

Myriam QUÉMÉNER



**ÉCOSYSTÈME
NUMÉRIQUE :
DÉFIS JURIDIQUES
ET SOCIÉTAUX**

IA, Métavers, Santé, Environnement,
Business, Finance, Cybersécurité

Préface de Christiane FÉRAL-SCHUHL

Myriam QUÉMÉNER

est Magistrat et docteur en droit.

Suivez-nous sur



www.gualino.fr

Contactez-nous gualino@lextenso.fr



© 2023, Gualino, Lextenso
1, Parvis de La Défense
92044 Paris La Défense Cedex
EAN 9782297217378
Hors collection

Myriam QUÉMÉNER

ÉCOSYSTÈME NUMÉRIQUE : DÉFIS JURIDIQUES ET SOCIÉTAUX

IA, Métavers, Santé, Environnement,
Business, Finance, Cybersécurité

Préface de Christiane FÉRAL-SCHUHL

Du même auteur, chez le même éditeur

- *Quels droits face aux innovations numériques ?*, 2020, Hors collection (en coll. Frédérique Dalle, Clément Wierre).
- *Le droit face à la disruption numérique*, 2018, Hors collection.



Préface

Le numérique constitue depuis plusieurs décennies un terrain de réflexion d'une extraordinaire richesse. En 40 ans, il a bouleversé nos règles sociétales, éducationnelles, institutionnelles, économiques... et bien sûr juridiques.

On pensait en avoir fait le tour !

C'était compter sans le talent de Myriam Quémener, toujours attentive aux évolutions du droit mis à l'épreuve du numérique.

Dans cet ouvrage, elle pointe du doigt les toutes nouvelles questions juridiques qui se profilent avec de nouveaux concepts, comme celui du *métavers*, des *NFT (Non Fongible Token)*, des cryptomonnaies ou encore avec les nouveaux métiers émergents, comme celui des influenceurs qui envahissent de plus en plus nos réseaux.

Si elle rappelle le dispositif légal qui s'est forgé au fil des années, l'auteure met bien en exergue les mesures prises par le législateur pour mieux protéger l'internaute. Il s'agit, par exemple, de celles qui visent à mieux lutter contre les comportements haineux ou les *fake news* ou encore celles qui renforcent la protection des mineurs. Il s'agit également des dispositions de la loi pour la confiance dans l'économie numérique et celles prévues désormais par le *Digital Service Act* et le *Digital Marketing Act*.

Si l'auteure souligne également le rôle central des autorités administratives indépendantes, notamment celui de la CNIL ou de l'Arcom, de certaines institutions comme l'ANSSI, et plus généralement, celui des autorités chargées d'enquêtes, elle décrypte la nécessaire collaboration « public-privé » qui s'impose dans le nouvel écosystème du numérique.

L'une des qualités les plus marquantes de cet ouvrage réside dans son approche méthodique et sa vision à 360 degrés. Dans cet objectif, si tous les acteurs du numérique doivent se conformer à un cadre contraignant, notamment pour collecter et traiter les données à caractère personnel sensibles, l'auteure opère un découpage très pertinent pour identifier la réglementation propre à chaque secteur d'activité. Aussi, qu'il s'agisse de la finance, de l'assurance, du droit ou de la santé, la startup dispose d'une grille de lecture des mesures à prendre.

Dans cette démarche originale et transversale, cet ouvrage constituera très certainement une mise à jour précieuse de nos pratiques numériques. Le lecteur, juriste comme non-juriste, devrait pouvoir y trouver une ou plusieurs clés juridiques pour avancer en toute sécurité dans le monde numérique.

Christiane FÉRAL-SCHUHL



Sommaire

<i>Préface</i>	5
Introduction	9
Chapitre 1 IA, DATA, Métavers, nouveaux défis des acteurs du numérique	11
§1. Intelligence artificielle (IA) et data	12
§2. Métavers	18
Chapitre 2 Numérique et dérives sociétales	23
§1. Haine en ligne et cyberharcèlement	24
§2. Lutte contre les fake news	29
§3. Autres atteintes	32
Chapitre 3 Numérique et santé	37
§1. Les activités numériques de santé	38
§2. Réglementation de l'e-santé	40
§3. Les données de santé face aux risques numériques	41
Chapitre 4 Numérique et environnement	45
§1. Les acteurs engagés	46
§2. Présentation des orientations conciliant numérique et environnement	46
Chapitre 5 Numérique et business	49
§1. Diversité des acteurs du e-commerce	50
§2. Les influenceurs	53
§3. Marketplaces et plateformes	56
§4. Art, culture et numérique	61
Chapitre 6 Numérique et finance	67
§1. Les Fintech, startups de la finance	67
§2. Les RegTechs (« Regulatory technologies »)	71
§3. Les plateformes financières	72
§4. Contrôle de l'AMF	76
§5. Positionnement étatique face à la digitalisation financière	76
Chapitre 7 Numérique et assurance	81
§1. Les assurtech, startups de l'assurance	81
§2. Cybersécurité et assureurs	82

Chapitre 8	Numérique et droit	85
§1.	Les legaltechs, startups du droit.....	86
§2.	Métiers de justice et numérique.....	87
§3.	Avocats et numérique : les incubateurs des barreaux	88
§4.	Notariat et numérique	89
§5.	Les délégués à la protection des données (DPO)	90
Chapitre 9	Numérique et sécurité	93
§1.	Cybercriminalité : auteurs et écosystème criminel	94
§2.	Cybersécurité et organismes étatiques	95
§3.	Services d'enquête spécialisés cyber	99
§4.	Justice et numérique.....	106
§5.	Évolution en matière de cybersécurité.....	109
§6.	Autres acteurs de la cybersécurité	110
Perspectives	121
<i>Index</i>	123



