

Enjeux juridiques de l'intelligence artificielle

Propriété intellectuelle et données personnelles

Esquisse du rapport final, à destination de la Mission Villani 17 décembre 2017



PARTICIPAN	тs	6
Auteurs		6
Équipe p	edagogique	6
Collabor	ateurs	6
Avec le s	soutien de	6
AVANT-PRO	P0S	7
TABLEAUX R	ÉCAPITULATIFS	9
IA et pro	tection des données personnelles	9
IA et pro	priété intellectuelle	16
1. /	Au stade de l'input	. 16
2.	Au stade de l'output	. 17
	NCE ARTIFICIELLE CONFRONTÉE À LA PROTECTION DES DONNÉES À CARACT	
PERSONNEL.		20
	introductifs	
1. l	L'IA est par défaut comprise dans la réglementation existante	. 21
2.	Structure du rapport	. 21
Réflexio	ns générales	22
Principe	s et obligations pour le traitement de données personnelles	23
	La qualification de données personnelles et les risques de réidentificat 23	ion
	Sur la potentielle évolution de qualification de données non personne lonnées personnelles	
1.2.	Sur le risque de réidentification des données anonymisées	. 25
1.3. sens	Sur la transformation de données personnelles en données personne sibles	
2. l	L'identité du responsable de traitement	. 28
2.1.	Responsable de traitement/fournisseur de services de traitement IA	. 29
2.2.	Statut d'un utilisateur d'une IA générale	. 31
3. l	La base légale du traitement	. 32
3.1.	Sur les possibilités de déroger au consentement	. 33
3.2.	Sur les critères du consentement explicite	. 34

4	Privacy by design et by default	35
5 u	Finalités de traitement déterminées, explicites et légitimes et traitement térieurs compatibles	
	5.1. Les finalités déterminées et ultérieures	38
	5.2. Légitimité des traitements	40
6	Principe de minimisation	40
	6.1. Sur l'effectivité du principe de minimisation	41
	6.2. Sur l'autojustification de la collecte de données par l'IA	42
7.	Principe d'un traitement juste et loyal et d'exactitude des données	42
8	Profilage et décision individuelle automatisée	45
	8.1. Sur l'absence d'intervention humaine dans la décision	46
	8.2. Obligation d'information	47
	8.3. Explicabilité de l'IA	49
Dro	ts des personnes concernées	51
1.	Droit à la portabilité	51
	1.1. Champ d'application des données	52
	1.2. Droit anti-monopole	53
2	Droit à l'effacement	54
	2.1. Champ d'application du droit à l'effacement	55
	2.2. Droit à l'effacement et paralysie de l'IA	56
	2.3. Risque de reverse engineering	57
L'INTE	LIGENCE ARTIFICIELLE CONFRONTÉE À LA PROPRIÉTÉ INTELLECTUELLE	58
Rap	pels introductifs	58
_	osé du contexte en droit de la propriété intellectuelle et des problématique rentes	
	stade de l'input : l'IA, utilisatrice illicite de données couvertes par des droits	
	priété intellectuelle ?	
1.	État des lieux des enjeux et solutions actuels	61
	1.1. L'input de données à une IA : l'exploration de données	61
	1.1.1. Explicitation du lien entre IA, données et propriété intellectuelle	61
	1.1.2. Point vocabulaire	61

	1.1.3.	Objectifs et fonctionnement du TDM	62
	1.1.4.	Problématique double posée par le TDM	63
1	I.2. Co	nfrontation aux principaux droits de propriété intellectuelle	64
	1.2.1.	L'absence d'atteinte aux droits de propriété industrielle	64
	1.2.2.	Le risque d'atteinte au droit d'auteur	65
	1.2.3.	L'atteinte au droit sui generis sur les bases de données	68
1	1.3. Le	s enjeux soulevés par une illicéité du TDM	69
	1.3.1.	L'application de la sanction : injuste, arbitraire ou impossible ?	69
	1.3.2.	Le risque de remise en cause du business model de l'IA	70
1	I.4. De	s solutions existantes diversifiées mais incomplètes	71
	1.4.1.	Positionnement de l'Europe et de l'OMPI	71
	1.4.2.	En France : des mécanismes inadaptés à l'exploration de données	72
	1.4.3.	Les solutions contractuelles	74
2.	Ébau	iche de solutions	75
2	2.1. La	légitimation du TDM, moyen de résoudre le problème d'application	des
5	sanction	IS	75
2	2.2. Un	e nouvelle exception au droit d'auteur	76
	2.2.1.	Justification de l'exception	76
	2.2.2.	Risques de l'exception	78
	2.2.3.	Une exception ne bénéficiant qu'au droit d'auteur	79
	2.2.4.	Une exception à quels droits exclusifs ?	79
	2.2.5.	Le triple test	80
	2.2.6.	Proposition de rédaction	80
2	2.3. Pa	iement d'un prix d'accès global pour l'accès aux bases de données	: . 81
	2.3.1.	Création d'une nouvelle société de gestion collective	81
	2.3.2.	Proposition : plateforme de téléchargement par abonnement	82
2	2.4. Alt	ernativement : inspiration du <i>fair use</i>	84
		e l'output : les créations d'IA protégées par un droit de prop e ?	
1.	Expo	sé du problème : une création en quête de reconnaissance	85

1.1. La	dilution de la notion de création	85
1.2. Un	e reconnaissance par le droit d'auteur ?	88
1.2.1.	Résumé des enjeux du droit d'auteur	88
1.2.2.	Une œuvre	89
1.2.3.	Une œuvre protégeable	91
1.2.4.	Le statut de l'œuvre créée par une IA	92
1.3. Un	e reconnaissance par le droit des brevets ?	93
1.4. Au	tres droits de propriété intellectuelle	96
1.5. Un	e création en quête de titulaire	96
1.5.1.	La titularité en droit d'auteur	97
1.5.2.	La titularité en droit des brevets	99
2. Ébau	che de solutions	100
2.1. Sol	lutions en droit d'auteur	100
2.1.1.	Réforme du droit d'auteur	100
2.1.2.	Nouveau droit d'auteur repensé	104
2.2. Sol	lutions en droit des brevets	105
2.2.1.	Modifications du droit des brevets	105
2.2.2.	Atténuation des effets de concentration	107
BIBLIOGRAPHIE		109
Avis, lignes d	lirectrices, délibérations	109
Rapports		110
Travaux de re	echerche et articles pertinents	110

Participants

Rapport commandité par — groupe de réflexion sur les enjeux juridiques du transhumanisme et de l'intelligence artificielle

Auteurs

Propriété intellectuelle : Félicité Bernard, étudiante du M2 « Droit de l'Innovation »

de l'École de droit de Sciences Po

Données personnelles: Gabriel Lecordier, étudiant du M2 « Entreprises, Marchés et

Régulation » de l'École de droit de Sciences Po

Équipe pédagogique

Sous la direction de : Hugo Ruggieri, élève-avocat, cofondateur de ThinkH+,

Galatea et Aeon

Lorenzo Colombani, élève-avocat, cofondateur de ThinkH+

Tuteurs: Pr Louis Assier Andrieu, directeur de recherche au CNRS,

professeur à l'École de droit de Sciences Po

Joachim-Nicolas Herrera, doctorant de l'École de droit de

Sciences Po

Collaborateurs

Mathias le Masne de Chermont, élève-avocat, cofondateur

d'Aeon

Adrien Aulas, élève-avocat, cofondateur d'Aeon

Avec le soutien de







Avant-propos

Il ne fait plus aucun doute que le développement de l'intelligence artificielle (IA) moderne est un enjeu stratégique, économique et politique. Le perfectionnement des techniques d'apprentissage machine allié à l'accroissement général des capacités de calcul et à l'accumulation de gigantesques bases de données a permis de créer des algorithmes capables d'exécuter des tâches qui n'avaient encore jamais été automatisées. Les impacts potentiels sur la productivité, la croissance économique et l'emploi sont prodigieux. C'est ainsi que les institutions se saisissent du sujet afin de permettre à la France (et à l'Europe) d'avoir une place sur le devant de la scène de l'IA: le rapport #FrancelA, le rapport de l'OPECST, et désormais le rapport Villani sont autant d'exemples des recherches stratégiques menées par la France.

Ce développement s'accompagne de questions éthiques légitimes. La réflexion à ce sujet est menée de multiples fronts : les rapports sus-cités abordent tous ces problématiques, tandis que la CNIL vient de rendre <u>son propre rapport</u> traitant exclusivement des aspects éthiques de l'essor de l'IA. La question est également envisagée par des instances internationales telles que l'<u>Al Initiative</u> ou <u>OpenAl</u>.

Au-delà des questions éthiques, le droit est lui aussi susceptible d'être bouleversé par l'intelligence artificielle. C'est tout d'abord le cas parce que les nouvelles formes d'IA sont susceptibles de considérablement modifier la pratique du droit : les métiers d'avocat et de juge sont appelés à évoluer pour prendre en compte la potentielle automatisation de certaines de leurs tâches habituelles. Surtout, c'est la matière juridique elle-même, en tant qu'ensemble de règles régissant la société, qui sera obligée de muter pour prendre en compte les évolutions induites par l'IA.

Afin de prendre de l'avance sur ces évolutions et de proposer des solutions concrètes aux enjeux juridiques soulevés par l'IA, ThinkH+¹ a décidé de saisir la Clinique de l'École de droit de Sciences Po d'un projet sur la régulation de l'IA. C'est dans ces conditions que Félicité Bernard et Gabriel Lecordier ont commencé à rédiger ce rapport, dont le but est de dégager les principales problématiques issues du développement de l'IA au sein du droit de la propriété intellectuelle et du droit des

⁻

¹ ThinkH+ est un groupe de réflexion autour de l'éthique et de la régulation du transhumanisme et de l'intelligence artificielle né d'un projet de la Clinique de l'École de droit de Sciences Po et soutenu par l'Oréal. Plus d'informations sur thinkH+ est un groupe de réflexion autour de l'éthique et de la régulation du transhumanisme et de l'intelligence artificielle né d'un projet de la Clinique de l'École de droit de Sciences Po et soutenu par l'Oréal. Plus d'informations sur thinkH+ est un groupe de réflexion autour de l'éthique et de la régulation du transhumanisme et de l'intelligence artificielle né d'un projet de la Clinique de l'École de droit de Sciences Po et soutenu par l'Oréal. Plus d'informations sur thinkH+ est un groupe de réflexion autour de l'École de droit de Sciences Po et soutenu par l'Oréal. Plus d'informations sur thinkH+ est un groupe de réflexion autour de l'École de droit de Sciences Po et soutenu par l'Oréal. Plus d'informations sur thinkH+ est un groupe de réflexion autour de l'École de droit de Sciences Po et soutenu par l'Oréal. Plus d'informations sur thinkH+ est un groupe de réflexion autour de l'École de droit de Sciences Po et soutenu par l'Oréal. Plus d'informations autour de l'école de droit de Science par l'Alle et l'Alle

données personnelles. Le projet est, à terme, de compléter cette esquisse afin d'obtenir un rapport entièrement rédigé et portant sur l'ensemble des domaines du droit restant à explorer, et notamment la responsabilité civile et de l'assurance, le droit de la concurrence, le droit de la consommation, le droit pénal, le droit de la presse et le droit de la communication.

La méthodologie adoptée a été, pour chaque matière, de suivre le processus suivant :

- 1. Établissement d'un bref état des lieux du droit positif applicable ;
- 2. Détermination des enjeux posés par le développement de l'IA;
- 3. Détermination des réponses déjà apportées par le droit positif ; et
- 4. Élaboration de solutions pour émettre des propositions concrètes de réforme répondant aux enjeux non traités.

Cette démarche avait pour but d'assurer qu'aucun biais n'impacterait l'élaboration des propositions émises, la régulation n'étant pas un but en soi mais une réponse à un problème donné. Dans cette optique, les suggestions de ce rapport ne relèvent pas uniquement du « droit dur » et du domaine législatif, mais également de la soft law et d'une approche régulatrice et de responsabilité sociale des entreprises (RSE).

Enfin, l'approche se veut également pratique et au fait des besoins et attentes de l'industrie. Afin de satisfaire à cette ambition, ce rapport sera repris et consolidé après rencontre et audition d'acteurs du secteur, et notamment de Google, des Éditions Lefebvre Sarrut et de l'association Open Law, ainsi que de chercheurs tels que MM. Serge Abiteboul et Rand Hindi.

Afin de faciliter la lecture des conclusions apportées, nous proposons des tableaux récapitulatifs permettant de synthétiser les développements ultérieurs.

Au nom de ThinkH+, je tiens à sincèrement remercier Félicité et Gabriel, les auteurs de ce rapport, pour leur immense travail et leur investissement régulier sur ce projet, mené en parallèle de brillantes études. Je souhaite également adresser mes remerciements aux tuteurs du projet Clinique, le Professeur Louis Assier Andrieu et à M. Joachim-Nicolas Herrera, ainsi qu'à MM. Adrien Aulas et Mathias le Masne de Chermont, sans qui cette première esquisse de rapport n'aurait pu aboutir.

Hugo Ruggieri Cofondateur de ThinkH

Tableaux récapitulatifs

IA et protection des données personnelles

Le tableau ci-dessous fournit un résumé synthétique des différentes problématiques juridiques de l'IA, classées selon leur importance, ainsi que les propositions et recommandations afférentes.

Enjeux juridiques	Type d'IA		Propositions/Recommandations
Protection des données dès la conception Comment apprécier le principe du privacy by design avec des traitements IA apprenants et évolutifs ?	Potentiellement tout type d'IA	1.	La promotion de codes de conduites, de labels et/ou l'élaboration de lignes directrices par la CNIL sur les meilleures pratiques techniques et organisationnelles de <i>privacy by design</i> . Une obligation de certification par la CNIL pour certains traitements d'IA déterminés (selon par exemple : l'obligation d'une analyse d'impact préalable, les catégories de données traitées, le nombre de personnes concernées).
Décisions individuelles automatisées de l'article 22 RGPD. Comment comprendre « fondée exclusivement sur un traitement automatisé » pour définir le champ d'application de l'article 22 RGPD.	Credit scoring, assurance, ressources humaines.	 2. 3. 	La mise en place d'audits internes des responsables de traitement afin de déterminer le pouvoir de détermination et le degré significatif d'actions de ses employés travaillant avec des outils de décisions individuelles automatisées. La publication de lignes directrices par la CNIL pour clarifier le degré d'intervention humaine concernant le champ d'application de l'article 22 RGPD, en se fondant sur le pouvoir de décision et d'action significative sur les outils de décisions individuelles automatisées. Une approche fonctionnaliste par le responsable du traitement de son devoir d'information, centré sur la personne concernée et utilisant par exemple un format d'information interactif avec des contenus visuels, des icones, des

Enjeux juridiques	Type d'IA	Propositions/Recommandations
Quelle est la portée du droit à l'information de la personne concernée concernant les traitements IA entrant dans le champ de l'article 22 RGPD ? Comment résoudre le problème de l'explicabilité de l'IA ?		simulations de décisions concernant la personne concernée sur la base de différents critères etc. 4. L'élaboration de lignes directrices de la CNIL sur le contenu exact des types d'informations à communiquer aux personnes concernées. 5. La mise en place par le responsable de traitement de mesures d'auditabilités des modèles d'IA et d'un ensemble de bonnes pratiques favorisant l'explicabilité de l'IA (travail sur les données input, création d'IA explicatives etc). 6. La création d'équipes techniques au sein de la CNIL, ayant les capacités techniques pour appréhender la problématique de l'explicabilité de l'IA. 7. L'élaboration par la CNIL, en partenariat avec les entreprises, les institutions spécialisées (ex : INRIA), d'un projet de réflexion sur les methodes techniques d'auditabilité de l'IA.
Les finalités déterminées, légitimes et ultérieures du traitement. Dans quelles mesures le responsable de traitement d'une IA pourrait-il traiter des données pour des finalités ultérieures permises par l'IA? Comment apprécier la légitimité des traitements de données par l'IA?	Potentiellement tout type d'IA	 La mise en place de mécanismes internes notamment par des règles d'entreprise contraignante approuvées par la CNIL, de vérification de compatibilité des finalités ultérieures avec notamment une mission permanente du DPD de mener des tests de compatibilité avec de potentielles nouvelles finalités. Pour des traitements IA sensibles, soumis à une obligation d'une analyse d'impact préalable, la CNIL devrait imposer au responsable de traitement de prévoir, dans la mesure du raisonnable, les possibilités de nouvelles finalités permises par son traitement IA. La promotion par la CNIL de codes éthiques sectoriels sur la légitimité des finalités des traitements, et/ou de chartes éthiques de traitement chez les responsables de traitement.

Enjeux juridiques	Type d'IA	Propositions/Recommandations
Traitement juste et loyal des données. Comment le responsable de traitement peut-il s'assurer que son traitement IA ne souffre pas de biais discriminants?	Credit scoring, assurance, ressources humaines.	 L'élaboration d'une nouvelle recommandation de la CNIL sur les bonnes pratiques de détection et de correction de biais dans des modèles IA. L'analyse par le responsable de traitement des données input et limitation au maximum de l'utilisation de données pouvant être sources de discrimination. La mise en place de mesures d'auditabilité des algorithmes, et l'appel à des tiers de confiance, à des consultants extérieurs. Des processus de tests et validations au niveau de l'output des traitements IA. Un partage d'informations entre les responsables de traitements, et entre ces derniers et avec les personnes concernées. Le recours à des outils novateurs, des IA, explicatives et analysant les biais des modèles.
Droit à l'effacement. Quel est le champ d'application du droit à l'effacement dans le cadre d'un traitement IA entre les données fournies et l'apprentisage par l'IA grâce à ces données? Le droit à l'effacement justifie-t-il de paralyser l'IA ?	IA basée sur des mécanismes de deep learning	 L'élaboration de lignes directrices par la CNIL sur l'étendue du droit à l'oubli dans des traitements IA sur la question des données inférées et la comparaison de leur statut avec la mise en œuvre du droit à la portabilité. La mise en place par le responsable de traitement de mesures de privacy by design afin de retracer les données personnelles du modèles d'IA et les données inférées de ces précédentes données. L'élaboration de lignes directrices de la CNIL sur les modalités de l'exercice d'un droit à l'oubli susceptible de paralyser des traitements IA de données personnelles qui concilient l'impératif de respect de la vie privé, les intérêts des autres utilisateurs de l'IA et ceux du responsable de traitement.

Enjeux juridiques	Type d'IA	Propositions/Recommandations
Comment assurer l'effectivité du droit à l'effacement au regard notamment du risque de reverse-engineering ?		Une réflexion de la CNIL en coopération avec l'ANSSI sur l'identification des risques de reverse engineering et la définition de bonnes pratiques techniques pour prévenir ces risques.
Identité du responsable de traitement. Quel serait le statut d'un développeur IA traitant des données personnelles pour le compte d'un client ? Quel serait le statut d'un utilisateur d'une IA aux finalités générales ?	IA générales : Cortana, Alexa, Google Home. IA marketing : Albert, Einstein, Watson.	 Le fournisseur de service IA devrait évaluer ex ante le degré de standardisation de l'offre de services de traitement IA et les moyens de contrôle et d'instructions accordés au client afin de déterminer son statut et de mettre en œuvre ses possibles obligations de responsable de traitement. La rédaction de lignes directrices ou d'une recommandation sur l'identification des moyens essentiels de traitement dans un souci de sécurité juridique dans les relations entre fournisseurs d'IA et clients, et entre ces derniers et les personnes concernées. La rédaction dans des contrats entre fournisseur d'IA et client, de clauses identifant les finalités du traitement et l'identité de la partie les déterminant, l'identification et la détermination des moyens essentiels du traitement. Le contrat devrait également préciser que l'amélioration de l'IA par les données recueillies ne saurait constituer une finalité du traitement. Une définition claire des finalités des développeurs d'IA à finalités générales, dans un ensemble prédéfini et limité de finalités.
Principe de minimisation. Comment est-il possible pour un responsable de traitement et pour le	IA de machine learning/ deep learning	 Au préalable du traitement, les responsables de traitement devraient préciser clairement les finalités du traitement pour déterminer la pertinence des données collectées et la proportionnalité de cette collecte, en définissant clairement les données dont ils auront besoin et en délimitant celles dont ils n'auront pas besoin.

Enjeux juridiques	Type d'IA	Propositions/Recommandations
régulateur d'assurer l'effectivité du principe de minimisation ? L'entraînement de l'IA constitue-t-il sa propre finalité, justifiant de déroger au principe de minimisation ?		 Pour certains traitements sensibles (données de santé par exemple), une obligation de certification par la CNIL du principe de minimisation ou par un organisme agréé pourraît être imposée. La promotion par la CNIL de codes de conduites dans certains secteurs clés (ex des voitures autonomes) selon un principe de comply or explain. Les responsables de traitement devraient privilégier des solutions techniques d'anonymisation et autres solutions techniques innovantes (exemple de la simulation de fausses données par la start-up SNIPS). Une réflexion de la CNIL sur l'opportunité d'une dérogation au principe de minimisation du traitement de données faite par des IA à des fins de recherche scientifique et non commerciale, sous réserve du bon respect des autres obligations de traitement et des droits des personnes concernées. A minima, un avis de la CNIL sur la portée du principe de minimisation pour les IA d'apprentissage profond.
	Credit scoring, assurance, ressources humaines.	 Le responsable de traitement d'une IA entrant dans le champ d'application de l'article 22 RGPD devra utiliser la base légale du consentement explicite pour son traitement et pourra difficilement déroger à cette base légale. Adoption par la CNIL de lignes directrices sur les possibilités de déroger au consentement explicite dans un souci de sécurité juridique des développeurs d'IA entrant dans le champ d'application de l'article 22 RGPD. La constitution par la CNIL d'un groupe de travail sur l'opportunité d'autoriser par dérogation législative certains types d'IA de l'article 22 RGPD, eu égard à leurs avantages économiques et leurs atteintes à la vie privée. L'élaboration de lignes directrices précisément les conditions et les modalités de recueil d'un consentement explicite au sens de l'article 22 RGPD.

Enjeux juridiques	Type d'IA	Propositions/Recommandations
faire pour respecter cette contrainte accrue de licéité et notamment le recueil d'un consentement explicite de la personne concernée ?		5. Le responsable de traitement devrait demander à la personne concernée une déclaration positive de consentement et fournir une information conforme aux articles 13(f) et 14(g) RGPD portant sur le droit à l'information sur les décisions individuelles automatisées ayant des effets juridiques ou équivalents sur la personne concernée, sans intervention humaine.
La qualification de donnée personnelle. Des données non personnelles collectées par l'IA pourraient in fine être requalifiées de données personnelles. Est-il possible d'anonymiser les données personnelles avec l'IA?	Potentiellement tout type d'IA	 Une analyse d'impact préalable sur la qualification des données collectée (s l'analyse est légalement requise) et un contrôle continu du DPD de la pertinence de la qualification des données. Cela serait possible si des moyens étaient mis en place pour tracer et identifier les données personnelles et non personnelles collectées par l'IA. La CNIL devrait constituer un groupe de travail pour déterminer de potentielles nouvelles catégories de données personnelles, en prenant en considération l'avancement des technologies IA. Le responsable de traitement devrait considérer l'anonymisation des données personnelles collectées. Cela permettrait d'éviter les obligations de traitements et in fine les sanctions de la réglementation. L'élaboration d'un code de conduite CNIL sur l'anonymisation sur l'exemple des lignes directrices du Groupe de Travail de l'Article 29, et du code de
Des données personnelles collectées pourraient se transformer en données		conduite sur l'anonymisation de l'Information Commissioner's Office ² . 5. Audit périodique des techniques d'anonymisation par le DPD pour s'assurer de la fiabilité des techniques d'anonymisation ³ .

² Anonymisation, managing data protection risk, code of practice; Information Commissioner's Office, 2012. ³ Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party, April 2014, p24.

Enjeux juridiques	Type d'IA	Propositions/Recommandations
personnelles sensibles (ex : données de santé).		 La CNIL devrait promouvoir des mécanismes de label, de certification des processus d'anonymisation conformément à l'article 60 de la Loi pour une République Numérique. Le développement d'IA permettant d'anonymiser les données de manière évolutive. Une analyse d'impact préalable sur l'évaluation du risque de transformation des données collectée en données sensibles (si l'analyse est légalement requise) et à minima un contrôle continu du DPD de ce risque.
Portabilité. Quel est le champ d'application des données à restituer à la personne concernée pour le droit à la portabilité ? Comment assurer l'effectivité de ce droit anti- monopole ?	Tout type d'IA	 La mise en place chez le responsable de traitement et le sous-traitant le cas échéant, de mesures techniques et organisationnelles, afin de différencier les données couvertes par le droit à la portabilité (données fournies directement et indirectement par le sujet sur la base du consentement) et celles non couvertes par ce droit (données inférées et celles portant atteintes aux droits des tiers). Une révision de l'article L224-42-1 du Code de la consommation et notamment de la mention « en toutes circonstances » pour mise en conformité avec le RGPD. L'élaboration de standards d'interopérabilité par l'industrie afin de garantir l'effectivité du droit à la portabilité. La proposition de standards techniques d'interopérabilité par l'EIF, l'AFNOR et la CNIL. La promotion par la CNIL d'initiatives privées et de plateformes de data stores pour les individus.

IA et propriété intellectuelle

L'analyse de la confrontation de l'intelligence artificielle à la propriété intellectuelle est divisée en deux étapes principales, selon que la propriété intellectuelle est utilisée par l'IA en tant qu'élément d'entrée pour l'apprentissage machine (« *l'input* ») ou que l'IA est utilisée pour produire des éléments susceptibles d'être protégés par la propriété intellectuelle (« *l'output* »).

1. Au stade de l'input

Enjeux juridiques	État du droit positif	Propositions et recommandations
Reproduction sans autorisation d'œuvres protégées par un droit de	Droit d'auteur : reconnaissance d'une exception de <i>Text and data mining</i> pour des activités de	 Droit d'auteur : Reconnaître une exception Text and data mining plus large, englobant également les usages à finalités commerciales tant
propriété intellectuelle.	recherche scientifique à des fins non commerciales.	que ces finalités sont différentes des finalités initiales des droits de propriété intellectuelle.
	Droit sui generis: reconnaissance d'une exception de reprise non substantielle de la base.	Favoriser le développement des licences libres autorisant le text and data mining au niveau européen, assorties le cas échéant d'un prix d'accès global (matérialisé par exemple par une plateforme d'open data à accès payant, avec redistribution équitable aux ayants droit).
Insécurité juridique dans		Droit sui generis :
le développement des		Prévoir un système généralisé de rémunération pour accès à la
activités liées à		totalité des bases de données.

l'exploration de données,		
particulièrement au		Proposition annexe : appliquer la méthode du <i>fair use</i> pour toute
regard du droit sui		utilisation de créations protégées par des droits de propriété
generis.		littéraire et artistique.
Difficultés d'application	Protection des droits de propriété	Plus besoin de sanction si les propositions énumérées ci-dessus
des sanctions lorsque les	intellectuelle par l'action en	sont adoptées, puisque les utilisations auront été légitimées.
œuvres reprisent dans	contrefaçon et le régime qui en	Dans le cas contraire, nécessité de clarifier que le contrefacteur
l'input l'ont été	découle, notamment la saisie-	est présumé être le propriétaire des données contrefaisantes.
illicitement.	contrefaçon.	

2. Au stade de l'output

Enjeux juridiques		État du droit positif	Propositions et recommandations
	 Prolifération de créations réalisées de manière autonome par des intelligences artificielles échappant du fait de leur spécificité aux catégories actuelles du droit 	Non prise en compte de la spécificité des créations de l'IA qui ne sont donc pas intégrées	Étendre le champ d'application des règles du droit d'auteur aux créations générées par l'IA, en reconnaissant notamment le statut d'œuvres collaboratives aux <i>outputs</i> du <i>Text</i>
Droit d'auteur	d'auteur. Risque de désintéresser les concepteurs d'IA de type créatives et d'entraver l'innovation dans ce secteur alors mêmes que les potentialités de rentabilité	dans le champ des propriétés intellectuelles (protection des seules œuvres créées par une intelligence humaine et	and data mining. La ventilation de la titularité du droit devrait alors être pensée de façon casuistique, en ayant égard par exemple à l'intervention plus ou moins grande de l'utilisateur dans la sélection de l'output.

