INTELLIGENCE ARTIFICIELLE :
DÉCIDER EN TOUTE CONNAISSANCE DE DONNÉE

Etude réalisée par
LE CERCLE DE LA DONNÉE

INTELLIGENCE ARTIFICIELLE : DÉCIDER EN TOUTE CONNAISSANCE DE DONNÉE

ETUDE RÉALISÉE PAR LE CERCLE DE LA DONNÉE

Le nouveau « *printemps* » de l'Intelligence Artificielle (« IA »). S'appuyant sur une technologie déjà ancienne, c'est aujourd'hui que l'IA connaît un engouement sans précédent en raison du développement récent et fulgurant des microprocesseurs dédiés aux calculs et d'une abondance de données disponibles. L'idée de développer une intelligence artificielle n'est pas neuve, loin s'en faut. Imaginée à la fin de la seconde guerre mondiale, elle a réellement pris corps avec le développement des algorithmes d'apprentissage[1], dans les années 80, fonctionnant selon un mécanisme de « renforcement » nécessitant de vastes capacités de calcul, à l'époque rares et coûteuses. C'est ainsi que l'IA n'a pas suscité d'intérêt particulier en dehors de l'univers de la recherche. Toutefois, à cet « hiver » a succédé un véritable « printemps » de l'IA. En effet, en réponse à la formidable déferlante de données numériques de la fin des années 2000 – ou « *révolution big data* » – résultant de l'utilisation généralisée des outils informatiques (par les administrations, les entreprises et les particuliers), les fabricants ont accompagné le mouvement par un progrès continu aboutissant à des capacités décuplées de calcul de leurs processeurs, centraux ou dédiés. Les résultats, rendus publics par certaines entreprises, semblent extrêmement prometteurs : taggage automatique de vidéos, reconnaissance automatique de langage (multi-locuteur).

Avant de qualifier l'IA d'« intelligente », la réflexion s'impose. Le choix d'attribuer le terme « intelligence », pour nommer ce type de technologie, n'est pas anodin : il induit que celle-ci réponde à la définition d'« intelligence », qui mérite d'être rappelée ; ce rappel permettra ensuite de mesurer le degré d'intelligence des technologies actuellement disponibles, et dont nous verrons que les données qui les nourrissent sont clés pour permettre de parvenir à des résultats fiables et cohérents. Ce rappel conceptuel permettra aussi de s'interroger sur l'opportunité et les risques de confier certaines tâches intellectuelles à des machines, en particulier lorsqu'il s'agit de l'expression du libre arbitre qui caractérise la dimension morale de l'intelligence humaine.

La nécessité d'une approche de l'IA par la donnée. Convaincu que pour être « intelligente », l'IA doit utiliser les bonnes données, le Cercle a souhaité mener une réflexion sur les dimensions technologique, économique, éthique et juridique de la donnée utilisée dans le cadre de projets d'intelligence artificielle. Fort de cette étude approfondie, le Cercle de la Donnée émet 12 propositions pour formaliser et définir une politique et des bonnes pratiques en matière de gestion de la donnée au service de l'intelligence artificielle, au niveau français et européen. Ces 12 propositions ont vocation à être largement diffusées, démarche indispensable, à notre sens, à l'intelligibilité de cette matière que les professionnels de tous horizons doivent s'approprier. Une réflexion qui devra se poursuivre…

1 Typiquement, l'algorithme de rétro-propagation du gradient (GPB : Gradient Back Propagation)

INTELLIGENCE ARTIFICIELLE (IA)

12 PROPOSITIONS

POUR UNE MEILLEURE UTILISATION DE LA DONNÉE

1. Définir et constitutionnaliser des principes fondamentaux que les technologies d'IA devront respecter (droits numériques de l'Homme).

2. S'engager dans une réflexion visant à définir des règles éthiques qui puissent s'appliquer dans le monde numérique.

3. Travailler à l'élaboration d'un texte général applicable aux données à caractère non personnel, complétant le Règlement communautaire 2018/807.

4. Définir une politique publique d'investissement massif visant à créer un champion étatique ou européen de l'IA, à l'image des succès créés dans les secteurs aéronautique ou énergétique.

5. Structurer une filière de la science de la donnée aboutissant à l'instauration de nouvelles professions règlementées.

6. Etudier l'opportunité d'une obligation légale imposant aux fournisseurs d'IA de déposer une documentation permettant d'expliquer le mode de fonctionnement et les résultats produits par l'IA, qui sera approuvée par une autorité publique française ou européenne, préalablement à sa mise en production, laquelle sera dotée de moyens suffisants pour attirer des spécialistes chevronnés.

7. Mettre en place des certifications ou labels qui seront gages de transparence et de confiance pour les utilisateurs.

8. Etablir des référentiels (thésaurus et ontologies) caractérisant des typologies de données en fonction de leur nature (dépendant de la façon dont elle a été captée, inférée ou créée), leur usage (finalité) et leur criticité (sous l'angle de la confidentialité et de la continuité d'activité), pour faciliter l'interopérabilité des systèmes et des activités, et en assurer la diffusion notamment à travers l'école et l'université.

9. Avant toute modélisation impliquant des données, définir le périmètre des données nécessaires et légitimes en s'assurant de leur bonne représentativité.

10. Introduire une phase de contrôle à l'issue du pré-traitement des données afin de s'assurer de leur neutralité et de ne pas introduire de biais.

11. Mettre en qualité (standardisation, exactitude ou représentativité) les données pour s'assurer que le système fonctionne.

12. Documenter de façon précise l'ensemble des données, du contexte et des traitements qui ont permis de construire le jeu de données et rendre cette documentation accessible à toutes les personnes qui ont à en connaître.

SOMMAIRE

I. DÉFINITIONS

Intelligence Artificielle : Un emballement actuel insuffisamment éclairé, propice aux fantasmes.

L'engouement actuel pour l'intelligence artificielle trouve sa source dans les nombreuses promesses que formulent ses adeptes : améliorer la diffusion et le traitement de l'information, faire progresser la médecine et allonger la durée de la vie… Tout ceci en automatisant et accroissant l'efficacité de certaines tâches réalisées jusqu'à présent par des êtres humains dont certaines touchent aux attributs les plus essentiels de ces derniers (la reconnaissance, l'analyse, voire même la décision…)., Au contraire, certains rejettent massivement cette évolution, en brandissant les pires scénarios dont quantité d'œuvres de science-fiction se sont fait l'écho depuis la seconde moitié du 20ème siècle, parfois non sans raison. Ce débat est aujourd'hui encore trop peu audible en raison du manque d'intelligibilité des concepts qui le sous-tendent, faute d'avoir été expliqués avec clarté et impartialité, en raison de la (relative) jeunesse de la matière et de son confinement dans les sphères de la recherche. Pour cette raison et fidèle à ses convictions plaçant la meilleure compréhension des concepts et des outils numériques comme élément central d'un renouveau civilisationnel, le Cercle de la Donnée a souhaité débuter la présente étude par une définition des termes de son sujet.

Le champ lexical de l'IA, emprunté à celui du monde biologique, appelle à examiner la justesse du parallèle entre « monde naturel » et « monde artificiel ».

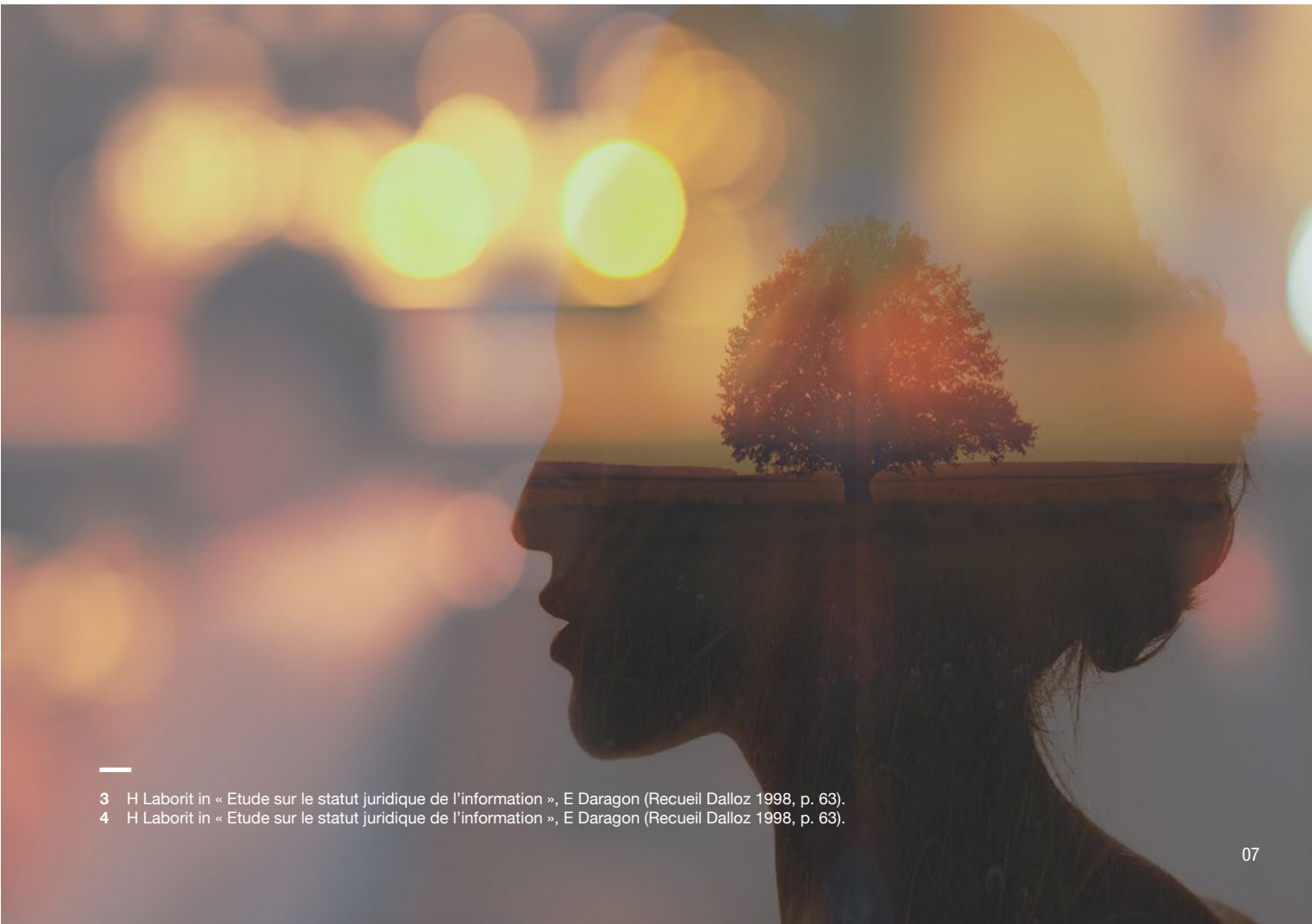
Pour décrire les progrès récents des technologies de traitement de l'information, les médias se sont emparés d'un terme désignant une réalité empruntée au monde naturel – *« l'intelligence »* – ainsi que le champ lexical associé (*« apprentissage », « autonomie », « décision »…*). C'est une première, puisque les inventions majeures des précédentes révolutions technologiques avaient été désignées par de nouveaux termes (*« automobile », « avion »…*), et non par des reprises de réalités naturelles avec lesquelles – bien que s'en inspirant parfois – elles s'en distinguaient (*« cheval » ou « oiseau*[2]*» « artificiel »…*). Or, l'ajout de l'adjectif *« artificiel »* ne suffit pas à dissiper le possible malentendu de la formule. En effet, synonyme de « imité » ou « feint », l'adjectif *« artificiel »* est aussi désigné pour décrire ce qui est *« fabriqué »* par l'homme pour imiter la nature dans les domaines les plus variés (tel le *« lac artificiel »*) et, parfois, se substituer à elle (tel le *« cœur artificiel »*). Aussi, la formule *« intelligence artificielle »* n'est pas neutre, car elle peut laisser entendre que cette(ces) technologie(s) peut(peuvent) imiter l'intelligence naturelle, voire pourra s'y substituer. Il nous apparaît donc bon de vérifier la justesse de cette appellation, en l'étudiant par comparaison au monde naturel.

2 A noter cependant que, en Français, le mot « avion » est l'acronyme de « Appareil Volant Imitant l'Oiseau Naturel »

1.1. DANS LE MONDE NATUREL

Matière première de l'intelligence, la donnée est clé pour tous les êtres vivants.

Pour exprimer ses facultés, l'intelligence, dans le monde naturel, se nourrit d'informations : qu'il s'agisse d'éléments innés (que certains biologistes dénomment *« information-structure »*[3], correspondant, par exemple, au patrimoine génétique) ou reçus lors de sa vie biologique (que ces mêmes biologistes dénomment *« information-circulante »*[4], fruit de l'expérience, l'information permet aux organismes vivants de percevoir le monde qui les entoure pour tenter de s'y adapter. Cette dernière faculté (l'adaptation) étant souvent citée comme l'une des caractéristiques essentielles de l'intelligence, nous voyons bien, ici, que le lien entre *« information »* et *« intelligence »* est étroit. Nous étudierons successivement ces deux notions, en traduisant la première par celle de *« donnée »* (dont nous verrons la grande proximité avec l'information).



3 H Laborit in « Etude sur le statut juridique de l'information », E Daragon (Recueil Dalloz 1998, p. 63).
4 H Laborit in « Etude sur le statut juridique de l'information », E Daragon (Recueil Dalloz 1998, p. 63).

1.1.1. LA DONNÉE

" Je ne connais pas d'être vivant, de cellule, tissu, organe, individu et peut-être même espèce, dont on ne puisse pas dire qu'il stocke de l'information, qu'il traite de l'information, qu'il émet et qu'il reçoit de l'information "

Michel Serres[5]

Etat du réel, et sa représentation perceptible par un être vivant, la donnée désigne à la fois le monde tel qu'il est et tel qu'il est ressenti par les organismes biologiques.

Si l'on s'appuie sur l'étymologie, issue du verbe *« donner »*, la *« donnée »* renvoie à l'état brut du réel : d'une part, l'état des organismes vivants (dotés, dès leur naissance, d'un patrimoine de données – le *« patrimoine génétique »*) ; d'autre part, l'état des éléments minéraux[6]. Cette acception – qui n'autorise, en soi, aucune perception ni communication entre les êtres vivants – nous paraît toutefois devoir être élargie pour intégrer une dimension dynamique. Ainsi, nous proposons de définir la donnée, sous une dimension biologique, comme *« la traduction, dans une forme compréhensible par un être vivant, d'une réalité*[7]*, qui est ensuite susceptible de provoquer une réaction*[8]*»*. Cette proposition ajoute à la donnée brute (le réel), sa représentation sous une forme (ici biologique[9]) qui permet à l'organisme vivant de la recevoir et de lui donner une signification. Ce sont là les deux caractéristiques essentielles, à nos yeux, de la donnée : l'état du réel, et sa perceptibilité par un agent. Autrement dit : une représentation du réel, qui peut circuler.

Dès lors qu'elle est caractérisée par une formalisation et un consensus, la donnée est un des composants du langage.

Indépendamment de la perception du monde, qui les entoure, la plupart des êtres vivants ont besoin de communiquer entre eux ou avec d'autres créatures. Pour ce faire, ils utilisent des signes (vocaux, gestuels, tactiles, olfactifs…) qui sont formalisés (son, geste, contact, sécrétion olfactive…) et qui sont communément perçus par l'agent émetteur et l'agent récepteur[10], et ce afin de pouvoir transmettre une signification (fruit de leur interprétation). Ces deux particularités (formalisation et consensus) caractérisent également le langage, qui permet à l'intelligence de se déployer pleinement en communiquant avec l'extérieur. Ce n'est probablement pas un hasard si le développement de l'intelligence humaine, et de ses réalisations, a connu un essor sans précédent avec l'apparition des langues, puis de l'écriture, dans lesquelles l'on peut voir une forme aboutie de référentiels de données caractérisés par une formalisation et un consensus partagés par l'ensemble des membres d'une communauté linguistique.

5 Cité in « Terra Data - Qu'allons-nous faire des données numériques ? », Editions Le Pommier (mars 2017), S Abiteboul et V Peugeot.
6 L'eau, les roches, l'air, et leurs composants.
7 Chaud/froid, silence/bruit, immobilité/mouvement, sécheresse/humidité…
8 Douleur/plaisir, peur, excitation…
9 La forme du message nerveux déclenché par le récepteur sensoriel, par exemple.
10 Par exemple : deux individus (celui qui parle et celui qui entend), deux animaux, ou encore deux organes (tels que le récepteur sensoriel de chaleur, et le cerveau qui reçoit le signal l'informant de la présence de chaleur).

1.1.2. L'INTELLIGENCE HUMAINE

Approche par la philosophie et les sciences cognitives. La définition de l'intelligence humaine[11] ne fait l'objet d'aucun consensus et pour cause : outre qu'il s'agit d'une notion faisant appel à de multiples disciplines, elle varie également selon les cultures. Néanmoins, et sans prétendre à une quelconque exhaustivité, il apparaît possible – et nécessaire pour l'objet de la présente étude – de rappeler quelques éléments significatifs à ce sujet, et que nous emprunterons à la philosophie ainsi qu'aux sciences cognitives.

A. APPROCHE PHILOSOPHIQUE

Sur le plan philosophique, l'intelligence présente, à notre sens[12], deux dimensions qu'il est utile de distinguer : une dimension matérielle, liée aux facultés, et une dimension morale liée à la direction vers laquelle celles-ci sont exercées.

A.1. LA DIMENSION MATÉRIELLE

Si l'on distingue sa substance de son aspect dynamique, l'intelligence confère des facultés qui sont exercées à travers des mécanismes. Sans prétendre à l'exhaustivité, il est utile d'en rappeler les plus connus que nous retrouverons - pour certain(es - avec l'intelligence artificielle.

(I) LES FACULTÉS

René Descartes distingue quatre facultés conférées par l'intelligence, et que nous retiendrons pour les détailler : la perception sensorielle, la mémoire, l'entendement et l'imagination[13].

La perception sensorielle. Cette faculté permet à l'être humain de percevoir (collecter) des données sur le monde extérieur grâce à ses cinq sens. Tout comme – nous le verrons plus loin – les données numériques avec l'intelligence artificielle, ces données peuvent être sources d'erreurs car elles sont parfois incomplètes ou peu explicites et exigent une interprétation qui peut être erronée[14].