Introduction

La transformation numérique des sociétés est un phénomène qui bouscule les équilibres économiques et modifie les usages à une vitesse fascinante. Le vocable numérique est tellement envahissant dans nos vies qu'il est désormais passé d'adjectif à un nom¹. Elle cible aussi bien les clients des entreprises numériques dans leurs activités, leurs chaînes de valeur et leurs organisations, que les individus dans leur vie quotidienne et la société en général. C'est tout le sens des travaux menés par le conseil national du numérique qui analyse les relations entre les humains et le numérique par exemple². Le numérique est à la fois porteur de promesses économiques fortes, comme d'éventuelles destructions de métiers et de risques pour l'environnement et la planète tout entière.

L'augmentation des projets développés grâce au numérique a entraîné l'apparition de nouveaux acteurs souvent encore méconnus du grand public et qui doivent prendre leurs marques. Ainsi le marché du numérique adapte ses missions à différents enjeux notamment économiques, stratégiques, politiques voire environnementaux.

Ces bouleversements numériques se traduisent par exemple en France par un nombre croissant de startups qui se développent sur des secteurs innovants en valorisant par exemple les données par le recours à l'intelligence artificielle (IA). Ces startups se regroupent au sein de campus comme la Station F³ créée par Xavier Niel en 2017 et qui en centralise plus de 1 000. On peut aussi noter la création de la « French tech⁴ » qui a pour objectif de créer une dynamique et un accompagnement personnalisé pour les startup en associant aussi les investisseurs et les décideurs.

On constate aussi la création d'organismes et de structures dédiées pour mesurer l'impact du numérique sur la société. Tel est le cas du Conseil national du numérique qui aborde régulièrement ses nouveaux enjeux⁵, et qui est chargé particulièrement d'interroger la relation de l'humain au numérique.

Le domaine du digital a pris une telle ampleur que l'on évoque désormais un véritable droit du numérique qui a fait l'objet récemment d'une étude menée par le cabinet d'avocats Féral, pionnier en la matière⁶.

-
1. Ainsi que le souligne R. Ollard, « Un an de droit pénal numérique », Droit pénal n° 12, décembre 2022, chron. 12, Lexis-Nexis.
 2. V <https://cnumerique.fr>
 3. V. <https://stationf.co/>
 4. V. <https://lafrenchtech.com/fr/>
 5. V. <https://cnumerique.fr>
 6. Journal Spécial des sociétés Numéro thématique : droit du numérique : panorama de l'actualité 2022, rédigé par le cabinet Féral n° 51, 21 décembre 2022.

Toutes ces nouvelles structures sont parfois complexes à cerner et ce d'autant qu'elles empruntent des noms au monde du rêve et du virtuel comme les termes « Licornes⁷ » et « Métavers ».

Dans cet univers envahi par le numérique, il apparaît essentiel aujourd'hui d'y voir plus clair en présentant tout d'abord le fil rouge qui guide ces évolutions créatrices de nouveaux métiers, à savoir le recours à l'intelligence artificielle (IA) et à l'exploitation des données numériques pour les valoriser au mieux. En effet, l'IA, la data et bientôt le Métavers irriguent l'ensemble des nouvelles activités humaines qui se regroupent par le biais d'associations et de communautés et constituent en quelque sorte le dénominateur commun de ces activités digitales innovantes.

Après cette présentation des grandes tendances dans un contexte global et communautaire, il est apparu clairement qu'aborder les acteurs en fonction de leurs activités diversifiées, allant de la modération des dérives sociétales à la santé, la finance, le commerce et le droit afin de cerner les réglementations qui émergent progressivement en ces domaines, était la méthode la plus pédagogique. On constate en effet l'émergence de nouveaux acteurs mais aussi une évolution notable des missions des acteurs classiques aussi bien publics comme les ministères et les autorités indépendantes que privés comme les professions du chiffre et du droit.

7. Le terme licorne (en anglais : unicorn) est employé pour désigner une startup, principalement de la Silicon Valley, valorisée à plus d'un milliard de dollars, non cotée en Bourse et non filiale d'un grand groupe. Cette expression a été inventée par Aileen Lee en 2013.



Chapitre

1

IA, DATA, Métavers, nouveaux défis des acteurs du numérique



Plan du chapitre

- §1. Intelligence artificielle (IA) et data
- §2. Métavers



Le recours au numérique, quels que soient les nouveaux métiers qu'il a engendrés depuis ces dernières années, fait appel à une masse des données de plus en plus considérable et également à l'intelligence artificielle qui permet désormais de s'aventurer vers de nouveaux territoires virtuels comme « le Métavers » ou « les métavers ». Les conséquences sont massives en termes d'éthique, de protection des données personnelles et donc de libertés qui peuvent être mises à mal par un recours mal maîtrisé à l'intelligence artificielle. Ces deux axes doivent guider en permanence les nouveaux acteurs. Les enjeux sont très forts notamment sur le plan économique puisque selon une étude récemment menée, « La taille du marché mondial de l'intelligence artificielle (IA) a été estimée à 119,78 milliards de dollars américains en 2022 et devrait atteindre 1 597,1 milliards de dollars américains d'ici 2030 avec un TCAC enregistré de 38,1 % de 2022 à 2030 »¹.