	économiques sont fortes (particulièrement	reflétant cette	OU
	dans le secteur audiovisuel et musical).	intelligence humaine).	Aménager un nouveau type de régime de
	■ Détermination de la titularité du droit d'auteur si celui-ci est accordé à l'œuvre : programmeur, propriétaire de la base de données, propriétaire des données, ou autre ?		propriété intellectuelle pour ce type de créations (plus ou moins similaire au droit d'auteur, excluant par exemple tout droit moral) afin de pouvoir les valoriser et assurer une incitation suffisante pour les investisseurs. Critère de protection objectif : la nouveauté de l'œuvre générée.
Brevet	 Génération de formules ou d'output d'une quelconque autre nature ayant les caractéristiques d'une invention valorisable sur le marché – risque de ne pas suffisamment protéger les entreprises innovantes en ce domaine. Risque inverse de concentration de la propriété industrielle entre les mains des seules entreprises capables de faire travailler des IA fortes (enjeu de concurrence). Détermination de la personne de l'inventeur (similaire à la question de la titularité en droit d'auteur, mais relative au dépôt du brevet). 	Potentielle inadaptation des critères d'accès à la protection du brevet (évaluation de l'inventive step par rapport à l'homme du métier) limitant de fait toute tentative de breveter une invention issue du travail d'une IA.	 Adapter la mise en œuvre des conditions de brevetabilité pour permettre l'appréhension de l'inventivité de la solution apportée par l'IA. Adapter la nécessité de dévoiler l'identité de l'inventeur pour permettre la déclaration de plusieurs personnes, y compris morales, ayant contribué à obtenir l'output. Tempérer les effets de concentration par l'application du droit de la concurrence actuel (position dominante, théorie des facilités essentielles).

L'intelligence artificielle confrontée à la protection des données à caractère personnel

Gabriel Lecordier

Rappels introductifs

- La donnée personnelle a une forte valeur marchande, elle est considérée comme la monnaie du XXIème siècle, comme le carburant de l'économie numérique.
- Le traitement de cette donnée personnelle s'est considérablement accru ces dernières années avec le développement d'une ère de *Big data*, ce qui permet de mieux connaître le consommateur, de prédire ses envies, d'adapter les produits etc.
- Les potentialités économiques sont énormes : le marché est estimé à 60 milliards d'euros en Europe en 2016, 80 en 2020. De manière indirecte c'est un marché de 300 milliards en 2016, estimé à 430 milliards en 2020⁴.
- L'IA s'est développée avec le développement de la vitesse et de la mémoire des processeurs informatiques et l'accès à de plus grandes bases de données : les techniques modernes d'IA (deep learning, machine learning, réseaux de neurones) reposent sur un grand jeu de données pour entrainer l'IA.
- En retour, l'IA promet d'optimiser, d'améliorer le traitement de données personnelles.
- La problématique de l'IA face à la règlementation des données personnelles est soulevée par de nombreux acteurs institutionnels⁵ ainsi que par la presse spécialisée et la plupart des parties prenantes.
- La clé du développement de l'IA est la confiance des utilisateurs, notamment dans le respect de la vie privée, de la règlementation des données à caractère personnel.
- L'utilisation de l'IA dans le traitement de données personnelles est déjà une réalité économique :

⁴ IDC, Analyse of the Future, European Data Market Smart 2013/0063 Final Report

⁵ Voir par ex: Artificial Intelligence, Robotics, Privacy and Data Protection, EDPS, october 2016; Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, Version 2.2, 09/04/2017

- Exemple de secteurs : publicité ciblée, banque et assurances (calculs de taux d'intérêts et de premiums), recrutement, assistance personnelle, développement marketing, éducation, etc.
- Exemple d'acteurs : Google, Amazon, Facebook, Apple, IBM, Microsoft,
 Alibaba, Baidu, Assos, Ebay, Amazon, Salesforce etc.
- Exemples d'IA :Siri, Watson, Alexa, Cortana, MilelQ, SwiftKey, Brennius Analytics, Albert, Einstein etc.
- Il existe une tendance à l'augmentation des traitements IA de données personnelles avec le développement des technologies de collectes (ex : Internet des Objets).

À la veille de l'entrée en vigueur du Règlement Général sur la Protection des Données (ci-après « **RGPD** »), quel est l'Impact de l'IA sur la réglementation des données personnelles ? Quels nouveaux enjeux se posent avec l'IA ? Quelles sont les possibles réponses qui peuvent être apportées ?

1. L'IA est par défaut comprise dans la réglementation existante

Champ d'application ratione materiae du Règlement : notion de traitement automatisée de données personnelles (article 2 RGPD). L'IA est par définition un traitement automatisé.

La définition du RGPD inclut donc l'utilisation de données personnelles par l'IA. Le RGPD s'applique donc à l'IA qui utiliserait des données à caractère personnel.

Par ailleurs, le règlement se veut indifférent aux technologies de traitement avec un principe de neutralité technologique du (considérant 15 RGPD).

2. Structure du rapport

La structure du raisonnement juridique en droit des données personnelles est la suivante :

- présence et qualification de données personnelles ;
- identité du responsable de traitement ;
- base légale du traitement ;
- principes de traitement des données personnelles ; et
- droits des personnes concernées.

Nous proposons de dérouler les différents enjeux juridiques de l'IA en matière de réglementation des données à caractère personnel selon cette logique, par souci de cohérence intellectuelle et juridique.

Nous nous sommes intéressés aux enjeux juridiques que posaient l'utilisation de traitements de données personnelles par des IA selon (i) leur importance et/ou (ii) leur spécificité à des traitements par des technologies d'IA.

Notre réflexion sera principalement articulée autour de la réglementation européenne qui sera d'application directe et entrera en vigueur le 25 mai 2018. La loi Informatique et Libertés est en cours de rénovation afin d'être mise en conformité avec le RGPD.

Enfin, il convient également de noter que certaines problématiques posent également des enjeux dans d'autres domaines juridiques (ex : droit de la consommation, propriété intellectuelle).

Réflexions générales

Quels sont les types de mesures pour adresser les problèmes ?

- Une typologie de mesures entre celles dites de « hard law » (loi, règlements, etc) et celles dites de « soft law » (recommandations, lignes directrices, certifications etc).
- La réglementation européenne est très récente et d'application imminente : 25 mai 2018.

L'IA est déjà intégrée à la réglementation existante.

- Il existe un degré d'incertitude technologique sur le développement de l'IA et sur ses conséquences en termes du respect de la règlementation des données à caractère personnel.
- Le manque de recul sur ces technologies induit un risque de sur-légiférer (avec le risque de pénaliser le développement technologique et économique de l'IA en France) voire de mal légiférer.⁶
- Il existe beaucoup d'outils de soft law dans le RGPD tels que la certification (article 42 RGPD), les codes de conduites (article 40 RGPD), les analyses d'impact préalables (article 35), le *privacy by design* (article 25), l'obligation de présence d'un

⁶ Voir par exemple: Law and Regulation of Artificial Intelligence and Robots: conceptual framework and normative implications. Nicolas Petit, 2017. Artificial Intelligence and Life in 2030, Report of the 2015 Study Panel, 2016.

Délégué à la Protection des Données au sein de du responsable de traitement (article 37, ci-après « **DPD** »), les règles d'entreprises contraignante (article 47).

Le principe de l'accountability est au cœur du RGPD. Celui énonce que revient à la charge des entreprises de montrer qu'elles respectent la réglementation et de trouver les solutions techniques et organisationnelles afin d'être en conformité avec le RGPD. Cela revient à un principe de l'auto-certification par l'entreprise.

Légiférer de manière spécifique, en plus de ne pas être adapté, efficace, renverserait toute la logique de l'accountability du RGPD.

- Les acteurs sont d'autant plus incités à développer des mesures de protection des données personnelles, sous peines de sanctions élevées : jusqu'à 4% du CA (article 83 RGPD).
- D'autre part, le besoin de confiance de l'IA des utilisateurs est vital pour les acteurs IA. Cette confiance ne peut être acquise que si les traitements IA de données personnelles respectent la réglementation et la vie privée des personnes concernées.
- En l'état de moyens limités de la CNIL, une certaine autorégulation du secteur est nécessaire, guidée et orientée par le régulateur.

Le rôle de la CNIL est d'aider et d'aiguiller les acteurs à respecter le RGPD.

La CNIL possède d'ailleurs de nombreux outils de soft law pour cela tels que des recommandations, la promotion de codes de conduite, des certifications et agréments d'organismes de certifications, des labels, ou bien la promotion de technologies respectueuses de la vie privée des utilisateurs etc.

Principes et obligations pour le traitement de données personnelles

1. La qualification de données personnelles et les risques de réidentification

- La définition d'une donnée personnelle est « toute information se rapportant à une personne physique identifiée ou identifiable » (article 4 RGPD).
- Pour déterminer si une personne est identifiable, il convient de prendre en compte l'ensemble des moyens raisonnablement susceptibles d'être utilisées et la présence d'informations et de données supplémentaires disponibles (considérant 26 RGPD).

- Avec le développement de la technologie on assiste à une extension de la catégorie de données à caractère personnel (ex. : adresse IP dynamique, adresse MAC etc).
- L'IA pourrait être capable d'analyser les données et de réidentifier les personnes par des procédés inconnus, en trouvant des corrélations nouvelles entre les données collectées et les données publiquement disponibles.
- La problématique de la réidentification, déjà importante avec le développement du *Big data*⁷, sera exacerbée avec le développement de l'IA.

Les enjeux juridiques sont les suivants :

- 1. Des données non personnelles collectées par l'IA pourraient in fine être requalifiées de données personnelles.
- 2. Est-il possible d'anonymiser durablement les données personnelles avec l'IA?
- 3. Des données personnelles collectées pourraient se transformer en données personnelles sensibles (ex : données de santé) avec des traitements IA.
- 1.1. Sur la potentielle évolution de qualification de données non personnelles en données personnelles
- Pour analyser si un responsable de traitement est en mesure d'identifier un individu, il convient de réaliser une étude sur les moyens raisonnablement susceptibles d'être utilisées à la disposition du responsable de traitement (article 2 loi Informatique et Libertés). Les critères suivants sont notamment utilisés : le coût objectif de l'identification, le temps nécessaire, et l'état de la technologie.
- Toutes les données permettant l'identification ne doivent pas être dans les mains d'une seule personne.8
- Par hypothèse, on ne peut qualifier de données personnelles toute donnée collectée par l'IA par défaut. Cela est non fondé juridiquement et technologiquement et préjudiciable économiquement.

⁷ Big data and Privacy. A Technological Perspective, President's Council of Advisors on Science and Technology, White House, May 2014.

⁸ CJUE, 19 octobre 2016, aff. C-582/14, pt 43.

- D'autre part, cela remettrait en cause tout l'équilibre et l'économie de la réglementation des données personnelles, qui repose sur une distinction entre données personnelles et non personnelles.
- Une obligation d'anonymisation des traitements IA nous paraît également excessive et non conforme au principe de neutralité technologique du RGPD.
- Il revient donc alors au responsable de traitement de s'assurer que les données non personnelles collectées ne puissent pas permettre d'identifier un individu.

À cette fin, nous recommandons :

- 1. Une analyse d'impact préalable sur la qualification des données collectée (si l'analyse est légalement requise) et un contrôle continu du DPD de la pertinence de la qualification des données. Cela serait possible si des moyens de privacy by design étaient mis pour tracer et identifier les données personnelles et non personnelles collectées par l'IA.
- 2. La CNIL devrait constituer un groupe de travail pour déterminer de potentielles nouvelles catégories de données personnelles, en prenant en considération l'avancement des technologies IA.
- 3. Le responsable de traitement devrait considérer l'anonymisation des données personnelles collectée. Cela permet d'éviter les obligations de traitements et in fine les sanctions.

1.2. Sur le risque de réidentification des données anonymisées

- Définition de l'anonymisation : « tout processus technique privant la ou les données d'un certain nombre d'éléments empêchant ainsi toute identification de la personne concernée par tout moyen raisonnable et probable » (considérant 26 RGPD).
- Le risque de la réidentification est accru avec l'IA : accès à plus de données, capacité de calcul et de réflexion accrues.
- Moyens de réidentification : singling out (capacité à isoler dans un groupe), inference (capacité à estimer, avec une probabilité suffisante, la valeur d'un élément

des autres valeurs du groupe d'éléments), *linkability* (capacité à déduire l'identité en effectuant des corrélations).⁹

- L'anonymisation fait sortir des obligations du RGPD (26 RGPD) mais reste la nécessité de collecter les données personnelles en premier lieu, et donc d'avoir une base légale pour cette collecte.
- Trois grandes techniques d'anonymisation ; data randomnisation (consiste à altérer la vérité des données pour supprimer les liens entre les données et l'individu) , généralisation des données (généralisation ou dilution des attributs des données par la modification de leur échelle ou de leur ordre de grandeur) et differential privacy.
- La méthode actuelle la plus au point et utilisée par les grands acteurs IA (Apple, Facebook) est le *differential privacy*: c'est une méthode d'anonymisation consistant à injecter du « bruit » dans la donnée afin de préserver l'identité de la personne, les spécificités de la donnée tout en permettant d'extraire des informations générales utiles.
- Quelles techniques d'anonymisation marchent? Le test est le suivant : l'anonymisation est effective si la réidentification n'est pas possible en utilisant des moyens raisonnables et probables.
- L'anonymisation est une obligation de moyen renforcé et non de résultat : on prend en compte l'état de la technologie, le coût, le savoir-faire, la présence d'autres données ouvertes au public (open data).
- L'IA pourrait également constituer un nouvel outil d'anonymisation. Une IA récente de Google Brain a permis de créer des algorithmes de machine learning dont la performance sur des tests de reconnaissance d'image était meilleure que la performance d'algorithmes créés par des humains.¹⁰

À cette fin nous recommandons :

1. L'élaboration d'un code de conduite CNIL sur l'anonymisation sur l'exemple des lignes directrices du Groupe de Travail de l'Article 29, et

⁹ Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party, April 2014, p11.

https://research.googleblog.com/2017/11/automl-for-large-scale-image.html

- du code de conduite sur l'anonymisation de l'Information Commissioner's Office¹¹.
- 2. Un audit périodique des techniques d'anonymisation par le DPD pour s'assurer de la fiabilité des techniques d'anonymisation¹².
- 3. La CNIL devrait promouvoir des mécanismes de label, de certification des processus d'anonymisation conformément à l'article 60 de la Loi pour une République Numérique (aussi article 11 (g) loi n°78-17).
- 4. Le développement d'IA permettant d'anonymiser les données de manière évolutive.

1.3. Sur la transformation de données personnelles en données personnelles sensibles

- Les données sensibles ou catégories particulières de données sont notamment les données de santé, les données révélant l'orientation sexuelle, les opinions politiques etc. (article 9 RGPD).
- Le traitement de ces données est par principe interdit, sauf à disposer d'une base légale (dix bases légales dont le consentement explicite de la personne concernée).
- L'IA pourrait conduire à transformer des données en données sensibles par sa capacité accrue de corrélation et de profilage (exemple de l'IA de Facebook en mesure de détecter des tendances suicidaires chez les utilisateurs, cette IA sera mise en place partout dans le monde, sauf dans l'Union Européenne).
- Le responsable de traitement utilisant une IA qui sur la base de données personnelles pourrait inférer des données sensibles¹³ (exemple d'opinions politiques sur la base de Likes Facebook) devrait trouver une nouvelle base légale pour ce traitement.

À cette fin, nous recommandons une analyse d'impact préalable sur l'évaluation du risque de transformation des données collectée en

¹¹ Anonymisation, managing data protection risk, code of practice; Information Commissioner's Office, 2012.

¹² Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party, April 2014, p24.

¹³ Slave to the algorithm? Why «a right to an explanation» is probably not the remedy you are looking for, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017, p14.

données sensibles (si l'analyse est légalement requise) et à minima un contrôle continu du DPD de ce risque.

2. L'identité du responsable de traitement

- Le responsable du traitement est la personne physique ou morale qui seul ou conjointement détermine les finalités et les moyens du traitement (article 4 (7) RGPD).
- Le sous-traitant est la personne physique ou morale qui traite des données personnelles pour le compte du responsable de traitement (article 4 (8) RGPD).
- La qualification juridique des différents acteurs prenant part au traitement est importante car, bien que le RGPD ait étendu les obligations des sous-traitants, la majorité des obligations du RGPD sont à la charge du responsable de traitement.
- Il convient ici de faire la distinction entre des IA générales (exemple des personal et virtual assistants) et des IA spécialisées (aide au recrutement, IA marketing etc).
- Les IA générales telles que des *virtual assistants* (exemple de Microsoft Cortana, Apple Siri, ou Amazon Alexa) ont des finalités très larges telles que l'amélioration de la vie de l'utilisateur, ou l'aide à l'utilisateur. Dans le cadre de ces finalités générales, en pratique c'est bien l'utilisateur qui détermine l'usage et la véritable finalité de l'IA.
- D'autre part, avec le développement de l'IA, se développe une industrie de traitement d'IA as a service (en référence au software as a service). Tel serait par exemple le cas d'une entreprise demandant à un développeur d'IA de traiter ses données clients pour augmenter ses ventes.
- Avec l'IA, le problème est que la conception du modèle et des paramètres de l'IA peuvent très vite devenir, par les choix du programmateur, une détermination des moyens voire des finalités du traitement.

Les enjeux juridiques sont les suivants :

- 1. Quel serait le statut d'un développeur lA traitant des données personnelles pour le compte d'un client ?
- 2. Quel serait le statut d'un utilisateur d'une IA générale aux fins générales ?

2.1. Responsable de traitement/fournisseur de services de traitement IA

- Dans l'exemple précité, la structure générale du RGPD tendrait à identifier le fournisseur et développeur d'IA comme le sous-traitant et le client comme le responsable de traitement.
- Par analogie, la CNIL et le Groupe de Travail de l'Article 29 avait déjà identifié une potentielle confusion similaire des statuts pour les fournisseurs de services cloud et SaaS (software as a service)¹⁴. La CNIL indiquait que dans certains cas (PaaS et SaaS publics) les clients ne pouvaient pas donner d'instructions et n'étaient pas en mesure de contrôler l'effectivité des garanties de sécurité et de confidentialité apportées par le prestataire. Cette absence d'instructions et de moyens de contrôle était due à des offres standardisées non modifiables par le client. Dans ces conditions, le prestataire de service pouvait être considéré comme co-responsable du traitement. Le Groupe de Travail de l'Article 29 considérait la même chose en déclarant que dans certaines situations, où notamment le niveau d'instruction et l'expertise sont du côté du fournisseur de service, ou encore le contrôle est in fine celui du fournisseur, le fournisseur de service pouvait devenir co-responsable ou responsable à part entière s'il traitait des données pour ses propres finalités.
- Un fournisseur d'IA pourrait donc potentiellement être qualifié de coresponsable de traitement s'il fournit un service suivant une offre standardisée laissant guère de moyens de contrôle et d'instructions au client.
- Une particularité avec l'IA serait de considérer l'amélioration du modèle de l'IA comme une finalité intrinsèque au traitement. En effet, plus le modèle d'IA traite de données, plus il devient efficace. En ce sens, le fournisseur de l'IA pourrait devenir responsable de traitement à part entière. Cependant, cette perspective nous paraît trop radicale en ce sens qu'elle imposerait *ab initio* un statut juridique trop contraignant pour des développeurs d'IA pouvant agir comme de simples sous-traitants.
- Dans son avis sur le responsable de traitement, le Groupe de Travail de l'Article 29 énonce que l'étude de la détermination des finalités et des moyens est une analyse *in concreto*¹⁵. Concernant les moyens, le responsable de traitement peut déléguer des questions techniques ou d'organisation.

¹⁴ Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, CNIL, 2012 ; Opinion 05/2012 on Cloud Computing, Article 29 Data Protection Working Party, 2012.

¹⁵ Avis 1/2010 sur les notions de « responsable de traitement » et de « sous-traitant », Groupe de Travail « Article 29 » sur la Protection des Données, 2010.

- Cette délégation trouve sa limite si elle consiste en une détermination des moyens essentiels par le sous-traitant, alors le fournisseur de l'IA devient coresponsable de traitement.
- Des exemples de moyens essentiels du traitement sont la catégorie de données à traiter, la durée de conservation des données, l'identité des personnes ayant accès aux données etc.
- Pour une IA où le fournisseur de services choisirait le data set de l'IA, ce dernier serait co-responsable de traitement.
- Ce critère des moyens essentiels semble être un bon critère car il donne de la souplesse et de la liberté au fournisseur d'IA pour s'occuper des questions purement techniques et d'organisation. D'autre part, les moyens essentiels renvoient aux obligations fondamentales de la réglementation des données personnelles devant être respectées, ce qui rendrait logique le changement de statut du fournisseur si ce dernier venait à les définir.
- La CNIL devrait établir des lignes directrices, une recommandation sur l'identification des moyens essentiels dans un souci de sécurité juridique dans les relations entre fournisseurs d'IA et clients, et entre ces derniers et les personnes concernées.
- Nous recommandons également la rédaction dans des contrats entre fournisseur d'IA et client professionnelle, des clauses identifant les finalités du traitement et l'identité de la partie les déterminant, l'identification et la détermination des moyens essentiels du traitement. Le contrat devrait également préciser que l'amélioration de l'IA par les données recueillies ne constitue pas une finalité du traitement.

Nous recommandons:

- Le fournisseur de service IA devrait évaluer ex ante le degré de standardisation de l'offre de services et les moyens de contrôle et d'instructions accordés au client afin de déterminer son statut et de mettre en œuvre ses possibles obligations de responsable de traitement.
- 2. La rédaction de lignes directrices ou d'une recommandation sur l'identification des moyens essentiels de traitement pour un souci de

- sécurité juridique dans les relations entre fournisseurs d'IA et clients, et entre ces derniers et les personnes concernées.
- 3. La rédaction dans des contrats entre fournisseur d'IA et client, de clauses identifant les finalités du traitement et l'identité de la partie les déterminant, l'identification et la détermination des moyens essentiels du traitement.
- 4. Le contrat devrait également préciser que l'amélioration de l'IA par les données recueillies ne constitue pas une finalité du traitement.

2.2. Statut d'un utilisateur d'une IA générale

- À titre d'exemple d'une lA générale, comme un assistant virtuel, l'IA Cortana permet des fonctions de design, de rappel, de calendrier etc.
- L'utilisateur décide de l'utilisation de l'outil pour son assistance.
- Dans ce cas précis, Microsoft se définit clairement comme le responsable de traitement dans la *privacy notice* de Cortana.
- Dans le cas d'espèce, la détermination des moyens est bien celle de Microsoft qui programme Cortana, la détermination des finalités est de manière générale celle de Microsoft, de manière plus spécifique celle de l'utilisateur. En l'espèce, Microsoft programme cependant les fonctionnalités de Cortana dans un ensemble fini. Ainsi, Cortana ne peut être utilisée pour coder un logiciel ou effectuer une reconnaissance faciale d'individus. Cortana ne peut être utilisée que pour des fonctions bien prédéfinies.
- D'autre part, l'article 2 de la loi Informatiques et Libertés précise que le responsable de traitement ne peut être la personne concernée par le traitement. Dès lors, la question du statut de l'utilisateur ne pourrait se poser que si l'assistant virtuel permet le traitement de données personnelles d'autres personnes. C'est le cas dès lors que l'IA traite les coordonnées d'un contact par exemple. Précisons tout de même, qu'il n'existe aucune opportunité pour le régulateur ou pour le responsable de traitement, fournisseur de l'IA, à remettre en cause le statut de l'utilisateur pour de tels traitements...
- Il nous semble, que malgré une volonté de responsabiliser l'utilisateur, dans la mesure où le fournisseur d'IA détermine des finalités générales, dans un ensemble de finalités prédéfinies, ainsi que les moyens du traitement, que l'utilisateur ne peut être en l'état un co-responsable de traitement, ou un sous-traitant. À partir du moment où les finalités de l'IA deviennent si générales, qu'elles permettent un traitement de

données personnelles dont les finalités sont définies par l'utilisateur, le statut de l'utilisateur pourrait être remis en cause. Cependant, il n'existe pas en l'état de telles technologies d'IA.

Le responsable de traitement doit alors bien délimiter les finalités de son IA.

Nous recommandons donc une définition claire des finalités des développeurs d'IA dite à des finalités générales, dans un ensemble fini de finalités.

3. La base légale du traitement

- Un traitement « classique » de données personnelles (pas de données sensibles, pas de décision individuelle automatisée) doit être licite et disposer d'une base légale (article 6 RGPD).
- Ces bases légales sont au nombre de six :
 - 1. consentement,
 - 2. obligation légale,
 - 3. exécution d'un contrat ou mesures précontractuelles,
 - 4. intérêts légitimes,
 - 5. mission d'intérêt public, ou
 - 6. sauvegarde des intérêts vitaux.
- L'article 22 du RGPD semble donner une base légale restreinte pour des décisions individuelles automatisées produisant des effets juridiques ou affectant la personne concernée manière significative, sans intervention humaine. ¹⁶ Certaines IA pourraient entrer dans le champ de cet article (ex : IA de *credit scoring*, de recrutement d'employés).
- La base légale de ce type d'IA serait une des suivantes :
 - consentement explicite,
 - exécution du contrat, ou

¹⁶ Guidelines on Automated Individual-decision making and Profiling for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 2017, p12. A noter cependant que cette interprétation d'une base légale restreinte n'est pas évidente à la lecture de l'article 22 RGPD.

autorisation par le droit de l'UE ou d'un Etat membre. 0

Les enjeux juridiques sont les suivants :

- 1. Quelles sont les possibilités pour le responsable de traitement de déroger à la base légale du consentement explicite pour ces traitements IA?
- 2. Comment les responsables de traitement doivent-ils faire pour respecter cette contrainte accrue de licéité?

3.1. Sur les possibilités de déroger au consentement

- Le consentement explicite constitue-t-il la base légale privilégiée ? Le consentement est seulement troisième dans la liste des bases légales.
- Selon le Groupe de Travail de l'article 29, le consentement explicite est la base légale privilégiée.¹⁷ Considérant le risque d'atteinte à la vie privée, le consentement explicite est la base légale qui donne le plus de contrôle à la personne concernée.
- Les possibilités de déroger au consentement sont interprétées de manière stricte par le Groupe de l'article 29, conformément à un avis rendu précédemment. 18
- Pour se prévaloir de la base légale d'exécution d'un contrat : la décision individuelle automatisée ne doit pas constituer une éventualité mais être indispensable à son exécution. 19
- Cas d'espèce : dans le cadre d'un contrat d'assurance ou de prêt, l'utilisation d'une IA entrant dans le champ de l'article 22 n'est pas absolument nécessaire, on peut toujours procéder à d'autres méthodes. La méthode peut cependant être jugée plus efficace.
- Cette interprétation paraît pertinente car (1) le RGPD vise à redonner plus de contrôle aux utilisateurs, (2) Le consentement explicite est la base légale la plus protectrice pour les personnes concernées et (3) les personnes concernées doivent

¹⁷ Guidelines on Automated Individual-decision making and Profiling for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 2017, p13.

¹⁸ Avis n°15/2011, Groupe de l'article 29, 2011, p8.

¹⁹ Guidelines on Automated Individual-decision making and Profiling for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 2017, p13. Voir également : CNIL, délib. n° 2013-420, 3 janv. 2014.

être à *fortiori* plus protégées face des traitements de décisions individuelles automatisées ayant des effets significatifs sur eux.

■ Faudrait-il que le législateur instaure une dérogation à l'obligation de consentement explicite, par autorisation législative? Une telle dérogation semblerait prématurée et nous ne disposons pas assez de recul sur ces types d'IA (par exemple sur la présence de biais), sur leurs avantages économiques et leurs potentiels atteintes aux droits des utilisateurs.

