'ensemble des acteurs publics et privés dans ce nouvel environnement. Dans ce cadre et en cohérence avec son parcours et la philosophie du rapport « AI is Law », Simon défend une vision du droit comme levier économique et stratégique, outil de souveraineté et accélérateur de transitions profitables à tous.

REMERCIEMENTS

Ce rapport n'aurait pu voir le jour sans le soutien et l'expertise de plusieurs personnes et organisations dont l'engagement et la vision ont été déterminants pour tracer les conditions et contours d'un droit à la fois bouclier et lance d'une IA européenne, ambitieuse et responsable.

Je tiens à exprimer ma plus profonde gratitude au think tank, et en particulier à Arno Pons et Olivier Dion. Leur confiance, leurs précieuses orientations et leurs conseils toujours constructifs ont permis de trouver des voies pertinentes et très concrètes.

Mes remerciements vont également à Martin Bussy et Thomas Saint-Aubin, pionniers dans la perception du droit comme levier de scalabilité. Leur travail sur le Legal Data Space constitue déjà un socle d'infrastructure essentiel, en avance sur l'architecture du droit proposée dans ce rapport.

Je souhaite remercier chaleureusement l'ensemble des acteurs, décideurs publics et conseillers qui ont bien voulu partager avec nous leur expérience du droit appliqué à l'innovation et au développement de l'intelligence artificielle, en particulier Criteo, Explain, France Digitale et Numeum. Vos expériences et idées ont été d'une grande richesse et ont contribué à l'approfondissement des analyses proposées.

Enfin, une reconnaissance toute particulière à Clara Koenig et François. Pour leurs conseils avisés, leur passion communicative pour ces sujets complexes, et leur regard d'une grande acuité qui a su enrichir ce rapport à des moments clés.

A tous, un grand merci. Ce rapport est désormais le nôtre, celui de ceux qui croient aux valeurs et à la force de notre chère et aujourd'hui si précieuse démocratie.

DIGITAL NEW DEAL
THINK-DO-TANK DE LA NOUVELLE DONNE

Digital New Deal accompagne les décideurs privés et publics dans la création d'un Numérique des Lumières, Européen et Humaniste. Notre conviction est que nous pouvons offrir une troisième voie numérique en visant un double objectif : défendre nos valeurs en proposant un cadre de confiance par la régulation (think-tank) ; et défendre nos intérêts en créant des écosystèmes de confiance par la coopération (do-tank).

Notre activité de publication a pour vocation d'éclairer de manière la plus complète possible les évolutions à l'œuvre au sein des enjeux de «souveraineté numérique», dans l'acception la plus large du terme, et d'élaborer des pistes d'actions concrètes à destination des organisations économiques et politiques.

Olivier Sichel (président fondateur) et Arno Pons (délégué général), pilotent les orientations stratégiques du think-tank sous le contrôle régulier du conseil d'administration (composition ci-dessous).

SÉBASTIEN BAZIN
PDG AccorHotels

NATHALIE COLLIN
General Manager, Consumer and Digital Division La Poste Group

NICOLAS DUFOURCQ
DG of Bpifrance

AXELLE LEMAIRE
Former Secretary of State for Digital Technology and Innovation

ALAIN MINC
President AM Conseil

DENIS OLIVENNES
DG Libération

ODILE GAUTHIER
DG de de l'Institut Mines-Telecom

ARNO PONS
General Delegate of the Digital New Deal think tank

BRUNO SPORTISSE
PDG Inria

ROBERT ZARADER
PDG Bona fidé

JUDITH ROCHFELD
Associate Professor of Law, Panthéon Sorbonne

OLIVIER SICHEL
President Digital New Deal
DGA Caisse des Dépôts

NOS PUBLICATIONS

IA générative : s'unir ou subir
Olivier Dion, Michel-Marie Maudet, Arno Pons - *novembre 2024*

Infrastructures publiques de partage des données : les grandes oubliées
Laura Létourneau - *septembre 2024*

Strengthening pan-european democracy in the era of AI
Axel Dauchez, Hendrik Nahar - *avril 2024*

Le numérique au service d'un futur durable
Véronique Blum, Maxime Mathon - *juin 2023*

IA de confiance, opportunité stratégique pour une souveraineté industrielle et numérique
Julien Chiaroni, Arno Pons - *juin 2022*

Data de confiance, le partage des données, clé de notre autonomie stratégiques
Olivier Dion, Arno Pons - *septembre 2022*

Cybersécurité, vigile de notre autonomie stratégique
Arnaud Martin, Didier Gras - *juin 2022*

RGPD, acte II : la maîtrise collective de nos données comme impératif
Julia Roussoulières, Jean Rérolle – *mai 2022*

Fiscalité numérique, le match retour
Vincent Renoux - *septembre 2021*

Défendre l'état de droit à l'ère des plateformes
Denis Olivennes et Gilles Le Chatelier - *juin 2021*

Cloud de confiance : un enjeu d'autonomie stratégique pour l'Europe
Laurence Houdeville et Arno Pons - *mai 2021*

Livres blancs : Partage des données & tourisme
Fabernovel et Digital New Deal - *avril 2021*

Partage de données personnelles : changer la donne par la gouvernance
Matthias de Bièvre et Olivier Dion - *septembre 2020*

Réflexions dans la perspective du Digital Services Act européen
Liza Bellulo - *mars 2020*

Préserver notre souveraineté éducative : soutenir l'EdTech française
Marie-Christine Levet - *novembre 2019*

Briser le monopole des *Big Tech* : réguler pour libérer la multitude
Sébastien Soriano - *septembre 2019*

Sortir du syndrome de Stockholm numérique
Jean-Romain Lhomme - *octobre 2018*

Le Service Public Citoyen
Paul Duan - *juin 2018*

L'âge du web décentralisé
Clément Jeanneau - *avril 2018*

Fiscalité réelle pour un monde virtuel
Vincent Renoux - *septembre 2017*

Réguler le « numérique »
Joëlle Toledano - *mai 2017*

Appel aux candidats à l'élection présidentielle pour un #PacteNumérique
janvier 2017

La santé face au tsunami des NBIC et aux plateformistes
Laurent Alexandre - *juin 2016*

Quelle politique en matière de données personnelles ?
Judith Rochfeld - *septembre 2015*

Etat des lieux du numérique en Europe
Olivier Sichel - *juillet 2015*

THINK-DO-TANK

DIGITAL NEW DEAL

Mai 2025

www.thedigitalnewdeal.org