1. V. la totalité du rapport sur <https://www.precedenceresearch.com/table-of-content/1635>

§1. Intelligence artificielle (IA) et data

Des acteurs de plus en plus nombreux participent au processus aboutissant à l'utilisation d'un système d'intelligence artificielle (IA) et il est important de connaître les réponses juridiques qui se construisent progressivement afin de développer ces nouvelles opportunités tout en les régulant.

A. Définition et enjeux

L'intelligence artificielle (IA) associe des techniques combinant données, algorithmes et puissance de calcul². La Commission européenne a publié un Livre blanc en février 2020³ dans lequel elle a tracé les axes de la vision européenne en la matière basés sur l'excellence et la confiance. L'IA représente pour la plupart des grands États l'un des vecteurs majeurs d'influence stratégique des années à venir et un facteur considérable de croissance économique.

B. Les risques de biais

Les techniques liées à l'IA peuvent être redoutées par les citoyens en raison des risques de dérives, qualifiés généralement de biais⁴. Le danger d'intrusions étatiques dans la vie privée et autres utilisations pouvant être discriminantes de l'intelligence artificielle ne sont pas pour autant l'apanage d'États totalitaires. On peut noter la montée en puissance du courant transhumaniste et de la fracture numérique avec notamment le développement d'outils criminalistiques basés sur des technologies de reconnaissance faciale afin d'évaluer le taux de dangerosité d'un individu en fonction de son comportement⁵, ou l'utilisation de l'intelligence artificielle pour licencier automatiquement des salariés peu productifs comme a pu le faire Amazon⁶, ou encore le détournement des données des réseaux sociaux pour truquer des élections.

Certaines startups⁷ proposent des solutions pour tester la qualité des modèles d'intelligence artificielle, éliminer les biais et mettre au point plus rapidement les solutions.

Les systèmes d'intelligence artificielle (IA) peuvent donner des résultats faussés car la technologie des moteurs de recherche n'est pas neutre. En effet, ces moteurs de recherche traitent des données complexes et hiérarchisent les résultats en fonction des préférences de l'utilisateur et de sa localisation. Ainsi, un moteur de recherche peut devenir une chambre d'écho qui maintient les préjugés du monde réel et les enracine davantage lorsqu'ils sont diffusés en ligne.

La loi pour une République numérique de 2016⁸ a confié à la CNIL la mission de conduire une réflexion sur les enjeux éthiques et les questions de société soulevées par l'évolution des technologies numériques. Dans son rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle en

2. V. Glossaire de l'intelligence artificielle produit par la CNIL : <https://www.cnil.fr/fr/intelligence-artificielle/glossaire-ia>

3. V. <https://fr.scribd.com/document/489693535/commission-white-paper-artificial-intelligence-feb2020-fr#>

4. C. Villani, rapport « Donner un sens à l'intelligence artificielle », pour une stratégie nationale et européenne : <https://www.vie-publique.fr/rapport/37225-donner-un-sens-lintelligence-artificielle-pour-une-strategie-nation>

5. S. Le Janne, « Une intelligence artificielle peut-elle réellement prédire un crime ? », 30 juill. 2017, disponible sur <https://www.ulyces.co/longs-formats/une-intelligence-artificielle-peut-elle-reellement-predire-un-crime/>

6. V. l'exemple de Amazon, <https://atranshumanisme.com/2019/04/28/amazon-a-utilise-une-ia-pour-licencier-automatiquement-des-travailleurs-peu-productifs/>

7. Par exemple Giskard : <https://www.giskard.ai/>

8. V. L. n° 2016-1321, 7 octobre 2016 pour une République numérique. G. Haas, S. Astier, « Les biais de l'intelligence artificielle : quels enjeux juridiques », Répertoire Dalloz IP/IT et Communication, juill. 2019.

date du 15 décembre 2017, la CNIL pose ainsi les bases de ces deux principes fondateurs devant gouverner l'encadrement des algorithmes et de l'intelligence artificielle.

Les préjugés de genre devraient être évités ou du moins minimisés dans le développement des algorithmes, dans les grands ensembles de données utilisés pour leur apprentissage. Le rapport du Conseil d'État⁹ propose de confier à la CNIL le rôle de régulateur des systèmes d'IA, notamment publics, que le projet de règlement européen envisage de consacrer. Sous-dimensionnée actuellement, elle devra être profondément transformée pour incarner à la fois l'enjeu de la protection des droits et libertés fondamentaux, d'une part, et de l'innovation et de la performance publique, d'autre part.

C. Réglementation et sanctions

Dans la mesure où l'intelligence artificielle (IA) utilise des données numériques en les maniant par des algorithmes, comme nous avons pu le constater ci-dessus, des risques de dérives et de biais ne sont pas à exclure¹⁰. C'est pourquoi un consensus se dégage afin d'encadrer le recours à l'intelligence artificielle. Dans ces objectifs, l'Union européenne a annoncé en avril 2021, la mise en place d'un nouveau cadre juridique spécialement dédié à l'IA, sur le modèle du Règlement général sur la protection des données (RGPD). Le Conseil de l'Europe, par la voix de son directeur de l'information, *Jan Kleijssen*, partage cette analyse en soulignant que la régulation de l'IA est désormais l'un des défis majeurs pour la société¹¹.