La mémoire. Cette faculté permet de conserver des informations et – avec l'aide d'autres facultés intellectuelles (entendement et imagination notamment) – de les mobiliser plus tard afin de les réutiliser en cas de besoin, à l'instar des capacités de stockage que possèdent les supports numériques.

L'entendement. Cette capacité permet de créer des concepts en ordonnant les informations perçues par les autres facultés de l'intelligence. Selon Kant, l'entendement élabore des représentations[15], des principes et des interprétations[16]. Selon Descartes, l'entendement s'exerce principalement[17] à travers deux types d'opérations : l'une immédiate (l'intuition[18]) et l'autre médiate (la déduction qui, avec l'induction, relève du mécanisme plus général de la logique[19]).

---

11 Le format contraint de la présente étude ne nous permet pas d'étendre notre exposé aux formes d'intelligence animales et végétales.
12 Il s'agit d'une lecture libre de notre part, inspirée pour partie des travaux de R. Descartes, qui ne prétend à aucune exhaustivité.
13 René Descartes, « Règles pour la direction de l'esprit », Règle XII (in « Œuvres et Lettres », La Pléiade, page 75).
14 « L'entendement ne peut jamais être trompé par une expérience (…) si (…) il ne juge pas (…) que les sens prennent les vraies figures des choses, ni enfin que la réalité extérieure est toujours telle qu'elle apparaît » (René Descartes, « Règles pour la direction de l'esprit », Règle XII in « Œuvres et Lettres », La Pléiade, page 84)
15 Formes sensibles permettant de rendre perceptible une idée, une chose ou une personne absente et ce à l'aide d'une image, d'un symbole, d'une description.
16 Recherche d'un sens clair pour élucider une information obscure.
17 Parmi les autres opérations mises en œuvre par l'entendement, Descartes cite également :
-l'impulsion, qui porte les individus à croire quelque chose « sans être convaincu par aucune raison » ;
- la conjecture lorsqu'un individu émet une hypothèse, opération qui, selon Descartes, « ne nous rend pas plus savants » (René Descartes, « Règles pour la direction de l'esprit », Règle XII (in « Œuvres et Lettres », La Pléiade, page 85).
18 L'intuition peut se définir comme le fait de comprendre quelque chose immédiatement, sans analyse ni raisonnement. Selon le chercheur Herbert Simon, l'intuition fonctionne ainsi : « la situation fournit un indice ; cet indice donne à l'expert un accès à une information stockée dans sa mémoire, et cette information, à son tour, lui donne la réponse ; l'intuition n'est rien moins que de la reconnaissance » (https://fr.m.wikipedia.org/wiki/Intuition).
19 La logique consiste à rechercher des règles pouvant être tirées d'un postulat ou de l'observation, afin de pouvoir tirer des conclusions. Parmi les mécanismes logiques, figurent notamment la déduction et l'induction. La première est « l'opération par laquelle nous entendons tout ce qui se conclut nécessairement d'autres choses connues avec certitude » (René Descartes, « Règles pour la direction de l'esprit », Règle III ; Editions La Pléiade « Œuvres et Lettres », page 44); autrement dit, une déduction est une inférence dans laquelle, si les postulats sont vrais, la conclusion est nécessairement vraie (https://dicophilo.fr/definition/deduction/): on descend des principes vers les faits. A l'inverse, l'induction consiste à tirer de plusieurs cas particuliers une conclusion générale En ce sens, la déduction logique ne produit aucune nouvelle connaissance, en ce sens que les propositions déduites sont virtuellement contenues dans leurs principes et est par conséquent analytique ; au contraire, l'induction enrichit la conscience de nouveaux faits : elle est synthétique (https://fr.m.wikipedia.org/wiki/Déduction_et_induction).

Certains systèmes d'IA sont « déductifs » : ils décrivent les étapes successives qui mènent à la conclusion et au résultat. D'autres sont plus « inductifs » (réseaux de neurones) : ils généralisent une conclusion sur la base d'exemples particuliers. Mais, dans le premier cas, le mécanisme de déduction est pré-existant et codé à travers des règles, tandis que, dans le second, la solution est le fruit d'une généralisation statistique dont le raisonnement peut toutefois être inaccessible.

L'imagination. Cette faculté permet de créer des objets ou des idées emmagasinés dans la mémoire, en se libérant de l'entendement. Permettant l'évasion hors du monde réel, l'imagination est, selon certains philosophes, le signe de la liberté humaine[20]. Transposée à l'Intelligence Artificielle, cette faculté peut se retrouver dans les travaux visant à apprendre à un réseau de neurones à composer une musique dès lors que l'imagination est considérée comme s'appuyant sur un ensemble d'éléments préexistants. Ainsi, après avoir fait « ingérer » à un réseau de neurones un grand nombre de morceaux de musique d'un même compositeur, le réseau en dégage de grandes règles et régularités de composition, de rythme et d'harmonie, celui-ci va être capable de composer un nouveau morceau… En l'état actuel, ces résultats sont toutefois jugés décevants par certains.

(II) LES MÉCANISMES

L'apprentissage. Présenté comme plaçant l'apprenant au cœur de l'action (au contraire de l'enseignement dont l'acteur serait l'enseignant[21]), l'apprentissage correspond au mécanisme d'acquisition de connaissances. Parmi les nombreuses méthodes (pouvant être combinées entre elles) figurent celles de l'apprentissage *« par imitation », « par induction », « par association »*[22], *« par essais et erreurs », « par explications », « par répétitions »* ou encore *« par renforcement »*. Parmi ces méthodes, c'est l'apprentissage *« par essais et erreurs »* que les technologies actuellement utilisées pour l'intelligence artificielle mettent en œuvre. Ainsi, par exemple, dans le cadre de la reconnaissance d'image, on commence par montrer à un réseau de neurones une image de chat, que celui-ci ne reconnaît pas initialement. Grâce à l'algorithme d'apprentissage, et comme nous le verrons plus loin, on fait en sorte de diminuer l'erreur afin que le système reconnaisse de mieux en mieux les images de chat. On peut également voir dans ce procédé une certaine forme d'apprentissage *« par répétitions »*, étant donné qu'il convient de montrer au système un très grand nombre d'exemples pour qu'il « apprenne ». Les intelligences artificielles ayant gagné contre des champions d'échec ou de go utilisent quant à elles l'apprentissage *« par renforcement »*, grâce auquel les coups ayant mené à la victoire sont privilégiés.

La décision. Fruit d'un acte délibératif, la décision est l'action de l'esprit qui tranche et choisit entre plusieurs solutions possibles. Herbert Simon a proposé, dans plusieurs articles et ouvrages des années 1960-70, un schéma de la prise de décision en quatre phases : (i) un *« renseignement »* [diagnostic du problème (phase d'intelligence au sens militaire de *« renseignement »*)], (ii) une *« conception »* (formulation des voies possibles offertes à la résolution du problème), (iii) une *« sélection »* (choix du mode d'action particulier), et enfin (iv) un *« bilan »* (pouvant déboucher sur la réactivation de l'une des phases précédentes, ou sur la validation de la solution)[23]. La prise de décision peut être biaisée par des sources d' erronées[24]. L'acte de décision est à distinguer des actes *« d'exécution »* (qui ne sont que la mise en œuvre la conséquence d'une décision). Ainsi que nous le verrons, les technologies actuellement utilisées pour l'intelligence artificielle ne mettent aucunement en œuvre un mécanisme autonome de prise de décision, au sens précité.

A.2. LA DIMENSION MORALE

Singularité de l'intelligence humaine : la question morale. Sous la stricte définition matérielle, l'être humain ne détient pas le monopole de l'intelligence, hormis : tous les animaux et végétaux possèdent des facultés sensorielles et mémorielles, et certains possèdent également des facultés de raisonnement. Pour saisir l'intelligence humaine, il faut ouvrir une dimension morale : celle-ci est liée à la « conscience », elle-même indéfectiblement liée à la notion de « bien » et de « mal », sur la base desquelles un être humain prend une décision. Bien que le sujet prête à débat, il est communément admis que cette faculté est le propre de l'être humain, ou à tout le moins que ces derniers l'aient développé bien au-delà de ce qu'a pu développer l'espèce animale : on en veut pour preuve les actes à signification religieuse ou guerrière, qui sont l'expression d'un choix moral et dont on ne connaît pas d'exemple significatif dans le règne animal ou végétal à ce jour.

20 Telle est la thèse de Jean-Paul Sartre dans « L'imaginaire ».
21 https://fr.wikipedia.org/wiki/Apprentissage
22 En associant un stimulus nouveau à un mécanisme déjà appris : par exemple, en associant une odeur - habituellement associée à un danger devant provoquer la fuite - avec un nouveau son, l'apprenant saura qu'au retentissement de ce son, il faut fuir.
23 « Philosophie et épistémologie de la décision », Daniel Parrochia (http://parrochia.wifeo.com/documents/La-decision.pdf
24 Les biais intrinsèques (à l'agent) sont, par exemple, le genre, les préjugés culturels et sociaux, etc. Les biais extrinsèques (à l'agent) résident, par exemple, dans l'incertitude. Les correctifs à ces biais sont, soit intrinsèques à l'agent (par exemple, l'expérience, l'éthique, l'intuition, …), soit extrinsèques à l'agent en amont (par exemple le devoir de s'expliquer sur certaines décisions de justice ou hiérarchiques), ou en aval (telle la responsabilité juridique de laquelle répond tout individu ayant pris une décision dont les conséquences causent un dommage à autrui ou aux biens d'autrui, et qui ne pourra s'exonérer qu'à la condition d'apporter une explication légitime à celles-ci.)

B. APPROCHE SCIENTIFIQUE

" L' être vivant peut être assimilé à une machine auto-programmée. Certains modèles informatiques démontrent que le hasard peut conduire à des systèmes ordonnés, donc fonctionnels. Quelles sont alors les places respectives du déterminisme et du libre-arbitre ? "

H. Atlan

Biologie et informatique, une inspiration réciproque. Dans un article publié en 1985 et intitulé « Intelligence Artificielle et organisation biologique » Henri ATLAN identifiait les passerelles existant entre deux disciplines qui, au premier abord, ne semblaient pas avoir de lien, à savoir :

- La biologie moléculaire ;
- les sciences et techniques de l'ordinateur.

Il notait que ces deux disciplines s'étaient très fréquemment inspirées l'une de l'autre, preuve d'un intérêt réciproque qui consistait :

- d'un côté à utiliser la compréhension du biologique pour qu'un « bio mimétisme » catalyse des avancées rapides de l'ordinateur ;
- de l'autre à identifier, dans les organismes vivants, un « mécanisme » dont les finalités pourraient être modélisées comme des processus mécaniques voire mathématiques.

Ainsi l'ordinateur programmé constituait un moyen séduisant pour modéliser la plupart des processus biologiques, l'ADN, le cerveau et plus récemment l'intelligence…

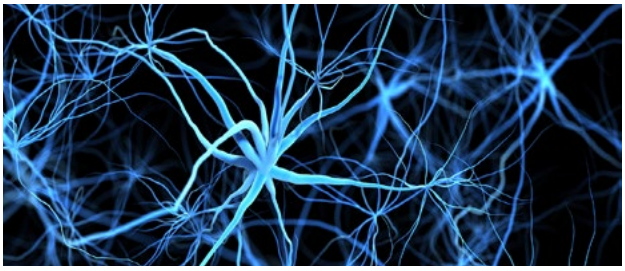
Dans la droite ligne de cette approche, l'intelligence artificielle a progressé en empruntant à la compréhension du cerveau ses fondamentaux conceptuels.
De manière schématique, la modélisation numérique du cerveau biologique[25] s'est construite de la manière suivante :

- Le **neurone** serait un **microprocesseur** (un microprocesseur est un processeur dont tous les composants ont été suffisamment miniaturisés pour être regroupés dans un unique boitier. Fonctionnellement, le processeur est la partie d'un ordinateur qui exécute les instructions et traite les données des programmes) ;
- la **synapse**, un **disque dur** ;
- l'**axone**, un **flux de données** ;
- le tout s'appuyant sur des supercalculateurs dont la simple augmentation de puissance résoudrait la question de l'intelligence.

Cependant, cette comparaison relève plus de la métaphore que de la réalité scientifique. Elle permet de tendre vers une intelligence « bio-inspirée » qui « simule » (dans ses mécanismes internes) un processus cognitif de l'intelligence biologique mais sans réellement le « reproduire ».

L'analyse mathématique permet d'intégrer dans des systèmes artificiels les nouvelles connaissances acquises sur le cerveau et sa structure. Elle rend possible l'étude de systèmes nerveux peu élaborés, comme ceux d'organismes aussi simples que des vers de terre. Ainsi le réseau neuronal d'un ver comme Caenorhabditis elegans est presque entièrement connu[26]. Au contraire, le cerveau humain, très complexe, ne constitue pas un bon modèle de réseaux de neurones. L'Homme n'a qu'une connaissance limitée de son fonctionnement très sophistiqué, ce qui rend difficile une modélisation exhaustive. Pour ce faire, il faudrait de toute façon disposer d'une puissance de calcul qui n'est aujourd'hui pas disponible. Et bien sûr, il est évident que modéliser des « émotions », modéliser la « pensée » ou reproduire « l'intuition » nous est toujours inaccessible. Et que serait une Intelligence sans « émotion », « pensée » ou « intuition »…? Les chercheurs qui utilisent des réseaux de neurones n'ont d'ailleurs pas la prétention de reproduire avec exactitude le comportement de neurones réels. Ils tirent en réalité parti de certaines de leurs caractéristiques pour améliorer et optimiser les modèles existants en intégrant les découvertes récentes acquises sur le cerveau et sa structure, dans les systèmes artificiels. C'est pourquoi cette démarche est qualifiée de bio-inspirée.

25 Article « Quelle est la puissance de notre cerveau ? » Source : https://couleur-science.eu consulté en ligne le 18 Février 2019 URL : http://bit.ly/2V36hMn
26 http://www.ipubli.inserm.fr/handle/10608/4789



Inspiration versus reproduction

« Le cerveau est tout sauf un calculateur mécanique tel que nous les avons conçus au travers des ordinateurs».

Thierry Vieville

L'intelligence biologique, en totale interaction avec son environnement. Au sein d'une intelligence biologique, il n'y a pas de traitement de l'information (la « pensée ») sans émotion, qui est elle-même directement en lien avec la « perception subjective » de son environnement. Il s'agit là d'un principe clé et indissociable du processus de décision d'un système biologique. Contrairement aux machines qui calculent à une vitesse considérable, le cerveau n'est pas rapide. Il est efficace. Son organisation est optimisée avec des zones spécialisées par catégorie d'information (auditives, visuelles, olfactives etc…) et des zones dites associatives qui construisent des représentations combinant les différentes informations sensorielles et motrices. Cette construction permet un fonctionnement cognitif, dynamique et flexible qui assimile en temps réel les sensations et émotions, organise et planifie en fonction de l'environnement et de manière unique, le comportement de chaque individu. Cette organisation, particulièrement riche en interconnections, tolère et même profite, des aléas « de traitement ». Mais l'une des plus grandes forces du cerveau humain réside dans la plasticité synaptique[27] définie comme « la propriété que les connexions entre les neurones, appelées synapses, ont de changer en force en fonction de l'usage qui en est fait[28]). En résumé, cette propriété fait le « cerveau ».

Le cerveau humain, aboutissement d'un processus millénaire. Ainsi, depuis plusieurs millions d'années, notre cerveau s' « entraîne » pour survivre. L'évolution, les mutations génétiques et le hasard ont permis l'émergence d'une forme d'« intelligence héréditaire », qui s'est transmise et améliorée d'une branche à l'autre des espèces puis d'une génération à la suivante. Le cerveau s'est doté de fonctions très « sophistiquées » qui ont permis la survie de l'Homo Sapiens.
En outre *« L'intelligence, n'est pas la seule forme de la pensée. Il existe d'autres facultés de connaissance, amenées également par l'évolution, qui se rapportent directement à la réalité : l'instinct et l'intuition. L'instinct est comme une intuition qui aurait tourné court et l'intuition comme un instinct qui se serait intensifié et dilaté jusqu'à devenir conscient et susceptible de s'appliquer à toutes choses. Sous sa forme achevée, l'intuition est un pouvoir propre à l'homme qui le rend capable d'une expérience pure.[29] ».*

Ainsi le concept d'intelligence biologique s'appuie sur des processus complexes et un potentiel qu'une Intelligence Artificielle ne pourra reproduire avant longtemps. Et bien qu'il soit difficile de donner une définition exhaustive à l'intelligence (biologique ou non), il semble possible d'affirmer que l'Intelligence Artificielle, si elle existe, n'est pas encore dotée d'une « Conscience Artificielle ». Ainsi il ne faut pas confondre reproduire (dans ses mécanismes internes) un processus cognitif et le fait de le simuler. Mais cette confusion, tenace, a des conséquences néfastes et notamment celles de nous détourner de véritables questions, telles que la valeur réelle des technologies numériques, les enjeux réels liés à leur déploiement massif, leur impact et leur évolution…

A l'issue de cette première partie, on voit bien que l'intelligence qui se nourrit de données dans le monde naturel a dégagé des propriétés qui pour le moment ne se retrouvent pas dans l'IA mais dont celle-ci s'inspire. Mais pour mieux s'en convaincre, nous allons vérifier ce constat en examinant en détail l'IA et les données dans le monde artificiel.