Nous recommandons que :

- 1. Le responsable de traitement d'une IA entrant dans le champ d'application de l'article 22 RGPD utilise la base légale du consentement explicite pour son traitement.
- 2. La CNIL adopte des lignes directrices sur les possibilités de déroger au consentement explicite dans un souci de sécurité juridique.
- 3. La CNIL constitue un groupe de travail sur l'opportunité d'autoriser par dérogation législative certains types d'IA entrant dans le champ d'application de l'article 22, eu égard à leurs avantages économiques et leurs atteintes à la vie privée.

3.2. Sur les critères du consentement explicite

- La base légale du consentement explicite n'est pas définie dans le RGPD (bien que mentionnée aux articles 9 et 49).
- La définition et l'interprétation du consentement explicite au sens de la Directive 95/46 ne sauraient être retenues en l'état, en raison de l'évolution de la définition du consentement « simple » du RGPD, bien plus exigeante que celle de la Directive.
- Le RGPD définit à l'article 4 (11) le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement. »
- L'article 7 précise que le consentement devrait être présentée sous une forme distincte, compréhensible, accessible, formulé en des termes simples et clairs et pouvant être retiré à tout moment.

- Le Groupe de l'Article 29 semble, en l'attente de lignes directrices sur le sujet, affirmer que le consentement explicite est un consentement qui doit être confirmée par une déclaration positive, plutôt que par une autre action positive. Cette proposition nous semble peu claire et sécurisante pour le responsable de traitement et les personnes concernées.
- Le consentement explicite dans le cadre de l'article 22 devrait aussi se comprendre, selon nous, d'un consentement informé conformément au devoir d'information des articles 13(f) et 14(g) RGPD.

Nous recommandons que :

- 1. Les lignes directrices européennes décrivent précisément les conditions et les modalités de recueil d'un consentement explicite au sens de l'article 22 RGPD.
- 2. Le responsable de traitement soit dans l'obligation de demander à la personne concernée une déclaration positive de consentement et fournir une information conforme aux articles 13(f) et 14(g) RGPD portant sur le droit à l'information sur les décisions individuelles automatisées ayant des effets juridiques ou équivalents sur la personne concernée, sans intervention humaine.

4. Privacy by design et by default

- Le *privacy by design* est l'ensemble de mesures techniques et organisationnelles mises en place par le responsable du traitement pour respecter les obligations du traitement (minimisation, finalités déterminées, traitement juste et loyal etc) et les droits des utilisateurs (droit d'opposition, droit à l'effacement etc) afin d'être en conformité avec le RGPD (RGPD article 25).
- Seulement, l'IA est un programme évolutif et apprenant ce qui nécessite de réévaluer périodiquement l'ensemble des mesures techniques et organisationnelles mises en place.
- Ce problème sera exacerbé avec la perspective d'IA dont l'apprentissage est de moins en moins supervisé.

L'enjeu juridique est donc de déterminer comment apprécier le principe du *privacy* by design avec des traitements IA apprenants et évolutifs ?

- Pour tout traitement de données personnelles, le principe de *privacy by design* ne s'entend pas seulement d'une protection uniquement au stade de la conception, mais aussi tout au long du traitement (article 25 RGPD).
- Un bon ensembles de stratégies de *privacy by design* devrait ainsi chercher le plus possible à minimiser les données, cacher les données personnelles et leurs corrélations, compartimenter les différentes données collectées, agréger les données, informer adéquatement les personnes concernées, permettre le contrôle des personnes concernées sur leurs données, mettre en place des règles d'entreprise contraignantes afin de garantir les obligations de traitement et les droits des personnes concernées et enfin à documenter ces stratégies pour démontrer la conformité du traitement.²⁰
- Ces stratégies devraient être modulées selon les différentes étapes du traitement des données par l'IA : c'est-à-dire la collecte, l'analyse, le stockage ou l'utilisation des données.
 - Exemples de mesures techniques et organisationnelles de privacy by design : anonymisation, cryptage, sécurité et responsabilité, transparence et accès, consentement, propriété et contrôle.
- Les traitements IA à l'heure actuelle ne requièrent pas d'adopter des stratégies de *privacy by design* spécifiques mais (i) d'adopter des mesures techniques spécifiques aux enjeux de l'IA et (ii) de mettre plus souvent à jour ces stratégies de *privacy by design* pour s'assurer de leur effectivité.
- Sur ce deuxième point, ces mises à jour pourraient prendre la forme d'audits périodiques internes ou externes (par des cabinets d'audit, des organes techniques) dont la périodicité et l'intensité varieraient selon la complexité et les risques du traitement par l'IA.
- Ce serait le rôle de la CNIL de déterminer l'intensité, les modalités et la périodicité des audits des mesures de *privacy by design*. Ces audits pourraient prendre la forme d'une certification, d'un label. Cette certification des mesures de *privacy by design* de l'IA pourrait porter sur des mesures techniques, des exigences d'input et d'output, des tests de conformité.
- Une certification pourrait être rendue obligatoire pour certains traitements IA sensibles (selon par exemple: l'obligation d'une analyse d'impact préalable, les

 $^{^{20}}$ Privacy by design in Big data, An overview of privacy enhancing technologies in the era of Big data analytics, ENISA, 2015, p22.

catégories de données traitées, le volume de personnes concernées) déterminés par la CNIL. *A minima*, pour les traitements IA ne présentant *ab initio* pas de risques particuliers, l'élaboration de codes de conduites et/ou de lignes directrices devrait s'avérer suffisants.

Nous recommandons:

- 1. La promotion de code de conduites, de labels et/ou l'élaboration de lignes directrices par la CNIL sur les meilleures pratiques techniques et organisationnelles de *privacy by design*.
- 2. Une obligation de certification par la CNIL pour certains traitements d'IA déterminés (selon par exemple : l'obligation d'une analyse d'impact préalable, les catégories de données traitées, le nombre de personnes concernées).

5. Finalités de traitement déterminées, explicites et légitimes et traitements ultérieurs compatibles

- Le responsable de traitement doit traiter les données personnelles pour des finalités déterminée, explicites et légitimes, et ultérieures non incompatibles (article 5(b) RGPD).
- La logique de l'IA, du *Big data* est contraire au principe des finalités déterminées : on collecte d'abord les données, puis on détermine les finalités en fonction des liens, des corrélations trouvées entre les données. Le fondement de l'IA et du *Big data* est de trouver de nouvelles finalités aux données collectées²¹.
- Pour certains, le principe même de finalités déterminées est incompatible avec le *Big data*²², et l'IA à fortiori.
- Une IA est un programme évolutif qui peut découvrir de nouvelles informations, de nouvelles corrélations et servir de nouvelles finalités in fine.
- En l'état actuel de la technologie, il semble peu probable qu'une IA programmée pour une finalité déterminée, soit en mesure de changer elle-même sa programmation.

²¹ Slave to the algorithm? Why «a right to an explanation» is probably not the remedy you are looking for, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017, p11.

²² Voir par exemple : *Notice and Consent in a World of Big data*, Fred Cate, Victor Mayer-Schönberger, International Data Privacy Law, 2013; *Homo Juridicus est-il soluble dans les données*?, Antoinette Rouvroy, 2017.

- Cependant, l'IA pourrait inférer de nouvelles corrélations, interprétations sur les données collectée.
 - Exemple : une IA d'aide à l'éducation à l'enfant pourrait collecter des données sur l'utilisateur indiquant la présence d'une pathologie (ex : troubles de l'attention) pour le responsable de traitement qui analyserait les données à postériori. Le traitement de cette finalité ultérieure est-il possible ?
- Le Superviseur Européen de Protection des Données s'inquiète notamment des IA de *natural language processing*, qui pourraient éroder le principe des finalités déterminées.²³
- Il convient aussi de faire la distinction entre des IA à apprentissage supervisé et non supervisé : dans le premier cas, l'output de l'IA est contrôlé, dans le second, c'est l'IA elle-même qui déterminera les corrélations dans le data set. La question des finalités déterminées est exacerbées par les IA à l'apprentissage non-supervisé.
- Les finalités doivent aussi être légitimes selon l'article 5 du RGPD.
- En raison des capacités de l'IA, certaines d'entre elles ont été utilisées pour des motifs pouvant être qualifiés d'illégitimes (exemples d'IA reconnaissant des orientations sexuelles, ou d'une IA reconnaissant des tendances suicidaires).

Les enjeux juridiques sont les suivants :

- 1. Dans quelles mesures le responsable de traitement d'une IA pourrait traiter des données pour des finalités ultérieures permises par l'IA?
- 2. Comment apprécier la légitimité des traitements de données par l'IA?

5.1. Les finalités déterminées et ultérieures

- Un responsable de traitement ne peut traiter des données pour des finalités ultérieures que si (i) elles sont compatibles ou (ii) si elles sont incompatibles, le responsable de traitement obtient le consentement de la personne concernée, ou est autorisé par le droit d'un État membre ou de l'Union (considérant 50 RGPD).
- Le test de compatibilité est soit un examen formel où le responsable de traitement doit regarder les finalités déterminées données aux personnes concernées

²³ Artificial Intelligence, Robotics, Privacy and Data Protection, EDPS, october 2016, p9.

et examiner si les finalités ultérieures sont comprises implicitement ou explicitement dedans, soit un véritable examen substantiel des nouvelles finalités, où le responsable de traitement regarde la relation entre les finalités initiales et ultérieures en prenant en considération le contexte de la collecte des données, les attentes raisonnables des personnes concernées concernant un traitement ultérieur, la nature de la donnée personnelle et l'impact du traitement ultérieur sur la personne concernée, ainsi que la mise en place de garanties (considérant 50 RGPD).

- Cet examen se fait in concreto.
- Le responsable de traitement aidé de son DPD doit différencier les scénarii d'incompatibilité *prima facie* et de doute.
- L'exemple d'une IA d'aide éducative qui permettrait le traitement de données de santé est *prima facie* une finalité ultérieure non compatible.
- Le responsable de traitement doit prévoir l'information de la personne concernée en cas de traitement de données pour des finalités ultérieures compatibles, et prévoir la possibilité pour la personne de mettre fin (opt-out) au traitement (considérant 61 RGPD).
- Du fait de cette obligation légale, des mécanismes internes notamment par des règles d'entreprise contraignante approuvées par la CNIL, de vérification de compatibilité des finalités ultérieures semblent suffisants en l'état avec notamment une mission permanente du DPD de mener des tests de compatibilité avec de potentielles nouvelles finalités.
- Pour des traitements IA sensibles, soumis à une obligation d'une analyse d'impact préalable, la CNIL devrait imposer au responsable de traitement de prévoir, dans la mesure du raisonnable, les possibilités de nouvelles finalités permises par l'IA.

Nous recommandons:

- La mise en place de mécanismes internes notamment par des règles d'entreprise contraignante approuvées par la CNIL, de vérification de compatibilité des finalités ultérieures avec notamment une mission permanente du DPD de mener des tests de compatibilité avec de potentielles nouvelles finalités.
- 2. Pour des traitements IA sensibles, soumis à une obligation d'une analyse d'impact, la CNIL devrait imposer au responsable de traitement

de prévoir, dans la mesure du raisonnable, les possibilités de nouvelles finalités permises par l'IA.

5.2. Légitimité des traitements

- Cette condition de traitement est très difficile à juger : le traitement doit non seulement respecter le principe de licéité (principe d'une base légale) mais également respecter les lois en vigueur dans d'autres domaines, ainsi que des normes éthiques et codes de conduite²⁴. Cette condition de traitement est donc extrêmement large.
- Si le respect des principes légaux est objectif, les considérations éthiques sont plus subjectives.
- La CNIL devrait donc promouvoir la rédaction de codes éthiques sectoriels sur les finalités des traitements, et/ou la rédaction de chartes éthiques de traitement chez les responsables de traitement.

Nous recommandons donc la promotion par la CNIL de codes éthiques sectoriels sur la légitimité des finalités des traitements, et/ou de chartes éthiques de traitement chez les responsables de traitement.

6. Principe de minimisation

Les données collectées doivent être adéquates, pertinentes et nécessaires au traitement (articles 5 et 25 RGPD).

- Cependant avec l'IA et les *Big data*, il existe un principe de collecte permanente et totale des données personnelles²⁵. C'est le principe du *data mining* qui est un procédé de collecte de données de différentes catégories, perspectives afin d'en tirer de nouvelles informations, ce qui nécessite des jeux très larges de données.
- Le principe de minimisation est déjà une gageure : 72% des responsables de traitement collectent des données qu'ils n'utilisent pas.²⁶

²⁴ Opinion 03/2013 on Purpose Limitation, Article 29 Data Protection Working Party, 2013, p20.

²⁵ Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, Version 2.2, 09/04/2017 p11.

²⁶ Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, Version 2.2, 09/04/2017 p40.

• Le bon fonctionnement d'un réseau de neurones d'une IA repose sur la quantité du data set initial pour entrainer l'IA.

On relève donc deux problématiques juridiques :

- 1. Comment est-il possible pour un responsable de traitement et pour le régulateur d'assurer l'effectivité du principe de minimisation ?
- 2. L'entraînement de l'IA constitue-t-il sa propre finalité, justifiant de déroger au principe de minimisation ?
- 6.1. Sur l'effectivité du principe de minimisation.
- Le caractère adéquat, pertinent et nécessaire de la collecte de données personnelles s'apprécie au regard des finalités du traitement, qui doivent être déterminées, explicites et légitimes (article 5 (b) RGPD).
- Les critères du principe de minimisation posent un véritable problème d'appréciation en pratique.
 - Exemple d'une IA de publicité ciblée : le but de la publicité ciblée est d'être la plus personnalisée pour son destinataire, ce qui justifie le traitement de nombreuses données personnelles.
 - Illustration de données personnelles pouvant être collectées par une IA d'application fitness: données de localisation, rythme cardiaque, taille, poids, âge, condition physique générale, historique de blessures, rythmes de sommeil. Cependant le traitement de tous les antécédents médicaux, des données de localisation en dehors des temps d'exercice ne seront pas considérées comme adéquates, pertinentes et limitées au nécessaire.
- L'appréciation de ce critère se fait donc in concreto.

Nous recommandons:

1. Au préalable du traitement, les responsables de traitement devraient préciser clairement les finalités du traitement pour déterminer la pertinence des données collectées et la proportionnalité de cette

- collecte, en définissant clairement les données dont ils auront besoin et en délimitant celles dont ils n'auront pas besoin.
- 2. Pour certains traitements sensibles (données de santé par exemple), une obligation de certification par la CNIL du principe de minimisation ou par un organisme agréé pourraît être imposée.
- 3. La CNIL promeuve des codes de conduites sectoriels dans certains secteurs clés (voiture autonome) selon un principe de *comply or explain*.
- 4. Les responsables de traitement devraient privilégier les solutions techniques d'anonymisation et autres solutions techniques innovantes (exemple de la simulation de fausses données par la start-up SNIPS).

6.2. Sur l'autojustification de la collecte de données par l'IA

- Un tel principe est en complète contradiction avec le principe de minimisation. La majorité des IA reposant aujourd'hui sur des mécanismes d'apprentissage profond (reconnaissance d'images, compréhension du langage humain), cela créerait de facto une exemption au principe de minimisation pour ces technologies IA.
- Une dérogation à ce principe pourrait étudiée, en considération de l'atteinte aux droits des personnes concernées, pour des IA à des fins de recherche scientifique et non commerciales.

Nous recommandons:

- 1. La création d'une exemption du principe de minimisation du traitement de données faite par des IA à des fins de recherches scientifiques et non commerciales, sous réserve du bon respect des autres obligations de traitement et des droits des personnes concernées.
- 2. A minima, un avis de la CNIL sur la portée du principe de minimisation pour les IA d'apprentissage profond.

7. Principe d'un traitement juste et loyal et d'exactitude des données

• L'article 5 du RGPD impose un traitement licite, loyal et transparent des données personnelles de la personne concernée. Le même article instaure un principe d'exactitude des données personnelles et l'article 18, sur la base de l'inexactitude des

données, donne un droit à la limitation du traitement au bénéfice de la personne concernée. Enfin l'article 9 du RGPD interdit par défaut le traitement de certaines catégories de données (par exemple l'orientation sexuelle, l'origine raciale ou ethnique).

- Le législateur européen note dans le RGPD les possibilités de discrimination résultant de traitements de données personnelles et notamment de méthodes de profilage (considérant 71 RGPD).
- Cet ensemble de dispositions proscrit tout traitement de données personnelles qui s'avérerait discriminatoire pour la personne concernée.
- Cette problématique n'est pas récente en droit des données personnelles²⁷ et n'est également pas spécifique à ce droit.
- La question de la discrimination du traitement est accentuée avec l'IA car celleci malgré des promesses d'objectivités, souffre de biais²⁸, qui peuvent être très difficiles à identifier. Avec le machine learning et le deep learning, les critères de décision de l'IA deviennent ainsi de plus en plus opaques.
- Des exemples d'IA discriminantes (produisant directement des discriminations ou permettant des discriminations) sont légions²⁹.

L'enjeu juridique est donc de déterminer comment le responsable de traitement peut s'assurer que son traitement IA ne souffre pas de biais discriminants ?

■ Il existe plusieurs manières pour une IA de souffrir de biais et d'être potentiellement source de discriminations. L'IA peut adopter un comportement discriminatoire sur la base de données d'apprentissage biaisées (exemple de l'IA reconnaissant des personnelles homosexuelles, sur la base de photos prises sur des sites de rencontre). Le biais peut également apparaître dans l'environnement où évolue l'IA (exemple du *chatbot* Tay de Microsoft ayant écrit des messages racistes, antisémites et complotistes sur Twitter). L'IA peut aussi discriminer en raison de

²⁷ Voir par exemple Mesure de la diversité et protection des données personnelles : les dix recommandations de la CNIL, CNIL, 2007.

https://www.technologyreview.com/s/608248/biased-algorithms-are-everywhere-and-no-one-seems-to-care/, accédé le 12 décembre 2017.

²⁹ A titre d'exemple: pour l'IA COMPAS évaluant aux Etats-Unis les probabilités de récidive https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm, accédé le 12 décembre 2017; ou encore une IA reconnaissant une orientation sexuelle par reconnaissance faciale, Deep neural networks can detect sexual orientation from faces, Yilun Wang, Michal Kosinski, American Psychological Association, 2017.

forces structurelles extérieures en raison d'objectifs conflictuels.³⁰ D'autres types de biais existent tels que des biais de similitude (exemple de recherches Google associées aux habitudes, mots clés des utilisateurs) ou des biais dits émergents (exemple du fil d'actualité Facebook qui se remplit en fonction des activités des amis de l'utilisateur).

- Comme indiqué précédemment, il est très difficile d'expliquer les mécanismes de certains types d'IA. Cependant, de bonnes pratiques existent pour analyser l'IA et détecter des biais dans son modèle.
- Une première catégorie de solutions envisagée est la transparence des algorithmes. Celle-ci est définie par l'Electronic Privacy Information Center comme le fait pour des entités qui traite des données personnelles d'indiquer les données traitées, leurs provenances, les moyens de traitement, les personnes y ayant accès, les finalités et dans un contexte *Big data*, le fait de rendre public l'algorithme utilisé³¹. La publicité de l'algorithme, bien que pouvant être encouragée, ne peut devenir le standard de lutte contre les biais pour des raisons évidentes d'atteinte aux droits des propriétaires de l'algorithme. Ce dernier pourrait cependant être envisagé pour des algorithmes utilisés par les pouvoirs publics.
- L'Association for Computing Machinery propose sept grands principes pour éviter les biais dans l'IA: l'attention aux biais des parties prenantes et notamment des développeurs, la promotion par les régulateurs de mécanismes permettant aux personnes concernées de questionner et contester l'IA (déjà de droit dans le RGPD), un principe de responsabilité des responsables de traitement pour des traitements discriminatoires, la promotion de mesures d'explicabilité de l'IA, un travail sur les données input, un principe d'auditabilité, et enfin des processus de validation et de tests.
- L'IA pourrait elle-même constituer la solution à son propre problème avec la création d'IA de contrôle.³²
- Le responsable de traitement pourrait également faire appel à des tiers de confiance, des consultants extérieurs pour détecter les biais de son modèle, ou en interne constituer des équipes consacrées à ces questions (exemple du programme GlassBox chez Google destiné à construire des modèles d'IA moins opaques).

³⁰ Voir Algorithmic Bias ? An empirical study into apparent gender-based discrimination in the display of STEM career ads, A. Lambrecht, C. Tucker, 2017.

³¹ Comments of the Electronic Privacy Information Center to the Office of Science and Technology Policy, Electronic Privacy Information Center, 2014.

³² A smart approach: counteract the bias in Artificial Intelligence, Giovanni Buttarelli, European Data Protection Supervisor, 2017.

Nous recommandons:

- 1. L'élaboration d'une nouvelle recommandation de la CNIL sur les bonnes pratiques de détection et de correction de biais dans des modèles IA.
- 2. L'analyse par le responsable de traitement des données input et limiter au maximum l'utilisation de données pouvant être sources de discrimination.
- 3. La mise en place de mesures d'auditabilité des algorithmes, et l'appel à des tiers de confiance, à des consultants extérieurs.
- 4. Des processus de tests et validations au niveau de l'output des traitements IA.
- 5. Un partage d'informations entre les responsables de traitements, et entre ces derniers et avec les personnes concernées.
- 6. Le recours à des outils novateurs, des IA, explicatifs et analysant les biais des modèles.

8. Profilage et décision individuelle automatisée

- Le profilage est tout traitement de données permettant d'évaluer certains aspects personnels relatifs à une personne physique (article 4 RGPD).
- Une décision individuelle automatisée est une décision fondée exclusivement sur un traitement automatisé produisant des effets juridiques ou des effets significatifs équivalents sur la personne concernée par le traitement (RGPD considérant 71, article 22).
- Ces deux types de traitement sont différents mais peuvent se recouper en pratique.
- Exemple d'une IA de calcul de *credit scoring*. Elle est à la fois une décision individuelle automatisée ainsi qu'un profilage.
- Le RGPD prévoit une obligation d'information renforcée des personnes concernées pour ces types de traitement (articles 13(f), 14(g) RGPD) entrant dans le champ de l'article 22 RGPD et étant qualifiés de décisions individuelles automatisées.
- Cette obligation renforcée entre directement en opposition avec l'une des plus grandes caractéristiques des traitements IA et du machine learning : le manque

d'explicabilité. A l'heure actuelle, les développeurs d'IA ne sont guère en mesure d'expliquer le raisonnement de leur programme, le chemin de l'input du modèle vers l'output.³³ Ce constat technologique remet en cause ce droit renforcé à l'information, que certains interprètent comme un droit à l'explication.³⁴

• L'article 22 (3) RGPD prévoit également un droit pour la personne concernée de contester la décision du traitement et d'obtenir une intervention humaine dans le processus de décision.

Les enjeux juridiques sont les suivants :

- 1. Comment comprendre « fondée exclusivement sur un traitement automatisé » pour définir le champ d'application de l'article 22 RGPD ?
- 2. Quelle est la portée du droit à l'information de la personne concernée concernant les traitements IA entrant dans le champ de l'article 22 RGPD ?
- 3. Comment résoudre le problème de l'explicabilité de l'IA?

8.1. Sur l'absence d'intervention humaine dans la décision

- En l'état, il serait très difficile de trouver des traitements IA qui ne demandent aucune intervention humaine dans la prise de décision.
- Le Groupe de Travail de l'Article 29 adopte une approche pragmatique de la question. Le critère de l'absence humaine ne saurait être pris littéralement et un traitement IA entre dans le champ d'application de l'article 22 RGPD si l'intervention humaine n'est pas significative et n'est pas l'œuvre d'une personne ayant la possibilité de changer la décision du traitement IA.³⁵
- Le critère de la faculté de changer la décision nous paraît bien plus approprié, car plus objectif, que celui vague, d'intervention significative.
- À titre d'exemple : un employé de banque qui n'aurait pas le pouvoir de changer un *credit score* ou un refus/acceptation d'une demande de crédit basé sur une décision

³³ Voir par exemple: https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/, accédé le 11 décembre 2017.

³⁴ Voir par exemple: *Robotics and artificial intelligence, Fifth report of Session 2016-17*, House of Commons, Science and Technology Comittee.

³⁵ Guidelines on Automated decision-making and profiling for the purposes of the Regulation 2016/679, Article 29 Data Protection Working Party, 2017, p10.

individuelle automatisée, aurait pour conséquence de faire entrer le traitement dans le champ de l'article 22.

- Le responsable de traitement devrait donc examiner le pouvoir de ses employés en présence de décisions individuelles automatisées.
- La CNIL devrait publier des lignes directrices plus précises sur le degré de nonintervention nécessaire pour l'application de l'article 22 RGPD, étant donné la courte explication sur le sujet du Groupe de Travail de l'Article 29.³⁶

Nous recommandons:

- 1. La mise en place d'audits internes des responsables de traitement afin de déterminer le pouvoir de détermination et le degré significatif d'actions de ses employés travaillant sur la base de décisions individuelles automatisées.
- 2. La publication de lignes directrices par la CNIL pour clarifier le degré d'intervention humaine concernant le champ d'application de l'article 22 RGPD.

8.2. Obligation d'information

- Le droit à l'information pour les traitements de l'article 22 RGPD est défini par le RGPD comme « les informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée » (article 14 (g) RGPD).
- Le Groupe de Travail de l'Article 29 reconnaît le degré de complexité de l'obligation d'information pour les modèles de machine learning et ne recommande pas une explication complexe ou bien la publication du code source du modèle. L'information doit être simple mais également porteuse de sens pour la personne concernée. Pour le Groupe de Travail, le responsable de traitement doit fournir les éléments, les critères, sur lesquels la prise de décision par l'IA repose.
- Application à un cas d'espèce : pour une demande de prêt, le responsable de traitement devrait indiquer les critères utilisées (données financières, historiques de paiement, situation professionnelle) et l'origine des données (questionnaires remplies

³⁶ Voir notamment la consultation de l'ICO à ce sujet : https://ico.org.uk/media/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf; accédé le 11 décembre 2017.

par l'appliquant, données publiques, données fournies par un tiers). Le responsable de traitement devrait également expliquer comment sont interprétées ces données et donc leur importance et leurs conséquences sur la prise de décision (exemple : des historiques de retards de paiement augmentent la probabilité de rejet de la demande).

- On pourrait reprocher la généralité de cette obligation d'information,³⁷ cependant l'alternative (publication du code source de l'IA et des mécanismes spécifiques de raisonnement de l'IA) n'est pas envisageable car elle porterait une grave atteinte aux droits du responsable de traitement (des droits de propriété intellectuelle,³⁸ voir même des droits constitutionnellement garantis) et serait inintelligible pour l'utilisateur.³⁹
- L'obligation d'information n'est pas une obligation d'explication de l'IA, qui n'est légalement pas requise, techniquement indigeste et fonctionnellement inutile.⁴⁰
- La fonctionnalité du droit à l'information de la personne concernée est d'informer la personne. L'objectif est de faire connaître à l'utilisateur sous un format clair et simple l'existence et le fonctionnement d'une décision individuelle automatisée pour qu'il puisse y consentir de manière éclairée ou s'y opposer et exercer ses différents droits (contestation, intervention humaine) quant à la décision, sur la base des critères et de la méthodologie utilisée dans la décision.
- L'information ne devrait donc pas être centrée sur l'algorithme de décision, mais sur la personne concernée (subject-centered model).
- Le responsable de traitement devrait alors favoriser un format d'information interactif avec des contenus visuels, des icônes, des simulations de décisions concernant la personne concernée sur la base de différents critères etc.⁴¹

³⁹ Voir en ce sens l'article L211-1 du code de la consommation et le concept de « transparency fallacy » évoqué dans *Slave to the algorithm ? Why «a right to an explanation» is probably not the remedy you are looking for*, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017.