Le Conseil d'État, dans son rapport récent « S'engager dans l'Intelligence artificielle pour un meilleur service public » publié en août 2022¹², indique qu'il est nécessaire d'anticiper l'entrée en vigueur du futur règlement européen et de mettre en place un cadre normatif des systèmes d'intelligence artificielle (SIA) dans la sphère publique. Des lignes directrices doivent être définies ce qui permettrait d'anticiper le texte européen. Ces lignes permettraient au législateur français de suivre les progrès de la technologie et d'anticiper les contentieux à venir et d'imaginer les sanctions qui devront être prises dans le cas du non-respect de la future législation européenne.

Le droit national dispose de plusieurs textes généraux en matière de lutte contre les discriminations numériques qui sont complétés par des législations spécifiques afin de protéger les citoyens. Il convient tout d'abord de rappeler que les dispositions du RGPD sont applicables en matière d'intelligence artificielle et elles garantissent la protection des droits des citoyens. Cependant, en l'état, il n'existe pas encore de cadre juridique global au plan international pour réglementer l'IA. Les cadres juridiques en vigueur fournissent des références seulement partielles, qu'il s'agisse de la protection des données personnelles – avec en particulier, au sein de l'Union européenne, le RGPD ou de la non-discrimination. Cela demeure toutefois insuffisant dès lors qu'un grand nombre de systèmes d'IA fonctionnent à partir de données non identifiantes et peuvent avoir des conséquences sur les droits fondamentaux excédant la protection des données personnelles et la non-discrimination, sans compter les formes de discriminations susceptibles de viser des groupes non couverts par les critères de discrimination prohibés par le droit.

9. V. <https://www.conseil-etat.fr/actualites/s-engager-dans-l-intelligence-artificielle-pour-un-meilleur-service-public>

10. V. Bensoussan A. et Bensoussan J., *Algorithmes et droit*, 2023, Lexing éditions.

11. V. J. Kleijssen, « Comment encadrer le développement de l'intelligence artificielle ? », in <https://www.coe.int/fr/web/artificial-intelligence/directeur-jan-kleijssen>

12. V. <https://www.conseil-etat.fr/actualites/s-engager-dans-l-intelligence-artificielle-pour-un-meilleur-service-public>

I – Projet de règlement de l'IA

Le règlement sur l'IA est une proposition législative pour réglementer la technologie de l'IA en fonction des risques qu'elle comporte. Au cœur de la proposition se trouve la catégorie à haut risque, qui implique des exigences plus strictes en termes de robustesse et de gestion des risques de la part des développeurs d'IA.

La proposition de règlement de la Commission européenne met en exergue le fournisseur du système, sur lequel repose le cadre de conformité. Les autres acteurs doivent néanmoins être vigilants, au risque d'être requalifiés de fournisseurs et d'être tenus des obligations inhérentes à ce statut.

La Commission européenne a rendu public le 21 avril 2021 un projet de règlement sur l'intelligence artificielle¹³ afin de créer un cadre juridique avec une vision européenne basée sur l'éthique en prévenant les risques liés à cette technologie pour éviter certaines dérives. Il vise à « renforcer les règles en matière de cybersécurité afin de garantir une plus grande sécurité des produits matériels et logiciels ». Ce règlement, le « Cyber Résilience Act¹⁴ » (CRA), a pour objectif de mieux sécuriser les objets connectés qui contiennent de l'IA (IoT). Le texte accroît la responsabilité des fabricants et des éditeurs en leur imposant la notion de « security by design ». Il pourrait devenir une norme mondiale, comme le RPGD.

Toujours selon le projet de texte, « les entités concernées doivent dès à présent entamer une réflexion sur la mise en conformité pour éviter les lourdes sanctions à venir en cas de non-respect. Les autorités seront habilitées à prononcer des amendes administratives pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel total d'une entreprise, le montant le plus élevé étant retenu. Le manquement à l'obligation de surveiller, détecter et corriger les biais par une politique de gouvernance des données adéquate sera quant à lui sanctionné par une amende pouvant atteindre 30 millions d'euros ou 4 % du chiffre d'affaires (500 000 € pour les institutions, agences et organes de l'UE). Enfin, le manquement aux obligations d'information à délivrer aux organismes notifiés et aux autorités nationales compétentes en réponse à une demande sera passible d'une amende de 10 millions d'euros ou de 2 % du chiffre d'affaires. »

Le règlement sur l'intelligence artificielle « EU AI Act »¹⁵ vise la mise en place d'une gouvernance forte des systèmes d'IA au sein des organisations en utilisant un principe de classification des risques en quatre catégories : inacceptables, élevés, avec obligation de transparence, minimaux. Cette catégorisation imposera des normes garantissant ainsi aux utilisateurs un degré de protection face au risque de biais, d'atteinte à la vie privée ou de manipulation cognitive. Cet ensemble de lois devrait être adopté et mis en place dans les deux prochaines années et s'appliquera aux fournisseurs de systèmes et aux utilisateurs de solutions dans l'UE, qu'ils soient eux-mêmes résidents ou non de l'Union.

Il faut relever que certains usages de l'IA peuvent être attentatoires à la liberté et aux droits des personnes. À cet égard, dans un avis de la CNCDH¹⁶, il est recommandé de privilégier, dans la communication institutionnelle, une terminologie plus neutre et objective que l'expression

13. V. https://ec.europa.eu/commission/presscorner/detail/fr/ip_21_1682

14. Proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'union Commission européenne, 21 avril 2021 (2021/0106 (COD)).