27 A dendritic disinhibitory circuit mechanism for pathway-specific gating https://go.nature.com/2V2Y4rt
28 https://fr.wikipedia.org/wiki/Plasticit%C3%A9_synaptique
29 Extraits adaptés à partir de Encyclopædia Universalis 1998 http://www.unisson06.org/dossiers/spiritualite/intuition_raison/intuition4.htm

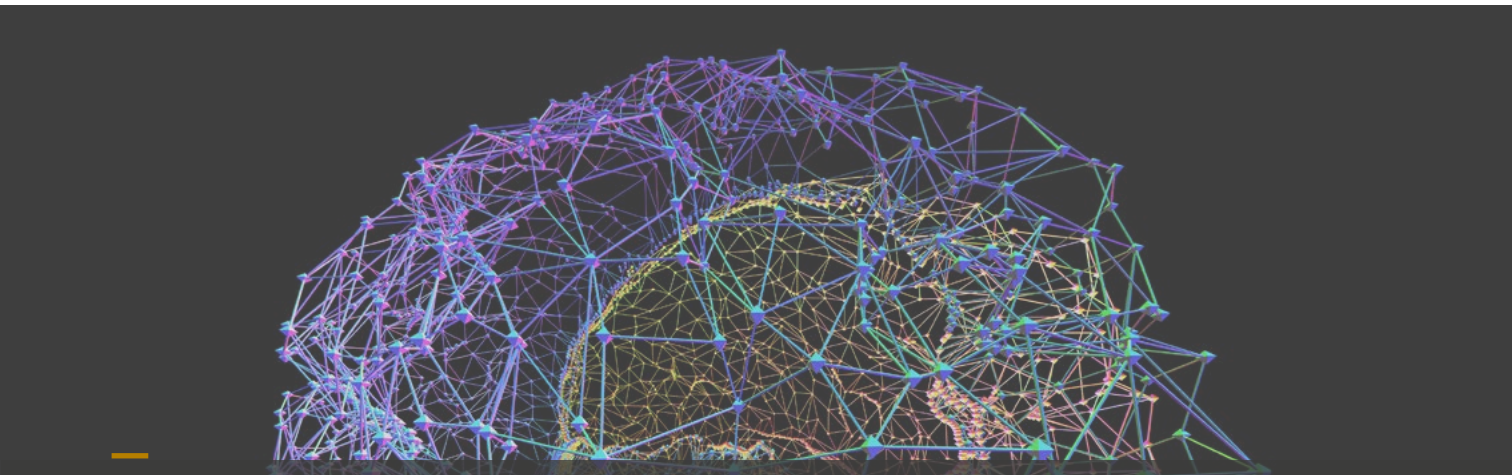
1.2.
DANS LE MONDE ARTIFICIEL

Tout comme l'intelligence naturelle, l'IA se nourrit de données.

1.2.1. LA DONNÉE

La distinction traditionnelle entre « donnée », « information » et « connaissance », opérée en science de la communication et de l'informatique.

Dans ces disciplines récentes, la « *donnée* » est traditionnellement entendue comme « *une description élémentaire d'une réalité* »[30], qui consiste soit en une observation, soit en une mesure (comparaison entre deux éléments ou événements), et est dépourvue de toute interprétation et, donc, en soi, de toute signification[31]. Ainsi comprise, la donnée se distingue de « *l'information* » dont les origines sémantiques[32] conduisent certains auteurs à définir comme le sens (la signification) dégagé(e) à partir d'une ou plusieurs donnée(s) par l'agent qui les reçoit[33].



30 S. Abiteboul et V. Peugeot, « Terra Data - Qu'allons-nous faire des données numériques ? », Editions Le Pommier (mars 2017).

31 Sources : https://fr.wikipedia.org/wiki/Donn%C3%A9e ; V. aussi B. Chaudet (Maître de conférence en sciences de la communication à l'Université Rennes 2) qui insiste, lui aussi, sur l'absence de signification attachée à une « donnée » (sources : https://brunochaudet.wordpress.com/2009/03/30/donnee-information-connaissance/ ; publié en mars 2009). Enfin, S. Abiteboul (membre du Collège de l'Autorité de Régulation des Communications Electroniques et des postes – ARCEP –, chercheur à l'Ecole Normale Supérieur de paris, et directeur de recherche au sein de l'Institut national de recherche en informatique et en automatique – INRIA) et V. Peugeot retiennent la même approche (« Terra Data - Qu'allons-nous faire des données numériques ? », Editions Le Pommier, mars 2017). Cette approche est partagée par d'autres auteurs, issus du conseil et de la gestion de projets : « Dans les technologies de l'information, une donnée est une description élémentaire, souvent codée, d'un objet, d'une transaction d'affaire, d'un événement » (F. Régnier-Pécastaing, M. Gabassi et J. Finet, « MDM Enjeux et méthodes de la gestion de données », 2008, Dunod).

32 Du latin « in » (marquant l'aboutissement d'une action), et « formare » (former, instruire) : cité in « Etude sur le statut juridique de l'information », E Daragon (Recueil Dalloz 1998, p. 63).

33 S. Abiteboul et V. Peugeot, « Terra Data - Qu'allons-nous faire des données numériques ? », Editions Le Pommier (mars 2017).

Enfin, la « *connaissance* » est entendue comme l'ensemble des informations comprises et assimilées par l'agent concerné[34], et qui – pour certains[35] – deviennent des « *lois* » que l'agent considère comme vraies. Ainsi, Serge Abiteboul, dans sa leçon inaugurale au Collège de France donnée en mars 2012, illustrait cette distinction par l'exemple suivant : (i) « *des mesures temporaires collectées par une station météo* » constitueraient des « données », car elles sont dénuées de sens ; (ii) « *une courbe donnant l'évolution des minimas et maximas moyens en un lieu suivant le mois de l'année* » constituerait une « *information* », car ayant « *un sens (pour construire une représentation de la réalité)* » ; (iii) l'indication selon « *la température sur terre augmente du fait de l'activité humaine* » serait, selon cet auteur, une « *connaissance* », car correspondant à une « *loi qui est considérée comme vraie* »[36].

La notion de « *donnée* » au sens de la présente étude : une acception plus large. Sur un plan conceptuel, tout d'abord, la distinction, illustrée par l'exemple précité, ne nous paraît pas évidente[37], dans la mesure où toute description du réel nous paraît porteuse de signification (à des degrés plus ou moins forts – mais ce n'est là qu'une différence de degré, non de nature). Sur un plan pratique, ensuite, la distinction nous paraît peu commode car, dans les faits, le phénomène d'amplification de production et de circulation des données (« *Big Data* ») vise à la fois les « *données* », les « *informations* » et les « *connaissances* » telles que définies précédemment. Textes, images, enregistrements vidéo et audio, tout ce que les parties prenantes (utilisateurs et fournisseurs de services numériques) ont pris pour coutume de désigner sous le terme de « données » (ou, plus fréquemment, son équivalent anglophone « *data* »), vise bien ce large ensemble : les descriptions et mesures du réel, mais aussi ses interprétations, voire les pures spéculations de l'esprit humain[38]. Cette acception plus large se trouve confortée par le rapport Gaudrat qui définissait la donnée comme « *la représentation conventionnelle d'une information dans une forme permettant d'en faire un traitement* »[39]. Aussi, dans un souci pratique, nous inclurons dans le terme « donnée » les informations.

Donnée (numérique) et langage : un idéal à atteindre. Traduisant – de manière plus ou moins riche – un état (du « *réel* » ou du « *créé* »), la véritable donnée, celle appelée à circuler d'un agent à l'autre, est – à notre sens – indissociable des notions de « *formalisation* » (représentation) et de « *convention* » – ou « *consensus* » – (commune perception par au moins deux agents). Ces deux particularités formelles caractérisent également le langage. Ainsi, tout comme l'intelligence naturelle se nourrit de données, il en va de même pour l'intelligence artificielle, ce qui exige que les données utilisées pour la mettre en mouvement soient formalisées à l'aide d'un référentiel ayant fait l'objet d'un consensus entre les parties prenantes. Ainsi, pour appartenir à un langage – étape ultime de leur évolution –, les données numériques doivent être perçues uniformément par plusieurs destinataires (individus ou machines) : c'est, par exemple, le cas des langages de programmation, mais également de certains référentiels de données[40] qui, lorsqu'ils sont partagés par une communauté d'utilisateurs formés ou éprouvés, remplissent une fonction de véritable langage. Malheureusement, ces exemples ne reflètent pas encore la majorité des situations, sur le terrain, ce qui explique que l'usage de données au sein et entre les organisations humaines rencontre de trop nombreux dysfonctionnements et incohérences (mauvaise qualité des données), notamment en raison de l'absence d'expertise, bonnes pratiques, qui révèlent bien souvent une absence de consensus sur l'usage de la donnée.

34 B. Chaudet (https://brunochaudet.wordpress.com/2009/03/30/donnee-information-connaissance/). V. aussi S. Abiteboul et V. Peugeot retiennent la même approche (« Terra Data - Qu'allons-nous faire des données numériques ? », Editions Le Pommier ; mars 2017).
35 S. Abiteboul et V. Peugeot, « Terra Data - Qu'allons-nous faire des données numériques ? », Editions Le Pommier (mars 2017).
36 https://www.college-de-france.fr/media/serge-abiteboul/UPL4129881692607880347_lecon_inaugurale.pdf
37 Ainsi, en quoi des mesures de température seraient davantage dénuées de sens – c'est à dire n'exprimeraient aucune signification – qu'une courbe qui ne fait que compiler ces mêmes températures. Dans les deux cas, il y a bien une description du réel, qui est porteuse de signification, même si celle-ci est plus riche dans le second cas que dans le premier. Seul le troisième exemple nous semble se distinguer réellement d'une « donnée », car, à la différence des deux exemples précédents, il met en œuvre une interprétation du réel (augmentation de la température causée par l'activité humaine) – qui peut être une opinion (vraie ou fausse) ou encore une croyance (non vérifiable).
38 Dont certaines peuvent se révéler fausses – problème fréquemment dénoncé sous le terme anglais de « fake news ».
39 Rapp. Gaudrat, Commercialisation des données publiques, Doc. fr, 1992.
40 Tel est le cas de certains standards utilisés par des communautés de professionnels pour décrire, en langage simplifié utilisant des codes normés, les caractéristiques techniques de produits. Ainsi, par exemple, le standard ETIM – édité par ETIM France (branche française d'ETIM International, association à but non-lucratif) – est « un modèle de données » permettant de décrire de manière simplifiée et surtout uniforme à l'échelle européenne, des informations relatives à des produits électriques et de génie climatique. Présenté comme étant « conçu pour réduire les ambiguïtés au minimum » et permettre « aux acteurs du secteur de communiquer sur les produits sans malentendus », ce standard, ce modèle permet de répondre à des besoins actuels pratiques comme la « création de catalogues », le « remplissage de fiches techniques, (l')alimentation de sites web, (la) modélisation en 3D pour le bâtiment, etc. » (https://www.etim-france.fr/fr).

En réponse aux difficultés : classification et gouvernance. Sur le plan opérationnel, les données numériques se répartissent en plusieurs catégories, qui permettent de les organiser et les administrer avec un ensemble de règles que les professionnels dénomment « la gouvernance des données », et qui, notamment pour une utilisation réussie de l'IA, sera clé. Sans prétendre à l'exhaustivité, compte-tenu du format contraint de la présente étude, voici quelques-unes de ces catégories :

- les *« métadonnées »* correspondent aux données qui décrivent d'autres données (sémantiquement les données *« sur»* les données). Il s'agit de l'information qui permet de retrouver les données stockées ; par exemple, bien avant l'arrivée du numérique, les métadonnées étaient (et restent) utilisées par les bibliothèques, sous la forme d'une codification des signalements des documents conservés ; dans le domaine du droit, les métadonnées correspondent, par exemple, à la référence d'une décision de jurisprudence exprimée sous une forme harmonisée et respectée par les professionnels et étudiants en droit (*« Cass. Civ 1ère, jour mois année, pourvoi n° XXX »*) ; les métadonnées sont essentielles pour l'efficacité des recherches d'informations et permettre l'interopérabilité entre les différentes bases de données contenant celles-ci ;
- les données *« de référence »* (aussi appelées *« données maîtres »* ou en anglais *« master data »*) sont *« des données partagées par l'ensemble des processus qui soutiennent l'activité courante d'une organisation et ses prises de décision »*[41] ; cette catégorie de donnée a pour caractéristique d'être partagée entre plusieurs applications et directions métiers de l'organisation[42], à travers différents processus (vente, comptabilité…) ; il s'agit, en principe, de données stables, qui ne changent pas entre différentes opérations[43]; appartiennent à cette catégorie, par exemple, les fiches client, fournisseur, employé, ou encore le numéro et de la description de produits ou services ;
- les données *« constitutives »*, qui peuvent changer plus souvent, viennent nourrir les précédentes ; par exemple, l'adresse de facturation/livraison, ou encore l'interlocuteur de facturation d'un client, appartiennent à cette catégorie ;
- les données *« opérationnelles »* sont celles qui varient à chaque opération, tel un numéro de commande, ou encore la liste ou le nombre de produis achetés par un client ;
- les données *« paramètre »* correspondent à des tables de valeurs ou des nomenclatures ; relèvent de cette catégorie, par exemple, la liste des communes et codes postaux (fichier Hexapost, normalisé par La Poste).

1.2.2. L'INTELLIGENCE ARTIFICIELLE

Délimitation de l'IA objet de la présente étude : l'algorithme d'apprentissage par rétropropagation du gradient. Pouvant être définie comme « l'ensemble des théories et des techniques mises en œuvre pour réaliser des machines dont le fonctionnement s'apparente à celui du cerveau humain »[44], l'IA est en réalité plurielle car elle peut s'incarner à travers différents types de technologies. Pour des raisons de format, la présente étude traitera uniquement de celle dont les résultats se sont montrés les plus remarquables au point de susciter un véritable engouement à l'origine du « printemps » actuel de l'IA : l'algorithme de rétro-propagation du gradient, issu notamment des travaux du chercheur français Yann LeCun, l'un des lauréats du prestigieux prix Turing en 2019. Nous en exposerons le fonctionnement, avant de voir en quoi la qualité des données qui le nourrissent est cruciale pour lui permettre de produire des résultats pertinents. La clé réside également dans l'interprétation de ces résultats qui ne devront jamais être regardés comme reflétant une vérité, mais simplement une probabilité… Car fortement dépendante de la qualité du jeu de données, reproduisant lui-même souvent nos propres biais, qu'ils soient sociologiques ou culturels.

41 https://fr.wikipedia.org/wiki/Donn%C3%A9es_de_r%C3%A9f%C3%A9rence
42 F. Régnier-Pécastaing, M. Gabassi et J. Finet, « MDM Enjeux et méthodes de la gestion de données », 2008, Dunod.
43 https://fr.wikipedia.org/wiki/Donn%C3%A9es_de_r%C3%A9f%C3%A9rence
44 Le Petit Larousse illustré (2012)

A. L'ALGORITHME D'APPRENTISSAGE DE RÉTRO-PROPAGATION DU GRADIENT

A.1. FONCTIONNEMENT

Le principe du « *Machine Learning* ». Aujourd'hui les systèmes d'intelligence artificielle sont basés sur les techniques d'apprentissage (*Machine Learning*). Ces techniques d'apprentissage s'appliquent à des réseaux de neurones artificiels dont le fonctionnement rappelle en infiniment plus simple celui des neurones biologiques : les différentes couches de neurones sont connectées entre elles par des liens appelées *« poids »* sur lesquels on intervient pour optimiser la correspondance entre les données d'entrée et de sortie. En fonction des enjeux et des objectifs recherchés, on détermine le seuil où se trouve la performance optimale du système, pour diminuer autant que possible les erreurs et renforcer les bonnes valeurs. Une fois ce seuil établi, il détermine l'activation ou non de la couche de neurones suivante.

Réseaux de neurones artificiels. Ces réseaux artificiels sont composés d'un ensemble de neurones organisés en couches. Une première couche, appelée « couche d'entrée » ou « rétine », est exposée à des données d'entrée. Par exemple, dans le cadre d'un système de reconnaissance d'images, cette couche d'entrée va se voir présenter un grand nombre d'images pour entraîner le système à reconnaître ce qui les compose (par exemple des chiens, des chats, des léopards…). La donnée d'entrée se propage de couche en couche jusqu'à la sortie. Il s'agit alors de regarder la sortie par rapport à ce qui était attendu (par exemple : cette image est un chat ou n'est pas un chat) et de mettre à jour les liaisons entre les neurones (les « poids ») pour améliorer le résultat final.

Processus d'apprentissage. Des algorithmes ont été développés pour progressivement adapter les connexions de tels systèmes et assurer la classification exacte. Ce processus d'apprentissage consiste à présenter une image, propager les activations jusqu'à la couche de sortie et à calculer l'écart entre les valeurs calculées et la bonne réponse (dans notre exemple : cellule du chien activée à l'exception de toutes les autres lorsqu'une image de chien est présentée sur la rétine d'entrée). L'algorithme consiste à modifier les poids entre la couche de sortie et la précédente de façon à ce que l'écart entre ce qui est calculé et la bonne réponse s'amenuise, puis rétro-propager ces modifications de proche en proche jusqu'à la rétine. Ainsi, lorsque le réseau de neurones aura prédit une réponse s'avérant être exacte, il modifiera les poids de façon à renforcer ce type de réponse ; à l'inverse, lorsqu'il se sera trompé, la modification des poids conduira à affaiblir ce type de réponse devant une image similaire. En faisant cela un nombre suffisant de fois, avec un nombre suffisant d'images (de chats, de chiens, de léopards…), on arrive finalement à classer convenablement les images d'animaux présentées à la rétine de ce réseau de neurones.