³⁷ A comparer avec le degré d'information recommandé par la CNIL dans sa délibération n°2017-023 du 16 février 2017 portant avis sur un projet de décret relatif aux modalités de communication des règles et caractéristiques des traitements algorithmiques.

³⁸ Voir en ce sens le considérant 63 du RGPD et l'article 39-1-5 de la Loi Informatiques et Libertés.

⁴⁰ Voir en ce sens *Why a right to explanation to automated decision-making does not exist in the General Data Protection Regulation*, S. Watcher, Brent Mittelstadt, Luciano Floridi, Oxford Internet Institute, 2017, *Slave to the algorithm? Why «a right to an explanation» is probably not the remedy you are looking for*, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017.

⁴¹ Guidelines on Automated decision-making and profiling for the purposes of the Regulation 2016/679, Article 29 Data Protection Working Party, 2017; Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, Version 2.2, 09/04/2017 p88.

• Par ailleurs, un modèle d'information centré sur l'utilisateur semble empiriquement plus approprié.⁴²

Nous recommandons:

- Une approche fonctionnaliste par le responsable du traitement de son devoir d'information, centré sur la personne concerné et utilisant par exemple un format d'information interactif avec des contenus visuels, des icônes, des simulations de décisions concernant la personne concernée sur la base de différents critères etc.
- 2. L'élaboration de lignes directrices de la CNIL sur le contenu exact des types d'informations à communiquer aux personnes concernées.

8.3. Explicabilité de l'IA

- S'il ne faut pas confondre droit à l'information et droit à l'explication dans le cadre du droit à l'information préalable de la personne concernée, le problème de l'explicabilité de l'IA demeure in fine avec le droit de contestation d'une décision individuelle automatisée avec l'article 22 (3) RGPD.
- Avec ce droit de contestation, le responsable de traitement devrait être en mesure d'expliquer plus en détails au contestataire le fonctionnement de l'IA dans son cas précis, sauf à vider le droit de contestation de sa substance. En effet dans l'hypothèse inverse, le responsable de traitement pourrait se contenter de redonner l'information donnée en premier lieu. La personne concernée doit être en mesure de pouvoir connaître le fonctionnement précis de l'IA sur son cas.
- L'incidence de ce droit à la contestation sur le degré d'information à donner à l'utilisateur concernée n'est pas claire. Cependant, l'article 15 (h) sur le droit d'accès, qui s'exerce après le traitement, mentionne la même obligation d'information que les articles 13(f) et 14(g).
- Il est également préférable pour les responsables de traitement de pouvoir expliquer leurs IA ou du moins de prouver leur bon fonctionnement notamment pour se prémunir de poursuites judiciaires (pour discrimination notamment).

⁴² Dianne C Berry and Donald E Broadbent, *Explanation and verbalization in a computer-assisted search task*, 39 THE QUARTERLY JOURNAL OF EXPERIMENTAL PSYCHOLOGY SECTION A 4, 585-609 (1987).

- Malgré de réelles difficultés, l'explicabilité de l'IA est un sujet de recherche en plein essor⁴³ et certaines méthodes existent telles que le *decompositional explanation*, les *model agnostic systems*, ou encore le *natural language generation*.⁴⁴
- Au-delà de méthodes spécifiques, un ensemble de bonnes pratiques peut être adopté afin d'expliquer l'IA ou du moins de s'assurer de son bon fonctionnement : analyse des données (input), étude des faux positifs et faux négatifs, sensibilisation des développeurs et data scientists, création d'IA explicatives, tests de résultats etc.
- Cet ensemble de bonnes pratiques correspond au principe plus général d'auditabilité des algorithmes. ⁴⁵ Ce principe veut qu'à chaque stade de développement de l'IA, le programme soit conçu pour permettre à des tiers de surveiller, revoir et critiquer le comportement et fonctionnement du modèle.
- Le principe d'auditabilité des algorithmes se développe avec notamment l'apparition d'entreprises d'audit des algorithmes.⁴⁶
- Une autre option est le recours à des techniques d'IA moins opaques, alternatives aux IA d'apprentissage profond qui sont les plus difficiles à expliquer. Ces méthodes alternatives pourraient être des réseaux bayésiens ou des modèles de machine learning peu profonds, à l'instar de l'algorithme Prometea développé en Argentine pour aider à la prise de décision en matière de fiscalité.⁴⁷ Il convient de noter toutefois, que les IA de deep learning sont les plus efficaces à ce jour.

Nous recommandons:

- 1. La mise en place par le responsable de traitement de mesures d'auditabilité des modèles d'IA et d'un ensemble de bonnes pratiques favorisant l'explicabilité de l'IA (travail sur les données input, création d'IA explicatives etc).
- 2. La création d'équipes techniques au sein de la CNIL, ayant les capacités techniques pour appréhender la problématique de l'explicabilité de l'IA.

⁴³ Voir par exemple : How the machine « thinks » : Understanding opacity in machine learning algorithms, Jenna Burrell, *Big data* & Society, 2016.

⁴⁴ Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, Version 2.2, 09/04/2017

⁴⁵ Diakopoulos, Nicholas and Friedler, Sorelle. *How to Hold Algorithms Accountable*. MIT Technology Review. 17 November 2016.

⁴⁶ A titre d'exemple : la société ORCAA http://www.oneilrisk.com/, accédé le 11 décembre 2017.

⁴⁷ https://innovacionyderecho.com.ar/prometea/

3. L'élaboration par la CNIL, en partenariat avec les entreprises, les institutions spécialisées (INRIA), d'un projet de réflexion sur les méthodes techniques d'auditabilité de l'IA.

Droits des personnes concernées

1. Droit à la portabilité

- La portabilité est un nouveau droit instauré par le RGPD (article 20 RGPD). La portabilité est le droit pour la personne concernée d'obtenir du responsable de traitement les données personnelles transmises, si (i) le traitement est automatisé et (ii) si le traitement est basé sur le consentement ou l'exécution d'un contrat.
- Le droit à la portabilité est légèrement différent dans la Loi pour une République Numérique (article 48 et codifié à l'article L. 224-42-1 et suivants du code de la consommation). Ce droit a un champ d'application plus large, étendu à tous les consommateurs.
- Ce droit à la portabilité a été considéré plus comme un outil anti-monopole visant à contester la domination des entreprises américaines du numérique⁴⁸ qu'un droit pour l'utilisateur.
- Ce droit sera d'autant plus important avec des traitements IA, qui nécessitent un jeu de donnée initial très grand, constituant une barrière à l'entrée au développement de l'IA.

Les enjeux juridiques sont les suivants :

- 1. Quel est le champ d'application des données à restituer à la personne concernée pour le droit à la portabilité ?
- 2. Comment assurer l'effectivité de ce droit anti-monopole ?

⁴⁸ Slave to the algorithm? Why «a right to an explanation» is probably not the remedy you are looking for, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017, p38; Guidelines on the right to data portability, Article 29 Data Protection Working Party, 2017.

1.1. Champ d'application des données

- Le Groupe de l'Article 29 énonce que les données à transmettre par le responsable de traitement sont les données personnelles concernant le sujet, et les données fournies par le sujet. ⁴⁹ La première condition vise à exclure les données anonymisées, qui ne concernent plus la personne concernée. La deuxième condition doit être entendue au sens large et représente les données fournies consciemment par la personne concernée (exemple d'un formulaire) et les donnée fournies par le sujet en conséquence de son utilisation du service, de l'appareil (données de trafic, géolocalisation, historique de recherche, données de connexion).
- Le droit à la portabilité s'arrête cependant aux données inférées et/ou crées par le responsable de traitement, selon le Groupe de l'Article 29.
- À titre d'exemple, des données inférées seraient des analyses issues d'un traitement de l'individu, des données créées par le responsable de traitement sur la base des données couvertes par le droit à la portabilité (note d'un *credit scoring*, probabilité de défaut, risque de santé).
- Cette restriction est à notre sens bienvenue pour une raison d'incitation économique. Ce type de données créé par une IA constitue la véritable source de revenus du responsable de traitement et la véritable plus-value du traitement et les méthodes de traitement seraient aussi susceptibles d'être protégées par des droits de propriété intellectuelle.
- Cette restriction nous semble aussi justifiée d'un point de vue de l'interprétation de l'économie générale du RGPD qui (i) ne vise pas à donner un droit de propriété sur les données personnelles, ce qui pourrait dès lors s'étendre aux données dérivées, mais bien un pouvoir de contrôle, et (ii) cherche à concilier les intérêts économiques d'une économie de données et les droits des personnes concernées.
- Cette distinction entre données couvertes par le droit à la portabilité, et celles non couvertes, bien que nécessaire, pourrait amener des difficultés de mise en pratique dans l'exercice de ce droit.
- Par ailleurs, le droit à la portabilité n'existant que pour des traitements basés sur le consentement, le responsable de traitement de l'IA et le sous-traitant le cas échéant, devraient être en mesure de pouvoir distinguer et rattacher les différentes données à leurs différentes bases légales, ainsi qu'à la qualité des différentes données, dans leur propre intérêt.

⁴⁹ Guidelines on the right to data portability, Article 29 Data Protection Working Party, 2017.

À cet égard, bien que subordonné dans sa mise en œuvre aux conditions du droit à la portabilité du RGPD (art L. 224-42-2 du Code de la consommation), la rédaction du droit à la portabilité énoncé à l'article L. 224-42-1 souffre d'ambiguïtés et d'incohérence, notamment en raison de l'expression « en toutes circonstances ».

Nous recommandons:

- 1. La mise en place chez le responsable de traitement et le sous-traitant le cas échéant, de mesures techniques et organisationnelles, afin de différencier les données couvertes par le droit à la portabilité (données fournies directement et indirectement par le sujet sur la base du consentement) et celles non couvertes par ce droit (notamment celles portant atteintes aux droits des tiers).
- 2. Une révision de l'article L224-42-1 du Code de la consommation et notamment de la mention « en toutes circonstances » pour mise en conformité avec le RGPD.

1.2. Droit anti-monopole

- La puissance de l'IA dépend à la fois des algorithmes de machine learning/deep learning mais aussi et surtout de la quantité et de la qualité des données. C'est pour cette raison que beaucoup d'IA développées sont en open source car leur valeur réside plus dans l'accès aux données que dans le modèle algorithmique.
- Le RGPD énonce que les données transmises devraient l'être sous un format structuré, couramment utilisé et lisible par machine (article 20 (1) RGPD). Le considérant 68 précise la notion d'interopérabilité pour le format des données transmises à l'utilisateur et/ou à un autre responsable de traitement.
- L'interopérabilité est cependant une obligation de moyens et non de résultat. Le responsable de traitement ne peut toutefois mettre en place de barrières à la portabilité (article 20 (1) RGPD).
- Les responsables de traitement devraient donc définir entre eux des standards d'interopérabilité pour être en conformité avec le RGPD et garantir le bon exercice de ce droit.
- Au niveau européen, l'EIF (European Interoperability Framework), et au niveau français, l'AFNOR et la CNIL pourrait développer des standards techniques

d'interopérabilité sur la base notamment de formats couramment utilisées (XML, JSON, CSV etc).

La CNIL devrait également encourager des initiatives de plateformes de stockage des données pour les individus, sous formes de data stores, leur donnant plus de contrôle sur les données fournies et permettant de mettre en œuvre plus facilement le droit à la portabilité. À titre d'exemple, le projet Mes Infos (http://mesinfos.fing.org) et notamment son projet Rainbow Button concernant le droit à la portabilité.

Nous recommandons:

- 1. L'élaboration de standards d'interopérabilité par l'industrie afin de garantir l'effectivité du droit à la portabilité.
- 2. La proposition de standards techniques d'interopérabilité par l'EIF, l'AFNOR et la CNIL.
- 3. La promotion par la CNIL d'initiatives privées et de plateformes de data stores pour les individus.

2. Droit à l'effacement

- Le droit à l'effacement est consacré avec le RGPD à l'article 17, après avoir été créé par la jurisprudence européenne.⁵⁰
- La mise en œuvre de ce droit est d'autant plus difficile avec des traitements IA et notamment des IA d'apprentissage profond.
- Les méthodes de deep learning et de machine learning jettent un doute sur les possibilités techniques de même retrouver la donnée personnelle traitée, de sorte qu'il serait très difficile d'effacer la donnée personnelle du modèle⁵¹.
- Un autre problème spécifique à l'IA et notamment aux réseaux de neurones, est que la donnée personnelle input aurait beau être effacée que l'IA aura appris de cet

⁵⁰ A noter cependant que le droit au déréférencement consacré par l'arrêt Costeja c. Google Spain, diffère du droit à l'effacement du RGPD; sur ce point voir par exemple: Le « droit à l'oubli », de Monsieur Gonzales au GDPR, Adrien Aulas, Aeon, 2017.

⁵¹ Slave to the algorithm? Why «a right to an explanation» is probably not the remedy you are looking for, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017, p37, note 179.

input. Est-il alors possible de faire oublier cet apprentissage? Le droit à l'effacement couvre-t-il cet apprentissage?

D'autre part, il semblerait également possible, dans le cadre de modèles de machine learning, de remonter par reverse engineering (en partant de l'output du modèle de l'IA) à la donnée personnelle effacée.⁵²

Les enjeux juridiques sont les suivants :

- 1. Quel est le champ d'application du droit à l'effacement dans le cadre d'un traitement IA entre les données fournies et l'apprentissage de ces données par ľIA?
- 2. Le droit à l'oubli justifie-t-il de paralyser l'IA?
- 3. Comment assurer l'effectivité du droit à l'effacement et notamment du risque de reverse-engineering?

2.1. Champ d'application du droit à l'effacement

- Sur la distinction entre les données personnelles transmises (input) et l'apprentissage de l'IA basé sur ces données (output), on peut raisonner par hypothèse. Cet apprentissage est soit hors champ du RGPD car l'apprentissage ne constitue pas une donnée personnelle (exemple d'un assistant virtuel qui a appris de l'utilisateur pour améliorer ses fonctions de langage) soit l'apprentissage est une donnée inférée, dérivée et constitue potentiellement une donnée personnelle⁵³.
- Il convient de noter qu'un cas existe où les données inférées sont inférées de multiples données personnelles de différents individus. La question clé est alors bien celle de la qualification de donnée personnelle de cette donnée inférée.
 - Dans le premier cas, le droit à l'effacement ne devrait pas s'appliquer car le droit à l'effacement ne concerne que des données à caractère personnel.
 - Dans le deuxième cas : en principe le droit à l'effacement devrait 0 s'appliquer. Ces données inférées sont potentiellement plus

53 Voir notamment Slave to the algorithm? Why «a right to an explanation» is probably not the remedy you are looking for, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017, p35.

⁵² Gary M. Weiss, Mining with Rare Cases, in DATA MINING AND KNOWLEDGE DISCOVERY HANDBOOK,

^{747-757 (}Oded Maimon and Lior Rokach eds., Springer, 2009).

attentatoires à la vie privée des personnes concernées que des données personnelles fournies en input à l'IA (comme peut être illustrée la différence entre un numéro de téléphone et une évaluation basée sur un profilage). La finalité de ce droit est bien de supprimer ce genre de données inférées et non les données brutes fournies.

• On note une différence avec le droit à la portabilité qui ne couvre pas les données inférées.

Nous proposons:

- 1. L'élaboration des lignes directrices par la CNIL sur l'étendue du droit à l'oubli dans des traitements IA sur la question des données inférées.
- 2. La mise en place par le responsable de traitement de mesures de privacy by design afin de retracer les données personnelles du modèles d'IA et les données inférées de ces précédentes données.

2.2. Droit à l'effacement et paralysie de l'IA

- Sur la base d'une IA qui serait paralysé par un tel droit, on peut distinguer plusieurs situations. Dans la première situation, l'IA est seulement basée sur les données personnelles d'un utilisateur (exemple d'assistants personnels virtuels). Dans le deuxième cas, l'IA repose sur les données personnelles de plusieurs personnes.
 - Dans le premier cas, le droit à l'oubli justifie aisément de paralyser l'IA car l'IA n'a d'autres fonctions que de servir la personne concernée.
 - Dans le second cas, la paralysie de l'IA pourrait légitimement constituer une dérogation au droit à l'effacement. L'article 17.1(c) permet une dérogation au droit à l'effacement s'il existe un motif légitime impérieux au traitement. Le bon fonctionnement de l'IA pourrait-il être qualifié de motif légitime impérieux? Une IA peut représenter un actif économique considérable, parfois le seul pour des petites entreprises. Une analyse in concreto aurait alors besoin d'être menée afin de déterminer (i) si l'IA est vraiment paralysée par le droit à l'effacement demandé et dans quelle proportion, (ii) le coût pour le responsable de traitement de cette paralysie, (iii) le coût pour les autres utilisateurs de l'IA, (iv) le risque pour la personne demandant l'oubli de voir ses données conservées et enfin (v) l'existence de safe guards.

• La CNIL devrait donc établir des lignes directrices sur les possibles tensions entre l'exercice du droit à l'oubli et la paralysie des traitements IA.

Nous proposons donc l'élaboration de lignes directrices de la CNIL sur les modalités de l'exercice d'un droit à l'oubli susceptible de paralyser des traitements IA de données personnelles qui concilient l'impératif de respect de la vie privé, les intérêts des autres utilisateurs de l'IA et ceux du responsable de traitement.

2.3. Risque de reverse engineering

- Ce risque, dû aux particularités des différents modèles de machine learning, est aujourd'hui tout à fait plausible.⁵⁴
- A titre d'exemple, une expérience a montré la possibilité de récupération de données génétiques de patients dans un modèle médical de machine learning. 55
- Étant donné la nature hautement technique du problème, la CNIL devrait en coopération avec l'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI), engager une réflexion sur ces risques, afin d'identifier et de promouvoir de bonnes pratiques.

Nous proposons donc une réflexion de la CNIL en coopération avec l'ANSSI sur l'identification des risques de reverse engineering et la définition de bonnes pratiques techniques pour prévenir ces risques.

⁵⁵ M. Fredrikson, E. Lantz, S. Jha, S. Lin, D. Page, and T. Ristenpart. *Privacy in pharmacogenetics: An end-to-end case study of personalized warfarin dosing*, USENIX Security Symposium, pages 17–32, 201.

⁵⁴ Voir par exemple *Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures,* Matt Fredrickson, Somesh Jha, Thomas Ristenpart, CCS, 2016; *Adversarial Machine Learning*, Ling Huang, Anthony D. Joseph, Blaine Nelson, Benjamin I.P. Rubinstein, J.D. Tygar, 4th ACM Workshop on Artificial Intelligence and Security, 2011.

L'intelligence artificielle confrontée à la propriété intellectuelle

Félicité Bernard

Rappels introductifs

- Compte tenu du fonctionnement de l'intelligence artificielle moderne, en grande partie basée sur l'apprentissage machine (machine learning et deep learning, notamment), le big data est d'une importance primordiale pour le développement de l'IA. La notion de big data renvoie directement à l'idée de base de données.
- En propriété intellectuelle, la notion de base de données renvoie principalement à deux notions : le droit *sui generis* sur les bases de données et l'exception de *text and data mining* (« **TDM** ») au droit d'auteur.
- La base de données est définie en droit européen par l'article 1.2 de la directive du 11 mars 1996 (la « **Directive Bases de Données** » ⁵⁶) comme étant « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière ».
- Nature des données : tous les contenus numériques peuvent potentiellement faire l'objet d'une exploration de données, et notamment l'écrit, la musique, les images, animées ou non, les données, sous forme ou non de bases de données.
- Classification des données selon leur accessibilité : on peut distinguer les données selon leur mode d'accès⁵⁷ :
 - o data accessible librement sur le web (web data),
 - data créée par le public et partagée sur des réseaux sociaux (social network data),
 - data créée par un organisme et dont l'utilisation est limitée par contrat (contractual data), et
 - data dont l'utilisation est strictement encadrée et protégée (confidential data).

⁵⁶ Directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données.

⁵⁷ Study on the legal framework of text and data mining (TDM), by Jean-Paul Triaille, De Wolf & Partners, March 2014 – **Rapport De Wolf**.

- Relativement aux données publiques, il existe aujourd'hui de nombreuses initiatives tendant à promouvoir une politique d'open data, et notamment le régime des données publiques, régi par le chapitre II de la Loi du 17 juillet 1978, la directive 2013/37/UE relative aux informations du secteur public et la Loi pour une République numérique du 7 octobre 2016.
 - Exemple : le catalogue Joconde qui regroupe près de 500 000 notices d'objets de toute nature (archéologie, beaux-arts, ethnologie, histoire, sciences et techniques) ou encore l'initiative de la Bibliothèque nationale de France qui depuis le 1er janvier 2014 met à disposition plus de 12 millions de notices bibliographiques et 2,5 millions de notices d'autorité pour tout type de réutilisation sous licence ouverte de l'État.
 - O Mise en pratique: « Il faut préciser que l'« open data » implique une ouverture de données pour toute réutilisation y compris commerciale mais cela ne signifie pas qu'il faille s'affranchir d'un encadrement contractuel rigoureux. En effet, tout acte de réutilisation de données publiques culturelles doit faire l'objet d'un contrat de licence » 58.
- Noter également l'existence de licences relatives au libre accès. « Le « libre accès » permet la mise à disposition en ligne des articles scientifiques afin de favoriser la circulation du savoir. Dès lors, il est notamment possible de lire, télécharger, copier, transmettre, imprimer les contenus sans barrière financière, légale ou technique »⁵⁹. L'exemple le plus courant de licence de libre accès est la licence Creative Commons⁶⁰. À noter cependant que 3 licences sur les 6 licences Creative Commons disponibles ne permettent pas l'exploitation commerciale, ce qui réduit pour notre cas l'intérêt de cet usage.

Exposé du contexte en droit de la propriété intellectuelle et des problématiques afférentes

L'analyse de la confrontation de l'intelligence artificielle à la propriété intellectuelle est divisée en deux étapes principales, selon que la propriété intellectuelle est utilisée par l'IA en tant qu'élément d'entrée pour l'apprentissage machine (« **l'input** », l'usage de

⁵⁸ Mission sur l'exploration de données du Conseil supérieur de la propriété littéraire et artistique, mission présidée par Jean Martin et rapportée par Liliane de Carvalho, juillet 2014 – **Rapport CSPLA**.

⁵⁹ Rapport CSPLA, ibid.

⁶⁰ http://creativecommons.fr/

données par l'IA) ou que l'IA est utilisée pour produire des éléments susceptibles d'être protégés par la propriété intellectuelle (« *l'output* », le rendu ou création finale de l'IA).

- Au stade de l'input : les droits de propriété intellectuelle peuvent devenir de véritables barrières au développement de l'IA, laquelle nécessite pour son développement la licéité de l'exploration de données.
 - Risque de sanctions pour des IA utilisant sans autorisation des œuvres protégées par un droit de propriété intellectuelle sous format numérique.
 - Pour ne pas tomber sur cet écueil, l'exploration de données doit être limitée aux œuvres en libre accès (le plus fréquemment parce que ces œuvres sont tombées dans le domaine public), restreignant d'autant la pertinence des résultats de l'IA.
 - L'exploration de données a été présentée en 2001 par le Massachussetts Institute of Technology comme l'une des dix technologies émergentes qui « changeront le monde au 21e siècle »⁶¹.
- Au stade de l'output : multiplication de créations de l'IA qui constituent actuellement des terres d'innovations et d'investissement exponentiel.
 - Ex.: DeepMind, la filiale de Google, a par exemple doté le Royal Free Hospital de Londres d'une application d'intelligence artificielle baptisée Streams, qui contrôle les paramètres vitaux de patients risquant un empoisonnement du sang (sepsis) et des infections rénales. Ce système est capable de prévoir - bien avant tout incident qui mettrait leur vie en danger - quand ils ont besoin d'être soumis à un traitement.
 - Ex.: la chanteuse Taryn Southern a créé le premier album de musique entièrement coécrit avec une intelligence artificielle, celle-ci s'occupant de la production et de la piste instrumentale, tandis que la chanteuse a écrit et chanté les paroles⁶².

⁶¹ Data mining et statistique décisionnelle – l'intelligence des données, Stéphane Tuffery, Editions Technip 2012.

⁶² « Intelligence artificielle : un robot compose un album, doit-on lui verser ses droits d'auteurs ? », Les Inrockuptibles, 24/08/17

Au stade de l'input : l'IA, utilisatrice illicite de données couvertes par des droits de propriété intellectuelle ?

1. État des lieux des enjeux et solutions actuels

1.1. L'input de données à une IA : l'exploration de données

Les contenus transmis à l'IA peuvent être de tous types (l'écrit, la musique, les images, animées ou non, les données) et constitués en bases de données ou non. Les contenus sont donc susceptibles de contenir des œuvres protégées par le droit d'auteur, des dessins et modèles, des marques, des brevets et être assemblés en bases de données protégées par le droit sui generis. Il convient de noter que les titres des œuvres protégées par le droit d'auteur sont tout autant protégeables que les œuvres en ellesmêmes.

1.1.1. Explicitation du lien entre IA, données et propriété intellectuelle

Le fonctionnement de l'IA repose aujourd'hui sur l'usage d'un vaste volume de données de diverses sources et de différentes natures. Les données sont le préalable indispensable à toute IA, influant directement sur l'efficacité et la pertinence du rendu (l'output) final de l'IA.

1.1.2. Point vocabulaire

L'exploration de données est définie par le rapport du CSPLA comme « un processus de recherche automatisé qui porte sur un ensemble de données numériques dans le but de découvrir de nouvelles connaissances ou de nouvelles idées. »⁶³

- **Processus de recherche automatisé**: automatisation par l'utilisation d'outils informatiques et d'algorithmes pour l'exploration de données différentes, de sources diverses et pouvant relever de statuts juridiques distincts.
- Quels sont les actes en cause lors d'une opération d'extraction de données ? Le processus de recherche automatisé implique de nombreux actes tels que l'extraction, la copie, le tri, la comparaison, le classement, la suppression,

⁶³ Rapport CSPLA, ibid.

l'interprétation des données différentes, de sources diverses et pouvant relever de statuts juridiques distincts.

L'équivalent de l'exploration de données en anglais est le « text mining ». Les terminologies sont variables : on peut aussi bien parler de « data mining » que de « text and data mining », qui apparaissent comme des sous-ensembles d'un concept plus général qui serait « l'analyse de données » (« data analysis «). L'analyse de données est définie comme « le traitement automatisé de contenus numériques, qui peuvent inclure des textes, des données, des sons, des images ou d'autres éléments, ou une combinaison de ceux-ci, afin de découvrir de nouvelles connaissances ou des idées » selon le rapport « Study on the legal framework of text and data mining (TDM) » remis en mars 2014.⁶⁴

Ci-après, les notions d'exploration de données et de « *text and data mining* » seront utilisées indistinctement et référencées sous le sigle « *TDM* ».

1.1.3. Objectifs et fonctionnement du TDM

- L'objectif du TDM est d'explorer et analyser de grands volumes de données (textes, statistiques, mesures, métadonnées, etc.) afin d'en extraire des informations significatives (corrélations, structures, etc.) par des traitements automatiques (algorithmes).
- La principale technique de TDM est la technique « *ELT* » pour « *Extract, Transform & Load* ». La technique ELT repose sur les étapes suivantes :
 - i. Définition des objectifs ;
 - ii. Inventaire des contenus numériques utiles (recenser les sources utiles, fiables, licites);
 - iii. Collecte des contenus numériques (implique une copie au moins temporaire de tout ou partie des contenus numériques);
 - iv. Préparation des données (transformation éventuelle des données afin que ces dernières soient exploitables);
 - v. Traitement des données (application des outils informatiques et des algorithmes mettant en œuvre diverses techniques : mathématiques, la linguistiques, la visualisation);

⁶⁴ Rapport De Wolf, ibid.