15. V. <https://artificialintelligenceact.eu/>

16. Avis relatif à l'impact de l'intelligence artificielle sur les droits fondamentaux (A – 2022-6), Journal Officiel du 17 avril 2022, n°91.

« intelligence artificielle », telle que celle de « système algorithmique d'aide à la décision » (SAAD). Une recommandation de l'Unesco¹⁷ rappelle que les « systèmes d'IA doivent, tout au long de leur cycle de vie, améliorer la qualité de vie des êtres humains, en laissant aux individus ou groupes le soin de définir la notion de "qualité de vie", tant qu'il n'y a ni violation des droits de l'homme et des libertés fondamentales, ni atteinte à la dignité humaine au sens de cette définition ». L'Unesco invite les États membres à « évaluer de façon continue l'impact humain, social, culturel, économique et environnemental des technologies de l'IA ».

De tels mécanismes sont de nature à instaurer la confiance nécessaire dans les systèmes à base d'intelligence artificielle. Il est prévu à cet égard la création d'un Comité européen de l'intelligence artificielle réunissant les autorités de contrôle nationales et le Contrôleur européen de la protection des données.

Les principales interdictions de l'Artificial Intelligence Act

L'usage de systèmes « reposant sur **des composants subliminaux que les personnes ne peuvent pas percevoir**, ou exploitant les fragilités des enfants et des personnes vulnérables en raison de leur âge ou de leurs handicaps physiques ou mentaux ».

La **notation sociale** (« social scoring »), pratiquée par exemple en Chine qui consiste, pour les autorités publiques, à évaluer des personnes en fonction de leur comportement social ou de leurs caractéristiques personnelles.

Le recours à des **systèmes d'identification biométrique à distance** « en temps réel » (reconnaissance des visages, des empreintes digitales, de la voix...) dans les espaces publics, à des fins répressives.

II – Conseils pratiques

Les acteurs dans le domaine de l'IA sont qualifiés par le projet de règlement « d'opérateurs » et peuvent être soit fournisseurs, soit utilisateurs, soit importateurs ou soit distributeurs.

Avant l'entrée en vigueur de ce règlement, il est impératif d'élaborer une liste des services et produits concernés, classés par niveau de risque et les préconisations pour mettre les systèmes d'IA en conformité.

III – Le règlement AI Liability Directive

La Commission européenne a proposé en septembre 2022 un nouveau règlement : l'« *AI Liability Directive* »¹⁸, afin de réguler plus efficacement la fabrication de drones, de robots et d'autres produits **équipés d'un logiciel d'intelligence artificielle**. La Commission européenne espère permettre aux particuliers et aux entreprises de poursuivre plus facilement les fabricants de produits équipés d'une intelligence artificielle. Avec l'AI Liability Directive, selon Valentin Cimino¹⁹, « les commissaires européens veulent se doter des moyens nécessaires pour faire face à l'utilisation croissante de produits et services basés sur l'intelligence artificielle. Cette réglementation sera applicable aux 27 pays de l'Union européenne dans un objectif d'harmonisation. »

17. V. <https://www.unesco.org/fr/artificial-intelligence/recommendation-ethics>

18. V. https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital-contracts/liability-rules-artificial-intelligence_en

19. V. <https://siecdigital.fr/2022/09/29/ai-liability-directive-lunion-veut-une-loi-pour-mieux-reguler-les-professionnels-de-lia/>

L'AI Liability Directive permettra aux victimes de demander réparation pour les atteintes à leur vie privée, à leurs biens et à leur santé dues à la faute ou à l'omission d'un fabricant ou d'un développeur d'une technologie d'intelligence artificielle. Le texte vise également à réglementer la discrimination dans le processus de recrutement utilisant l'intelligence artificielle. Une pratique qui prend de l'ampleur et qui fait débat à travers le monde entier. Le texte allège la charge de la preuve pour les victimes avec une « présomption de causalité ».

Si cette loi est votée, les victimes devront simplement démontrer que le non-respect de certaines exigences par un fabricant ou un développeur a causé le préjudice, puis établir un lien avec la technologie d'intelligence artificielle dans leur action en justice. En vertu d'un « droit d'accès aux preuves », les victimes pourront demander au tribunal d'ordonner aux entreprises concernées de fournir toutes les informations utiles et nécessaires sur les systèmes d'IA afin de pouvoir identifier la faute qui a causé le dommage. La Commission européenne a également annoncé une mise à jour de la directive sur la responsabilité. Ainsi, les fabricants seront responsables de tous les produits dangereux, matériels et immatériels, y compris les logiciels et les services numériques, et également après la vente des produits. L'AI Liability Directive devra être approuvée par les États membres et les législateurs de l'Union européenne avant d'entrer en application. »

D. Les risques liés à l'IA

I – La reconnaissance faciale

La reconnaissance faciale est un développement de la vidéosurveillance. C'est une technologie biométrique qui permet d'analyser, grâce à des algorithmes, les traits de visages de personnes filmées ou photographiées et de les comparer à des images stockées dans une base de données.

Selon la CNIL²⁰, la reconnaissance faciale permet d'authentifier une personne en vérifiant qu'elle est bien celle qu'elle prétend être et d'identifier une personne, c'est-à-dire de retrouver une personne au sein d'un groupe d'individus, dans un lieu, une image ou une base de données.