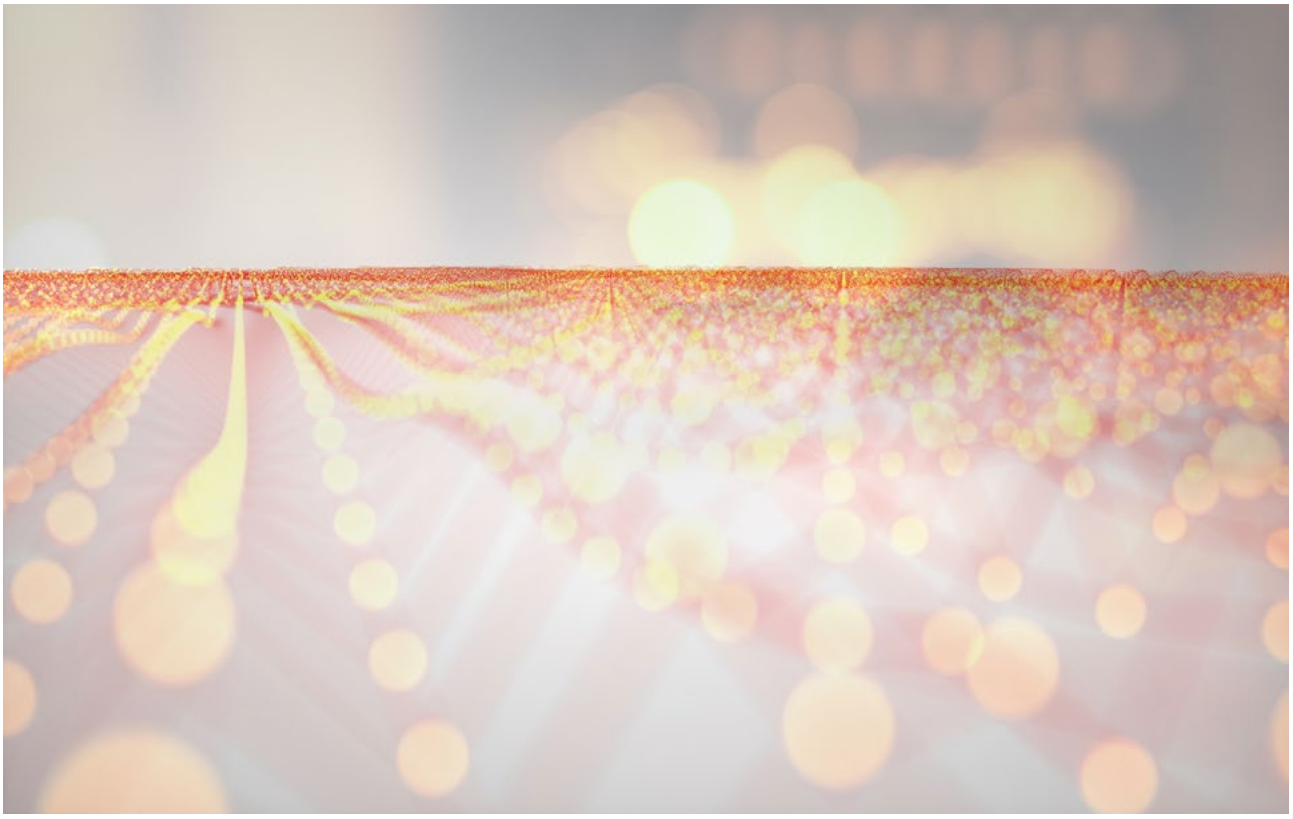
Données. Pour cela, il est bien sûr nécessaire au préalable d'identifier les animaux présents sur les différentes images et de fournir la bonne réponse au système de façon à ce qu'il puisse optimiser sa réponse : c'est ce qu'on appelle la supervision. Cet apprentissage supervisé consiste donc à fournir la bonne réponse sur un grand nombre d'exemples de façon à ce qu'à travers l'algorithme de modification des poids le système converge vers les bonnes réponses.

Résultats et analyse. Le système sera même capable de donner les bonnes réponses sur des images de chiens, de chats ou autres sur lesquelles il n'aura pas été entraîné : c'est ce qu'on appelle la généralisation. Dans le cas de l'analyse et de la classification d'images, les premières couches de ces réseaux ont un fonctionnement qui consiste à identifier des régularités « simples » dans les images (lignes verticales, lignes horizontales, cercles, etc.), les suivantes « combinent » ces informations (deux cercles horizontaux séparés d'une ligne verticale qui surmontent une ligne horizontale formant les prémisses d'un visage), et plus on avance dans les couches, plus la combinatoire se complexifie pour finalement permettre une distinction fine des images et en extraire à la fois les régularités globales et les particularités spécifiques. Si l'on simplifie, on retrouve le même type de traitement dans le cerveau avec des neurones « proches » des capteurs sensoriels qui se chargent d'une analyse des caractéristiques primaires et les zones neuronales suivantes se chargeant des tâches de reconnaissance et de classification.

A.2. PORTÉE

Le bien-fondé de l'attribut « intelligence » pour l'IA.
Certes, les résultats sont impressionnants : disposer dans son téléphone d'un dispositif capable de s'activer uniquement lorsqu'il reconnait un visage ou une voix parmi tous les autres visages ou voix du monde et cela sans passer des heures à le programmer peut sembler relever d'une certaine intelligence. Pourtant, si intelligence il y a, elle réside probablement bien plus dans la capacité à fournir durant la phase d'apprentissage les « bons » exemples - autrement dit, les bonnes « données » - à la fois en termes de caractéristiques et en termes de label que dans « l'algorithme ». Le seul algorithme consiste en termes mathématiques à minimiser une fonction de coût en propageant au mieux des dérivées partielles à travers une série de calculs élémentaires. Que le système se trompe plus ou moins (l'écart étant plus ou moins important entre la sortie calculée et le label attendu), la procédure programmée tend de toute façon à ce que cette erreur se réduise. La procédure d'apprentissage quant à elle consiste à présenter des exemples jusqu'à ce que l'erreur ne se réduise plus significativement. Bien sûr, si de nouveaux exemples sont disponibles, on peut les intégrer après cet apprentissage initial, et continuer ainsi à affiner le système.

La dimension décisionnelle de l'IA.
Il est à noter que la sortie d'un tel système n'est pas binaire. Le score calculé présente un continuum entre 0 (la mauvaise réponse) et 1 (la bonne réponse). A partir de quelle valeur alors doit-on considérer que la sortie calculée représente 0 ou 1 ? Comment fixer cette valeur, ce seuil ? Comment la machine décide-t-elle ? Il s'agit encore une fois d'optimisation : une méthode simple consiste à calculer pour tous les exemples présentés en entrée la valeur de sortie. On obtient donc pour chaque exemple une valeur entre 0 et 1. On fait alors varier continument de 0 à 1 la valeur du seuil et l'on compte pour chacune de ces valeurs combien on a de bonnes réponses. C'est-à-dire combien d'exemples dont la bonne réponse est 0 se trouvent en-dessous du seuil et combien d'exemples dont la bonne réponse est 1 se trouvent au-dessus du seuil : la valeur du seuil pour laquelle la somme de ces deux comptages est maximale est retenue. On optimise ainsi l'efficacité du système. Peut-on véritablement parler de prise de décision ? Il s'agit plutôt d'une procédure efficace de choix…



B. LE RÔLE CLÉ DES DONNÉES

Les données ne sont pas neutres. Le triomphe des sciences dures, mathématiques en tête, a installé durablement chez certains le mythe selon lequel les chiffres, qui seraient plus neutres que les mots, permettraient de saisir le monde avec davantage d'exactitude. Partant de là, l'IA, qui s'appuie sur des données - parfois des chiffres - analysés à l'aide de méthodes mathématiques, apparaît comme source de vérité. Et pourtant, l'on oublie souvent que l'IA ne fait que reproduire ce que révèlent les données qui lui sont fournies et qui peuvent reproduire des anomalies matérielles ou éthiques, fruits de biais culturels ou sociologiques.

Les exemples d'IA ayant révélé des résultats sexistes, ou encore racistes, reflétant en réalité simplement des biais contenus dans les données. En 2018, Amazon a tenté d'automatiser le recrutement en ayant recours à une intelligence artificielle[45]. Pour ce faire, l'IA s'appuyait sur les recrutements effectués par l'entreprise depuis 10 ans. Etant donné que 60% des employés de l'entreprise sont masculins, et l'algorithme utilisé se basant sur les données préexistantes, il s'est avéré que cette IA pénalisait les CV des candidates. Le côté sexiste ne venait alors pas du système en soi, mais bien du jeu de données disponible. Autre exemple illustrant en quoi le jeu de données perpétue voire amplifie des biais pré-existants : en 2015, le logiciel de reconnaissance faciale Google Photo a classé dans la catégorie « gorille » l'image de deux personnes noires[46]. En cause : les images composant le jeu de données initiales, qui manquaient de diversité.

Le rôle clé de la donnée et de son interprétation, dans l'usage de l'IA : une position de plus en plus partagée par la communauté scientifique. De plus en plus de scientifiques et chercheurs prennent conscience de l'importance de disposer de données vérifiées et variées, mais également et surtout de l'absolue nécessité de sensibiliser et d'éduquer le public pour interpréter, avec toutes les précautions qui s'imposent, les résultats qui produisent les IA. C'est ce qu'exprime très clairement Laurence Devillers (Professeure en Informatique et Intelligence Artificielle à Sorbonne Université) en indiquant :
« avec l'IA et le Big Data, on peut par exemple chercher à modéliser les comportements sociaux afin de pouvoir les prédire. (...) ces modèles présentent souvent des biais, liés au choix des données par l'ingénieur. (...) Il faut être conscient que le choix des données est primordial mais aussi les paramètres qui sont choisis et optimisés par les concepteurs. Si, bientôt, les robots apprennent tout seuls à partir des données qu'ils collectent sans surveillance, ces biais refléteront aussi ceux de notre société.[47]»
Ainsi, poursuit la chercheuse, *« si l'on demande à une machine d'effectuer un recrutement à haut niveau, après lui avoir fourni des données représentant la sélection de ce type de candidats telle qu'elle est faite par des humains, alors elle sélectionnera principalement des hommes[48]».*

45 http://www.slate.fr/story/168413/amazon-abandonne-intelligence-artificielle-sexiste
46 http://www.lefigaro.fr/secteur/high-tech/2015/07/02/32001-20150702ARTFIG00144-la-technologie-de-reconnaissance-faciale-est-elle-raciste.php
47 https://www.usinenouvelle.com/blogs/laurence-devillers/les-representations-des-femmes-en-robotique-et-en-ia.N750239
48 https://www.google.com/amp/s/www.numerama.com/politique/330075-les-intelligences-artificielles-sont-elles-sexistes-des-specialistes-nous-repondent.html/amp.

II. RÉFLEXIONS

Ainsi, même si, comme certains de ses partisans peuvent le laisser entendre, l'IA, n'est pas une reproduction de l'intelligence humaine et – surtout – les données qui l'alimentent sont clé, il n'en demeure pas moins que son usage généralisé va entraîner de profonds bouleversements technologiques, économiques et juridiques, et soulever des questions éthiques.

Il est en conséquence nécessaire de prendre conscience des risques que certaines dérives pourraient entraîner tout en gardant à l'esprit les bénéfices que l'usage de l'IA pourrait apporter afin de tenter d'en dégager des principes, règles et bonnes pratiques d'utilisation.

Commençons par les questions éthiques, qui détermineront en partie les enjeux juridiques – en raison du lien étroit existant entre morale et droit –, puis nous aborderons ensuite la dimension technologique pour achever ces réflexions sur les impacts économiques de l'IA.

2.1. DIMENSION ÉTHIQUE

Si la technologie est moralement neutre, son usage ne l'est jamais. Comme l'évoquait Yann LeCun lors d'un entretien avec le Cercle de la Donnée, la technologie n'est *a priori* ni bonne, ni mauvaise. Tout dépend de l'usage qu'on en fait. Ainsi, la même technologie de reconnaissance d'image qui permet de déceler des tumeurs a été utilisée par la Chine pour mettre au point la reconnaissance faciale généralisée dont on entend parler avec effroi. Les progrès médicaux rendus possibles par l'IA (*cf supra*) peuvent également conduire à des risques d'eugénisme ou de médecine à deux vitesses. Ainsi, par exemple, aux Etats-Unis se développent des algorithmes capables de déterminer les chances de survie des patients atteints de maladies cardiaques admis dans les hôpitaux ; de là à traiter en priorité les cas estimés le plus « sauvables », il n'y a qu'un pas. La dimension éthique de l'IA est donc cruciale car elle est la clé d'un développement positif de ces technologies et de leur acceptation par la société. Nous évoquerons les enjeux éthiques de l'IA avant d'envisager les mesures à mettre en place pour s'assurer du développement d'IA éthiques. Nous verrons alors que la dimension étatique n'est pas suffisante et que des instances supranationales doivent être créées pour veiller aux aspects éthiques de l'IA.

2.1.1 LES ENJEUX ÉTHIQUES LIÉS À L'IA

Le risque d'une dépossession de toute réflexion. De notre téléphone à notre GPS, en passant par notre ordinateur portable, partout, dans notre vie quotidienne, l'IA nous assiste dans une recherche permanente du « plus facile, plus rapide, plus efficace ». Au-delà du fait que nous n'habituons plus nos cerveaux à réfléchir ou retenir (quel besoin de retenir un itinéraire puisque le GPS est là pour nous guider), nous cédons par là-même une partie de notre libre-arbitre et de notre autonomie de réflexion à des machines, sans connaître dans le détail la façon dont elles font leurs choix. Comme le dit Éric Schmidt, Directeur général de Google : *« Nous savons en gros qui vous êtes, en gros ce qui vous intéresse, en gros qui sont vos amis. La technologie va être tellement bonne qu'il sera très difficile pour les gens de voir ou de consommer quelque chose qui n'a pas été quelque part ajusté pour eux*[49]*. »* Ajusté pour eux… mais au bénéfice de qui ? Entre prévenir les besoins des consommateurs et les créer, la limite est ténue… Et les choix proposés par les machines ne sont pas forcément au bénéfice de ceux-ci : on peut par exemple citer les sites de ventes en ligne des billets de train, ou d'avion, dont le prix du billet est adapté à la hausse entre deux visites sur le même site. Ou encore les applications GPS, dont on pourrait soupçonner qu'elles favorisent les trajets avec péage, ou incitent leurs utilisateurs à emprunter un itinéraire de délestage, même s'il est plus long et lent que l'itinéraire principal. Si déléguer à la machine le soin d'analyser et de choisir pour nous est un gage d'efficacité et de simplicité, nous devons nous assurer d'être au clair sur les critères qui déterminent les choix proposés par ces intelligences artificielles.

Une exposition extrême de notre existence. Si certains voient dans les enceintes connectées de potentiels espions à la solde des géants mondiaux du numérique (ou autres), force est de constater que l'intelligence artificielle est déjà présente dans nos foyers et en mesure de révéler tout – ou presque – de nous. Ainsi, des chercheurs ont pu démontrer qu'à partir des données Netflix d'un foyer, on pouvait à peu près tout savoir des personnes qui le composent : leur âge, leur orientation sexuelle, leur tendance politique, leurs centres d'intérêt. De la même façon, les compteurs connectés Linky peuvent déceler qui est où et quand dans son habitation et laisser deviner ce qu'il fait. Cela pose naturellement la question du droit à la vie privée… Et interroge sur ce qu'il pourrait advenir si ces données tombaient dans des mains malintentionnées. Numérisation pourrait alors rimer avec surveillance généralisée.

Une possible déresponsabilisation. Dès lors que l'on délègue à des machines certaines de nos actions, se pose la question de la déresponsabilisation. Ainsi, le développement d'armes autonomes, rendu possible grâce aux progrès de l'IA, rend la décision de tuer moins difficile. Moins sujettes aux erreurs humaines, permettant d'engager moins de soldats sur des zones de guerre, elles peuvent en contrepartie avoir pour écueil de diminuer l'aversion aux conflits des populations, et de déresponsabiliser les chefs d'état-major.

49 https://www.numerama.com/magazine/16522-le-patron-de-google-pense-que-les-jeunes-changeront-de-nom-a-la-majorite.html

2.1.2. QUELLES MESURES POUR Y REMÉDIER ?

Des choix de société qui engagent tout le monde.

Les questions éthiques soulevées par les projets d'IA doivent être posées et tranchées de façon ouverte et collective et non pas confisquées par les grands acteurs du numérique ou les experts de la donnée. Des débats collectifs et publics sont en effet nécessaires pour établir des choix structurants pour nos sociétés. Ces décisions devront être reprises et traduites dans le code des IA de façon précise et fidèle par les experts de la donnée. L'éducation et la culture doivent également se faire l'écho de ces choix de société, de façon à développer un sens civique et sensibiliser aux enjeux éthiques liés à ces questions.

Une démarche étatique pour une utilisation éthique de l'IA.

L'éthique est désormais prise en considération au niveau des entreprises, conscientes de l'impact de l'usage de l'IA sur leur image. Ainsi apparaît une nouvelle fonction, celle de Chief Ethics Officer avec l'objectif clairement affiché d'ajouter un «traitement déontologique» des données de leurs clients à celui purement technologique et mercantile. Au vu des enjeux soulevés, il semble cependant évident qu'un encadrement de l'IA est nécessaire au niveau étatique et donc politique, et qu'il passe par l'examen et la détermination de ce qui justifie, aux yeux de la société, l'utilisation de ces technologies, et les rend acceptables. C'est bien au niveau des Etats qu'il faut encadrer la façon dont les IA seront programmées et utilisées. Les données disponibles jouant un rôle clé dans le développement des intelligences artificielles, on peut envisager, à l'instar de Guillaume Poupard, directeur de l'ANSSI (*cf annexe 4.3*), la mise en place au niveau étatique de sentinelles des données, gardiens du temple, qui décideraient d'ouvrir ou non la porte aux Intelligences Artificielles qui en demanderaient l'accès. On pourra ainsi mieux contrôler qui vient et qui ne vient pas. Et ne donner que le résultat du « machine learning » et non pas la source.

Une « éthique universelle » de l'IA difficile à définir mais nécessaire.

Cependant, l'IA et les problématiques qu'elle soulève transcendant les frontières, la définition d'une « éthique universelle » de l'IA semble nécessaire. Elle sera sans doute difficile à mettre en œuvre, compte tenu des disparités culturelles entre les pays, et des niveaux d'acceptabilité disparates. Ainsi, par exemple, le Japon, confronté à une population vieillissante et une main d'œuvre qui se raréfie, voit dans les robots et l'IA une opportunité considérable pour maintenir la productivité du pays là où d'autres populations, européennes notamment, sont très réticentes face au développement de ces technologies. Reposant sur une vision commune, cette éthique universelle de l'IA pourrait se matérialiser par la création d'un organe supra-étatique de « contrôle » qui veillerait au respect de règles éthiques élémentaires collectivement reconnues et acceptées.

2.2. DIMENSION JURIDIQUE

Ethique et droit : un lien évident. *« Le droit apparaît comme la médiation entre la politique et l'éthique (…) : on n'obéit qu'à un ordre juste, et pas seulement parce qu'il est établi »* déclarait le Professeur Bruno Oppetit[50], qui soulignait avec justesse les liens forts qu'entretiennent éthique et droit. Ainsi, le droit ne peut pas ignorer l'éthique dont il doit reprendre les valeurs les plus essentielles. En ce sens, il s'appuie sur un ensemble de principes fondamentaux : les droits et libertés primordiaux pour les individus qui, bien souvent, traduisent des valeurs éthiques, sorte de morale collectivement admise qui légitime la contrainte juridique. Ce lien entre éthique et droit apparaît avec d'autant plus d'évidence lorsqu'il s'agit de réguler des bouleversements aussi fondamentaux que ceux qu'annonce l'arrivée de l'IA, car, derrière la règle de droit, se profile le projet de société dans lequel nous voulons vivre. Les développements précédents ont montré combien l'usage de l'IA était porteur de promesses, mais également de risques pour la quiétude et la vie privée des personnes ainsi que pour la sécurité des organisations. C'est donc un exercice de mise en balance auquel les acteurs de droit (législateur, juges, praticiens…) doivent se livrer pour parvenir au bon équilibre entre le juste et l'utile. Pour mener cet exercice, nous verrons que le juriste dispose d'un cadre normatif qui, contrairement à certaines idées reçues, existe et peut s'appliquer à l'IA, même s'il présente certaines limites dans sa mise en pratique, à ce jour. Ces limites peuvent néanmoins être dépassées en appliquant pleinement et mieux ce cadre qui peut constituer un vecteur de confiance, devenant alors un véritable atout pour le développement d'une IA vertueuse. Compte-tenu du format de la présente étude, les développements qui suivent ne prétendent à aucune exhaustivité.