- vi. Résultat de l'exploration des données, qui aboutit généralement à la production de nouvelles connaissances, ne contenant pas les données extraites dans la plupart des cas.
- L'utilité du TDM varie selon les acteurs qui y recourent :
 - O Pour la recherche scientifique : sélectionner plus rapidement la littérature scientifique utile pour un sujet. Ex : le projet Text2genome qui a permis de cartographier le génome humain en compilant automatiquement trois millions de publications a souvent été très souvent cité en exemple.
 - Pour la presse, l'activité de veille média est grandement enrichie par la possibilité de fournir une information utile, triée, contextualisée pourrait tirer de grands profits du développement de l'activité d'exploration de données.
 - Pour les entreprises commerciales, il s'agit d'un levier économique potentiel à explorer, dont l'aspect marketing. Ex : M6 publicité a présenté aux membres du comité de pilotage un outil de « data mining » permettant d'évaluer et d'améliorer les performances publicitaires. Par ailleurs, selon certaines informations, l'exploration de données permettrait à Amazon de réaliser 20% de son chiffre d'affaires.
 - Pour les services du Ministère des Finances et Comptes publics, après une délibération de la CNIL, se sont également dotés d'un outil de « data mining » pour lutter contre la fraude fiscale.
 - Pour les bibliothèques, le développement de l'exploration de données constitue un enjeu considérable dans la mesure où elles sont productrices et détentrices de données.⁶⁵

1.1.4. <u>Problématique double posée par le TDM</u>

■ Pour les ayants droit : l'activité d'exploration de données se développe sur la création et l'investissement d'autrui (base de données) et l'utilisation d'œuvres éventuellement protégées par le droit d'auteur — il y a donc atteinte par l'IA de ces droits de propriété intellectuelle (ci-après les « *DPI* »), qui, du point de vue d'un ayant droit, doit être sanctionnée.

⁶⁵ Exemples tirés de *Journal Article Mining*, Eefke Smit and Maurits van der Graaf, Publishing Research Consortium, May 2011.

• Pour les développeurs et propriétaires d'IA: les développeurs et propriétaires d'IA ont besoin d'une autorisation pour l'usage de bases de données car cet usage est potentiellement illicite lorsque les données utilisées par l'IA sont couvertes par un DPI. L'exploration de données impose, pour les fouiller, d'en prendre possession et de les stocker, et donc de porter atteinte aux DPI.

1.2. Confrontation aux principaux droits de propriété intellectuelle

1.2.1. L'absence d'atteinte aux droits de propriété industrielle

- Concernant le droit des brevets: l'atteinte au droit de brevet est constituée quand il y a acte de contrefaçon, c'est à dire au terme de l'article L. 613-3 du Code de la propriété intellectuelle, « la fabrication, l'offre, la mise dans le commerce, l'utilisation, l'importation, l'exportation, le transbordement ou la détention aux fins précitées du produit objet du brevet (...) du produit obtenu directement par le procédé objet du brevet ». L'objet du brevet est délimité par des revendications qui délimitent le champ de protection. Dans le cas du text and data mining il n'est pas porté d'atteinte à l'objet du droit des brevets en lui-même mais aux caractéristiques qui le composent. Le brevet protège l'invention en tant que création permettant une application industrielle, et sanctionne les atteintes à cette fonction industrielle du droit. Il ne devrait donc pas y avoir contrefaçon de brevet si des données relatives à un brevet sont utilisées comme input d'une IA, l'objet de la protection ne portant pas sur le titre en lui-même mais sur l'objet du titre.
- Concernant le dessin et modèle : le raisonnement est similaire à celui développé pour le brevet. L'article L. 513-4 du Code de la propriété intellectuelle dispose en effet que sont interdits « la fabrication, l'offre, la mise sur le marché, l'importation, l'exportation, le transbordement, l'utilisation, ou la détention à ces fins, d'un produit incorporant le dessin ou modèle ». Une action sur le dessin et modèle en luimême, en tant que donnée, n'est donc pas une atteinte au droit et ne constitue pas une contrefaçon.
- Concernant le droit des marques : l'atteinte au droit des marques est constituée si plusieurs conditions sont réunies, dont celle de l'atteinte à la fonction essentielle de la marque (garantie d'origine du produit et exclusivité dans la spécialité). Or l'IA n'opère pas sur le même terrain que la marque et l'utilisation d'une marque est prise en tant que donnée et non en vertu d'une de ses fonctions essentielles que l'IA chercherait à détourner. On peut donc écarte d'emblée la possibilité d'atteinte à un droit de marque par l'utilisation d'une marque comme *input* d'une IA.

1.2.2. Le risque d'atteinte au droit d'auteur

S'il n'y a pas de risque de contrefaçon de marque ou de brevet au stade de l'*input*, il est probable que de nombreuses données fournies à l'IA comme *input* seront protégées par le droit d'auteur. Il convient donc d'étudier les droits patrimoniaux et le droit moral que confère le droit d'auteur pour déterminer les risques de contrefaçon de droit d'auteur. Cette recherche est nécessaire car l'exception de TDM introduite par la Loi pour une République numérique n'est applicable qu'aux explorations réalisées à des fins de recherche, et excluent donc toute utilisation commerciale de l'IA ainsi entrainée. 66

1.2.2.1. Droits patrimoniaux

Les droits patrimoniaux sont usuellement distingués en deux grands droits : le droit de représentation et le droit de reproduction.

- **Droit de représentation** (L. 122-2 du Code de la propriété intellectuelle) : l'atteinte à ce droit suppose une communication au public, or l'exploration de données extrait des connaissances mais ne présente pas l'œuvre en tant que telle au public. Il n'y a donc pas d'atteinte au droit de représentation.
- **Droit de reproduction** (L. 122-3 du Code de la propriété intellectuelle) : l'atteinte au droit de reproduction requiert la fixation matérielle de l'œuvre par tous procédés (numérique y compris) et la communication au public de manière indirecte (id est par la médiation du support). Le droit de reproduction est donc de conception finaliste. Il est donc nécessaire de caractériser la reproduction effectuée dans le cadre de l'utilisation d'une œuvre en tant qu'*input* : en effet, l'analyse de données ne donne pas toujours lieu à une communication de ces images au public.
- La reproduction est a priori constituée dans le cas du TDM, même si l'on peut interroger le cas d'une reproduction minime, ainsi que le laisse supposer la décision Infopaq de la CJUE, dont le considérant 48 dispose que le fragment d'une œuvre bénéficie d'une protection du droit d'auteur s'il témoigne également d'une originalité⁶⁷. On pourrait donc avancer qu'une base d'entraînement d'IA qui reproduirait des portions très réduites d'une œuvre ne serait pas contrefaisante, ces portions n'étant pas originales. Seule la reproduction de portions conséquentes serait alors illicite, ce qui

⁶⁶ Article L. 122-5 10° du Code de la propriété intellectuelle.

⁶⁷ Cour de justice de l'Union Européenne, *Infopaq*, 16 juillet 2009, C-5/08.

poserait un problème de détermination au cas par cas de l'originalité de la portion d'œuvre analysée dans le cadre du TDM et de l'IA.

Se pose ainsi la question de savoir si l'exploration de données en tant que telle porte atteinte au droit d'auteur.

- La contrefaçon ne devrait pas pouvoir être caractérisée au regard de la finalité visée par l'exploration de données (l'information en elle-même): en effet, l'exploration de données, qui consiste à opérer des traitements informatisés de gisements de contenus, quelle que soit leur nature impose, pour les fouiller, d'en prendre possession et de les stocker, donc de les reproduire, au sens du droit d'auteur. Cependant, l'exploration de données est un traitement dont l'objet est informationnel, or le droit d'auteur protège la forme d'expression et non les idées. L'exploration de données utilise, exploite, l'œuvre, non pour la reproduire ou la représenter, au sens du droit d'auteur, mais pour produire de la connaissance. De cette connaissance pourront naître de nouvelles connaissances, de nouveaux produits et services à valeur ajoutée. 69
- Il y a donc distinction entre *l'information à l'état brut*, que sont les données, et *l'expression originale*, objet du droit d'auteur. Dans l'exploration de données, ce ne serait pas l'œuvre en elle-même qui serait exploitée, mais plutôt la donnée, sans expression originale. Il est possible de dresser une analogie avec la décision *Être et Avoir* lors de laquelle la Cour de cassation a pu juger que « *les illustrations* [objet du droit d'auteur] *ne sont à aucun moment (...) représentées pour elles-mêmes* »⁷⁰ : il n'y aurait emprise du droit d'auteur qu'en cas de représentation partielle de la forme d'expression des œuvres explorées (ex : extraits), ce qui implique de <u>concevoir le droit</u> comme un droit finalisé.
- L'exploration de données s'attachant au sens, aux informations, et non à la création en tant que telle, la protection légale par le droit d'auteur ne devrait pas trouver à s'appliquer. L'exploration de données n'emprunte pas la forme de l'œuvre et ne s'exerce pas dans le même périmètre que la fonction pour laquelle la protection a été instaurée.
- Cependant, la contrefaçon est susceptible d'être constituée par la mise en œuvre d'actes de reproduction intermédiaires préalables à l'exploration de données.
- L'exploration de données requiert des actes de reproduction préalables au traitement, et notamment la collecte des données et de leur préparation, le

⁶⁸ Cass. Civ. 1^{ère}, 29 novembre 2005, n°04-12.721.

⁶⁹ L'ensemble des développements de ce paragraphe sont tirés du Rapport CSPLA, ibid.

⁷⁰ Cass. Civ. 1ère, 12 mai 2011, n°08-20.651.

changement de format pouvant impliquer une copie préalable des contenus numériques. Il s'agit alors de faire application de la Directive 2001/29/CE⁷¹ et des règles du Code de la propriété intellectuelle, la copie de tout ou partie du contenu objet du traitement étant qualifiée d'acte de reproduction.

- On peut se demander si l'exception de copie provisoire est applicable, mais cette application serait très limitée car on ne peut en faire un argument que pour l'exploitation d'œuvres dont l'exploitant a obtenu les droits (donc ni pour les œuvres pour lesquelles l'exploitant n'a pas les droits, ni pour les logiciels et les bases de données).⁷²
- En conclusion, il semble donc que le TDM ne constitue pas une atteinte au droit d'auteur en tant que tel, mais les actes de reproduction préalables à la mise en œuvre du TDM sont probablement en eux-mêmes des contrefaçons des droits patrimoniaux si les œuvres n'ont pas été licitement acquises.

1.2.2.2. Droit moral

Le droit moral est lui-même divisé en plusieurs composantes.

- **Droit de divulgation** : pas de possibilité d'atteinte, l'exploration d'une œuvre présente dans une base de données suppose que celle-ci ait été préalablement divulguée, sauf cas exceptionnels.
- **Droit de retrait et de repentir** : ce droit n'offre aucune spécificité directe avec l'exploration de données, tant que les données sont supprimées si l'auteur manifeste son intention d'exercer son droit de retrait.
- **Droit à la paternité** : l'atteinte au droit de paternité suppose que l'œuvre soit utilisée pour elle-même, en tout ou en partie substantiellement suffisante. Par ailleurs, le droit de paternité suppose également que l'œuvre soit communiquée à un public, sinon il perd de sa substance. Or, dans le cas de l'exploration de données, l'œuvre n'est pas utilisée pour être divulguée : il n'y a donc pas d'atteinte au droit à la paternité.
- Droit au respect et à l'intégrité de l'œuvre : le Rapport CSPLA rappelle que, « en raison de sa qualité, l'auteur peut s'opposer à toute déformation, démantèlement, mutilation ou autre modification de son œuvre. Certains pourraient considérer que les actes nécessaires à l'exploration de données constituent dans certains cas une

⁷¹ Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001 sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (la « **Directive Société de l'Information** »).

⁷² Article L. 122-5 6° du Code de la propriété intellectuelle.

dénaturation de l'œuvre ».⁷³ Notre interprétation est plus nuancée, le changement de forme de l'œuvre n'entraînant pas automatiquement selon nous une altération de l'intégrité de l'œuvre. Il faut donc que l'altération soit perceptible par le public pour que le droit moral rentre en jeu, comme le confirme la jurisprudence La Cinq du TGI de Paris, par laquelle les magistrats français ont ainsi considéré que l'élément déterminant de l'atteinte à l'intégrité était l'altération de la perception de l'œuvre par le public.⁷⁴

En conclusion, le TDM ne semble pas constituer en lui-même une atteinte au droit d'auteur : ni les droits patrimoniaux, ni le droit moral ne semblent s'opposer directement à l'exploration de données. Le droit de reproduction est susceptible d'empêcher la collecte d'œuvres aux fins de constituer la base de données d'input de l'IA, tandis que le droit à l'intégrité de l'œuvre peut potentiellement servir à empêcher la transformation et le morcèlement de l'œuvre en données.

1.2.3. L'atteinte au droit sui generis sur les bases de données

- Conditions de la protection de la base de données : la protection est accordée à une base de données sous réserve de la justification d'un investissement financier, matériel ou humain substantiel.⁷⁵ Le critère d'investissement substantiel est apprécié par les juges du fond, au regard notamment des coûts récurrents de gestion, de contrôle et de maintenance de la base de données
- **Pour qui?** Le droit sui generis bénéficie aux seuls producteurs de bases de données, à savoir les personnes qui prennent "...l'initiative et le risque des investissements correspondants".⁷⁶
- **Objectif**: éviter toute appropriation et/ou utilisation frauduleuse du résultat d'investissements majeurs.
- Droits conférés au producteur base de données : le producteur peut interdire :
 - l'extraction, par transfert permanent ou temporaire, de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données⁷⁷;

⁷³ Rapport CSPLA, ibid.

⁷⁴ TGI Paris, 29 juin 1988, La Cinq.

⁷⁵ Article L. 341-1 du Code de la propriété intellectuelle.

⁷⁶ Même article.

⁷⁷ Article L. 342-1 du Code de la propriété intellectuelle.

Ex : la Cour d'appel de Paris, dans un arrêt du 12 septembre 2001 a condamné une société pour avoir utilisé à des fins commerciales des catalogues appartenant à une autre société et incorporé à son fichier les données informatives figurant dans ces catalogues, de tels agissements constituant une extraction par transfert permanent ou temporaire d'une partie quantitativement substantielle du contenu d'une base de données sur un autre support.⁷⁸

- o la réutilisation par la mise à disposition du public de la totalité ou d'une partie substantielle du contenu de la base, quelque qu'en soit la forme ; et
- l'extraction ou la réutilisation répétée et systématique de parties non substantielles du contenu de la base de données lorsque ces opérations excédent manifestement les conditions d'utilisation normale de la base de données.
- Application à l'exploration de données : il existe un risque que les traitements de TDM soient considérés comme une « réutilisation » des informations des bases de données d'où les informations sont puisées après une « extraction » au sens de l'article L. 342-1 du Code de la propriété intellectuelle. L'enjeu pour les opérateurs est donc de pouvoir justifier en amont qu'il n'existe pas un lien avec la source des données qui les placerait dans le cadre de l'interdiction du droit sui generis.
- L'effet économique est donc négatif : le risque juridique d'atteinte au droit sui generis existant pour le moment au sein de l'Union Européenne n'offre pas un cadre de protection suffisant aux entreprises traitant de grandes quantités de données. Ces dernières préfèreront ainsi s'établir hors de l'Union Européenne (surtout en ce qui concerne la collecte des données). Il semble ainsi nécessaire d'offrir à ces entreprises un cadre d'action afin qu'elles ne voient plus leurs activités contrecarrer par le droit.

1.3. Les enjeux soulevés par une illicéité du TDM

1.3.1. L'application de la sanction : injuste, arbitraire ou impossible ?

La multiplicité des intervenants complique l'application d'une éventuelle sanction : doit-elle être imposée au programmeur, comme créateur de l'IA ? Au propriétaire de l'IA ? À l'utilisateur qui aura fait la demande d'exploration qui aura été à l'origine des

⁷⁸ CA Paris, 12 septembre 2001, SARL Tigest Communication c/ Sté Reed Expositions France

reproductions/extractions non autorisées? Il y a ainsi un parallèle à faire avec les questions qui se posent en matière de responsabilité civile. On pourrait néanmoins trouver un palliatif dans une demande in solidum – la répartition incomberait alors aux défendeurs et non au demandeur.

Il y aurait d'ailleurs une question intéressante si l'IA en cause avait objectivement vocation à fonctionner sur des data sets de manière illicite (si l'IA était spécifiquement conçue pour avoir un fonctionnement contrefaisant). Dans ce cas, il serait plus légitime de se poser la question de la responsabilité du propriétaire de l'IA, non pas sur le fondement de la propriété intellectuelle car ce n'est pas lui qui effectue en tant que tel les actes illicites (il n'y a que fourniture de moyens), mais plutôt sur le fondement de la responsabilité de droit commun car la faute, le lien de causalité et le préjudice seraient éventuellement qualifiées.

1.3.2. Le risque de remise en cause du business model de l'IA

La soumission du TDM aux droits de propriété intellectuelle aurait des implications économiques. En effet, l'efficacité du TDM dépend de la richesse de la base de données, ce qui implique un important coût d'accès à ces bases de données pour de nombreux tissus industriels se développant actuellement autour de l'IA. Il y a donc un risque de destruction du tissu de startups si le TDM était assujetti aux droits de propriété intellectuelle.

Cette analyse est néanmoins à nuancer, étant donné qu'il existe peu de chiffres aujourd'hui quant à l'existence d'une économie actuelle effective se développant autour du TDM à des fins commerciales.

Au-delà du développement du business model de la fourniture de bases de données, c'est évidemment l'essor du *machine learning* en lui-même qui est susceptible d'être impacté par l'illicéité du TDM du fait de la propriété intellectuelle. En effet, puisque l'apprentissage machine repose sur des quantités gigantesques de données, soumettre l'exploration et l'exploitation des résultats de cette exploration à une autorisation préalable reviendrait à soumettre la majeure partie des initiatives de *machine learning* à une autorisation préalable.

Il s'agit donc de déterminer comment rendre licite l'utilisation d'éléments protégés par la propriété intellectuelle pour l'apprentissage machine d'une intelligence artificielle, sans porter atteinte aux intérêts des ayants droit.

Des solutions existantes diversifiées mais incomplètes 1.4.

Le droit positif apporte déjà un certain nombre de solutions aux enjeux et questions soulevés ci-dessus, que ce soit au niveau européen ou français. Cependant, ces solutions ne répondent pas à l'ensemble des enjeux posés et n'offrent pas une sécurité juridique complètement satisfaisante.

1.4.1. <u>Positionnement de l'Europe et de l'OMPI</u>

- Creative Commons (initiatve supra européenne) : toutes les licences Creative Commons permettent la reproduction et la rediffusion des œuvres (y compris en ligne). Mais l'auteur garde la faculté de maintenir des conditions à la réutilisation en sélectionnait certaines des options proposées par les licences (NC = pas d'usage commercial, ND = pas de modification, SA = partage à l'identique). Ces restrictions maintenues par le créateur trouvent pleinement leur fondement dans le droit d'auteur. Il existe des licences CC pour les producteurs de base de données (Licence CC 4.0) mais elles supposent préalablement l'accord des titulaires de droit.
- L'initiative des « licences for Europe » : il s'agit d'un programme lancé par la Commission européenne le 4 février 2013 afin « d'aplanir les obstacles concrets à la circulation des contenus à l'ère numérique. »79 Le Rapport CSPLA mentionne que l'initiative en est toujours à une phase contractuelle : « l'association internationale des éditeurs scientifiques, techniques et médicaux STM et l'Association of Learned and Professional Society Publishers et l'industrie pharmaceutique ont mis au point un contrat-type et trois groupes d'édition, Elsevier, Springer et Wiley ont mis en place des procédures sur l'exploration de données ».80
- Potentielle exception au droit d'auteur de TDM : historiquement, de nombreux développements pointent vers la mise en œuvre d'une exception européenne au droit d'auteur pour l'exploration de données.
 - Directive du 14 mai 1991, Art.7: interdiction de tout moyen neutralisant 0 des mesures techniques de protection pour des programmes d'ordinateurs⁸¹;
 - Directive Société de l'Information : sanctionne la fabrication et commercialisation des mécanismes de contournement de la protection

⁷⁹ http://ec.europa.eu/internal_market/copyright/licensing-europe/index_fr.htm

⁸⁰ Rapport CSPLA, ibid.

⁸¹ Directive 91/250/CEE du Conseil, du 14 mai 1991, concernant la protection juridique des programmes d'ordinateur.

accordée par la propriété intellectuelle, sans pour autant mentionner le TDM ;

O Proposition de nouvelle directive⁸²: le projet de réforme de la Directive Société de l'Information semble prévoir, à l'instar de la France, une exception au droit d'auteur pour le TDM. De la même manière que l'exception française, le texte s'appliquerait aux finalités non commerciales et couvrirait les activités de recherche scientifique. Il serait également valable dans le cadre de partenariats impliquant des acteurs commerciaux. Surtout, le texte prévoit explicitement que les clauses contractuelles contraires seront inopérantes, même si une marge de manœuvre est laissée aux titulaires de droits pour fixer des restrictions techniques aux opérations d'extraction, avec un appel aux États pour déterminer à leur niveau les bonnes pratiques en la matière.

1.4.2. En France : des mécanismes inadaptés à l'exploration de données

1.4.2.1. Des exceptions au droit d'auteur strictement cantonnées

■ Exception de courte citation : cette exception ne répond pas à la logique et à la technique du TDM qui procède par décomposition.⁸³

Conditions d'application :

- La citation doit s'incorporer à une seconde œuvre : nous sommes donc face à deux œuvres, l'œuvre citée et l'œuvre citant. L'œuvre citant est alors une œuvre composite.
- Deuxième condition: elle doit être justifiée par le caractère critique, polémique, pédagogique, scientifique ou d'information de la seconde œuvre.
- Troisième condition : la citation doit être courte, ce qui s'apprécie au regard de la durée de l'œuvre citée et de l'œuvre citant, et doit mentionner le nom de l'auteur et la source.

Aucune de ces conditions n'est remplie par le traitement de données nécessaire à l'apprentissage machine.

⁸² Proposition de Directive du Parlement Européen et du Conseil sur le droit d'auteur dans le marché unique numérique 2016/0280.

⁸³ Article L. 122-5 3° du Code de la propriété intellectuelle

- Exception de copie provisoire et transitoire : se pose la question de savoir si la copie de la donnée protégée effectuée aux fins du TDM est une copie provisoire.

 84 Les conditions d'application de cette exception ont été précisées par les arrêts Infopaq de la CJUE en date du 16 juillet 2009⁸⁵ et du 17 janvier 2012⁸⁶. Il ressort ainsi de ces arrêts que la reproduction de données peut être soumise au droit d'auteur si le fragment repris est lui-même protégé par le droit d'auteur. Par ailleurs, l'exception ne s'applique que si trois conditions cumulatives sont remplies : (i) la reproduction fait partie intégrante et essentielle d'un procédé technique, (ii) la reproduction poursuit une finalité unique, l'utilisation licite d'une œuvre protégée, et (iii) la reproduction ne doit pas avoir une signification économique indépendante. Il semble donc que cette exception ne s'applique pas au TDM : la source de la reproduction doit être licite, la durabilité de la copie des données dépend du bon vouloir de l'utilisateur et elle n'est donc ni provisoire, ni transitoire, ni accessoire, et le TDM dégage une valeur économique du fait des recoupements nouveaux de données.
- Exception de TDM: introduite en droit français par la loi du 7 octobre 2016 pour une République numérique⁸⁷. Cette exception est limitée aux usages non commerciaux, et exclut donc toute exploration de données aux fins d'une réexploitation commerciale de l'algorithme apprenant. Il est à noter que cette exception requiert un décret d'application pour être mise en œuvre, décret qui tarde à arriver compte tenu des développements européens sur le même sujet.

1.4.2.2. Les exceptions au droit sui generis

Les exceptions en matière de droit sui generis sont différentes de celles prévues en matière de droit d'auteur ou de droits voisins : il n'y a pas d'exception de copie provisoire ou d'exceptions à des fins d'actualité ou des revues de presse.

■ Exception concernant l'extraction ou la réutilisation non substantielle (appréciation qualitative ou quantitative) : l'article L.342-3, 1° du Code de la propriété intellectuelle prévoit la licéité d'une extraction non substantielle d'une base de données protégée, à condition que la base de données soit mise à la disposition du public par le titulaire des droits, et donc qu'il y ait un accès licite. En matière d'exploration de données, même si l'utilisateur possède un accès licite à la base de données, il semble

⁸⁴ Article L. 122-5 6° du Code de la propriété intellectuelle, introduite par l'article 5 paragraphe 1 de la directive 2001/29/CE52

⁸⁵ Cour de justice de l'Union Européenne, Infopaq, 16 juillet 2009, C-5/08.

⁸⁶ Cour de justice de l'Union Européenne, *Infopaq*, 17 janvier 2012, C-302/10.

⁸⁷ Article L. 122-5 10° du Code de la propriété intellectuelle

qu'il n'y a jamais d'extraction qui ne soit pas quantitativement ou qualitativement substantielle. Par conséquent, cette exception ne semble pas pouvoir s'appliquer.

- **Exception à des fins de copie privée** : prévue par l'article L. 342-3, 2° du Code de la propriété intellectuelle, qui précise qu'il est possible d'extraire une partie quantitativement ou qualitativement substantielle d'une base de données dès lors que la copie est réalisée à des fins privées. Ainsi, l'exploitation de données dans un cadre non privé (et donc une entreprise) empêche l'application de cette exception.
- Exception à des fins d'enseignement et de recherche : enfin, l'article L. 342-3, 4° du Code de la propriété intellectuelle prévoit une exception pour extraction et réutilisation à des fins d'enseignement et de recherche. L'exception ne s'applique ni aux bases de données conçues à des fins pédagogiques ni aux bases de données réalisées pour une édition numérique de l'écrit. Dans ce cas, l'extraction et la réutilisation sont destinées à un public composé majoritairement d'élèves, d'étudiants, d'enseignants ou de chercheurs. La source doit être indiquée et il ne doit pas il y avoir d'exploitation commerciale. En outre, elle doit être compensée par une rémunération négociée sur une base forfaitaire. Les conditions de mise en œuvre de cette exception étant très strictes, elle sera très difficile à mettre en œuvre dans le cadre des activités d'exploration de données.

1.4.3. Les solutions contractuelles

Au-delà des droits garantis par la propriété intellectuelle, les acteurs de l'IA peuvent toujours recourir au contrat. Cette solution présente cependant des limites évidentes :

- Les négociations très chronophages peuvent décourager les initiatives;
- Ces solutions sont soumises à un fort aléa : aléa de l'autorisation des titulaires de droits multiples et aléa dans la désignation finale de la titularité des droits sur les contenus;
- Il existe un fort risque de constitution de grands monopoles restreignant drastiquement les possibilités de négociation ; et
- Ces solutions ne sont valables qu'entre les parties, au cas par cas (exception : les licences Creative Commons).

C'est pourquoi la majorité des représentants des bibliothèques et des instituts de recherche ont souligné que l'exploration de données sur des contenus pour lesquels un accès légal a été obtenu ne devrait pas nécessiter de nouvelle licence ni de nouvelle rémunération.

Ex. : un projet comme Text2genome, qui impliquait l'exploration de millions d'articles, a pris trois ans car l'accès aux données pour l'exploration a été négocié avec chaque éditeur au cas par cas.

2. Ébauche de solutions

« La diversité des activités d'exploration de données et des acteurs concernés conduit à rechercher des solutions souples et non figées. Le présent rapport encourage donc le développement de solutions contractuelles. »⁸⁸

Dans la lignée du Rapport du CSPLA, nous avons tenté de trouver des solutions souples et novatrices aux enjeux non traités par le droit positif actuel. Comme précisé en **1.3**, les enjeux principaux de la confrontation de l'IA à la propriété intellectuelle au stade de l'input sont (i) la remise en cause du fonctionnement même de l'IA, qui dépend sur le TDM pour s'améliorer et (ii) la difficulté d'application de la sanction, le cas échéant.