Parmi les technologies associées à l'IA, la reconnaissance faciale²¹ fait souvent débat car elle implique le traitement de données biométriques. Consciente des risques associés au développement des outils intégrant de la reconnaissance faciale, la CNIL avait appelé dès 2018 à un débat démocratique sur les enjeux techniques, juridiques et éthiques.

À cet égard, il faut signaler que le projet de loi relatif aux jeux olympiques et paralympiques de 2024²² a exclu le recours à la reconnaissance faciale mais crée un cadre juridique expérimental jusqu'au 30 juin 2025 permettant le recours à la vidéosurveillance « intelligente » en vue d'assurer la sécurité des manifestations sportives, récréatives ou culturelles. Ces traitements par l'intelligence artificielle (IA), appelées « caméras augmentées », seront en mesure de détecter des événements prédéterminés comme des mouvements de foules, des colis ou des comportements suspects dans des lieux accueillant des événements et dans les transports en commun. Ils seront autorisés par décret pris après avis de la Commission nationale de l'informatique et des libertés (CNIL).

20. V. <https://www.cnil.fr/fr/definition/reconnaissance-faciale>

21. La reconnaissance faciale est une technique d'analyse des traits du visage fondée sur l'élaboration, à partir d'images fixes ou animées dont sont extraites des données, de « gabarits » ou modèles uniques à partir desquels sont comparés les visages des individus présentés au système.

22. V. <https://www.vie-publique.fr/loi/287639-jo-de-2024-projet-de-loi-olympique-2024>

Le 17 octobre 2022, la Commission nationale de l'informatique et des libertés (Cnil) a prononcé la sanction pécuniaire maximale de 20 millions d'euros prévue par le règlement général sur la protection des données (RGPD), soit 20 millions d'euros, à l'encontre de l'entreprise américaine Clearview AI, société américaine dédiée à la reconnaissance faciale. Cette startup construit ses bases de données à partir de la technique du web-scraping²³ qui consiste pour un logiciel à aspirer de façon automatique le contenu des pages web et en particulier sur les photos collectées sur les médias sociaux.

Délibération Cnil SAN-2022-019 du 17 oct. 2022.

Le RGPD encadre le traitement des données personnelles sur le territoire de l'Union européenne. Il s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non.

Le consentement libre est obligatoire pour récolter les données nécessaires à l'usage de la reconnaissance faciale. Le recours à une identification biométrique ne peut être imposé à un individu et ces données récoltées ne peuvent être conservées par la suite.

II – La guerre des Chatbot : ChatGPT et Bard

Lancé en novembre 2022, ChatGPT²⁴ est un outil conversationnel basé sur une intelligence artificielle soutenu par Microsoft qui permet d'échanger avec un interlocuteur en répondant à ses questions de façon précise et argumentée²⁵. Cette IA a un potentiel très important qui lui permet de réaliser des écrits proches de ce que peut faire un humain ce qui n'est pas sans inquiéter les scientifiques et universitaires²⁶. Il est capable de rédiger par exemple des dissertations ou des réponses à des questions d'analyse, ce qui inquiète le monde de l'enseignement et qui a conduit Sciences Po à en interdire l'utilisation en raison des risques de plagiat. Ainsi, dans un courrier adressé aux étudiants et aux enseignants, la direction de Sciences Po annonce que l'utilisation de ChatGPT est pour l'instant strictement interdite lors de la production de travaux écrits ou oraux par les étudiants sous peine de sanctions qui peuvent aller jusqu'à l'exclusion de l'établissement voire de l'enseignement supérieur. L'interdiction s'applique à tout autre outil ayant recours à l'intelligence artificielle.

Le recours à ce chatbot présente des risques notamment au regard des protections des données à caractère personnel et de propriété intellectuelle sur les œuvres exploitées par cette IA. Ce chatbot fait le buzz car il peut fournir des discours entiers et des réponses élaborées structurées si bien qu'il pourrait à l'avenir concurrencer les moteurs de recherche comme Google qui s'en inquiète légitimement²⁷ et qui a réagi aussitôt à en présentant un nouveau Chatbot, Bard²⁸ qui va aussi offrir un service conversationnel réservé dans un premier temps à un groupe de testeurs de confiance.

Il convient aussi de relever que la société *Open AI* qui a lancé cet outil se réfère non pas au RGPD mais à la législation de l'État de Californie (*California privacy rights*) ce qui n'est pas sans interroger le dispositif quant au respect des droits des individus et de leurs données personnelles.

Il apparaît certain que les enjeux liés à ces outils de génération de langage vont faire évoluer les métiers de l'enseignement et de la recherche mais face à ces prouesses technologiques, il ne faudra jamais oublier l'humain qui doit rester au centre de ces évolutions numériques.

23. Le web scraping est la récupération de données de pages web, de façons automatique.

24. G. Loiseau, A. Martinon, BJT févr. 2023, n° BJT202e1, 1^{er} février 2023.

25. V. <https://platform.openai.com/docs/quickstart/introduction>

26. D. Leglu, « Chat GPT-3 sème un vent de panique dans le monde réel », Challenges n° 772, p. 45.

27. V. <https://www.ladn.eu/tech-a-suivre/google-en-panique-face-a-chatgpt-rappelle-ses-fondateurs>

28. Bard, en référence à William Shakespeare, surnommé le Barde d'Avon.

§2. Métavers

En octobre 2021, une nouvelle tendance est apparue suite à l'annonce, faite par Mark Zuckerberg, du changement de la dénomination du réseau social le plus populaire au monde qui compte 2,8 milliards d'utilisateurs mensuels. Facebook est ainsi devenu Meta et le géant américain a promis « de donner vie au métavers et d'aider les gens à se connecter, à trouver des communautés et à développer des entreprises »²⁹. Il est important de définir la notion de métavers pour ensuite envisager de façon prospective les incidences juridiques que ces nouveaux univers, parfois dénommés Web 3 vont induire.