50 B. Oppetit, « Philosophie du droit », Précis Dalloz (1999), §134, p. 142.

2.2.1 LE DROIT ACTUEL ET SES QUESTIONS

S'il est coutume, pour certains juristes qui se sont intéressés à l'IA, de souligner les limites du droit actuel face à ce phénomène, il est plus rare de voir l'exercice inverse, lequel a pourtant pour principale vertu d'amener les praticiens à (re)découvrir la puissance et la souplesse de certains mécanismes de droit ancien, sans encombrer un univers législatif déjà bien surchargé. Voyons donc ce qui existe, avant d'examiner ses limites.

A. SES FORCES

Aucun régime juridique spécifique n'encadre l'intelligence artificielle en tant que telle. Pour autant, le droit existant n'est pas dénué de ressources pour, d'une part, protéger les individus des éventuelles dérives de cette technologie et, d'autre part, permettre aux acteurs de l'IA de protéger leurs actifs.

A.1. LE DROIT OFFRE DES GARDE-FOUS AUX UTILISATEURS DE L'IA

a. PROTECTION DES DONNÉES PERSONNELLES

Un cadre de protection doté désormais de sanctions dissuasives. La réglementation sur la protection des données personnelles[51] va trouver à s'appliquer très fréquemment dans les projets d'intelligence artificielle dès lors que l'IA implique un traitement de données *« personnelles »* ou *« à caractère personnel »*[52]. Cette règlementation est régie par des grands principes (loyauté, licéité, transparence, minimisation, information etc.), que le RGPD a récemment assorti de sanctions significatives[53]. Ces principes appliqués à l'IA vont protéger l'homme face à la machine et à ses dérives, notamment lorsque ces dernières peuvent être amenées à prendre de véritables décisions qui peuvent être aveugles (ne prenant pas suffisamment en compte certaines circonstances de fait), opaques (phénomène des *« boîtes noires »*), et erronées (si les auteurs de l'algorithme ont retranscrit imparfaitement les règles matérielles édictées par les autorités)[54].

L'interdiction des IA décisionnelles, sauf cas exceptionnels. Le recours aux décisions automatisées qu'une machine peut prendre emportant des conséquences cruciales pour les personnes (telles que, par exemple, l'octroi d'un crédit), le législateur (communautaire et français) a pris soin de les encadrer en les subordonnant à la nécessité d'une intervention humaine, sauf dans certains cas limitativement énumérés par les textes[55]. Ces règles permettent ainsi de confiner à des cas exceptionnels le recours à l'IA pour des prises de décisions, puis, dans de tels cas, oblige le responsable de traitement à une transparence permettant à l'individu de comprendre le fonctionnement de l'IA et de pouvoir, le cas échéant, exercer ses droits.

---

51 Règlement Général sur la Protection des Données (« RGPD ») n° 2016/679, entré en application le 25 mai 2018, les lois nationales applicables (à savoir, en France, la loi n° 78-17 du 6 janvier 1978 – dite « loi Informatique et libertés » ou « LIL » – modifiée dernièrement par l'ordonnance n°2018-1125 du 12 décembre 2018 entré en vigueur le 1er juin 2019).

52 Cette notion est entendue très largement, puisqu'elle vise non seulement les données directement identifiantes, mais également celles qui le sont indirectement (comme des numéros, des identifiants de moyens matériels ou logiciels permettant de se connecter à un réseau, ou encore les données de localisation).

53 Les sanctions prévues par le RGPD vont jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent de l'entité responsable.

54 Rapport enregistré à la Présidence du Sénat en date du 18 avril 2018 (p.40).

55 En France, les textes prévoient ainsi trois cas exceptionnels dans lesquels il est possible de déléguer à un dispositif artificiel une prise de décision : (i) toute d'abord lorsque ce recours est « fondé sur le consentement explicite de la personne » (Article 47, alinéa 2, 1° nouveau de la LIL, se référant à l'article 22.2, c) du RGPD), (ii) ensuite celle-ci est « nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable de traitement » (Article 47, alinéa 2, 1°nouveau de la LIL, se référant à l'article 22.2.a) du RGPD), et (iii) enfin pour les prises de « décisions administratives individuelles » à condition (iii.1) qu'un tel traitement ne porte sur aucune donnée sensible, (iii.2) que les décisions automatisées générées ne se prononcent pas « sur un recours administratif » et (iii) qu'elles comportent « à peine de nullité » une mention à ce sujet (article 47, alinéa 2° nouveau de la LIL, étant précisé que cette dernière obligation d'information n'entre en vigueur qu'à compter du 1er juillet 2020 (Article 37 de la loi n°2018-493 du 20 juin 2008 ».

b. RESPONSABILITÉ CIVILE

La responsabilité délictuelle. Tout d'abord, le régime de responsabilité du fait des choses peut s'appliquer à l'IA. Il suppose qu'un individu cause à autrui un préjudice par le biais d'une chose, dont il aurait eu l'usage, la direction et le contrôle au moment du dommage[56]; en pratique, on pourrait ainsi imaginer que l'utilisateur d'une IA lui délivrant des résultats financiers incohérents au regard des données sources – exactes et vérifiées – mises à sa disposition, pourrait engager la responsabilité de la société (gardienne de l'IA) lui ayant fourni un tel service. Ensuite, le régime de responsabilité du fait des produits défectueux est aussi envisageable : pour engager la responsabilité d'un producteur sur ce fondement, il faut prouver qu'un produit est défectueux (c'est-à-dire présente un défaut de sécurité), cause un dommage et que la victime soit en mesure de démontrer un lien de causalité entre le défaut et le dommage subi[57]. Ce régime s'applique déjà en matière de logiciels[58], mais seulement pour *« les situations où ceux-ci seraient à l'origine directe d'une atteinte à la sécurité des personnes ou des biens »*[59]. L'IA s'appuyant sur des algorithmes informatiques, ce régime pourrait donc s'appliquer à celle-ci.

La responsabilité contractuelle. Lorsque la victime est liée à l'exploitant de l'IA par un contrat, il est toujours envisageable d'avoir recours au mécanisme de responsabilité contractuelle pour se protéger des éventuelles dérives de l'IA. Dans la tradition jurisprudentielle française – tout comme celle-ci n'a cessé de le faire avec les différentes évolutions technologiques et économiques tout au long des 19ème et 20ème siècles –, on peut faire confiance aux juges pour interpréter, voire même compléter, le contenu des contrats qui, en la matière, seront probablement lacunaires.

56 Art. 1242 du Code civil.
57 Art. 1245 du Code civil.
58 Commission européenne, réponse parlementaire du 15 novembre 1988.
59 Réponse ministérielle n°15677 : JOAN R, 24 août 1988.

A.2. LE DROIT PROTÈGE LES INVESTISSEMENTS DES ACTEURS DE L'IA

a. PROTECTION DES ALGORITHMES ET DES DONNÉES ALIMENTANT L'IA

Le secret des affaires : une piste intéressante de protection. Compte tenu des limites présentées par les droits de propriété intellectuelle pour protéger efficacement l'IA[60], la règlementation, adoptée récemment[61], sur le secret des affaires est intéressante : celle-ci permet d'obtenir une protection pour toute information qui n'est pas généralement connue ou aisément accessible et qui revêt une valeur commerciale du fait de son caractère secret. Ainsi, un acteur de l'IA va pouvoir bénéficier d'une protection pour son algorithme, ainsi que les données que celle-ci utilise, dès lors qu'il pourra prouver avoir mis en œuvre les mesures de protection raisonnables pour en conserver le caractère secret.

b. DROIT DES CONTRATS

Un outil utile indispensable pour définir les responsabilités des différents acteurs. Dans les solutions d'IA complexes où plusieurs acteurs interviennent, le contrat va permettre de répartir la responsabilité de chacun par le jeu des garanties notamment, et d'offrir par la même occasion des recours plus clairs aux différents acteurs de la chaîne (y compris les utilisateurs finaux) en cas de litiges.

Quelques clauses essentielles. Tout d'abord, la clause de responsabilité revêt une importance particulière. Pour s'exonérer de sa responsabilité, le concepteur ou programmateur de l'IA aura tout intérêt à bien définir l'usage attendu de la solution pour qu'il lui soit plus facile d'exclure les dommages éventuels qui n'étaient absolument pas prévisibles, sous réserve toutefois qu'ils ne soient pas dus à une faute lourde ou dolosive[62] et que cela n'ait pas pour résultat de priver le contrat de sa substance[63]. Ensuite, il faudra veiller à prévoir une clause de confidentialité, notamment lorsque la protection par le brevet n'a pas été souhaitée ou possible, afin de bénéficier de la protection au titre du secret des affaires. Enfin, une clause pourra utilement restreindre l'usage des données alimentant l'IA, permettant de protéger contre les extractions faites par les utilisateurs lorsque les données ne répondraient pas aux critères exigés pour obtenir une protection par le droit *sui generis*, comme l'a montré la jurisprudence Ryanair[64].

60 Entendue comme une suite d'instructions permettant de résoudre un problème, l'algorithme est au cœur de l'IA, et n'est pas protégeable, en tant que tel, ni par le droit des brevets ni par le droit d'auteur. A supposer même que l'algorithme puisse être protégé lorsqu'il est intégré dans une invention brevetable, ou par le droit d'auteur lorsqu'il est transcrit en code informatique, dans un logiciel (sous réserve d'être original, ce qui s'avère bien souvent complexe à démontrer en pratique), ces protections manquent d'efficacité : la première car elle contraint à révéler l'algorithme dans les revendications du brevet, la seconde parce que le droit d'auteur ne protégeant pas l'algorithme en tant que tel, un tiers pourrait ainsi parvenir à extraire l'algorithme et à l'utiliser de façon tout à fait légale. Quant aux données alimentant les solutions d'IA, la personne à l'origine de l'IA pourra éventuellement bénéficier du droit sui generis de producteur de base de données s'il peut prouver, d'une part qu'il a réalisé des investissements significatifs, financiers, matériels et humains, pour la constituer, et d'autre part que les données sont structurées, ce qui, en pratique, ne sera pas toujours possible à prouver.

61 Directive (UE) du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites ; Loi n° 2018-670 du 30 juillet 2018 et Décret n° 2018-1126 du 11 décembre 2018 relatifs à la protection du secret des affaires.

62 Article 1231-3 du Code civil

63 Article 1170 du Code civil

64 CJUE, 15 janvier 2015, Ryanair Ltd c. PR Aviation BV, aff. C-30/14. Dans cette affaire, les magistrats communauté ont condamné un tiers ayant utilisé la base de données d'une société qui, bien que non couverte par le droit *sui generis*, l'était en revanche par un contrat fixant les limites d'utilisation des données que le tiers avait violées.

B. SES LIMITES

Le droit existant s'avère toutefois encore insuffisant pour lutter contre les effets néfastes de l'IA ou les conséquences de sa complexité et se présente même parfois comme une contrainte.

B.1. AU REGARD DES DONNÉES

L'absence de cadre juridique d'ensemble protégeant les données à caractère non personnel. L'IA se nourrit de données qui ne sont pas toutes personnelles, et peut avoir des impacts non seulement au niveau individuel mais également collectif. Le régime de protection des données personnelles offre donc une protection partielle, en l'absence, à ce jour, de texte général équivalent applicable aux données à caractère non personnel[65].

La complexité du RGPD, entravant la collecte massive de données, peut paradoxalement favoriser les biais. Une quantité de données insuffisante et imparfaitement représentative de l'ensemble d'une population, est source de biais qui faussent les résultats d'une IA. Les contraintes exercées par le RGPD sur les acteurs de l'IA (minimisation des données, consentement, information des personnes, etc.) peuvent occasionner des biais mais aussi freiner l'innovation dans des domaines tels que la recherche médicale.

B.2. AU REGARD DE LA RESPONSABILITÉ

Imputabilité du fait dommageable : la complexité de l'IA. Face à une discrimination, il peut être complexe de démontrer en quoi la discrimination est due à un dysfonctionnement de l'IA, notamment pour les systèmes grâce auxquels la machine acquiert une autonomie relative au fil de son apprentissage, d'autant que les acteurs de l'IA, dans un souci de protection de leurs actifs, ont plutôt tendance à manquer de transparence. Il en découle une vraie difficulté pour les individus à faire valoir leurs droits et à obtenir réparation, le cas échéant. La transposition des régimes de responsabilité à l'IA soulève aussi des difficultés quant à la responsabilité des différents acteurs et au critère de prévisibilité des dommages. En matière de responsabilité du fait des produits défectueux, il sera par exemple difficile de déterminer qui a la qualité de « producteur » entre le vendeur de l'objet fini, le concepteur ou le programmeur. Dans la responsabilité du fait des choses, le critère de la garde impose d'identifier le gardien de la chose qui a causé le dommage. Mais le robot autonome s'émancipe de son gardien, ce qui lui permet de prendre des décisions imprévues par le concepteur à l'origine.

Imprévisibilité du dommage : le défi de l'IA. Alors que notre régime du droit de la responsabilité est fondé avant tout sur le caractère prévisible du dommage à la conclusion du contrat[66], l'IA fonctionne sur un principe d'apprentissage continu par la machine qui rend très difficilement prévisible les dommages qui surviendront en cours d'exécution du contrat. Ainsi, pour certains, le concepteur d'une IA autonome pourra arguer qu'il ne pouvait pas anticiper toutes les décisions de l'IA, et être dès lors tenu responsable de ses décisions imprévues. Pour d'autres, en créant un algorithme autonome, le concepteur connaissant par principe le caractère imprévisible des décisions à venir de la solution, devrait donc à ce titre être considéré comme son gardien.

65 Certes, il existe le Règlement communautaire n°2018/1807 « établissant un cadre applicable au libre flux de données à caractère non personnel au sein de l'union européenne » (adopté le 14 novembre 2018 et entrant en vigueur le 19 juin 2019), mais celui-ci traite d'aspects partiels (prohibition de restriction de localisation de données au sein de l'UE, libre accessibilité des données par les autorités nationales, etc.) sans prévoir un régime d'ensemble comme le fait le RGPD pour les données à caractère personnel.

66 Article 1231-3 du Code civil

2.2.2 LA PRATIQUE DE DEMAIN ET SES RÉPONSES

Si certains courants prônent la création de droits *sui generis* comme la responsabilité spéciale du fait de l'IA (calquée sur la responsabilité du fait des animaux) ou une responsabilité indépendante (droit des robots[67]), il nous semble que l'IA autonome qui échapperait totalement au contrôle de son créateur relève plutôt du mythe que de la réalité, car, au stade actuel de développement de cette technologie, il y a toujours derrière l'IA une personne qui la paramètre et en détermine les choix[68] . Le principal défi n'est donc pas de créer un nouveau régime juridique spécifique dédié à l'IA, mais plutôt d'aménager le droit existant afin de le rendre favorable à une IA vertueuse – c'est-à-dire respectueuse des droits fondamentaux –, en privilégiant la souplesse et la simplicité.

A. RENDRE LE DROIT FAVORABLE À UNE IA VERTUEUSE

Afin que le droit existant apparaisse comme favorable à l'IA et non comme un frein, il faut que le respect du droit devienne un gage de confiance pour les individus qui accepteront, dès lors, d'y recourir plus largement, ce qui fera de la conformité un véritable avantage concurrentiel pour les offreurs d'IA conformes.

A.1. FAIRE DU DROIT UN GAGE DE CONFIANCE DANS L'IA

Généraliser à toutes les IA l'obligation de transparence sur la logique algorithmique (explicabilité). Pour mieux accepter les IA, les individus doivent en comprendre le fonctionnement, c'est-à-dire saisir celui de l'algorithme (explicabilité). Dans son rapport de décembre 2017[69], la CNIL préconise de renforcer les principes d'intelligibilité, de transparence et de loyauté afin de rendre les systèmes algorithmiques compréhensibles. La Commission européenne dans ses lignes directrices Ethiques pour une IA « *digne de confiance* » publiées le 8 avril 2019 confirme cette orientation en insistant sur la nécessité d'exiger une explicabilité de l'IA ; celle-ci se traduit notamment par la transparence de l'IA lors de son développement, son déploiement et lors de son utilisation, et permettrait de rendre plus facile son auditabilité. Cette exigence, qui figure déjà dans le RGPD pour les IA amenées à prendre des décisions[70], pourrait être généralisé pour toutes les IA, y compris celles ne traitant pas de données à caractère personnel[71].

Favoriser la médiation, l'audit et les certifications. Par ailleurs, la CNIL recommande la mise en place d'une médiation entre les responsables des systèmes algorithmiques et leurs utilisateurs (afin de rendre les premiers joignables ou accessibles pour fournir les informations et explications nécessaires), et préconise aussi de constituer une « *plateforme nationale d'audit des algorithmes* », mais cela suppose que la puissance publique ait les moyens et les capacités d'assurer ce rôle d'auditeur[72]. Enfin, la mise en place de certifications, comme les certifications ISO, ou le recours à des labels pourrait également être un gage de transparence et de confiance.