2.1. La légitimation du TDM, moyen de résoudre le problème d'application des sanctions

Il va de soi que la légitimation du TDM implique la résolution du problème d'applicabilité de la sanction, puisque celle-ci n'aurait plus lieu d'être, l'utilisation des éléments protégés en tant qu'input étant autorisée. Nous avons donc avant tout creusé les pistes permettant d'autoriser le TDM tout en respectant les droits des auteurs d'œuvres et des producteurs de bases de données.

Dans le cas cependant où une sanction serait cependant nécessaire, il convient de clairement déterminer l'identité du contrefacteur. Puisque l'élément contrefaisant se trouve dans la base de données, le contrefacteur premier doit nécessairement être le propriétaire de la base de données au sein de laquelle se trouve les éléments contrefaisants. Si cette personne est la même que l'utilisateur des données en tant qu'input de l'IA, il n'y a qu'un seul contrefacteur aisé à trouver. Si le propriétaire de la base de données et l'utilisateur de l'IA (et du jeu de données ainsi acquis auprès du propriétaire) sont deux personnes différentes, l'utilisateur de l'IA est nécessairement également contrefaisant, la contrefaçon ne connaissant ni bonne ou mauvaise foi. Cependant, il serait inéquitable de laisser à cette personne la charge de la

⁸⁸ Rapport CSPLA, ibid.

condamnation : il convient de légitimer le principe contractuel de garantie d'éviction dans ce genre de cas, en mettant à la condamnation à la charge du premier contrefacteur, propriétaire de la base de données. Le propriétaire des droits de propriété intellectuelle a alors un recours contre les deux personnes, qui pourront ensuite se retourner l'une contre l'autre pour déterminer les responsabilités.

Nous proposons donc de supprimer la nécessité de sanction en légitimant les utilisations d'éléments protégés en tant qu'input.

Dans les cas où une sanction s'avérerait néanmoins nécessaire, il convient de faire peser sur le propriétaire des données servant d'input une présomption de contrefaçon, à charge pour lui de prouver que ce n'est pas le cas. Lorsque l'utilisateur de l'IA et le propriétaire des données sont deux personnes distinctes, la victime de la contrefaçon dispose d'une action in solidum contre les deux personnes, à charge pour elles de résoudre la répartition de la condamnation après son prononcé et sur la base de la présomption de contrefaçon.

2.2. Une nouvelle exception au droit d'auteur

La première piste développée se place dans la lignée du travail déjà initié par la France et l'Union Européenne, à savoir la création d'une exception au droit d'auteur permettant d'effectuer du TDM, et donc d'entrainer des intelligences artificielles sur des *datasets* comprenant des œuvres protégées. Cette exception se doit cependant d'être plus recherchée qu'en l'état actuel pour permettre une utilisation commerciale.

2.2.1. <u>Justification de l'exception</u>

Le droit d'auteur connait un certain nombre croissant d'exceptions listées à l'article L. 122-5 du Code de la propriété intellectuelle. Il est intéressant, si l'on veut construire une nouvelle exception, de revenir sur les raisons ayant poussé à développer le régime déjà existant d'exceptions.

La justification est double : l'article 47 de la Déclaration Universelle des Droits de l'Homme consacre un droit d'accès à la culture, tandis que l'article 10 de la Déclaration des Droits de l'Homme et du Citoyen entérine la liberté d'expression. Aussi bien l'accès à la culture que la liberté d'expression justifient d'avoir des accès aux œuvres, ce qui explique non seulement la durée limitée des droits patrimoniaux mais également le régime d'exceptions pour certains usages. De nombreuses exceptions sont déjà

justifiées par l'accès à la culture (copie privée, exceptions aux fins de recherche ou pédagogiques, exceptions d'accessibilité) ou la liberté d'expression (courte citation, parodie). L'IA permettant de multiples usages, les deux fondements sont susceptibles de jouer. On pourrait d'ailleurs déterminer un droit de libre création sur lequel serait fondée cette nouvelle expression.

L'exception se justifie également au regard des utilisations et de la particularité du TDM. Il s'agit ainsi d'adopter un regard finalisé sur le droit d'auteur : Il faut envisager le droit dans sa finalité, les œuvres reproduites ne sont qu'un moyen. Il est possible d'arguer que l'exploration de données ne devrait pas faire l'objet d'une compensation financière au profit des titulaires de droit dans la mesure où l'exploration de données ne constitue pas un préjudice dont pourraient se prévaloir les titulaires de droits, puisque la pratique ne porte pas véritablement atteinte aux intérêts légitimes de l'auteur - on est sur un type d'utilisation très particulier (faire apprendre à la machine) et pas sur une consommation « normale » ou « habituelle » de l'œuvre par une personne physique ou morale. Un excellent exemple à cet égard est l'utilisation d'œuvres d'art par les intelligences artificielles de Google aux fins de classement de ces œuvres : il ne s'agit donc pas de reproduire l'œuvre en elle-même mais de l'identifier et de la comparer à d'autres œuvres afin de la classifier⁸⁹.

À ce titre, l'exception serait légitimée car sa mise en œuvre poursuivrait des fins de créations non concurrentes de celles initialement poursuivies par l'œuvre utilisée, cette dernière n'étant qu'un vecteur pour l'aspect véritablement intéressant au regard du TDM, les données relatives à l'œuvre.

Il s'agit ici d'établir un distinguo entre données *de l'œuvre* et données *sur l'œuvre*: les données utilisés dans le cadre du *machine learning* et du TDM sont des informations relatives à l'œuvre, des informations à propos de l'œuvre, et non pas les informations composant l'œuvre elle-même. En d'autres termes, les données utilisées ne sont pas celles constituant l'œuvre, support immatériel, mais bien des données sur cette œuvre: non seulement nom de l'auteur, date de création, mais aussi « pixel rouge à telle position » ou « son de telle fréquence à telle minute ». Enfin, et surtout, s'il est possible in fine de recréer l'œuvre à partir de telles informations, ce n'est pas le cas une fois qu'elles ont été traitées par l'outil de TDM ou par le *machine learning*. Rappelons en effet que le *machine learning* se base, de manière concrète, sur l'ajustement des réponses des neurones composant le réseau neuronal à l'input: en pratique, il s'agira donc de modifier les valeurs des neurones du réseau neuronal en

⁸⁹ Voir les « AI Experiments » menée par Google Arts & Culture : https://experiments.withgoogle.com/arts-culture.

fonction de la donnée de l'input, mais pas de conserver cette donnée, ni de la reproduire d'une quelconque manière (ce qui fait qu'aucune ingénierie inverse ne permettrait de retrouver la donnée après son input).

Enfin, il convient de rappeler que plusieurs exceptions portent déjà sur des contenus à finalités commerciales : l'exception de reprise journalistique est exploitée de manière commerciale par la presse, 90 et il en va de même pour les parodies 91, ou, a fortiori, l'exception de catalogue de vente judiciaire. 92 En l'occurrence, si l'IA est bien exploitée commercialement, il est rappelé qu'in fine ce n'est pas l'œuvre en elle-même qui sert, mais bien des informations relatives à ses qualités, et celles-ci n'ont que pour but de permettre à l'IA de reconnaitre des récurrences sur lesquelles fonder les prochains traitements de donnés.

2.2.2. Risques de l'exception

L'exception n'est pas un régime sans défauts :

- Un aménagement contractuel est-il possible? La Directive Société de l'Information confère un caractère d'ordre public aux exceptions⁹³ mais le juge français ne s'est jamais penché sur la question.
- Quid des droits moraux des ayants droits et héritiers ? L'exception ne permettra que de faire exception aux droits patrimoniaux, mais ne pourra être opposée à l'exercice du droit moral, le cas échéant.
- Quid des bénéfices que peuvent retirer les ayants droits du fait du statut de l'œuvre dérivée ou composite? L'exception risque-t-elle de porter atteinte à cette potentielle source de profit? Le cas échéant, il s'agit donc de déterminer comment mettre en œuvre l'exception sans porter atteinte de manière démesurée aux intérêts légitimes de l'auteur. Ce risque est cependant minime selon nous, puisque l'œuvre ne se retrouve pas, a priori, dans l'output: si tel est bien le cas, il n'y a pas atteinte au marché de l'œuvre composite et dérivée, qui est toujours possible par ailleurs. Un cas qui reste néanmoins à envisager est celui d'IA créatrices d'œuvres « à la manière de »: de telles IA seront forcément entrainées sur des datasets d'œuvres protégées de l'auteur que l'on cherche à imiter et produiront un output ressemblant à ces œuvres. Dans ces conditions, l'exception risque de porter atteinte aux droits de l'auteur si elle n'est pas correctement circonstanciée.

⁹⁰ Article L. 122-5 9° du Code de la propriété intellectuelle.

⁹¹ Article L. 122-5 4° du Code de la propriété intellectuelle.

⁹² Article L. 122-5 3°d) du Code de la propriété intellectuelle.

⁹³ Article 5 de la Directive Société de l'Information.

• Enfin, si l'exception au droit d'auteur permettrait de se passer d'une autorisation expresse, il n'en reste pas moins que les exceptions sont extrêmement encadrées et généralement très mal vues par les sociétés de gestion et autres représentants d'ayants droit. Les négociations risquent ainsi d'être longues, et le processus législatif encore plus, ce qui est à prendre en compte dans la réflexion.

2.2.3. Une exception ne bénéficiant qu'au droit d'auteur

L'exception ne peut en effet que difficilement s'appliquer au droit sui generis sur les bases de données. Ainsi que précisé ci-dessous, les exceptions au droit d'auteur et au droit sui generis doivent passer le « triple test », qui implique notamment que l'exception ne porte pas atteinte aux intérêts légitimes du producteur de la base de données ou porte atteinte à l'exploitation normale de la base de données. Le triple test s'applique à la fois aux exceptions au droit d'auteur et aux exceptions au droit sui generis. Pans le cas de la base de données, l'exception pour exploration de données reviendrait donc à permettre l'extraction du contenu de la base de données pour le réutiliser, ce qui est justement le but du droit sui generis en lui-même. Ainsi, il est probable que l'exception de TDM soit inapplicable au droit sui generis sur les bases de données car il impacterait directement les intérêts légitimes protégés. Il convient ainsi d'explorer plus en détail cette piste pour déterminer si une formulation très circonstanciée pourrait concilier les divers intérêts, même si cela semble improbable en l'état actuel de nos recherches.

2.2.4. Une exception à quels droits exclusifs?

Maintenant que le principe d'une exception au droit d'auteur est justifié, il convient d'explorer son contenu, et notamment les droits auxquels il est fait exception. En l'occurrence, il semble que l'exception de TDM puisse être limitée aux actes suivants :

■ le droit de reproduction, tant que la reproduction ne fait pas l'objet en elle-même d'une publicité ou diffusion auprès du public − il faut que la reproduction ne soit qu'accessoire dans le processus d'exploration de données, que la donnée ne soit stockée que temporairement, le temps du processus d'apprentissage machine, et supprimée ensuite; et

⁹⁴ Le triple test est issu de la Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886, et a été repris par la suite par la Directive Société de l'Information, et, pour le droit sui generis, par la Directive Bases de Données (article 6.3).

le droit d'adaptation – puisque l'œuvre doit être transformée en données, voire même en métadonnées, il convient d'autoriser l'adaptation et la transformation de l'œuvre en question afin de légitimer non seulement l'exploration de données mais le façonnage de la donnée issue de l'œuvre pour la rendre lisible et intelligible par l'IA.

2.2.5. Le triple test

Le triple test a été introduit dans la Convention de Berne pour la protection des œuvres littéraires et artistiques du 9 septembre 1886 pour permettre la création de nouvelles exceptions qui respectaient certains principes, tout en garantissant l'existence des exceptions préexistantes, certains États ayant été plus diligents que d'autres en cette matière. Depuis, ce test a été repris par la suite par la Directive Société de l'Information, et, pour le droit sui generis, par la Directive Bases de Données (article 6.3). Il a été transposé en droit français dans les articles relatifs aux exceptions au droit d'auteur⁹⁵ et au droit sui generis⁹⁶.

Le triple test a pour but de vérifier que l'exception porte bien sur (i) un cas particulier (ii) qui ne porte pas atteinte à l'exploitation normale de l'œuvre et (iii) ne cause pas un préjudice injustifié aux intérêts légitime de l'auteur.

Il est de notre avis qu'introduire une exception généralisée de TDM au droit d'auteur peut remplir le triple test. Si l'exception est correctement circonscrite, elle devrait bien correspondre à un cas particulier, celui d'extraire des informations afin d'améliorer un algorithme. Cette utilisation, comme on l'a vu, ne porte pas atteinte à l'exploitation normale de l'œuvre puisqu'il ne s'agit pas de traiter l'œuvre en elle-même ni de la reproduire, mais de traiter des informations relatives à cette œuvre. Il reste à déterminer si les intérêts légitimes de l'auteur ne sont pas atteints de manière injustifiée. Il convient de pousser la réflexion sur ce point ; toujours est-il qu'a priori les principaux intérêts protégés par le droit d'auteur ne seraient pas atteints par une telle exception, dont la portée selon nous est limitée à l'information relative à l'œuvre. Il ne nous semble pas qu'une telle exception mette en péril les intérêts légitimes de l'auteur de l'œuvre, dans la mesure où celle-ci ne sert bien qu'à extraire de la donnée et peaufiner les réglages d'un algorithme.

2.2.6. Proposition de rédaction

⁹⁵ Article L. 122-5 3ème alinéa du Code de la propriété intellectuelle.

⁹⁶ Article L. 342-3 3ème alinéa du Code de la propriété intellectuelle.

Nous proposons donc une exception au droit d'auteur qui pourrait être insérée à la suite de la liste limitative d'exceptions de l'article L. 122-5 du Code de la propriété intellectuelle et pourrait être rédigée de telle manière :

Lorsque l'œuvre a été divulguée, l'auteur ne peut interdire :

12. La copie de données relatives à l'œuvre ou extraites à partir de celleci, dès lors que cette copie n'est qu'un acte intermédiaire visant à utiliser l'œuvre non pour elle-même mais comme information dans un traitement algorithmique, à la condition de ne pas porter préjudice à l'œuvre et au droit moral de l'auteur.

Cette proposition est évidemment à travailler, mais peut servir de base à des suggestions ultérieures.

2.3. Paiement d'un prix d'accès global pour l'accès aux bases de données

Comme détaillé au point **2.2.3**, il est improbable que l'on puisse mettre en œuvre une exception au droit sui generis sur les bases de données sans porter atteinte à l'intérêt légitime du producteur de la base ou à son exploitation normale, puisque l'extraction de données est précisément l'objet du droit exclusif sui generis.

Il convient cependant de réaliser que le droit de propriété intellectuelle le plus susceptible d'empêcher le TDM et le *machine learning* reste le droit sui generis, puisqu'il porte sur des bases de données pouvant comprendre n'importe quel type de donnée, y compris des données non protégées en elles-mêmes.⁹⁷ Il est donc important de trouver une solution pour donner accès aux bases de données protégées par le droit sui generis.

2.3.1. Création d'une nouvelle société de gestion collective

Une solution trouvée à ce sujet en droit d'auteur pour permettre l'existence des radios ou des cinémas est le regroupement des auteurs dans des sociétés de gestion collective qui offrent l'accès à leur catalogue. Ainsi, les auteurs s'affilient à la société

⁹⁷ Sous réserve d'une éventuelle patrimonialité des données, qui reste une thèse en suspens non déterminée pour l'instant. L'arrêt Bluetouff de la Cour de cassation (Cass. crim., 20 mai 2015, n° 14-81.336) laisse ainsi planer un doute puisqu'il consacre un « vol » de données.

de gestion afin de lui confier la gestion de leurs droits patrimoniaux. Les sociétés de gestion de collective, après avoir conclu des contrats de licence de droits aux entités souhaitant accéder aux œuvres et les diffuser, redistribuent les droits perçus aux adhérents.

Il est donc possible d'imaginer la création d'une telle société pour les bases de données protégées par le droit sui generis. Ce genre d'organisation, bien qu'envisageable, ne nous semble pas optimale car elle implique que les acteurs du monde de l'IA négocient et concluent des contrats pour chaque nouveau projet. En effet, les sociétés de gestion collective concluent généralement des contrats au cas par cas, pour certaines parties de leur catalogue. Il est donc aisé d'imaginer qu'un producteur de bases de données ait à changer de dataset entre deux projets et qu'il doive à nouveau contractualiser avec la société de gestion collective. Cela risque probablement de limiter l'innovation et l'investissement en IA, au-delà des éventuels problèmes d'identification des producteurs de bases de données à rémunérer une fois les droits perçus. L'hypothèse de la société de gestion collective ne nous parait donc pas la plus opportune, bien que la solution proposée lui ressemble en partie.

2.3.2. Proposition : plateforme de téléchargement par abonnement

Notre proposition est issue de réflexions autour de la notion de « licence globale » ou « contribution créative » 98, du développement de plateformes telles que Spotify et de l'idée des sociétés de gestion collective.

Proposition : créer une plateforme publique française (voire européenne) d'abonnement et de téléchargement illimité de bases de données protégées.

En somme, il s'agit de créer un « Spotify » public et européen (ou à défaut français) de la data. Nous suggérons ainsi de créer un système similaire au principe de société de gestion collective, sans ses désavantages : il s'agit de centraliser sur une plateforme publique l'ensemble des bases de données soumises à un droit sui generis et de permettre à toute entité de s'abonner à cette plateforme pour en utiliser les données pendant la durée de son abonnement. Toute utilisation de données hors abonnement devra évidemment être soumise à une autorisation préalable du

Pour en savoir plus, accéder à ce site web: http://controverses.sciences-po.fr/archive/licenceglobale/.

producteur de la base. Dans le cas du TDM, les données n'ont à être utilisées que ponctuellement, ce qui permet des abonnements temporaires pour les personnes souhaitant recourir à ce service pour des fins de *machine learning*. En revanche, toute personne souhaitant extraire les données devra prolonger son abonnement pour toute la durée d'utilisation de ces données. Il est par ailleurs possible d'envisager des grilles de prix croissantes selon la quantité de données téléchargée.

Selon nous, cette solution a plusieurs avantages majeurs. Elle permet tout d'abord à toute personne souhaitant s'essayer à l'apprentissage machine de dépasser le cas de l'acquisition de données et d'avoir à sa disposition, moyennant paiement, une base de données gigantesque. Cela assure la sécurité juridique pour les entrepreneurs et inventeurs. Par ailleurs, elle permet d'éviter les écueils et les risques d'une action judiciaire en contrefaçon de droit sui generis : celle-ci est en effet constituée par l'extraction soit répétée, soit substantielle de données de la base. Or, la notion d'usage substantiel n'a pas été définie : le législateur européen précise qu'elle peut être évaluée de « façon qualitative ou quantitative »⁹⁹, tandis que le juge français retient de plus en plus une interprétation maximaliste. Ce système de guichet unique pour les téléchargements de données protégées permettrait ainsi d'éviter les aléas de l'action judiciaire.

En ce qui concerne la mise en œuvre, nous pensons souhaitable que cette initiative naisse du public plutôt que du privé. Il s'agit tout d'abord d'éviter la création d'un mastodonte de la donnée qui finirait en monopole, ce marché étant clairement un marché de winner takes all. Le fait que l'initiative soit publique permettra également d'assurer un prix juste et neutre et une redistribution qui repose sur les mêmes critères. Cela devrait également assurer la confiance des utilisateurs comme des producteurs dans l'efficacité et la neutralité de la plateforme. Le fait que la plateforme soit européenne est également important si l'on souhaite faire émerger l'Europe sur la scène de l'IA, pour le moment toujours dominée par la Chine et lest États-Unis. Harmoniser l'utilisation des données à un tel niveau aurait pour effet positif de pouvoir plus facilement créer des intelligences artificielles, et donc de se concentrer sur la partie algorithmique et relative à l'infrastructure. Il est même possible d'imaginer de limiter l'accès à cette plateforme aux seuls citoyens et entreprises européens ou de faire varier les prix selons l'origine, notamment par le biais de l'utilisation des identifiants elDAS.

⁹⁹ Article 7 de la Directive Base de Données.

2.4. Alternativement: inspiration du fair use

Une alternative aux deux solutions exposées ci-dessus est de s'inspirer du système du fair use américain et de consacrer une notion de responsabilisation des acteurs et de résolution jurisprudentielle des contentieux. Sur la base du triple test exposé ci-dessus, il serait ainsi possible de déterminer si un cas particulier de TDM porte atteinte aux droits de l'auteur ou du producteur de bases de données.

Utiliser le triple test comme « fair use » européen et déterminer au cas par cas si l'utilisation de données protégées par le droit sui generis ou un droit d'auteur (i) est bien un cas isolé et circonscrit à un projet en particulier, (ii) ne porte pas atteinte à l'exploitation normale de l'œuvre ou de la base et (iii) ne cause pas un préjudice injustifié aux intérêts légitimes de l'auteur ou du producteur.

Il s'agirait cependant d'une réforme en profondeur de la propriété littéraire et artistique franco-européenne, qui ne connait pas d'équivalent pour le moment. S'il s'agirait donc potentiellement d'une solution permettant l'utilisation de bases de données à des fins de TDM, elle impliquerait d'obtenir un changement total de paradigme de la part des ayants droit, ce qui est loin d'être une possibilité.

La solution est par ailleurs porteuse d'une certaine insécurité juridique durant les premiers temps, puisqu'elle repose sur une appréciation jurisprudentielle des comportements. La distinction entre comportements licites et illicites interviendra donc après plusieurs jurisprudences, ce qui fera régner un certain doute durant cette période de formation jurisprudentielle.

Au stade de l'output : les créations d'IA protégées par un droit de propriété intellectuelle ?

1. Exposé du problème : une création en quête de reconnaissance

"Above mentioned legal IP systems are based on the fact that computers are inert tools, so that current intellectual property regimes usually only apply to humans or legal persons creations and not to creations coming from computers or inert tools. However, artificial technologies have advanced rapidly to the point that intelligent agents do not assist humans in the creation of works, but generate them autonomously. Thus, intelligent agents are capable of creativity". 100

En d'autres mots, l'enjeu principal de la création par intelligence artificielle est de savoir s'il y a création de l'intelligence artificielle, de savoir si l'IA peut être créatrice. Il y a ainsi deux enjeux sous-jacents : l'output d'une IA peut-il être une création protégée par un droit de propriété intellectuelle ? et par ailleurs, à qui revient la titularité de ce droit ? Le cas échéant, comment définir ces droits et les circonstancier ? Enfin, la reconnaissance d'un droit de propriété intellectuelle aux créations d'une IA ne reviendrait-il pas à diluer la notion même de création ?

Pour la suite de cette partie, on considérera que la création par une IA seule et la création dans laquelle un être humain intervient sont équipollentes, sauf lorsque précisé autrement, la distinction étant importante pour certaines considérations.

1.1. La dilution de la notion de création

La création assistée par ou directement par l'intelligence artificielle est en plein essor du fait du perfectionnement des réseaux neuronaux. Des enjeux économiques importants se dessinent ainsi pour déceler les schémas économiques rémunérateurs des créations. Il ne s'agit en effet pour l'heure que de potentialités qui promettent des possibilités de création généralisée par l'IA, et donc d'une explosion d'un marché de la culture déjà industrialisé.¹⁰¹

Les exemples de création mêlant IA sont nombreux :

¹⁰⁰ C. Leroux et al., *Suggestion for a green paper on legal issues in robotics*, euRobotics Contribution to Deliverable D3.2.1 on ELS issues in robotics.

¹⁰¹ À ce sujet, lire L'économie de la culture, F. Benhamou, La Découverte, coll. « Repères », 1996-2004.p

- Armand Leroi, chercheur de la BBC, a ainsi cherché à identifier la structure commune des hits de la musique pop pour un programme nommé *The Secret Science* of Pop^{102} ;
- D'importants acteurs tels que Google s'intéresse fortement à l'IA créative ;ntérêt d'acteurs important comme Google : «Google a en tout cas décidé de consacrer une équipe de recherche à cette question, nommée Magenta, qui sera lancée officiellement en juin. (..) L'équipe se concentrera d'abord sur la création musicale, puis devrait s'intéresser à l'image et à la vidéo. Elle a prévu de fonder ses travaux sur la plateforme d'intelligence artificielle de Google TensorFlow » 103;
- Comme dernier exemple, reprenons celui de la chanteuse Taryn Southern a créé le premier album de musique entièrement coécrit avec une intelligence artificielle, celle-ci s'occupant de la production et de la piste instrumentale, tandis que la chanteuse a écrit et chanté les paroles.¹⁰⁴

Il est donc factuel que la création au moyen de l'IA est déjà existante, et est amenée à se développer. La question de la protection par des droits de propriété intellectuelle de ces créations est donc à réfléchir. Nous proposons de commencer le raisonnement a contrario : quelles conséquences en cas de non reconnaissance des créations par une IA par un droit de propriété intellectuelle ?

Celles-ci seraient alors dans le domaine public, ce qui est une possibilité de solution envisageable en soi – considérer que toute création assistée par ou par une IA relève du domaine public. Cela risquerait cependant d'avoir des retombées négatives sur la diffusion de ces créations du fait du manque de valorisation de ces œuvres, ainsi que sur l'incitation à la création. L'absence de protection des créations réalisées par une IA pourrait priver les entreprises de la valorisation de certains actifs immatériels, ce qui aurait certainement pour effet de limiter ce type de création.

Il convient évidemment de se demander si cela ne peut pas être un but en soi, dans le cas où l'on souhaiterait réserver la création au pur domaine de l'humanité et en exclure de fait l'IA. L'absence de reconnaissance d'un droit de propriété intellectuelle aux

-

¹⁰² http://www.bbc.co.uk/programmes/b08gk664.

http://www.lemonde.fr/pixels/article/2016/05/23/google-lance-un-projet-de-recherche-pour-rendre-l-intelligence-artificielle-creative_4924971_4408996.html.

 $^{^{104}}$ « Intelligence artificielle : un robot compose un album, doit-on lui verser ses droits d'auteurs ? », Les Inrockuptibles, 24/08/17

¹⁰⁵ À propos de la fonction incitatrice de la propriété intellectuelle, lire Arrow K. (1962), « Economic welfare and the allocation of resources for invention », in : Nelson, R. (ed), *The rate and direction of inventive activity : Economic and social factors*, Princeton University Press, Princeton, pp. 609-626.

créations auxquelles l'IA aurait participé est ainsi une possibilité conservatrice qui permet cependant de garantir la primauté de la création humaine sur celle de l'IA.

Cependant, le domaine de la création par l'IA est manifestement porteur de très nombreuses initiatives, qui vont des simples créations de loisir à des créations susceptibles de valorisations futures :

- Exemple dans la littérature avec Thom Leavy, « Artificial Intelligences are Writing Poetry for a New Online Literary Magazine », *Popular Science*, 27 juillet 2016, www.popsci.com/ai-poetry-literary-magazine;
- Exemples dans la chanson avec <u>Jukedeck</u>, une IA qui compose de la musique libre de droits à la demande ; <u>FlowMachines</u>, un système conçu par Sony pour créer du jazz et de la pop ; <u>DeepBach</u>, qui cherche à imiter le génie de Jean-Sébastien Bach ; <u>Magenta</u> de Google, qui vise à créer des chefs d'œuvre ; ou encore <u>Brain.fm</u> ;
- Exemples dans le domaine de la peinture avec e-David, robot peintre développé par des chercheurs de l'Université allemande de Konstanz¹⁰⁶, et, à plus large mesure des arts graphiques, comme les créations « fantasmées » de DeepDream, le réseau neuronal profond de Google, qui ont récemment suscité l'attention des médias¹⁰⁷;
- Et enfin, exemple dans l'audiovisuel avec l'IA Benjamin, créée par un chercheur, Ross Goodwin, et le réalisateur Oscar Sharp.¹⁰⁸

Les possibilités de créations sont donc extrêmement nombreuses, mais surtout, intéressantes. Si ne pas les reconnaitre est ainsi une possibilité, elle implique néanmoins d'intentionnellement mettre de côté des potentialités culturelles jamais imaginées jusqu'alors.