A. Cerner le concept

I – Définition

Le « métavers » ou métavers³⁰ est un concept anglais (meta universe), qui correspond à un univers numérique et à un nouvel environnement virtuel. Il peut être défini comme un ensemble numérique dans lequel chacun peut avoir une existence personnelle et personnalisée grâce à un alter ego numérique. Selon un rapport récent commandé par le gouvernement³¹, « un métavers est un service en ligne donnant accès à des simulations d'espaces 3D temps réel, partagées et persistantes, dans lesquelles on peut vivre des expériences immersives ».

Suite à la création des objets numériques uniques ou Non-fongible token (NFT), comme le note Alain Bensoussan³² certains jeux vidéo en ligne ont commencé à être assimilés à des métavers notamment The Sandbox, Decentraland ou encore Second Life. Certaines grandes marques se lancent aussi dans le métavers pour s'assurer une présence dans ces mondes virtuels. C'est le cas d'Adidas qui a créé sa première collection d'accessoires numériques associés à des NFT et utilisables dans le jeu de réalité virtuelle The Sandbox. Le terme est régulièrement utilisé pour décrire une version future d'Internet où des espaces virtuels, persistants et partagés sont accessibles via interaction 3D ou 2D en visioconférence.

II – Fonctionnement

Les métavers correspondent à des plateformes numériques interactives en 3D dans lesquelles évoluent et interagissent des avatars. L'utilisateur accède au métavers par le biais d'un avatar disposant d'une identité virtuelle. Bien que la plupart des systèmes aujourd'hui permettent de créer un avatar sans demander d'informations personnelles, cela ne veut pas dire que cette création reste anonyme. L'avatar est relié à un compte, compte qui effectue des actions susceptibles de générer des données.

Les métavers sont très présents dans l'univers du jeu (lieu où les joueurs peuvent acheter des objets avec de la monnaie virtuelle) et ces plateformes fonctionnent via la blockchain qui permet à ses utilisateurs – connectés en réseau – de partager des données sans intermédiaire. Par exemple, The Sandbox Game, est un métavers décentralisé fonctionnant sur la blockchain Ethereum qui offre aux utilisateurs la possibilité de créer, utiliser, acheter ou vendre toute sorte d'items numériques associés

29. C. Lequesne Roth, « Métavers, Web 3 : la révolution juridique en trompe-l'œil », Recueil Dalloz 2022, p. 1714.

30. Rapport de la mission sur le développement des métavers, 24 oct. 2022, disponible sur : <https://www.culture.gouv.fr/Presse/Communiqués-de-presse/Remise-du-rapport-de-la-mission-sur-le-développement-des-métavers>

31. C. François, A. Basdevant, R. Ronfard, « Mission exploratoire sur les métavers », 24 oct. 2022, disponible sur : <https://www.vie-publique.fr/rapport/286878-mission-exploratoire-sur-les-métavers>

32. V. <https://www.alain-bensoussan.com/avocats/metavers-nouveau-monde-virtuel-comment-le-definir/2022/08/09/>

chacun à un jeton non-fongible dit NFT (Non Fongible Token)³³. Le métavers permet de créer des espaces 3D immersifs et différents secteurs économiques – luxe, sport, mode, musique, art – se lancent dans le métavers et bâtissent des projets.

Toutes les transactions sont faites en **crypto-actifs** admis sur la marketplace comme, l'Ethereum ou le Polygon.

B. Quel droit applicable ?

Le métavers³⁴ pose la question de l'application ou non des réglementations existantes. Il faut souligner que le métavers n'est pas une zone de non-droit³⁵. Comme dans le monde physique, de nombreuses interrogations juridiques apparaissent : confidentialité et collecte des données, comportement anti-trust ou anticoncurrentiel, liberté d'expression et diffamation, ainsi que des questions liées à la propriété intellectuelle concernant aussi bien le droit d'auteur que les brevets ou les marques. Pour les propriétaires de marques, il est indispensable qu'ils les protègent par une stratégie juridique adaptée.

S'agissant des utilisateurs des métavers, comme le souligne Christiane Féral-Schuhl, « ils sont personnellement responsables des actions de leurs avatars, ces derniers agissant à leur initiative et sous leur contrôle. Les transactions conclues dans le métavers engagent les utilisateurs. Il peut donc y avoir violation du droit des contrats, voire du droit de la consommation lorsque les avatars sont dans une relation directe entre une entreprise et des consommateurs finaux (BtoC).

Sur le plan pénal, les infractions en ligne, comme la fraude, l'escroquerie, la diffamation, l'injure, l'usurpation d'identité peuvent être sanctionnées au même titre que les infractions commises dans le monde physique, dès lors que tous les éléments de l'infraction sont réunis. »³⁶.