67 https://www.alain-bensoussan.com/droit-des-robots/
68 L'intelligence artificielle n'existe pas, Luc Julia, First éditions, janvier 2019
69 Synthèse du débat public animé par la CNIL dans le cadre de la mission de réflexion éthique confiée par la Loi pour une République numérique : https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf
70 Articles 13.2, f) et 14.2, g) du RGPD. Le droit d'accès prévoit une disposition analogue (article 15.1, h) du RGPD).
71 L'explicabilité ne devrait, en revanche, pas nécessairement résulter de la publication du code source. Celle-ci pourrait d'ailleurs s'avérer impossible dès lors que l'algorithme remplit les critères de protection par le secret des affaires.
72 Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle du 15 décembre 2017 : https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de

A.2. STRUCTURER DAVANTAGE L'ACCÈS AUX DONNÉES

Favoriser l'accès aux données. La donnée étant la matière première de l'IA, il est primordial d'en favoriser l'accès, ainsi que la circulation et le partage, afin d'assurer la pertinence et la justesse de l'IA. C'est d'ailleurs ce que préconise le Rapport Villani de mars 2018[73]. Il s'agit tout d'abord de poursuivre le mouvement d'ouverture des données publiques (dit « open data ») initié par l'Union européenne depuis une dizaine d'années et introduit en France par plusieurs lois telles que la loi Lemaire[74] ou d'autres lois spéciales sectorielles comme la loi Macron[75]. Plusieurs plateformes publiques « open data » ont ainsi vu le jour, afin de faciliter la recherche et par conséquent la réutilisation des données publiques concernées, comme par exemple la plateforme nationale d'accès aux données de transport et de mobilité mise en place par l'Etat[76] ou encore la toute nouvelle plateforme publiée par Etalab concernant la publication des demandes de valeurs foncières[77]. Ces plateformes créent en quelque sorte un cercle vertueux permettant aux (ré)utilisateurs d'enrichir l'IA qu'ils développent grâce à ces données, mais aussi de fiabiliser cette IA, d'une part en remontant d'éventuelles erreurs aux producteurs de données, et d'autre part, en diminuant le risque de biais du fait de la plus grande diversité des données accessibles. Le rapport Villani va plus loin en recommandant la constitution de « communs de la donnée » : la puissance publique doit inciter les acteurs économiques, y compris du secteur privé, au partage et à la mutualisation de la donnée, voire imposer l'ouverture des données dans certains cas.

Encadrer néanmoins cet accès. Toutefois, l'accès aux données ne signifie pas, selon nous, permettre une circulation anarchique de celles-ci, aboutissant à leur prolifération, ce qui serait un facteur de risques importants pour la cyber-sécurité et la vie privée notamment : l'accès aux données devra être encadré. Ainsi, des professionnels agissant sous le contrôle de la loi pourraient être nommés chargés d'inspecter la qualité et la licéité des données utilisées par une IA : des « commissaires à la donnée », à l'image des commissaires aux comptes. Par ailleurs, l'accès à la donnée pourrait être permissionné, c'est-à-dire réalisé sous le contrôle rigoureux de son producteur ; c'est l'idée émise par Guillaume Poupard, Directeur Général de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), dans son interview accordée au Cercle de la Donnée en avril 2019[78] : *« La vraie question est la suivante : comment casser l'idée communément admise et faussement intuitive que la donnée doit être amenée et transmise à ceux qui en ont besoin ? Pourquoi les Intelligences artificielles ne se déplaceraient-elles pas ? Pourquoi ne fonctionnerait-on pas avec des accès permissionnés ? Après tout, quand nous apprenons nous-même, nous nous déplaçons. Depuis des années, on s'escrime à vouloir désensibiliser des données, qui, au final, ne valent plus grand-chose pour les transmettre. Pourquoi ne pas imaginer des sentinelles des données, gardiens du temple, qui décideraient d'ouvrir ou non la porte aux intelligences artificielles qui en demanderaient l'accès ? On pourra ainsi mieux contrôler qui vient et qui ne vient pas. Et ne donner que le résultat du « machine learning » et non pas la source. »*

Protéger les investissements des producteurs de données. L'incitation des pouvoirs publics doit selon nous faire l'objet d'une grande vigilance et d'une certaine souplesse. En effet, la collecte et la mise à disposition des données nécessitent la plupart du temps des investissements importants de la part des acteurs qui en sont à l'origine. Le dimensionnement et la sécurisation de la plateforme, l'anonymisation, la mise au format et la mise à jour des données ont un coût que le producteur doit assumer. Il faudra donc veiller à ce que le système de partage ou de mutualisation des données mis en place reste attractif et permette un retour sur investissement à l'entité qui en est à l'initiative, faute de quoi cela pourrait produire l'effet inverse de celui escompté, à savoir moins de diversité et de pertinence des données.

73 Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne : https://www.aiforhumanity.fr/pdfs/9782111457089_Rapport_Villani_accessible.pdf
74 La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, dite loi Lemaire, vient modifier le code des relations entre le public et l'administration sur ce point
75 La loi n° 2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques, dite loi Macron, crée un nouvel article dans le code des transports concernant la mise à disposition en open data des données des services réguliers de transport public de personnes et des services de mobilité.
76 https://transport.data.gouv.fr/
77 https://app.dvf.etalab.gouv.fr/
78 cf annexe 2 de la présente étude

B. EN FAVORISANT LA SOUPLESSE ET LA SIMPLICITÉ

B.1. LA SOUPLESSE AU SERVICE DES ACTEURS

Eviter l'adoption précipitée de nouveaux textes. Un cadre légal trop rigide risque de devenir très rapidement obsolète du fait de l'évolution des technologies. Ainsi, plutôt que d'adopter des textes très précis, il semble préférable de favoriser l'émergence de lois décrivant des principes d'ordre général, assorties de dispositifs applicatifs souples tels que les chartes, pactes de conformité ou règles éthiques. Un corpus de droit souple semble en effet plus adapté au domaine de l'IA puisqu'il sera plus facile de le faire évoluer au même rythme que la technologie. Sur le plan historique, notre droit a déjà su s'adapter à des mutations économiques et technologiques décisives, sans évolution textuelle précipitée : on en veut pour preuve l'apparition du machinisme, à la fin du 19ème siècle, qui a vu naître une doctrine (celles du risque-profit) et une jurisprudence (celle ayant fait émerger les mécanismes de droit de la responsabilité sans faute – qui, pendant très longtemps, se sont appuyés sur les textes du code Napoléon, sans qu'il ne soit nécessaire d'adopter une multitude de lois spéciales) ayant permis d'accueillir, dans notre droit, les bouleversements de la grande révolution industrielle précédente, sans succomber à une frénésie législative, source de complexification. Les acteurs concernés doivent voir dans l'application des règles un avantage compétitif, ce qui sera le cas si le cadre juridique est reste lisible et souple.

B.2. LA SIMPLICITÉ AU SERVICE DES PERSONNES

Privilégier un droit de principe, sur une règlementation de détails. Pour bon nombre de personnes, l'IA est source de craintes car elle est encore perçue comme une machine incontrôlable par l'homme, pouvant avoir des effets potentiellement néfastes sur leur vie. Dans cette optique, il est important de favoriser l'accès à l'information des personnes concernées et du grand public en général en veillant à ce que l'information soit présentée de la façon la plus simple et la plus claire possible. Ainsi, il nous semble essentiel de ne pas fixer de manière détaillée la liste des informations que les acteurs de l'IA devraient fournir, mais de privilégier au contraire un devoir général d'information à la charge des acteurs de l'IA tout en leur laissant une certaine latitude quant aux informations à fournir et à la manière dont celles-ci seront exposées aux personnes concernées. En permettant que l'information soit donnée au juste nécessaire, c'est-à-dire qu'elle soit plus ou moins détaillée en fonction de la complexité et surtout des impacts de l'IA, cela évitera que les personnes ne se retrouvent noyées dans un trop plein d'informations de nature à rendre l'IA encore plus anxiogène. La condamnation de Google LLC par la CNIL le 21 janvier 2019 est une bonne illustration de l'effet contraire d'une information trop complexe[79].

Favoriser le droit souple, établi avec le concours des acteurs de l'IA (offreurs et utilisateurs). Etablir des lignes directrices par secteur d'activité ou type d'IA permet tout d'abord de faire une application de la règle de droit à l'IA sans perdre de vue son objectif tout en s'adaptant au contexte. Mais ces guides ont également vocation à vulgariser la loi afin d'informer les personnes de manière simple et accessible. C'est le cas par exemple des «packs de conformité» de la CNIL en matière de domotique[80] ou sur les compteurs Linky[81]. De telles pratiques devraient être généralisées afin de rassurer les personnes en rendant l'IA moins opaque et leur permettre de faire appliquer leurs droits.

79 https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000038032552&fastReqId=2103387945&fastPos=1
80 https://www.cnil.fr/sites/default/files/atoms/files/pack_silver_economie_v4.pdf Insérer lien pack domotique
81 https://www.cnil.fr/sites/default/files/typo/document/Pack_de_Conformite_COMPTEURS_COMMUNICANTS.pdf

2.3. DIMENSION TECHNOLOGIQUE

Le lien entre intelligence artificielle et technologie est profond et complexe. D'un côté, les avancées de l'IA sont intimement liées aux progrès – et limites – technologiques ; de l'autre, l'intelligence artificielle permet des avancées technologiques indéniables, dont on doit percevoir les risques, comme pour n'importe quel système d'information… utilisé par des humains.

2.3.1 DES AVANCÉES DE L'IA INTIMEMENT LIÉES AUX PROGRÈS OU LIMITES TECHNOLOGIQUES

Si les 30 dernières années ont été marquées par l'avènement de l'informatique, l'effervescence et l'engouement actuels pour l'intelligence artificielle laissent penser qu'il s'agit de la nouvelle révolution technologique qui va bousculer les 30 prochaines années.

Le terme d' « intelligence artificielle » introduit un malentendu.
Utilisé par les chercheurs John McCarthy et Marvin Minsky en 1956 lors de la conférence de Dartmouth, il crée une confusion entre intelligence naturelle et artificielle, certainement voulue sciemment par ces chercheurs qui souhaitaient retenir l'attention de leurs financiers. Cette confusion laisse entendre que la technologie pourrait reproduire, voire dépasser l'intelligence humaine. Un tel raisonnement conduit au rêve ultime de transhumanisme, c'est-à-dire à l'interconnexion entre le cerveau humain et la machine. Une des théories transhumanistes, l'uploading, estime que grâce à la technologie, l'homme pourra enfin s'affranchir des limites du corps que Platon décrivait déjà comme « le tombeau de l'âme ».
De telles théories reposent sur la foi dans le progrès perpétuel et exponentiel de la science et la technologie, s'appuyant notamment sur la loi de Moore, selon laquelle la puissance de l'informatique double tous les 18 mois. Il nous semble qu'il faut démystifier ces théories car :

- d'une part, la loi de Moore ne tient pas compte des facteurs limitant qui peuvent survenir (crise énergétique ou écologique par exemple) ;
- d'autre part, nous ne savons rien du fonctionnement de l'intelligence humaine, ni des mécanismes complexes de notre cerveau (*cf supra – Approche scientifique*). Nous ne sommes donc technologiquement pas en mesure, aujourd'hui, de modéliser un système capable de reproduire l'intelligence humaine.

Depuis sa création, l'IA se heurte aux limites technologiques. En effet, si on en parle beaucoup depuis quelques années, l'intelligence artificielle ne date pas d'hier. Ainsi, dès 1957, Franck Rosenblatt, un psychologue américain invente un algorithme d'apprentissage, appelé perceptron, sensé simuler les fonctions d'un neurone pour classifier des images. Le perceptron est à l'origine des réseaux de neurones, qui constituent aujourd'hui encore l'une des bases de l'apprentissage des machines, le « Machine Learning ». Le développement de l'IA a été marqué par une succession de phases d'euphorie et de phases de découragement, surnommées « hivers de l'IA » (AI Winter). L'intelligence artificielle en a déjà connu deux. Au début des années 1970, tout d'abord, après plus de dix ans passés à essayer en vain de résoudre des problèmes liés au langage, à la traduction automatique ou à représenter des problèmes complexes avec les réseaux de neurones simplistes de l'époque. Le second hiver est survenu à la fin des années 1980, décennie durant laquelle l'essor des ordinateurs personnels avait remis l'IA à la mode, laissant espérer qu'on allait disposer d'une plus grande puissance de calcul, et donc croire à l'émergence d'un ordinateur intelligent grâce à grâce à la mise en réseau des ordinateurs. A nouveau, les résultats ont tardé à arriver, plongeant une nouvelle fois l'IA dans une phase d'hibernation. C'est l'émergence d'internet à la fin des années 1990, avec sa quantité massive de données et la naissance du Big Data qui a relancé l'IA et son lot de promesses. Ainsi, les progrès de l'intelligence artificielle sont intimement liés aux évolutions technologiques de ces dernières années, qui ont permis d'augmenter les capacités de mémoire et la vitesse de calcul.

L'IA est fortement dépendante des progrès technologiques réalisés dans le domaine matériel. Les performances de l'intelligence artificielle sont en effet intimement liées à la capacité de mémoire et à la puissance de calcul. A titre d'exemple, pour qu'une machine reconnaisse un chat avec une précision de 95%, il faut lui fournir près de 100 000 images de chats. Or, comme l'indique Luc Julia[82] *« les machines sont incapables de contextualiser. Si, lors de la phase d'apprentissage, on n'a pas fourni d'images de chats prises de nuit, il y a peu de chances que le système reconnaisse un chat la nuit… On peut bien sûr multiplier les paramètres et augmenter les jeux de données, mais outre le fait qu'il sera difficile de modéliser tous les états et toutes les circonstances […], des problèmes de capacité mémoire et de puissance de calcul se poseront ».* On voit donc les limites technologiques de l'IA, qui nous indiquent qu'il faut raison garder quant aux promesses qui lui sont associées.

2.3.2 DES BÉNÉFICES INDÉNIABLES…

Incontestablement, l'IA permet des avancées positives pour l'homme : en prenant en charge de plus en plus de tâches répétitives, la machine permet de diminuer la pénibilité du travail, permettant à l'homme de se concentrer sur les tâches les plus poussées, de gagner du temps et du confort. Au-delà de cette baisse de la pénibilité, qui est fortement liée à l'automatisation et la robotisation, l'IA permet notamment des avancées significatives dans de nombreux domaines demandant de grandes capacités de traitement. Ci-après quelques exemples relatifs à la lutte contre les maladies.

- **Algorithme de reconnaissance d'images pour déceler les tumeurs**

  On voit déjà ses premières applications en termes de recherches contre le cancer, les algorithmes de reconnaissance visuelle permettant de déceler des tumeurs avec précision. Ces avancées technologiques, loin de faire disparaître les médecins cancérologues, leur permettent de gagner un temps précieux, qu'ils peuvent utiliser pour s'occuper des cas les plus complexes.

- **Séquençage du génome humain pour lutter contre la leucémie**

  Un autre exemple emblématique concerne le séquençage du génome humain. Un ordinateur est capable aujourd'hui de décrypter 1,8 terabit de données en 3 jours, l'équivalent de 16 génomes humains. Ce qui coûtait dix ans de travail et plusieurs milliards est donc réalisable aujourd'hui en moins de 24 heures. Forts de ces progrès, des spécialistes de la génétique travaillent sur la leucémie, s'attachant à séquencer les génomes de 1500 personnes atteintes de cancers pour repérer quelles mutations de l'ADN peuvent être associées au développement de la maladie. Sur 1500 patients, 5000 mutations et 1000 combinaisons différentes ont été trouvées. Cette approche représente un gain de temps considérable et permet aux praticiens de prendre des décisions beaucoup plus rapides et plus renseignées.

- **Pharmacovigilance**

  L'IA peut également favoriser la pharmacovigilance. Ainsi, en 2015, une collaboration entre le CNAM et l'école Polytechnique a déjà débouché sur la création d'une formule capable de détecter un médicament potentiellement cancérigène, grâce à l'analyse de la base de données du Système national d'information inter-régimes de l'Assurance maladie (STNIIRAM), ainsi que l'a expliqué le responsable du projet, le chercheur en mathématiques appliquées Emmanuel Bacry.

Ces exemples illustrent la force du binôme machine-humain.

On le voit, l'IA peut être complémentaire de l'humain, pour son plus grand bénéfice.

82 Luc Julia, « L'intelligence artificielle n'existe pas » (First Editions, 2019).

2.3.3 …MAIS DES RISQUES À PRENDRE EN COMPTE

Si les bénéfices de l'IA sont indéniables, il faut également prendre en compte les aspects plus problématiques liés au développement de ces technologies.

Sur le plan écologique, une consommation d'énergie exponentielle. Ainsi, pour battre le champion du monde de Go, AlphaGo a nécessité pas moins de 1500 CPU, 300 GPU et 300 TPU consommant pas moins de 400 kW/heure. En comparaison, un cerveau humain consomme seulement 20kW/heure. Et là encore, il semble important de préciser que cette machine, aussi puissante soit-elle, n'était en mesure de dépasser le cerveau humain que sur un seul domaine très spécifique, le jeu de go. On imagine dès lors les capacités de calculs et donc les ressources énergétiques associées qui seront nécessaires dans le cadre d'IA encore plus complexes.

Des systèmes d'information vulnérables aux cyberattaques. Aussi sophistiquées soient-elles, les IA sont vulnérables aux attaques et, comme tout système d'information, méritent donc d'être protégées. Parmi les risques identifiés, on peut citer notamment :

(I) Les attaques touchant à la disponibilité de l'IA

Elles visent à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service[83]. Une attaque majeure de ce type visant les services de Domain Name System (DNS) de la société Dyn a ainsi paralysé une partie du web pendant près de 10h à l'automne 2016, rendant inaccessible de nombreux sites utilisant ce service (Twitter, Netflix, Paypal, Ebay…)[84]. Ces attaques, vieilles comme l'informatique, peuvent bien évidemment affecter des Intelligences Artificielles, pour les rendre inaccessibles. Ainsi, par exemple, saturés de questions, des bots ne pourraient plus répondre aux sollicitations des internautes. Les spécialistes de la cybersécurité s'accordent à dire que ces menaces sont aujourd'hui bien identifiées et prises en compte par les grands acteurs du numérique.

(II) Les attaques concernant les jeux de données de référence

Comme nous l'avons déjà évoqué plus haut (*cf partie 1.2.2.B*), un jeu de données de référence pas assez représentatif peut conduire à des biais. Ainsi, par exemple, le programme Compas (Correctional Offender Management Profiling for Alternative Sanctions) développé par la société Northpointe pour « prédire » la récidive et utilisée par certains juges comme une aide à la décision s'est révélé bien plus sévère à l'égard des prévenus afro-américains[85] qu'à l'égard des autres prévenus. Une des raisons identifiées ? La prise en compte dans le jeu de données de référence de critères comme le nombre de condamnations, qui trahissent eux-mêmes des inégalités raciales : à crimes et délits égaux, les noirs sont plus souvent condamnés que les blancs[86].
Dès lors, on peut imaginer les conséquences particulièrement néfastes si, de façon insidieuse ou indétectable, une personne malintentionnée venait polluer un jeu de données de référence, de façon à introduire un biais dans les décisions prises par la suite par l'IA. Vue l'importance des jeux de données de référence dans le processus d'apprentissage et de décision des IA, une attention particulière devra être portée à la protection de ces derniers, afin d'être sûrs que les systèmes interprètent des données intègres.