En revanche, il convient de circonscrire les droits accordés sur ces œuvres compte tenu de la capacité de production inégalable d'une IA. Le risque est en effet de voir se diluer complètement la notion même de création : si toutes les œuvres créées par une IA sont protégées par les mêmes droits que ceux accordés aujourd'hui, le risque est de voir la dilution de la notion de création et d'acte créatif. C'est ainsi que la réflexion amène à se pencher sur la nature de ce qu'est la création : « s'agit-il d'une œuvre rationnelle, liée à l'intelligence, ou au contraire d'une capacité de surprise, liée à l'imagination et à l'émotion ? ». 109 Plusieurs auteurs ont écrit à ce sujet qu'il convient

_

¹⁰⁶ http://graphics.uni-konstanz.de/eDavid/.

¹⁰⁷ Le Monde 9 juill. 2015, M. Tual et G. Coutagne, « On a testé pour vous... Deep Dream, la machine à « rêves » psychédéliques de Google ».

¹⁰⁸ Le Monde 10 juin 2016, M. Tual, « Une intelligence artificielle écrit le scénario d'un court-métrage ». ¹⁰⁹ Durand, E. (2016). Chapitre 3 - Des créateurs sous influence. Dans E. Durand, L'attaque des clones: La diversité culturelle à l'ère de l'hyperchoix (pp. 43-56). Paris: Presses de Sciences Po (P.F.N.S.P.).

ainsi de développer – on pourra notamment se référer aux articles d'Alyssa Rosenberg pour le Washington Post ou aux travaux de Nathalie Heinich sur l'émergence du statut d'auteur comme construction sociale.

L'enjeu de la dilution de la création s'illustre le mieux par un exemple parlant : l'IA Melomics109, programme développé par une équipe de l'université de Malaga reposant sur une association d'algorithmes génétiques et de règles de composition, a ainsi déjà produit une base publique d'environ un milliard d'œuvres musicales uniques, disponibles en format Midi et libres de droits dans ce cas. 110 Protéger l'ensemble de ces œuvres pour 70 ans après la mort de leur auteur, à supposer que l'on détermine précisément qui est cet auteur (question qui fera l'objet de développements ultérieurs),

1.2. Une reconnaissance par le droit d'auteur?

Les créations d'une IA peuvent-elles être déjà protégées par le droit d'auteur ? Il convient de détailler les critères du droit d'auteur et de vérifier leur applicabilité en l'état. Pour être protégée par le droit d'auteur, une œuvre doit exister, être mise en forme et être originale, ce qui signifie qu'elle doit porter l'empreinte de la personnalité de l'auteur.

1.2.1. Résumé des enjeux du droit d'auteur

En résumé, l'application du droit positif actuel en droit d'auteur pose les problèmes suivants :

La caractérisation de l'œuvre :

- L'intervention humaine: la conception traditionnelle du droit d'auteur nécessite une intervention humaine dans la création. Celle-ci peut se trouver dans le choix de l'input ayant servi à la création. Une adaptation du droit est cependant possible, voire souhaitable.
- La réalisation d'une forme : le droit d'auteur implique que l'œuvre prenne forme, qu'il y ait matérialisation de l'intention de l'auteur. A priori cette exigence ne pose pas de problèmes, l'output ayant forcément une forme numérique.
- Une œuvre protégeable : pour être protégée par le droit d'auteur, une œuvre doit être originale. Ce critère de l'originalité connait plusieurs interprétations, selon que l'on adopte une interprétation traditionnelle française ou objective européenne. La

¹¹⁰ http://www.bbc.com/future/story/20140808-music-like-never-heard-before/.

conception traditionnelle est de considérer qu'une œuvre est originale lorsqu'on peut y trouver *l'empreinte de la personnalité de l'auteur*, critère qui semble difficilement conciliable avec la création par l'IA. La conception objective, issue de la jurisprudence européenne, consiste à rechercher si l'œuvre est nouvelle, ce qui semble plus conciliable avec la création par l'IA.

• Le statut de l'œuvre : si reconnaissance de l'originalité de l'œuvre il y a, il reste à déterminer son statut. S'agit-il d'une œuvre en tant que telle, ou faut-il la considérer comme étant dérivée de l'input ? Y-a-il plusieurs auteurs ?

1.2.2. Une œuvre

1.2.2.1. Une intervention humaine

Le premier critère d'existence d'une œuvre est que celle-ci doit comporter une intervention humaine. Il s'agit d'un critère non textuel mais qui se déduit aisément à la fois de la définition de l'œuvre et de la jurisprudence. Ainsi, si une création n'est pas issue d'un acte d'une personne physique humaine, il ne peut y avoir ni œuvre ni protection par le droit d'auteur. L'intervention doit être active : une découverte, la révélation d'un élément existant ou une mise à jour ne suffisent pas à caractériser cette intervention.

La question de l'intervention humaine a déjà été posée à propos de la création par ordinateur – le problème n'est qu'amplifié par l'IA mais pas forcément spécifique à celle-ci.¹¹¹

Il faut donc se demander s'il y a intervention humaine dans la création par une IA :

- Dans le cas du *machine learning*, le mécanisme à l'origine de la création, donc de la génération d'une forme, consiste en un apprentissage statistique. Aujourd'hui, les tâches de décision et de modélisation jusqu'alors dévolues à l'homme sont désormais laissées à la machine capable elle-même de formaliser ses propres règles de raisonnement et de décider de manière autonome.
- On assiste donc à un transfert de compétences et la marge d'intervention de l'homme s'amenuise puisque les machines prennent elles-mêmes en charge les actes d'interprétation et de modélisation de nouvelles formes en s'appuyant uniquement sur un corpus de données (d'exemples) qu'elle analyse. Le seul degré d'intervention humaine réside donc dans le choix dans la base d'entraînement de la machine : c'est

 $^{^{111}}$ Larrieu, Jacques, « Les robots et la propriété intellectuelle », Propriété Industrielle, Lexis Nexis, Février $2013 - n^{\circ} 2$.

sans doute avec le critère de choix que l'on peut le plus caractériser la notion d'originalité.

• On note que, depuis l'introduction d'un article L. 112-3 du Code de la propriété intellectuelle par la Loi du 18 décembre 1996, le choix suffit à caractériser une intervention créative :

« Les auteurs de traductions, d'adaptations, transformations ou arrangements des œuvres de l'esprit jouissent de la protection instituée par le présent code sans préjudice des droits de l'auteur de l'œuvre originale. Il en est de même des auteurs d'anthologies ou de recueils d'œuvres ou de données diverses, tels que les bases de données, qui, par le choix ou la disposition des matières, constituent des créations intellectuelles ».

Il y a bien intervention humaine dans le choix de la base de données car l'humain se projette dans sa création: il ne faut pas nécessairement que l'humain ait « su exactement dès le début, quelle allait être sa création finale, dans le détail de sa forme et de son résultat sonore », mais seulement qu'il ait eu « une conscience suffisante du résultat à atteindre, c'est-à-dire la construction générale de son œuvre, donc qu'il ait eu la maîtrise intellectuelle du processus créatif »¹¹².

Une jurisprudence de la Cour d'appel de Paris va en ce sens en disposant que « la composition musicale assistée par ordinateur dès lors qu'elle implique une intervention humaine, du choix de l'auteur (..) conduit à la création d'œuvre originales ».¹¹³

On peut donc considérer qu'il y a intervention humaine dans les créations d'une IA du fait du choix des *datasets* sur lesquels l'IA par l'humain s'est entrainée avant sa création. Cette notion est évidemment à compléter dans les cas où il n'y aurait qu'un seul gigantesque dataset disponible et ceux où l'IA aurait choisi les données pertinentes au regard d'instructions spécifiques.

1.2.2.2. La réalisation d'une forme

¹¹² A.-E. Kahn, Fascicule 1190 : Objet du droit d'auteur – Titulaires du droit d'auteur, JCl. Propriété Littéraire et Artistique, Lexis Nexis, Actualisation septembre 2008.

¹¹³ Cour d'appel de Paris, 15 mars 2016, n° 14/17749.

L'œuvre doit être matérialisée sous une forme, les idées étant de libre parcours. 114 Ce célèbre adage attribué à Henri Desbois permet de caractériser l'objet de la protection du droit d'auteur. L'œuvre ne peut être protégée que si elle existe, si elle a été concrétisée d'une manière ou d'une autre. Se posent évidemment les questions de savoir si cette forme doit être tangible et du seuil à partir duquel on peut considérer qu'une idée est matérialisée (est-ce qu'un plan suffit à caractériser l'œuvre future ?). Ces considération sont cependant sans objet au regard d'une création par une IA, qui connait une formalisation forcée au stade de l'output – on demande à l'IA de produire une création, qu'elle doit matérialiser au moins de manière numérique, ce qui suffit à caractériser une matérialisation.

À noter que c'est sur l'étude de la forme que la Cour de cassation considère qu'une fragrance ne constitue pas une œuvre par défaut de forme : « la fragrance [sic] d'un parfum, qui, hors son procédé d'élaboration, lequel n'est pas lui-même une œuvre de l'esprit, ne revêt pas une forme présentant cette caractéristique, ne peut dès lors bénéficier de la protection par le droit d'auteur ».¹¹⁵

In fine, il est donc probable que la création de l'IA puisse être considérée comme une œuvre, en ce qu'elle implique une intervention humaine dans le choix de la base de données et qu'elle revêt une forme à l'output.

1.2.3. <u>Une œuvre protégeable</u>

Il s'agit maintenant de déterminer si l'œuvre ainsi créée est une œuvre protégeable par le droit d'auteur. Pour être protégeable, une œuvre doit être **originale**, notion non définie dans le Code de propriété intellectuelle. Il s'agit donc de déterminer ce qu'est une œuvre originale et si l'œuvre créée par l'IA peut être qualifiée comme telle.

Traditionnellement, l'originalité s'analyse sous l'angle de « l'empreinte de la personnalité de l'auteur », ce qui signifie que l'on retrouve une trace de l'apport intellectuel de l'auteur dans l'œuvre, l'auteur étant le créateur de l'œuvre. La notion d'empreinte de la personnalité n'est pas beaucoup moins floue que celle d'originalité, mais elle renvoie donc à l'existence d'une personnalité chez l'auteur ainsi que d'une volonté de transmettre cette personnalité via la création. Il est ainsi évident qu'une telle conception de l'originalité ne peut être appliquée à une œuvre créée par une IA, ou du

¹¹⁴ Caron, Christophe, « Droit d'auteur - Les idées sont résolument de libre parcours ! », *Communication Commerce électronique* n° 9, Septembre 2003, comm. 80

¹¹⁵ Cass. com., 10 déc. 2013, n° 11-19.872.

moins tant que l'IA ne se voit pas reconnaitre une personnalité, idée que les auteurs de ce rapport ne soutiennent pas.

Cette conception traditionnelle (et française) de l'originalité de l'œuvre se heurte à une conception plus objective issue de la jurisprudence de la Cour de justice de l'Union Européenne. La conception objective consiste à considérer l'originalité comme un apport intellectuel de l'auteur : une œuvre est originale si elle a bénéficié d'une contribution intellectuelle de la part de son auteur. Une telle conception permettrait d'étendre le champ de l'originalité aux œuvres créées par une IA. Ainsi, pour le professeur Jacques Larrieu :

« si une conception objective de l'œuvre de l'esprit et de l'originalité parvenait à s'imposer, le créations des robots autonomes pourraient se glisser assez aisément dans les interstices du droit d'auteur »¹¹⁶

Ainsi, l'éventualité de la protection par le droit d'auteur d'une œuvre créée par une intelligence artificielle repose avant tout sur la conception de l'originalité qui sera promue : une conception traditionnelle de l'IA exclut a priori toute originalité d'une œuvre conçue par une IA du fait du défaut d'empreinte de personnalité (par définition), tandis qu'une conception objective de la notion d'originalité aboutirait probablement à la reconnaissance d'un droit d'auteur sur ce type d'œuvres.

1.2.4. Le statut de l'œuvre créée par une IA

En admettant qu'une œuvre créée par une IA puisse être protégée par le droit d'auteur, il reste à déterminer son statut, notamment au regard de la participation de l'IA : faut-il considérer l'œuvre ainsi créée comme étant dérivée de son input ? Le droit français admet plusieurs types d'œuvres mêlant plusieurs participants, qu'il convient de détailler pour vérifier si une œuvre créée par une IA remplit les critères :

L'œuvre de collaboration : régies par l'article L. 113-3 du Code de la propriété intellectuelle. Il s'agit d'une œuvre à la création de laquelle ont concouru plusieurs personnes physiques animées par une inspiration commune et concertée. L'IA est donc de fait exclue de cette définition, ne remplissant ni le critère de la personne physique, ni le critère de la création concertée. Il s'agit donc de déterminer si plusieurs personnes ont participé à l'obtention de l'output de l'IA, de cet output en particulier : est-ce que la programmation de l'IA ou le jeu de données ayant servi à son

¹¹⁶ Larrieu, Jacques, ibid.

apprentissage étaient particulièrement nécessaires à l'obtention de cet output ? En d'autres termes, il s'agit de déterminer si les personnes ayant participé à la création de l'output l'ont fait de manière concertée ou non. Le cas échéant, l'œuvre de collaboration peut donc convenir, les auteurs étant les personnes ayant permis à l'IA de produire cet output en particulier.

- L'œuvre collective: L'article L. 113-2 du Code de la propriété intellectuelle définit l'œuvre collective comme une œuvre créée par plusieurs personnes à l'initiative d'un tiers qui ne participe pas forcément à la création. En l'occurrence, il s'agirait donc de considérer que l'IA prend l'initiative de la création, ce qui n'est pas encore le cas. Il semble donc que cette définition ne soit pas applicable à l'IA en elle-même. Il est en revanche envisageable de considérer qu'une personne donne des instructions précises répliquées dans la programmation de l'IA, dans le jeu de données et dans le paramétrage ultérieur de l'IA, ce qui pourrait faire de l'output une œuvre collective par le biais d'une IA.
- L'œuvre dérivée: l'article L. 112-3 du Code de la propriété intellectuelle consacre la notion d'œuvre transformative en accordant un droit d'auteur, sans préjudice des droits antérieurs, aux auteurs de « traductions, d'adaptations, de transformations ou d'arrangements » d'œuvres préexistantes. Cette définition pourrait trouver à s'appliquer aux créations réalisées par une IA, celle-ci effectuant bien une étude d'un ensemble d'œuvres préexistantes pour créer son œuvre. Il est cependant également possible de confier à l'IA un jeu de données non protégées par le droit d'auteur, et d'avoir pourtant une création de sa part. Ainsi, si la définition peut correspondre à certains cas de création par IA, elle ne couvre certainement pas tout le champ des possibles.
- L'œuvre composite: l'article L. 113-2 du Code de la propriété intellectuelle définit l'œuvre composite comme une « œuvre nouvelle à laquelle est incorporée une œuvre préexistante sans la collaboration de l'auteur de cette dernière ». Le problème est donc le même que pour l'œuvre dérivée : la définition peut trouver à s'appliquer aux cas où l'output de l'IA est la conséquence d'un input d'œuvres protégées, mais pas aux cas où l'input ne serait pas protégé par le droit d'auteur.

1.3. Une reconnaissance par le droit des brevets?

Outre le droit d'auteur, il convient de s'intéresser au brevet : est-ce que l'output d'une lA peut être déposé auprès d'un registre des brevets et se voir accorder la protection par le droit des brevets ? Le brevet est accordé lorsque l'objet du dépôt est une

invention : il s'agit ainsi de déterminer les critères déterminants de l'invention et de chercher à savoir s'ils sont potentiellement applicables à l'output d'une IA.

L'article L. 611-10 du Code de la propriété intellectuelle définit les critères de brevetabilité suivants : (i) il faut une invention, qui est en soi un critère, qui doit (ii) être nouvelle, (iii) impliquer une activité inventive et (iv) être susceptible d'application industrielle.

- (i) L'invention est un produit ou un procédé qui apporte une nouvelle solution technique à un problème technique donné. 117 Du moment que l'output de l'IA répond à cette définition, il ne semble pas y avoir de difficulté particulière. Nous ne possédons pas les compétences techniques requises pour déterminer s'il s'agit d'une possibilité réaliste à court ou moyen terme ou non : au-delà de la particularité du questionnement théorique, est-il réellement envisageable que l'output d'une IA soit une invention au sens d'une nouvelle solution technique à un problème technique ? Il s'agit d'une question à creuser avec un spécialiste.
- (ii) Nouveauté de l'invention : il s'agit du critère objectif de déterminer si l'invention a déjà été divulguée ou non. Il n'y a pas de spécificité relative à l'output d'une IA, une invention pouvant évidemment se baser sur l'état antérieur de la technique, et donc d'autres inventions, du moment que celle-ci reste nouvelle.
- (iii) Activité inventive : l'invention doit être non seulement nouvelle au regard de l'état antérieur de la technique, mais également au regard de la pratique habituelle de l'homme du métier. Il faut que l'invention ne soit pas la suite logique des actions usuelles d'un homme du métier mais bien une disruption des ces habitudes. Ce référentiel est à préciser en fonction de l'utilisation de l'IA : l'homme du métier est éventuellement à considérer comme étant lui-même un utilisateur de l'IA.
- (iv) Application industrielle : il s'agit à nouveau d'un critère qui ne pose aucune spécificité relative à l'output d'une IA, l'invention issue de l'IA pouvant simplement répondre ou non à ce critère.

L'appréciation de l'activité inventive a fait l'objet d'une étude par l'Office européen des brevets (OEB). Il est à noter que les directives de l'OEB ne sont qu'indicatives en ce qui concerne l'interprétation française du droit français des brevets. Ces directives sont cependant généralement suivies par les tribunaux, dans un souci d'harmonisation du

¹¹⁷ Définition tirée du site de l'INPI, https://www.inpi.fr/fr/comprendre-la-propriete-intellectuelle/le-brevet/ce-qui-est-brevetable-ou-pas

droit. Selon cet organisme, la démarche à suivre pour déterminer si une invention implique une activité inventive est la suivante :

- détermination du domaine technique de l'invention pour permettre de limiter l'état de la technique ;
- détermination de l'homme du métier ;
- détermination de l'état de la technique le plus proche;
- détermination du problème technique objectif;
- détermination de l'évidence de l'invention.

Le problème qui se pose est donc dans la considération de l'homme du métier, qui n'est pas forcément équipé d'une IA. Ainsi, d'après les directives de l'OEB, l'homme du métier s'entend d'un praticien¹¹⁸:

- normalement qualifié, expert dans son domaine;
- qui possède les connaissances générales dans le domaine concerné;
- qui a une connaissance omnisciente de l'état de la technique ;
- qui dispose des moyens et de la capacité pour procéder à des travaux et expériences courants.

Ainsi, l'utilisation d'une intelligence artificielle, lorsqu'elle ne fait pas partie de la technique usuelle (ce qui est pour le moment le cas de la majorité des industries), constitue un pas de côté par rapport à la définition de l'homme du métier. Il serait donc judicieux d'adapter l'appréciation de l'activité inventive, soit de manière large en considérant que l'utilisation d'une IA est un moyen parmi d'autres de trouver une solution inventive, soit de manière restrictive en considérant que tout homme du métier dispose d'une IA équivalente.

Il semble ainsi que les critères de brevetabilité d'une invention soient plus accueillants pour l'output d'une IA que ceux de la protection par le droit d'auteur. La raison en est que l'appréciation de l'invention est réalisée en termes essentiellement objectifs. Cette appréciation postule un désintéressement de la genèse de la création qui peut aussi bien procéder d'une recherche systématique que du hasard ou encore d'un processus informatique. Dans ces conditions, la brevetabilité de l'output d'une IA ne semble pas poser de difficultés particulières, hormis lors de l'étude de l'activité inventive de l'invention, qu'il convient ainsi de préciser à l'aune des possibilités ouvertes par l'IA.

¹¹⁸ G-VII, 3. Homme du métier - Directives relatives à l'examen pratiqué du 28.9.2017 (European Patent Office)

1.4. Autres droits de propriété intellectuelle

Il convient de consacrer un bref moment de la réflexion pour s'attarder sur les éventuels enjeux posés par les autres droits de propriété intellectuelle, la question de la titularité étant traitée au point **1.5** :

- La marque ne pose a priori aucun enjeu particulier, étant donné que tout signe peut constituer une marque et que le test de validité de la marque repose (i) sur l'existence d'éventuelles antériorités et (ii) sur l'appréciation du signe en lui-même par rapport aux produits et services qu'il désigne (il ne doit pas être descriptif). Il est donc parfaitement possible d'envisager qu'une IA soit source d'inspiration pour le dépôt d'une marque, mais il n'y a pas de question spécifique relative au dépôt comme marque d'un output d'une IA.
- Le dessin et modèle pose des problèmes similaires à ceux du brevet. Il s'agit d'une protection accordée selon un critère objectif, celui de la nouveauté par rapport aux précédents dessins et modèles. Le dessin et modèle doit faire l'objet d'un dépôt. En ce sens, il s'agit donc de questions très similaires à celles traitées en brevet, et l'on pourra donc reproduire les raisonnements et solutions *mutatis mutandis*.
- Le droit sui generis ne pose a priori pas de question particulière : si l'IA est utilisée pour créer un grand nombre d'œuvres, celles-ci pourront être constituées en une base de données. Si cette base de données a été l'objet d'un investissement conséquent, la protection sera donc accordée à celui qui aura effectué cet investissement, qui doit être de nature économique. Il s'agit donc d'un droit où la question de l'intervention de l'IA n'intervient même pas, puisque le droit nait sur la personne ayant effectué l'investissement, quelle qu'elle soit.

1.5. Une création en quête de titulaire

Il a été montré que certains droits de propriété intellectuelle, et notamment le droit d'auteur, le brevet et le dessin et modèle, peuvent s'accommoder de la création par intelligence artificielle et voir leur protection accordée à l'output d'une IA (avec, dans certains cas, quelques réformes néanmoins). Il convient désormais de déterminer la personne titulaire des droits de propriété intellectuelle ainsi accordés.

À ce sujet, un préambule s'impose : les auteurs de ce rapport ne croient pas en la nécessité ou même l'opportunité d'accorder une personnalité à l'intelligence

artificielle. Cette idée fait son chemin chez certains auteurs,¹¹⁹ mais il nous semble improbable de réellement considérer qu'une IA, au stade de développement de ces technologies aujourd'hui, puisse réellement être considérée comme méritant le développement d'une personnalité juridique. L'IA actuelle est en effet un traitement probabiliste et statistique extrêmement avancé, tout en étant relativement simple au regard de la conscience humaine. La nécessité d'une fiction juridique telle que la personnalité morale ne se fera sentir que lorsque l'IA aura la possibilité de réellement se servir de ces droits de propriété intellectuelle dont elle aura été nommée la titulaire.

D'ici là, la question de la titularité des droits de propriété intellectuelle protégeant une création issue d'une IA doit donc être considérée selon nous comme relevant la question de la recherche de la personne, physique ou morale, la plus appropriée pour détenir ces droits parmi celles ayant participé au développement de l'IA et de son input, que cette participation soit effective ou économique.

Ainsi, la question de la titularité des droits de propriété intellectuelle peut se réduire à un champ limité de potentiels titulaires : le ou les développeurs de l'IA, l'entreprise employant le ou les développeurs de l'IA, le ou les créateurs de l'input, ou le titulaire des droits sur l'input, ainsi que l'éventuelle personne ayant supervisé l'apprentissage de l'IA.

1.5.1. La titularité en droit d'auteur

Le droit d'auteur nait sur la personne de l'auteur, du créateur. Cette personne est nécessairement une personne physique. Ce principe est issu de la concordance de divers textes, parmi lesquels le tout premier article du Code de la propriété intellectuelle, l'article L. 111-1, qui dispose que « l'auteur d'une œuvre de l'esprit jouit sur cette œuvre, du seul fait de sa création, d'un droit ». Il faut donc déterminer la (ou les) personne(s) pouvant potentiellement répondre à cette définition.

Dans la conception traditionnelle de l'originalité, l'auteur est celui qui marque l'œuvre de l'empreinte de sa personnalité. Si ce critère est conservé et appliqué, on peut tenter d'appliquer le distinguo suivant :

L'auteur peut être la personne qui a constitué la base d'entrainement des données ou qui a ordonné ces données, ou

=

¹¹⁹ Voir par exemple les écrits d'Alain Bensoussan, avec lesquels nous sommes en désaccord. Un exemple : https://alain-bensoussan.com/avocats/iot-business-forum-personnalite-robot/2017/06/14.

• L'auteur peut être la personne ayant réajusté le réseau neuronal de l'IA pour modifier l'output selon ses instructions.

Ces deux cas permettent ainsi de préserver l'utilisation du critère traditionnel d'empreinte de la personnalité de l'auteur, malgré le fait qu'une IA soit intervenue dans la création. Il s'agit néanmoins d'admettre que l'empreinte de la personnalité de ces deux personnes puissent se retrouver dans l'output, ce qui est loin d'être une évidence. Le droit d'auteur admet depuis un certain temps que l'empreinte de la personnalité d'un auteur puisse se retrouver dans une base de données, à condition que celle-ci ait été organisée d'une manière réfléchie. Cependant, il est fort peu probable que cette organisation ait un quelconque impact sur l'apprentissage de la machine, pour qui l'ordre des données importe peu. Il s'agirait donc de considérer que c'est le choix des données constituant la base en lui-même qui constitue la marque de l'auteur, ce qui est largement contestable. L'ajustement des poids du réseau neuronal est probablement plus propice, puisqu'il s'agit là d'une manifestation claire de la recherche de la manifestation d'une certaine vision dans l'output. Cependant, cela ne signifie pas que la personne effectuant la manipulation est bien elle-même l'auteur de cette vision, et par ailleurs, cela ne concerne in fine qu'un certain type de créations et d'IA. Ce critère manque donc en universalité.

Si en revanche la nouveauté devient le véritable prisme d'appréciation de l'originalité d'une œuvre, l'auteur ne devra plus être cherché comme étant celui ayant marqué l'œuvre de sa personnalité, mais bien comme étant celui ayant initié la création. Dans ce cas, l'hypothèse d'une cotitularité est probablement la seule envisageable dans le cas d'une pluralité de collaborateurs à l'output. Comme précisé au point 1.2.4, il s'agirait donc de considérer qu'il y a soit œuvre collaborative, soit œuvre collective, selon qu'une personne ait pris l'initiative de la direction de la création ou non. Il faudrait cependant considérer qu'il y a convergence entre la démarche du propriétaire de l'IA, du propriétaire des jeux de données, et des éventuelles autres personnes intervenant dans le processus de création.

A priori, les mécanismes actuels de dévolution des droits fonctionneraient dans le cadre de l'IA: si une entreprise est à l'origine de la création de l'œuvre en assurant la direction de cette création, le mécanisme de dévolution des droits en matière d'œuvre collective seront applicables. Dans le cas contraire, il s'agira de céder les droits des personnes physiques ayant participé à la création à la personne morale les employant, si celle-ci est propriétaire de l'IA. Ce genre de clauses ne sera pas différent des clauses actuellement en pratique.

Il convient par ailleurs de noter que l'article L. 113-1 créé une présomption simple de possession de la qualité d'auteur au bénéfice de « celui ou ceux sous le nom de qui

l'œuvre est divulguée ». Puisque l'auteur ne peut être qu'une personne physique, cette présomption de qualité d'auteur ne peut donc peser que sur des personnes physiques ayant divulgué l'œuvre. Il conviendra donc de modifier cet article afin de créer une présomption de *titularité des droits* sur la personne, physique ou morale, ayant divulgué l'œuvre sous son nom.

1.5.2. La titularité en droit des brevets

Le titulaire du brevet est le déposant de ce brevet, celui qui fait la demande d'obtention du brevet. En ce sens, le brevet ne pose pas de question de titularité spécifique, puisque le déposant peut être une personne morale : l'invention faite, à la juger protégeable, doit revenir au revendiquant. L'article L. 611-7 du Code de la propriété intellectuelle caractérise même une attribution à l'employeur des inventions réalisées par le salarié durant son travail. Il semble ainsi que les questions de titularité soulevées en droit d'auteur soient correctement résolues en droit des brevets.