Il est évident que le développement du métavers va aussi attirer le crime organisé. Les métavers pourraient permettre le développement d'une variété de cyberdélinquance, le Dark verse³⁷

Le laboratoire d'innovation numérique de la CNIL (LINC)³⁸ a souligné les difficultés de la protection des données dans le métavers par essence international. Cependant, il convient de souligner que le RGPD³⁹ s'applique bien de façon extraterritoriale et donc au métavers, la protection des données numérique étant au cœur des enjeux liés à ces nouveaux univers virtuels.

33. « Les métavers et la propriété intellectuelle : quelle protection pour les titulaires de marques ? », Joffe & Associés (joffeassociés.com).

34. A. Bensoussan, « Droits et devoirs – Vers un droit des métavers ? », Planète robots n°72, Mars/avril 2022.

35. C. Féral-Schuhl, « Point de vue. Le Métavers n'est pas une zone de non-droit », 22 sept. 2022, disponible sur : <https://www.ouest-france.fr/reflexion/point-de-vue/point-de-vue-le-metavers-n-est-pas-une-zone-de-non-droit-f1c5f406-398e-11ed-a939-a7e1706647a0>

36. V. C. Féral-Schuhl, « Le métavers n'est pas une zone de non-droit ! », Ouest-France, 22/09/2022, <https://www.ouest-france.fr/reflexion/point-de-vue/point-de-vue-le-metavers-n-est-pas-une-zone-de-non-droit-f1c5f406-398e-11ed-a939-a7e1706647a0>

37. A. Bensoussan, « Darkverse, le côté obscur du métavers », Planètes Robots n° 76, Lexing Editions.

38. V. <https://inc.cnil.fr/fr/metavers-realites-virtuelles-ou-collectes-augmentees>

39. RGPD, art. 3.

C. Exemples d'utilisation et de contentieux

I – Les cas d'usage

Les marques investissent dans le métavers, comme Nike qui a lancé son propre métavers sur la plateforme Roblox : Nikeland. Les entreprises de luxe expérimentent des projets indépendants sur le métavers comme Gucci⁴⁰ qui propose un espace dans lequel les gens peuvent découvrir des pièces de mode numériques exclusives et participer à des jeux.

Autre exemple, Interpol a annoncé le lancement de son propre métavers lors de sa 90e assemblée générale annuelle qui s'est déroulée le 18 octobre 2022 à New Delhi, en Inde⁴¹. Lors de l'introduction de ce métavers à l'assemblée générale d'Interpol, les différents délégués internationaux présents à l'événement ont pu directement s'immiscer dans ce monde virtuel « déjà pleinement opérationnel » à l'aide de casques virtuels. Lors de cette session de présentation interactive, les membres présents ont pu pénétrer dans une **reproduction virtuelle à l'identique des bureaux du siège d'Interpol**, situé à Lyon. Ce métavers, dénommé INTERPOL, va permettre aux personnes concernées de suivre des formations immersives et d'interagir avec d'autres membres via leur avatar, et ce sans aucune restriction géographique.

Mise en place par Meta et Simplon⁴² avec le soutien financier de la Région Provence-Alpes-Côte d'Azur, l'Académie du Métavers, lancé en octobre 2022 à Marseille, va former à sa première promotion de concepteur/développeur en technologies immersives et de technicien support/assistance.

Selon le premier rapport sur le métavers remis au gouvernement⁴³, qui a pour but d'ouvrir le débat sur ces univers virtuels, les secteurs qu'ils visent sont nombreux, tourisme, culture, éducation, médecine, médias, travail et administrations publiques. Les métavers apparaissent comme des espaces dématérialisés **dans une nouvelle ère du Web**. Les marques y créent par exemple leurs espaces pour présenter leurs produits et faire des développements marketing.

II – L'émergence de contentieux

Face aux développements des NFT valorisant des créations, comme dans le domaine de la mode et du luxe (bijoux, produits d'horlogerie, vêtements, chaussures, sacs, packaging...), sans autorisation des titulaires des droits, un contentieux va se développer⁴⁴.

Le groupe Hermès a engagé une procédure pour contrefaçon à l'encontre de l'artiste américain Mason Rothschild, qui s'est inspiré des sacs Hermès Birkin pour créer et vendre des objets numériques NFT dans le monde virtuel du métavers⁴⁵. La maison Hermès dénonce une atteinte à son image de marque et à ses droits de propriété intellectuelle. Mason Rothschild a poursuivi sur la même voie en lançant une centaine de « MetaBirkins » qu'il a mis en vente en cryptomonnaie pour l'équivalent de quelques

40. V. <https://vault.gucci.com/en-US/story/metaverse>

41. V. <https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2022/INTERPOL-launches-first-global-police-Metaverse>

42. Startup Simplon, l'école inclusive qui forme aux métiers du numérique dans toute la France et à l'international. Site : <https://simplon.co/>

43. C. François, A. Basdevant, R. Ronfard, « Mission exploratoire sur les métavers », 24 oct. 2022 : <https://www.vie-publique.fr/sites/default/files/rapport/pdf/286878.pdf>

44. M.-H. Fabiani, GPL 8 mars 2022, n° GPL433f2.

45. M.-J. Cougard, « Métavers : Hermès attaque Mason Rothschild pour spéculation sur les sacs Birkin », 23 janv. 2022 : <https://www.lesechos.fr/industrie-services/conso-distribution/metavers-hermes-attaque-mason-rothschild-pour-speculation-sur-les-sacs-birkin-1381199>