83 https://www.cybermalveillance.gouv.fr/nos-articles/deni-de-service/
84 https://www.lemonde.fr/pixels/article/2016/10/21/une-cyber-attaque-massive-perturbe-de-nombreux-sites-internet-aux-etats-unis_5018361_4408996.html
85 https://www.theguardian.com/inequality/2017/aug/08/rise-of-the-racist-robots-how-ai-is-learning-all-our-worst-impulses
86 https://www.sciencesetavenir.fr/high-tech/intelligence-artificielle/pour-predire-la-recidive-l-interet-limite-des-algorithmes_120238

(III) Les attaques visant à perturber les données soumises à l'IA

Sans s'en prendre au jeu de données de référence, on peut également perturber un système de reconnaissance d'image en déformant les images qui lui sont soumises de façon subtile, indécelable à l'œil nu. Ainsi, par exemple, des tests ont été réalisés par l'université de Washington sur des panneaux de signalisation routière[87]. Des panneaux sur lesquels avaient été préalablement apposés des autocollants ont été présentés à une intelligence artificielle entrainée à identifier différents panneaux de signalisation. Alors que l'œil humain ne confondait pas ces panneaux avec d'autres, la machine, a été perturbée et s'est régulièrement trompée. Par exemple, un panneau Stop a été confondu avec un panneau de limitation de vitesse.

Au vu de l'importance grandissante que nous donnons à ces IA, aux tâches que nous leur confions, il est fort à parier que, de plus en plus, elles deviendront des cibles de choix pour hackers, cybercriminels et autres cyberterroristes. Nul n'est besoin de créer de nouvelles technologies de défense ou de sécurité, l'état de l'art des écosystèmes techniques sur lesquelles les IA s'appuient sont suffisamment performants pour les supporter, dès lors qu'elles sont mises en œuvre avec rigueur et conformément aux bonnes pratiques du domaine de la cybersécurité.

87 https://lesclesdedemain.lemonde.fr/technologie/modifier-les-panneaux-de-signalisation-embrouille-les-voitures-autonomes_a-88-6286.html

2.4. DIMENSION ÉCONOMIQUE

Pour Erik Brynjolfsson, économiste américain, professeur à la MIT Sloan School of Management, directeur de l'initiative MIT sur l'économie numérique, les « *machines digitales* » ouvrent une nouvelle ère de prospérité et l'essor des technologies de l'information annonce la prochaine révolution industrielle, non plus mécanique, mais cognitive[88].

Parce qu'il permet d'automatiser des tâches de façon exponentielle et d'agréger des technologies et des domaines jusque-là distincts, le potentiel économique de l'IA semble hors de toute mesure, et, par la multitude des champs d'application envisageables, les promesses qui lui sont associées sont considérables, sans être toutefois dénuées de risques à prendre en compte.

88 https://www.lesechos.fr/2014/05/erik-brynjolfsson-les-machines-digitales-ouvrent-une-nouvelle-ere-de-prosperite-303854

2.4.1 L'INTELLIGENCE ARTIFICIELLE, UNE ÉCONOMIE AUX CONSÉQUENCES SOCIÉTALES

L'IA vecteur de rupture. En permettant de traiter la donnée, et donc l'information contenue par celle-ci de façon beaucoup plus rapide et volumineuse, l'IA est une technologie de transformation profonde. Par la multitude de ses champs d'application, et parce qu'elle permet de générer du lien entre des domaines et des sujets très différents, elle dispose d'un pouvoir à la fois disruptif et multiplicateur de valeur. A ce titre, elle peut être comparée au pétrole, à la chimie du carbone associé et au déploiement des complexes militaro-industriels qui les ont supportés et qui ont profondément transformé nos modèles économiques et sociétaux.
Ainsi, et par exemple, l'IA couplée à l'industrie automobile, à l'internet des objets et à des infrastructures de communication 5G laisse envisager une mobilité nouvelle, marquée par l'arrivée de divers véhicules autonomes et de nouveaux services de transport. Cette nouvelle mobilité aura des conséquences profondes sur l'urbanisation et sur notre rapport aux territoires. Cette combinaison de technologie et d'infrastructures confère aux acteurs qui maîtrisent l'IA un pouvoir de marché évident, qui leur permet d'exploiter à plein la valeur des données qu'ils détiennent ou exploitent.

Nous ne sommes qu'aux prémices des conséquences économiques de l'IA. Si l'Intelligence Artificielle ne date pas d'hier (*cf supra – Dimension technologique*), le développement constant des capacités de calculs et de stockage et l'accroissement sans précédent des données disponibles depuis les années 2000-2010 sont à l'origine d'un nouveau « printemps de l'IA ».
Toujours selon Erik Brynjolfsson, une augmentation de la productivité ne devient sensible que 15 à 20 ans après la date d'apparition d'une technologie. Ce printemps de l'IA ne fait donc que commencer, et ses effets sur la productivité ne sont pas encore mesurables. Ainsi, parler de « l'économie de l'IA » aujourd'hui semble prématuré, au même titre qu'il aurait été prématuré de parler de révolution industrielle en 1712, lorsque Thomas Newcomen inventa sa machine.
Cependant devons-nous succomber à un « technoptimisme » béat ? Le paradoxe de Solow[89], démontre que l'informatisation de la société n'a pas apporté l'accroissement de performance attendue. L'IA permettra-t-elle de dépasser ce paradoxe, et d'autres déjà visibles et relevés par les instances économiques mondiales[90] entre les milliards de croissance attendus, secteur par secteur, et l'éventuelle paupérisation de populations ou la relocalisation d'emplois aujourd'hui fortement valorisés et qui ne le seront plus demain.
De même la valeur des biens physiques fabriqués industriellement, même de très haute technologie, baisse de manière continue alors que les productions artisanales ou manuelles restent coûteuses. Un lecteur Blu-Ray, concentré de technologies, vaut moins de 50 euros alors qu'un saladier en faïence fait main coûte dix fois plus. Même constat si on compare les quelques euros d'un morceau de musique en streaming et le prix d'une place de concert. Le savoir-faire ou le moment d'exception sont valorisés.

89 Ethan Dreyfuss, Andrew Gadson, Tyler Riding, Arthur Wang, https://cs.stanford.edu/people/eroberts/cs181/projects/productivity-paradox/background.html
90 https://www.oecd.org/fr/innovation/inno/technologies-transformatrices-et-emplois-de-l-avenir.pdf

Alors quels constats dresser ?
Premier constat : à titre individuel, les métiers d'avenir sont des métiers créatifs ou de service à la personne, qui ne pourront pas être remplacés par des machines. Mais cette stratégie est-elle adaptable à la taille d'une civilisation ?
Second constat : l'IA est une extraordinaire technologie de captation de valeurs (et donc de capitaux), *a minima* de manière transitoire, dans l'attente de mécanisme de régulation et de redistribution. Des puissances économiques majeures apparaitront, absorbant des pans de l'économie et, à l'échelle mondiale, des renversements régionaux sont à prévoir.

Un nouveau cycle de « destruction créatrice ». L'IA redistribue les cartes, rendant « automatisables » des métiers qui ne l'étaient pas auparavant (programmeurs, médecins, juges, avocats, traders, conseillers financier, etc…). On peut y voir une menace. C'est également une opportunité. Ainsi, délestés des tâches, les plus répétitives, certains métiers devront se réinventer et se concentrer sur les tâches à valeur ajoutée actuelles et à inventer. On peut faire le parallèle avec l'arrivée du tableur dans la profession d'expert comptable, qui n'a pas fait disparaître celle-ci mais lui a permis de se réinventer, et de se concentrer sur l'analyse et le conseil. Ne nous leurrons pas, l'IA va également créer des métiers à faible valeur ajoutée. C'est déjà le cas pour les 35 000 personnes employées par Facebook pour étiqueter des images et vidéos, et déceler celles qui doivent être retirées. Ces fourmis ouvrières du web, très précaires et sous-payées, représentent également une face – souvent cachée – de ces technologies.
Ainsi de nouveaux métiers à forte valeur ajoutée sont en train d'apparaître, qui seront en charge notamment du paramétrage, de l'interprétation ou encore du contrôle des intelligences artificielles. Ces nouveaux métiers répondent à l'émergence de nouvelles tâches qui vont prendre de plus en plus d'importance. Une véritable filière de la donnée doit émerger et se structurer, pour former et valoriser ces métiers de demain.
D'autres métiers, à plus faible valeur ajoutée, vont être fortement impactés – voire remplacés – par l'IA. A cet égard, une politique de formation volontaire, structurée et de grande ampleur doit être mise en place dès maintenant pour permettre aux personnes concernées d'évoluer vers de nouveaux métiers. Une anticipation nécessaire pour que ces profils ne soient pas condamnés à rester au bord du chemin[91].
Des changements sociétaux plus radicaux seront peut-être à prévoir quant à la nature même de la valeur du travail dans un monde « automatisé »[92] [93].

91 France Stratégie, Salima Benhamou, Lionel Janin, Agnès Bocognano, Julia Charrié et Guillaume Thibault, https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-intelligence-artificielle-28-mars-2018_0.pdf
92 France Stratégie, Michel Yahiel, Pierre-Cyrille Hautcœur, Antoine Petit, Lionel Janin, Adélaïde Ploux-Chillès, Céline Mareuge, https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-mut-mut-compte-rendu-24-novembre-2017.pdf
93 Zhen Jie Im, Nonna Mayer, Bruno Palier, Jan Rovny, https://tuhat.helsinki.fi/portal/en/publications/the-losers-of-autom(4b3c5768-53fa-4dec-9ca5-f48823809cba).html

2.4.2 L'INTELLIGENCE ARTIFICIELLE EN ENTREPRISE

A. LE MARCHÉ FOURNISSEURS

Une tendance globale de forte croissance. La croissance du marché des systèmes cognitifs et d'intelligence artificielle est très dynamique depuis plusieurs années (entre 50 et 80% annuels, en fonction des usages et des sources), celle-ci diminuera légèrement jusqu'en 2022 tout en restant au-dessus des 50% (avec des différences importantes en fonction des industries ou des types de technologies creusant des écarts inédits). En termes de dépenses, essentiellement en technologies et services, et ici encore en fonction des sources, cela signifie un montant allant de 33,5 Milliards d'euros à 68,3 Milliards d'euros d'ici 2022. Ce montant progressant sur une fourchette de 78,2 Milliards d'euros ou 149,8 Milliards d'euros en 2025. Les écarts restent importants mais les taux de progression semblent eux constants d'une étude à l'autre. Ces écarts ne changent en rien le caractère stratégique de cette technologie[94] [95] [96].

Les technologies de l'IA les plus dynamiques. Sous l'angle technologique, Deep Learning, Machine Learning, Machine Reasoning, Machine Vision, Natural Language Processing, Strong AI sont les segments de marché les plus étudiés. Deep Learning, Machine Learning, Machine Reasoning sont les technologies les plus utilisées et depuis plus longtemps. Elles représentent encore la plus importante part de marché, même si leurs croissances commencent à, légèrement, se tasser. L'usage de ces technologies sera d'autant renforcé que, d'ici 2022, plus de 40 % des déploiements de cloud par les entreprises se feront en Edge (informatique répartie) et 25 % des terminaux (endpoint) exécuteront des algorithmes d'IA, répartissant ainsi la charge de calcul entre le terminal et les centres de données. Les technologies de Machine Vision sont en forte progression, dans absolument tous les secteurs : dans l'industrie pour le contrôle de production ou la maintenance prédictive, dans la sécurité au travers de la reconnaissance faciale, dans l'organisation des espaces de travail et de visio-conférence, dans le ciblage publicitaire ou encore l'aide aux visiteurs, comme cela est déjà relativement répandu en Chine. D'ici 2024, les interfaces utilisateur basées sur l'intelligence artificielle remplaceront un tiers des applications actuelles basées sur écran. Par exemple, les différentes technologies de Natural Langage Processing et les usages associés (ex. chat bot), explosent et sont génératrices d'importantes transformations dans diverses industries. La distribution en particulier, mais aussi l'industrie des loisirs ou celle de l'attention. D'ici 2022, 30 % des entreprises utiliseront la technologie conversationnelle pour l'engagement des clients. C'est aujourd'hui sur ces technologies que se portent le plus les investissements. En revanche l'IA Dure (ou Strong AI)[97] reste marginale et ne représente encore qu'un champ de recherche, ou seules les entreprises les plus matures investissent.

B. LE MARCHÉ UTILISATEURS

Des investissements dominés par les géants du numérique. Un tiers des investissements[98] dans l'intelligence artificielle porte sur les logiciels et les services IT. Ces entreprises interviennent sur l'ensemble des technologies, secteurs et cas d'usage. On remarquera que la pénurie récurrente de profils IT (développeurs ou datascientists) fait prédire à IDC[99] qu'une nouvelle génération d'application de programmation « sans script » permettra une augmentation de 30% de cette population en créant une nouvelle catégorie de développeurs assistés par l'IA, d'ici 2024. Il ne sera plus besoin de connaître un langage de programmation.

94 Statista, https://www.statista.com/statistics/607716/worldwide-artificial-intelligence-market-revenues/
95 Garner, https://www.garnerinsights.com/Global-Artificial-Intelligence-Market-Size-Status-and-Forecast-2019-2025
96 Louis Columbus, https://www.forbes.com/sites/louiscolumbus/2018/11/04/idc-top-10-predictions-for-worldwide-it-2019/#61c659c37b96
97 L'IA Dure (Strong AI) est un type de l'intelligence artificielle ayant des capacités mentales et des fonctions qui imitent le cerveau humain. Dans la philosophie de l'IA Dure, le logiciel, qui est l'IA, imite exactement les actions du cerveau humain, et les actions d'un être humain, y compris son pouvoir de compréhension et même sa conscience. L'IA Dure est également connue sous le nom d'intelligence artificielle complète (Full AI).
98 Aman Naimat, https://www.oreilly.com/ideas/the-new-artificial-intelligence-market
99 International Data Corporation

Ce sont les géants technologiques qui font la course en tête en ce qui concerne les brevets liés à l'IA. Avec une nette domination pour Microsoft (18 365), suivent IBM (15 046), Samsung (11 243), Qualcomm (10 178) et Google (9 536)[100]. 78.085 brevets ont étés déposés sur l'AI pour la seule année 2018. On note cependant des stratégies de mise à disposition des technologies (ex. Tesla ou Facebook). Ceux sont aussi les géants qui alimentent pour une bonne part les investissements. D'abord directement en investissant dans leurs propres laboratoires partout dans le monde (ex. AAAI, Google Brain, Facebook AI research), et en montant au capital de certaines startups. Mais aussi indirectement car les différents rachats opérés depuis le début 2010 ont grandement stimulé le marché et encouragé le capital risque à s'intéresser à l'IA[101], avec plus de 200 entreprises de capital risque recensées.

Quelques exemples sectoriels. Concernant la distribution, Gartner[102] prédit que d'ici 2020, 30 % de la croissance du secteur proviendra de l'intelligence artificielle, et que 60 % des retailers utiliseront cette technologie d'une manière ou d'une autre. Logistique amont et aval, CRM, engagement client, support, automatisation des processus de vente, micro-ciblage sont autant de sujets abordés. Le marché de l'intelligence artificielle appliquée à la santé[103], estimé à 1,3 Md $ dans le monde en 2018, sera décuplé d'ici 2025 pour dépasser 13 Mds $. Là aussi les champs d'applications sont multiples : imagerie médicale, aide au diagnostic, recherche pharmaceutique, rationalisation des parcours de soin, traitements ciblés, observance… En agriculture[104], l'IA permet d'importants gains sur l'efficience des pratiques culturales, en s'appuyant comme sources sur tous types de données (satellites, climatologie, rendements précédents, sondes diverses dans les champs, les étables les cuves …) et s'appuient déjà sur des machines automatisées afin de répartir au mieux les ressources et adapter de manière fine les pratiques (ensemencement calculé au mètre près, traite automatisée, date de récolte, supervision par drones …). Sur ce marché, l'IA passera de 458,9 millions d'euros (518,7 m$) en 2017 à 2,3 milliards d'euros (2,6M$) en 2025, soit une progression de plus de 22,5% par an. Pour les entreprises de services financiers, Cap Gemini Consulting[105] prévoit pour 2020 un marché de 512 milliards de dollars (512 M$, soit 457 M€) ; la banque représentant 269 m$ (240M€) et l'assurance 243 M$ (217M€). Aujourd'hui les investissements se portent majoritairement sur l'automatisation des tâches à basse valeur (RPA[106]) ou le contact client (ChatBot). Cependant les perspectives se portent aussi sur les investissements à haute valeur (conseil en investissement, trading haute fréquence, assurance personnalisée…). Concernant les véhicules et les transports de personnes ou de marchandises[107] [108], le marché mondial de l'intelligence artificielle automobile devrait passer de 445,8 millions de dollars en 2017 à près de 9 milliards de dollars en 2025 (8 M€)[109]. De même les sous-traitants les plus matures devraient augmenter leurs marges de 16%. Le marché de l'IA dans l'aviation devrait croître de 30% par an d'ici 2022[110] et dépasser les 2,2 milliards de dollars en 2025 (2M€)[111]. L'Intelligence Artificielle sur le marché de la chaîne logistique devrait passer de 730 millions de dollars en 2018 (648m€) à 10,1 milliards de dollars (9M€) en 2025[112].
Véhicules autonomes et co-voiturage, interopérabilité des moyens de transports, ajustement des correspondances multimodales en temps réels, gestion des incidents de circulations, écologie des transports de fret, assistance à la conduite et à la consommation d'énergie, … sont autant de champs investis par l'IA dans le transport.