En revanche, il convient de noter que le dépôt du brevet doit mentionner le nom de l'inventeur, personne physique. L'article R. 612-10 du Code de la propriété intellectuelle prévoit ainsi que la demande de brevet doit faire figurer « la désignation de l'inventeur », et, lorsque l'inventeur n'est pas le demandeur, « les nom, prénoms et domicile de l'inventeur ainsi que la signature du demandeur ou de son mandataire ». Le défaut de divulgation ou l'erreur dans la divulgation de cette identité sont sanctionnés par un rejet de la demande.

L'inventeur est donc supposé être une personne physique identifiée, puisque les mentions obligatoires ne comprennent pas d'alternatives pour une personne morale. Il y a ainsi une condition tacite dans le droit des brevets qui suppose toujours que l'invention procède d'une activité humaine – il s'agit ainsi d'un recoupement avec le droit d'auteur où cette condition tacite existe aussi.

Ainsi, si le problème de la titularité du brevet en lui-même ne pose pas de problème, celui-ci appartenant au revendiquant, il s'agit néanmoins de déterminer la personne qui pourra être qualifiée d'inventeur. Une possibilité ici est de consacrer l'intervention des différentes personnes ayant pu avoir un impact sur l'output. Ces personnes restent le développeur de l'IA et la personne ayant conçu le jeu de données. Puisque l'inventeur est une personne physique, il faut écarter les cas où des entreprises seraient propriétaire de ces divers éléments, à moins de considérer qu'une réforme de ce point soit nécessaire.

2. Ébauche de solutions

Il s'agit de nouveau de tenter de proposer des solutions adaptées aux enjeux de la protection de l'output de l'IA par la propriété intellectuelle. Ceux-ci peuvent être déclinés selon les deux grands droits susceptibles d'être appliqués à l'output d'une IA et de poser des problèmes, le droit d'auteur et le brevet.

En droit d'auteur, les enjeux sont (i) le risque de dilution de la notion de création au regard des possibilités infinies de création de l'IA, mis en opposition avec (ii) le risque de désintéresser les concepteurs d'IA créatrices et d'entraver l'innovation dans ce secteur alors mêmes que les potentialités de rentabilité économiques sont fortes (particulièrement dans le secteur audiovisuel et musical), et (iii) la détermination de la titularité du droit d'auteur si celui-ci est accordé à l'œuvre : programmeur, propriétaire de la base de données, propriétaire des données, ou autre ?

En matière de brevet, (i) le problème de la titularité n'est pas posé en tant que tel, mais le dépôt d'un brevet requiert néanmoins la précision d'un inventeur personne physique, soulevant des questions similaires à celles posées en droit d'auteur. Par ailleurs se pose également (ii) la question de la protection par le droit des brevets des outputs de l'IA compte tenu des potentielles difficultés d'application du critère de l'activité inventive, et (iii) de manière similaire au droit d'auteur, un risque de concentration des moyens d'invention au sein d'oligopoles.

2.1. Solutions en droit d'auteur

Nous proposons deux approches afin de répondre aux enjeux soulevés. La première consiste à proposer quelques pistes de réforme du droit d'auteur actuel afin de le rendre plus adapté aux créations de l'IA. La seconde est de créer un droit de propriété intellectuelle spécifique aux créations par l'IA.

2.1.1. Réforme du droit d'auteur

La première piste que nous proposons est d'apporter quelques réformes au droit d'auteur actuel afin de le rendre plus praticable vis-à-vis des créations de l'IA.

2.1.1.1. Sur la caractérisation de l'œuvre

On rappelle que le principal enjeu de la caractérisation de l'œuvre créée par l'IA est de trouver une intervention humaine dans l'output, et ce alors que l'intervention humaine reste un critère déterminant du droit d'auteur. Le critère de la forme est en effet

parfaitement opérant pour un output d'intelligence artificielle, le numérique étant accepté comme étant une forme.

Il n'y a de fait qu'une seule solution plausible à la résolution de cette problématique et qui ne remette pas complètement en cause le droit d'auteur : amoindrir l'exigence en ne requérant que la participation, à un stade de la création, d'un être humain, même en tant que superviseur. La suppression de l'exigence aboutirait à complètement remettre en cause l'essence même du droit d'auteur, qui reste dans sa conception lié à une personne physique humaine.

Comme détaillé dans les développements précédents, il y a pour le moment nécessairement une intervention humaine *a minima* dans le choix de l'input de l'IA, et parfois dans le réajustement de certains critères. Plus largement, on peut considérer que les choix de programmation effectués pour créer l'IA peuvent être pris comme une intervention humaine dans le processus de création. Le point prégnant de cette réflexion est que, pour le moment et pour le futur prévisible, il n'y aura pas d'IA sans intervention humaine à un stade ou un autre de la production. L'amenuisement du critère de l'intervention humaine permettrait donc d'encapsuler les outputs de l'IA sans pour autant complètement bouleverser les notions préexistantes.

Nous proposons donc de minimiser l'exigence d'intervention humaine dans la caractérisation d'une œuvre. Cette minimisation peut notamment ressortir d'une réécriture de l'article L. 111-2 du Code de la propriété intellectuelle ainsi :

« L'œuvre est réputé créée, indépendamment de toute divulgation publique, du seul fait de la réalisation, même inachevée [ou même sous sa supervision ou par l'expression de ses choix], de la conception de l'auteur ».

2.1.1.2. Sur l'originalité

Une œuvre protégeable ne se verra accorder le bénéfice de la protection par le droit d'auteur que si celle-ci est originale. Comme démontré au point **1.2.3**, l'originalité est un problème pour la protection des œuvres réalisées par une IA tant que celle-ci est considérée comme étant « *l'empreinte de la personnalité de l'auteur* ». Cette conception subjective de l'originalité, ancrée dans la tradition française du droit d'auteur, exclut de fait les œuvres créées en grande partie par une IA. Il est donc nécessaire, afin d'appréhender les œuvres créées par une IA, de modifier l'interprétation de la notion d'originalité.

Il convient ainsi de dépasser la conception traditionnelle et d'adopter un critère plus objectif. C'est déjà ce qu'a initié la jurisprudence européenne au moyen des arrêts Infopaq¹²²² et Painer¹²¹ en définissant l'œuvre originale comme « une création intellectuelle propre à son auteur ». Pour la jurisprudence européenne, une œuvre est donc originale lorsqu'elle bénéficie d'un apport intellectuel de l'auteur. Cette définition permet notamment d'inclure plus aisément l'art contemporain qu'avec le critère traditionnel. Il pourrait également trouver à s'appliquer dans le cas des œuvres créées par une IA, puisqu'il a été montré que ces œuvres découlent forcément d'une série de choix effectués par des personnes physiques. Ces choix pourraient ainsi être considérés comme étant un apport intellectuel de l'auteur.

Une autre solution consisterait à écarter le critère de l'originalité au profit de celui de la nouveauté, déjà utilisé en brevet. Il s'agirait cependant d'une réforme en profondeur du droit d'auteur qui consisterait à remettre en cause certains de ses fondements. Cette solution nécessite également de définir un référentiel de base qui servirait de comparaison pour rechercher l'aspect nouveau de l'œuvre. S'il s'agit ainsi d'une possibilité, la consécration d'une conception plus objective de l'originalité reste la solution la plus consensuelle.

Nous proposons de consacrer la conception objective de l'originalité en introduisant clairement le critère dans le Code de la propriété intellectuelle, ce qui n'est pas encore le cas. Cela peut notamment être fait en modifiant l'article L. 111-1 du Code de telle manière : « L'auteur d'une œuvre de l'esprit jouit sur cette œuvre, [si celle-ci bénéficie de l'apport intellectuel de l'auteur, et] du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous ».

Il est également possible de complètement mettre de côté le critère de l'originalité pour consacrer une conception objective de la nouveauté, bien que cela soit une solution plus propice à la controverse : « L'auteur d'une œuvre de l'esprit [nouvelle] jouit sur cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous ».

¹²⁰ CJUE, 16 juillet 2009, *Infopaq*, C-5/08.

¹²¹ CJUE, 1^{er} décembre 2011, *Painer*, C-145/10.

2.1.1.3. Sur la titularité du droit et le statut de l'œuvre

Une fois le droit d'auteur adapté pour mieux appréhender les œuvres créées par une IA, il convient de régler le statut des œuvres ainsi protégées par rapport à l'input de l'IA et de déterminer le ou les titulaires des droits ainsi concédés.

À ce sujet, il convient de confronter la création finale aux apports successifs qui ont permis sa création : la programmation de l'IA, l'input, composé d'une ou de plusieurs bases de données, la constitution d'un corpus d'apprentissage propre et l'ajustement éventuel des paramètres de l'IA. Comme rappelé au point 1.5.1, la titularité est présumée acquise au bénéfice de celui qui divulgue l'œuvre, présomption simple qui peut notamment être mise de côté lorsque l'auteur véritable prouve qu'il a réalisé l'acte créatif essentiel. Le fondement de la répartition des droits d'auteur repose ainsi sur l'idée de « maitrise légitime » de la création.

Il s'agit donc de procéder à une appréciation casuistique, au cas par cas, de la participation de chaque personne à la création : la titularité dépend de la marge de manœuvre de chaque participant à la chaine de création par l'IA. Selon les cas, les droits sur l'œuvre peuvent donc être attribués soit respectivement, soit cumulativement, au programmeur, au propriétaire de l'input ou à l'utilisateur de l'IA. Les présomptions et dévolutions de titularité peuvent fonctionner dans ces cas de la même manière qu'en droit d'auteur classique, à partir du moment où les œuvres sont bien comprises dans le prisme du droit d'auteur. Le contrat reste donc a priori le mécanisme le plus sûr pour les différentes parties à la création pour gérer les droits d'auteur sur les créations de l'IA, qui seraient alors pour la plupart des œuvres collaboratives.

Au-delà de ces applications du droit d'auteur classique, il semble néanmoins que la majeure partie des cas de création seront dirigés par une personne effectuant les choix principaux : il semble en effet assez rare que la création par IA soit le fruit d'actions non concertées et non coordonnées entre un programmeur, un propriétaire de données et un utilisateur de l'IA. Il est ainsi probable que la plus grande partie des créations par IA tomberont dans le champ de l'œuvre collective, dont les limites peuvent également être définies par contrat.

Il reste cependant la possibilité d'une œuvre à laquelle plusieurs personnes auront participé sans pour autant se concerter ou suivre une ligne directrice commune, au moyen de l'IA. Il s'agirait ainsi d'un autre niveau d'œuvre transformative avec plusieurs coauteurs non coordonnés. Dans ce cas il convient de revenir à la notion première de présomption de titularité à la personne ayant divulgué l'œuvre, à charge pour les autres auteurs de contester cette titularité le cas échéant.

Il ne nous semble pas nécessaire de modifier les mécanismes de titularité du droit d'auteur, qui peuvent s'accommoder de la création par l'IA tant que les œuvres issues de l'output sont bien reconnues. Il s'agit cependant de laisser libre cours à la liberté contractuelle et à l'appréciation casuistique de chaque création.

2.1.2. Nouveau droit d'auteur repensé

Outre les solutions de réformes ciblées au droit d'auteur formulées ci-dessous, il nous parait opportun de réfléchir à un droit d'auteur repensé pour prendre en compte l'ensemble des enjeux de l'IA. En effet, la solution visant à modifier légèrement le droit d'auteur actuel pour qu'il englobe à coup sûr les créations de l'IA aboutirait à confier des durées de protection extrêmement longues à un énorme ensemble d'œuvres, ce qui peut aboutir à une dilution de la notion de création, comme décrit au point 1.1. Nous proposons donc un régime de droit d'auteur spécifique aux créations de l'IA, qu'il s'agirait dans l'idéal d'introduire à un niveau européen afin de maintenir l'harmonisation du droit de la propriété intellectuelle au sein de l'UE.

Ce droit aurait ainsi pour but de régler l'ensemble des enjeux de l'output de l'IA tout en conférant une certaine protection aux créations issues de l'IA. Le désavantage de cette solution reste qu'il s'agit d'un projet très, voire trop, ambitieux et requérant un important processus législatif.

Les caractéristiques de ce droit spécifique aux créations de l'IA seraient les suivantes :

- <u>Durée de la protection</u>: plus courte que le droit d'auteur actuel, afin d'éviter la mainmise des industries culturelles. Proposition de se calquer sur le brevet, soit 20 ans après la première divulgation.
- Droit moral: pas de droit moral. La figure de l'être humain est minimisée dans la création par l'IA, et le droit moral a donc beaucoup moins de raison d'être dans ce droit spécifique.
- <u>Droits patrimoniaux accordés</u>: mêmes droits qu'en droit d'auteur traditionnel.
- Droit conféré sur enregistrement pour éviter l'inflation des créations : on peut même penser à jouer sur le coût de l'enregistrement pour éviter l'enregistrement d'un ensemble trop important d'œuvres.

- Ce droit d'auteur n'est accordé que si l'œuvre est le produit de choix libres et créatifs de la part des auteurs : l'œuvre doit constituer une nouveauté en tant que distinction par rapport à l'état antérieur de l'art.
- Le titulaire des droits est donc <u>la personne ayant procédé à l'enregistrement</u>, à charge pour elle d'avoir obtenu l'autorisation pour ce faire.

2.2. Solutions en droit des brevets

Comme il l'a été montré au point **1.3**, la confrontation entre le droit des brevets et les créations de l'IA pose moins de questions qu'en droit d'auteur, notamment du fait que la notion d'invention est appréciée sur des critères plus objectifs que ceux du droit d'auteur et que l'enregistrement écarte tout débat sur la titularité. Il convient néanmoins d'apporter quelques ajustements à la notion d'activité inventive et à l'exigence de désignation de l'inventeur. Nous pensons également que le droit de la concurrence peut trouver à s'appliquer pour limiter les effets de concentration.

2.2.1. Modifications du droit des brevets

2.2.1.1. Activité inventive

Ainsi que détaillé au point **1.3.(iii)**, le droit des brevets est généralement ouvert à la reconnaissance des œuvres issues de l'IA, à l'exception de la condition de l'activité inventive. L'activité inventive fait partie des conditions explicitement citées par le Code de la propriété intellectuelle et ne peut donc être supprimée sans remettre entièrement en cause le droit des brevets actuel.¹²²

Nous pensons que la notion d'activité inventive, dont l'appréciation repose sur les fictions juridiques de l'homme du métier et de l'état de l'art, peut justement se modifier de deux manières en ajustant les appréciations que l'on fait de l'homme du métier :

• soit de manière large et permissive, en considérant que l'état de l'art exclut l'utilisation d'une IA. Dans ce cas, l'objet de la demande de brevet sera examiné comme aujourd'hui, et l'utilisation de l'IA dans le processus inventif ne sera pas pris en compte;

¹²² Article L. 611-10 du Code de la propriété intellectuelle.

• soit de manière plus restrictive, en considérant que l'homme du métier dispose également d'une IA et d'un jeu de données équivalents. Dans ce cas, l'activité inventive se recherche justement dans le fait que l'obtention de l'invention requiert une étape supplémentaire à la simple utilisation d'une IA, qui pourrait révéler un grand nombre d'inventions par son application à un jeu de données.

Le but du brevet étant bien de protéger une invention dont l'obtention relève d'un certain mérite, puisqu'elle a nécessité une « activité inventive », nous sommes de l'opinion que l'homme du métier doit disposer des mêmes outils que l'inventeur, afin de déterminer si celui-ci a bien fait preuve d'une activité inventive.

Nous proposons donc de modifier l'appréciation de l'activité inventive en précisant que celle-ci doit s'apprécier au regard des outils utilisés par l'inventeur, y compris le recours à une IA. L'activité inventive doit résider dans le fait qu'un homme du métier disposant de la même IA et des mêmes données n'aurait pas forcément découvert l'invention.

2.2.1.2. Identité de l'inventeur

Ainsi que détaillé au point **1.5.2**, le brevet appartient à son déposant, mais ledit dépôt doit nécessairement faire figurer l'identité de l'inventeur si celui-ci n'est pas le déposant. Il convient donc, dans la chaine de parties prenantes à la création de l'output de l'IA, de déterminer la ou lesquelles peuvent prétendre à la qualification d'inventeur.

Cette désignation est essentiellement informative puisque l'inventeur ne dispose pas de droits sur le brevet. Il n'en reste pas moins que l'inventeur doit, pour le moment, être une personne physique identifiée par ses noms, prénoms et adresse. L'output de l'IA, cependant, ne sera pas forcément l'œuvre d'une seule personne. La pluralité d'inventeurs est déjà intégrée au brevet européen, mais ne figure pas clairement dans le Code de la propriété intellectuelle, ce qu'il faut donc corriger.

L'output de l'IA ne sera par ailleurs pas forcément l'œuvre d'une personne physique, ou plutôt, d'une personne physique seulement : il y aura forcément intervention d'une personne physique, mais pas forcément en son nom propre. Il est ainsi beaucoup plus probable que le programmeur ou que le propriétaire des données de l'input soit ou travaille pour une personne morale.

À ce sujet, il convient de s'inspirer du régime existant à propos des inventions de salariés : même pour les inventions de mission, prévues dans le cadre du contrat de travail, l'inventeur salarié a le droit d'être cité comme tel. L'implication est donc que

même lorsqu'une personne morale est à l'initiative de l'invention, la personne physique à la réalisation reste considérée comme inventeur. Afin de ne pas bouleverser un régime préexistant, il convient donc d'adapter la divulgation de l'inventeur pour préciser que lorsque l'invention a été obtenue via une intelligence artificielle, l'ensemble des personnes physiques ayant participé à cette obtention doivent être citées comme telles, avec la précision de leurs apports respectifs.

Nous proposons donc de réécrire l'article R. 612-10 ainsi :

3° La désignation de l'inventeur : toutefois, si le demandeur n'est pas l'inventeur ou l'unique inventeur, la désignation est effectuée dans un document séparé contenant les nom, prénoms et domicile de[s] inventeur[s], ainsi que la signature du demandeur ou de [leur] mandataire ; [...]

Si l'invention a été découverte au moyen d'un procédé algorithmique, les inventeurs sont les personnes physiques ayant participé à la création de l'algorithme et à son apprentissage. Elles sont désignées comme telles dans le document de désignation de l'inventeur.

2.2.2. Atténuation des effets de concentration

À l'instar du droit d'auteur, il existe un véritable risque de concentration des moyens de production entre les mains d'une poignée d'entreprises. Ce risque est lié à l'IA de manière générale, puisque l'on assiste déjà à la concentration des jeux de données et des capacités de calcul entre les mains de quelques acteurs. Il y a cependant un accroissement de ce risque si le droit des brevets reconnait les inventions issues de l'IA, puisque cela implique que la majeure partie de la production inventive sera concentrée entre les mains de ces acteurs qui bénéficient déjà d'un avantage concurrentiel dans d'autres domaines.

Il convient donc d'appliquer les mécanismes du droit de la concurrence afin d'atténuer les effets de concentration sur l'innovation. À ces fins, il pourra être fait usage des outils de sanctions des abus de position dominante, mais également de la théorie des facilités essentielles.

Cette théorie est issue du droit américain de la concurrence, mais a été peu à peu intégrée au droit européen et français, notamment par le biais de la sanction des abus

de position dominante.¹²³ Le principe de cette théorie est qu'une entreprise en situation de monopole ou de position dominante sur un marché et qui détient un élément essentiel à l'accès à ce marché peut être contrainte de permettre l'accès à cet élément essentiel, afin de « protéger le jeu de la concurrence sur un marché aval, amont ou complémentaire ».

Compte tenu des impacts d'une telle théorie sur la liberté contractuelle, la liberté d'entreprise et le droit de propriété, l'application des facilités essentielles est extrêmement limitée par la jurisprudence. Ainsi, pour être qualifiée d'essentielle, l'élément en cause doit être :

- indispensable ou strictement nécessaire à l'entrée sur le marché, ce qui signifie qu'aucune alternative technique ou économique n'existe. L'appréciation ne se fait que sur l'aspect purement matériel de la possibilité : si une alternative moins avantageuse existe, l'élément en cause ne sera pas considéré comme étant essentiel¹²⁴;
- impossible ou extrêmement difficile à reproduire de manière économiquement raisonnable¹²⁵ : afin de justifier l'atteinte aux droits fondamentaux cités ci-dessus, il faut que l'infrastructure essentielle ne puisse être obtenue d'une autre manière que par le biais de son propriétaire.

Cette théorie peut être résumée par ce commentaire de la Cour de cassation :

« Ce n'est que si une ressource détenue par une entreprise (ou un groupe d'entreprises) dominante revêt un caractère essentiel que son libre accès, s'il est possible, doit être ouvert et offert dans des conditions justes et non discriminatoires aux entreprises pour lesquelles cet accès est incontournable. »¹²⁶

Ainsi, au cas où l'IA deviendrait une véritable nécessité pour le développement d'inventions nouvelles, il pourrait être fait de l'application de la théorie des facilités essentielles pour ouvrir l'accès, soit aux algorithmes apprenant, soit aux données nécessaires à leur apprentissage. Cela ne devrait cependant être le cas que si l'IA est véritablement devenue essentielle, au sens de la jurisprudence de la Cour de cassation.

Rapport annuel de la Cour de cassation, 2005, https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2005_582/quatrieme_partie_jurisprudence_cour_590/activites_economiques_commerciales_financieres_603/droit_concurrence_7870.html.

¹²⁴ Cass. Com., 12 juillet 2005, n° 04-12.388.

¹²⁵ Avis n° 02-A-08 du Conseil de la concurrence du 22 mai 2002.

¹²⁶ Rapport annuel de la Cour de cassation, ibid.

Bibliographie

Avis, lignes directrices, délibérations

- Délibération CNIL n°2017-023 du 16 février 2017 portant avis sur un projet de décret relatif aux modalités de communication des règles et caractéristiques des traitements algorithmiques.
- Guidelines on the right to data portability, Article 29 Data Protection Working Party, 2017.
- Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 2017.
- Guidelines on Data Protection Officers ("DPOs"), Article 29 Data Protection Working Party, 2017.
- Guidelines on Automated Individual-decision making and Profiling for the purposes of Regulation 2016/679, Article 29 Data Protection Working Party, 2017.
- Opinion 05/2014 on Anonymisation Techniques, Article 29 Data Protection Working Party, April 2014.
- Opinion 03/2013 on Purpose Limitation, Article 29 Data Protection Working Party, 2013.
- Anonymisation, managing data protection risk, code of practice; Information Commissioner's Office, 2012.
- Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing, CNIL, 2012.
- Opinion 05/2012 on Cloud Computing, Article 29 Data Protection Working Party,
 2012.
- Avis 1/2010 sur les notions de « responsable de traitement » et de « soustraitant », Groupe de Travail « Article 29 » sur la Protection des Données, 2010.
- Avis n°15/2011, Groupe de l'article 29, 2011.
- CNIL, délib. n°2013-420, 3 janv. 2014.

- Mesure de la diversité et protection des données personnelles : les dix recommandations de la CNIL, CNIL, 2007.
- G-VII, 3. Homme du métier Directives relatives à l'examen pratiqué du 28.9.2017 (European Patent Office)

Rapports

- Pour une intelligence artificielle maîtrisée, utile et démiystifiée, Claude de Ganay, Dominique Gillot, Office Parlementaire d'Evalutation des Choix Scientifiques et Technologiques, 2017.
- Big data, artificial intelligence, machine learning and data protection, Information Commissioner's Office, Version 2.2, 2017.
- Artificial Intelligence, Robotics, Privacy and Data Protection, EDPS, octobre 2016.
- Robotics and artificial intelligence, Fifth report of Session 2016-17, House of Commons, Science and Technology Comittee.
- Artificial Intelligence and Life in 2030, Report of the 2015 Study Panel, 2016.
- Privacy by design in Big data, An overview of privacy enhancing technologies in the era of Big data analytics, ENISA, 2015.
- Big data and Privacy. A technological Perspective; President's Council of Advisors on Science and Technology, White House, May 2014.
- *Mission sur l'exploration de données* du Conseil supérieur de la propriété littéraire et artistique, mission présidée par Jean Martin et rapportée par Liliane de Carvalho, juillet 2014.
- Study on the legal framework of text and data mining (TDM), by Jean-Paul Triaille,
 De Wolf & Partners, March 2014
- *L'informatique et le droit d'auteur*, Rapport du Congrès de l'Association Littéraire et Artistique Internationale, 1989

Travaux de recherche et articles pertinents

- Law and Regulation of Artificial Intelligence and Robots: conceptual framework and normative implications. Nicolas Petit, 2017.
- Artificial Intelligence and the "Good Society": the US, EU, and UK approach, C. Cath, S. Wachter, B. Mittelsdadt, M. Taddeo, L. Floridi, 2017.
- The Regulation of Artificial Intelligence, João Paulo de Almeida Lenardon, Tilburg Institute for Law, Technology and Society, 2017.
- Slave to the algorithm? Why "a right to an explanation" is probably not the remedy you are looking for, Lilian Edwards & Michael Veale, Duke Law and Technology Review, 2017.
- Les usages de l'Intelligence artificielle, Olivier Ezratty, 2017.
- Homo Juridicus est-il soluble dans les données ?, Antoinette Rouvroy, 2017.
- Deep neural networks can detect sexual orientation from faces, Yilun Wang,
 Michal Kosinski, American Psychological Association, 2017.
- Algorithmic Bias? An empirical study into apparent gender-based discrimination in the display of STEM career ads, A. Lambrecht, C. Tucker, 2017.
- Why a right to explanation to automated decision-making does not exist in the General Data Protection Regulation, S. Watcher, Brent Mittelstadt, Luciano Floridi, Oxford Internet Institute, 2017.
- How the machine "thinks": Understanding opacity in machine learning algorithms,
 Jenna Burrell, Big data & Society, 2016.
- Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures, Matt Fredrickson, Somesh Jha, Thomas Ristenpart, CCS, 2016.
- The Europeanisation of Data Protection Law, Orla Lynskey, Cambridge Yearbook of European Legal Studies, 2015.
- Comments of the Electronic Privacy Information Center to the Office of Science and Technology Policy, Electronic Privacy Information Center, 2014.
- Notice and Consent in a World of Big data, Fred Cate, Victor Mayer-Schönberger, International Data Privacy Law, 2013.
- Adversarial Machine learning, Ling Huang, Anthony D. Joseph, Blaine Nelson, Benjamin I.P. Rubinstein, J.D. Tygar, 4th ACM Workshop on Artificial Intelligence and Security, 2011.

- Data mining et statistique décisionnelle l'intelligence des données, Stéphane Tuffery, Editions Technip, 2012.
- Journal Article Mining, Eefke Smit and Maurits van der Graaf, Publishing Research Consortium, May 2011.
- Suggestion for a green paper on legal issues in robotics, C. Leroux et al., euRobotics Contribution to Deliverable D3.2.1 on ELS issues in robotics, 31 December 2012.
- Law and Regulation of Artificial Intelligence and Robots: Conceptual Framework and Normative Implications, N. Petit, 9 march 2017.
- Durand, E. (2016). Chapitre 3 Des créateurs sous influence. Dans E. Durand, L'attaque des clones: La diversité culturelle à l'ère de l'hyperchoix (pp. 43-56). Paris: Presses de Sciences Po (P.F.N.S.P.).
- Rosenberg, A., « Art is about surrender. Stop asking for it to be custom-tailored. », *The Washington Post*, 15 August 2016.
- Heinch, N., Être artiste. Les transformations du statut des peintres et des sculpteurs, Paris, Klincksieck (rééd. 2005, 2012).
- Larrieu, Jacques, « Les robots et la propriété intellectuelle », *Propriété Industrielle*, Lexis Nexis, Février 2013 n° 2.
- A.-E. Kahn, Fascicule 1190 : Objet du droit d'auteur Titulaires du droit d'auteur, JCl. Propriété Littéraire et Artistique, Lexis Nexis, Actualisation septembre 2008.