100 https://www.iplytics.com/wp-content/uploads/2019/03/IPlytics-AI-report.pdf
101 BPI France, https://www.bpifrance.fr/A-la-une/Actualites/Infographie-comprendre-le-marche-de-l-intelligence-artificielle-28379
102 Garner, https://www.garnerinsights.com/Global-Artificial-Intelligence-Market-Size-Status-and-Forecast-2019-2025
103 Global Market Insights, https://www.gminsights.com/pressrelease/healthcare-artificial-intelligence-market
104 Johanna Diaz, https://www.actuia.com/author/johanna/?#https://www.actuia.com/dossiers/sera-limpact-de-lintelligence-artificielle-lagriculture/
105 https://www.capgemini.com/fr-fr/news/lautomatisation-intelligente-pourrait-generer-un-gain-de-512-milliards-de-dollars-pour-le-secteur-des-services-financiers-dici-2020/#
106 RPA ou Robotic Process Automation est une technologie d'automatisation reposant sur l'intelligence artificielle. C'est une technologie permettant d'automatiser des tâches répétitives
107 http://www.andsi.fr/wp-content/uploads/2017/04/Microsoft-Word-ANDSI-CR-du-14-mars-2017-De-La-Fortelle-pdt.pdf
108 https://www.ge.com/reports/the-moneys-really-in-self-driving-trucks-trains-and-ships-not-cars/
109 https://www.alliedmarketresearch.com/automotive-artificial-intelligence-market
110 https://www.technavio.com/report/global-artificial-intelligence-in-aviation-market-analysis-share-2018?utm_source=t10&utm_medium=bw_wk1&utm_campaign=businesswire
111 https://www.researchandmarkets.com/research/n533gh/global_2_2_bn?w=5
112 https://www.capgemini.com/research/accelerating-automotives-ai-transformation/

Nous sommes ici loin d'être exhaustifs, mais nous remarquons qu'il y a une certaine ironie à compiler toutes ces prévisions sectorielles, tant les chiffres, les échelles d'analyses, les conclusions sont pour les uns absurdement incohérents, pour les autres outrageusement optimistes, ou inversement. Toutes ces données, quelles ques soient leurs sources et leurs conclusions, sont donc à prendre avec les plus grandes précautions.

Il reste cependant évident que l'Intelligence Artificielle est la clef des transformations économiques à venir, avec comme sous-jacent la maîtrise des données.

III. PROPOSITIONS

INTELLIGENCE ARTIFICIELLE (IA)

12 PROPOSITIONS

POUR UNE MEILLEURE UTILISATION DE LA DONNÉE

1. Définir et constitutionnaliser des principes fondamentaux que les technologies d'IA devront respecter (droits numériques de l'Homme).

2. S'engager dans une réflexion visant à définir des règles éthiques qui puissent s'appliquer dans le monde numérique.

3. Travailler à l'élaboration d'un texte général applicable aux données à caractère non personnel, complétant le Règlement communautaire 2018/807.

4. Définir une politique publique d'investissement massif visant à créer un champion étatique ou européen de l'IA, à l'image des succès créés dans les secteurs aéronautique ou énergétique.

5. Structurer une filière de la science de la donnée aboutissant à l'instauration de nouvelles professions règlementées.

6. Etudier l'opportunité d'une obligation légale imposant aux fournisseurs d'IA de déposer une documentation permettant d'expliquer le mode de fonctionnement et les résultats produits par l'IA, qui sera approuvée par une autorité publique française ou européenne, préalablement à sa mise en production, laquelle sera dotée de moyens suffisants pour attirer des spécialistes chevronnés.

7. Mettre en place des certifications ou labels qui seront gages de transparence et de confiance pour les utilisateurs.

8. Etablir des référentiels (thésaurus et ontologies) caractérisant des typologies de données en fonction de leur nature (dépendant de la façon dont elle a été captée, inférée ou créée), leur usage (finalité) et leur criticité (sous l'angle de la confidentialité et de la continuité d'activité), pour faciliter l'interopérabilité des systèmes et des activités, et en assurer la diffusion notamment à travers l'école et l'université.

9. Avant toute modélisation impliquant des données, définir le périmètre des données nécessaires et légitimes en s'assurant de leur bonne représentativité.

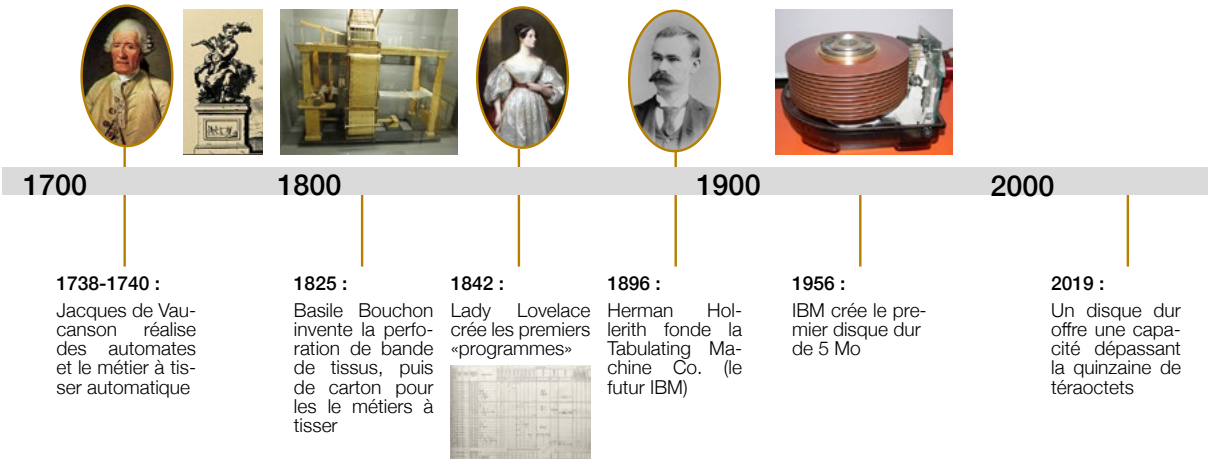
10. Introduire une phase de contrôle à l'issue du pré-traitement des données afin de s'assurer de leur neutralité et de ne pas introduire de biais.

11. Mettre en qualité (standardisation, exactitude ou représentativité) les données pour s'assurer que le système fonctionne.

12. Documenter de façon précise l'ensemble des données, du contexte et des traitements qui ont permis de construire le jeu de données et rendre cette documentation accessible à toutes les personnes qui ont à en connaître.

IV. ANNEXES

UNE PETITE HISTOIRE DE LA DONNÉE



En ce qui concerne la donnée, les premières capacités de stockage étaient particulièrement faibles et proviennent de technologies pré-informatiques.

C'est d'abord pour l'automatisation de la restitution musicale que des recherches sont faites dès le IXe siècle.

Plus proche de nous, **Jacques de Vaucanson** au XVIIIe réalisera de célèbres automates, puis des métiers à tisser automatiques.

Mais attention, nous sommes encore, à ce moment, dans une approche que Descartes, avec son « animal-machine », aurait qualifiée de mécaniste. En effet, nous reproduisons le vivant ou une capacité du vivant (le travail de tissage) grâce à une machine, mais ce sont les mécanismes internes de la machine qui sont eux-mêmes porteurs de son « programme ». Une telle machine fait ce pour quoi elle est construite et ne peut changer de fonction, de programme. Il y a une « hyper-contextualisation » de l'outil vis-à-vis de son programme et des données incluses, les uns et les autres ne pouvant être différenciés.

C'est à un Français que nous devons le premier stockage d'informations permettant l'exécution par une machine d'une réalisation partiellement indépendante de sa technique interne. **Basile Bouchon**, en 1825, à Lyon, invente la perforation de bande de tissus, puis de carton, afin de permettre la modification de la production de ses métiers à tisser. Ce principe de « carte perforée » est repris par **Herman Hollerith**, d'abord pour son travail au bureau américain du recensement, puis pour fonder les principes de la mécanographie.

Entre temps, les algorithmes de **Lady Lovelace** sur la machine de C. Babbage sont considérés comme les premiers « programmes ».

En 1896, Herman Hollerith fonde la Tabulating Machine Co. qui deviendra, au travers de fusions, l'International Business Machines Corporation (IBM).

C'est IBM qui créera en 1956 le premier disque dur, l'IBM 350, d'une capacité de 5 mégaoctets pour un débit de 8,8 ko/s en utilisant 50 disques de 24 pouces, pour un poids d'environ une tonne et la taille d'un grand frigo américain.

Aujourd'hui nos capacités de stockage d'information sont sans commune mesure. Un disque dur offre une capacité dépassant la quinzaine de téraoctets, son débit est de plus de 550 mégaoctets par seconde et l'ensemble tient sur un disque de 2,5 pouces pour quelques centaines de grammes.

En ce qui concerne la mémoire vive, l'évolution est similaire, un ordinateur de bureau dispose aisément de 8 ou 16 giga-octets pour des temps d'accès de 5 à 6 giga-octets par seconde (soit un rapport de 1 à 1000 entre mémoire vive et mémoire de masse). La capacité d'un serveur dépasse la centaine de giga-octets.

INTERVIEW

Yann LeCun

CHERCHEUR EN APPRENTISSAGE MACHINE, LAURÉAT DU PRIX TURING 2019

1. ***On fait souvent l'analogie entre le pétrole et la donnée désignée comme le « carburant » de l'économie numérique. Pourtant, alors que les réserves de pétrole arrivent à leur fin, la donnée est partout, elle se multiplie et a même tendance à s'auto-alimenter au moins en termes de volumétrie. Qu'en pensez-vous ?***

« C'est un vaste sujet !
De plus en plus de données sont effectivement collectées mais il faut avoir conscience que cette masse de données n'est pas homogène. Ainsi, dans certains domaines – par exemple la classification de textes, la reconnaissance de la parole ou de l'image – les entreprises sont submergées de données, elles en détiennent plus qu'elles ne peuvent en utiliser.
D'autres domaines au contraire se heurtent à des restrictions qui engendrent un manque de données étiquetées[113]. C'est le cas par exemple pour les données de santé, soit parce qu'elles ne sont pas disponibles (secret médical) ou car tout simplement elles n'existent pas.
Or, l'utilisation de telles données pourrait permettre des avancées significatives et positives pour l'homme dans le domaine de la médecine, notamment en termes de découvertes médicales, protocoles de traitement, amélioration des diagnostics… Mais encore faut-il que ces données soient disponibles pour les chercheurs.
Cela pose nécessairement des questions juridiques, relatives aux données privées. Les réglementations à venir vont certainement changer la donne. »

2. ***Certaines entreprises ont compris avant les autres l'intérêt et la valeur que recèle la donnée. Elles en ont fait un avantage technologique et /ou économique en l'exploitant dans des domaines jusqu'ici inexplorés ou en industrialisant un usage jusqu'alors artisanal. L'un de ces domaines est bien sûr celui de l'IA. Y a-t-il selon vous une limite à cette exploitation et si oui, cette limite se trouve-t-elle dans la donnée elle-même (sa source, son type, les moyens de sa collecte, …) ou dans son exploitation, l'objet de son usage, la finalité de son exploitation ?***

« Démystifions tout d'abord l'idée selon laquelle il faut forcément avoir accès à une quantité massive de données pour commencer à développer de nouvelles méthodes en intelligence artificielle, et, partant de là, l'avantage que l'on attribue à Google, Facebook ou Amazon qui ont accès à des bases de données gigantesques. C'est absolument faux puisque le développement de nouvelles méthodes d'intelligence artificielle ne repose pas sur des données privées, mais bien sur des jeux de données publiques, accessibles à tous les chercheurs.
Cela pose nécessairement des questions juridiques, relatives aux données privées. Les réglementations à venir vont certainement changer la donne. En effet, pour s'assurer qu'une nouvelle méthode fonctionne bien ou est plus performante qu'une autre, il faut pouvoir la comparer avec d'autres méthodes déjà publiées dans la littérature, grâce à des méthodologies bien établies.
Il n'est donc pas nécessaire d'accéder ou de disposer d'importantes bases de données pour développer de nouvelles méthodes. Il n'est certainement pas nécessaire de disposer de données privées.
Pour preuve, par exemple, les entreprises qui ont voulu s'engager dans le domaine de la voiture autonome ont pu rapidement collecter les données nécessaires.

113 Une donnée étiquetée est une donnée à laquelle on a associé une description, correspondant à ce que l'on souhaite apprendre à la machine. Par exemple, dans le cadre de la reconnaissance de caractères manuscrits, l'étiquette correspond à la lettre de l'alphabet présente dans l'image que 'on veut reconnaitre.

Une entreprise comme Tesla ayant de nombreux de véhicules en circulation, dispose certes d'un certain avantage, mais une autre entreprise peut, en quelques mois, collecter plus de données qu'elle ne pourra jamais en traiter.
De plus, de nouvelles méthodes d'apprentissage permettant de s'affranchir de l'étiquetage des données vont se développer dans le futur. Avec ces méthodes « non supervisées » ou « auto-supervisées » qui commencent à émerger sur des sujets comme la compréhension du texte et de l'image, la volumétrie des données étiquetées disponibles et l'avantage que l'on pourra en tirer va avoir tendance à diminuer.
Si l'accès aux données n'est pas un problème, le choix pour une entreprise d'investir dans des technologies d'intelligence artificielle va dépendre de l'exploitation qu'elle pourra faire de ces données. La donnée n'a donc pas intrinsèquement de valeur, c'est bien son utilisation finale qui en détermine la valeur potentielle.
Par le passé, de nombreuses technologies d'intelligence artificielle ont été développées, puis sont restées dans les cartons, faute d'une exploitation, d'une application pertinente. Ainsi, par exemple, IBM a des difficultés à exploiter les technologies de reconnaissance de la parole et de traduction qu'elle a développées car elle n'est pas sur le bon segment de marché.
Au contraire, les technologies développées par Facebook, Google ou Amazon apportent à leurs clients un vrai plus.
La donnée seule ou la technologie seule ne servent à rien sans un business model pertinent. »

3. ***On entend dans nos sociétés bon nombre de voix qui s'élèvent contre l'omniprésence de l'IA dans nos vies ; des inquiétudes voire des angoisses qui s'expriment concernant le dépassement voire l'asservissement de l'humanité par les machines. Même si ces scénarios sont peut-être de l'ordre du fantasme, n'y a-t-il pas quelques précautions à prendre pour éviter qu'ils ne deviennent réalité, et cela ne commence-t-il pas par une prise de conscience, une meilleure connaissance et un usage mieux maîtrisé et éthique de la donnée ?***

« Dès lors qu'avec ces technologies, nous défrichons de nouveaux territoires, on ne peut pas prévoir toutes les conséquences – bénéfiques ou non - de ces nouveaux services et de ce fait, bien sûr, des précautions doivent être prises. Il faut donc rester ouvert et à l'écoute de ce qui se passe et corriger les problèmes lorsqu'ils apparaissent.

Là encore, certaines questions sont de l'ordre du fantasme : l'idée selon laquelle les robots finiront par dominer l'humanité relève de la science-fiction. En effet, les technologies pour faire des machines réellement intelligentes n'existent pas encore. Les machines que nous créons peuvent avoir des performances supérieures à l'homme dans des domaines très spécifiques (jouer aux échecs ou au go, déceler une tumeur sur une radio, être capable de lire un texte en x langues et de la traduire dans x autres…), mais il n'existe aucune machine qui ait autant de bon sens qu'un chat de gouttière ! Ce n'est pas une question de puissance des ordinateurs, c'est bien plus profond que cela. En réalité, nous ne disposons pas des principes de base, des techniques, des paradigmes pour apprendre comme un humain. Réfléchir à ce risque d'asservissement de l'humanité dès maintenant me semble prématuré, car on n'a aucune idée de ce à quoi ces machines pourraient ressembler. Il sera peut-être temps de se poser ces questions dans plusieurs décennies lorsqu'on en saura plus sur leur architecture et il conviendra alors, le cas échéant, de faire en sorte que leur comportement s'aligne avec les valeurs humaines.
Ce mythe suppose en outre que les machines voudraient dominer. En un mot, on projette sur ces entités intelligentes une volonté humaine, liée au caractère social de notre espèce, aux structures hiérarchiques qui ont émergé de notre évolution. Il n'y a absolument aucune raison pour que ce type de comportement soit présent dans les machines intelligentes car c'est quelque chose qu'il faut construire explicitement. Si on veut faire un parallèle, les orangs-outans, qui sont quasiment aussi intelligents que les humains, n'ont aucune volonté de dominer. Mise à part la relation de la mère et son enfant, ils restent solitaires, n'ont pas de vie sociale et de ce fait n'ont aucune velléité de dominer qui que ce soit car ce ne sont pas des animaux sociaux. Je pense que les machines intelligentes seront probablement plus proches des orangs-outans que des humains. La volonté de dominer chez les animaux sociaux n'est pas liée à l'intelligence, mais plutôt à la testostérone !
Au-delà de ces fantasmes, cependant, certains problèmes sont réels et doivent être pris à bras le corps. Par exemple : comment réduire les biais dans la donnée ? La plupart des acteurs du numérique se sont rendu compte que, même sans mauvaise intention, il est facile de construire un système biaisé sans s'en apercevoir. Ils ont également constaté que les biais ne venaient pas des algorithmes d'apprentissage utilisés (modèles statistiques, deep learning, ou autres) mais des données utilisées pour entraîner les machines.

C'est pourquoi des livres blancs, des standards, des recommandations pour de bonnes pratiques, dans l'utilisation de la donnée sont utiles et doivent être développés.
La réduction des biais dans les données est une des questions sur lesquelles le « Partnership on IA » travaille.
Cette association regroupe aujourd'hui 80 membres, dont plus de 50 % d'associations, d'ONG et d'universités, le reste étant des entreprises qui évoluent dans le monde de la donnée et de l'IA et qui ont déjà, pour la plupart, été confrontées au fait que les systèmes qu'elles avaient développés étaient biaisés. Quelquefois, elles s'en sont aperçu trop tard, une fois que les utilisateurs en avaient pâti.
Ainsi, parmi les exemples célèbres, on peut citer le système de reconnaissance d'images de Google qui a catégorisé un certain nombre de personnes à la peau noire en tant que gorilles. Cela était-il dû au fait que Google est raciste ? Que les personnes qui ont écrit les algorithmes étaient blanches ? En aucune façon. En réalité, ce problème était lié au fait que l'échantillon représentatif de la population américaine utilisé pour développer cet algorithme comportait 10 à 15% de personnes à la peau sombre et que, du coup, la technologie développée était moins efficace sur ces personnes. Là encore, le biais n'est pas dans la technologie en tant que telle mais dans les données qui ont été utilisées pour la construire.
Bien évidemment, il faut s'attacher à corriger ce genre de dysfonctionnements.
A l'instar des problèmes de sécurité informatique, les entreprises peuvent garder le secret et réparer les choses dans leur coin ou, au contraire, partager de façon ouverte pour que les soucis rencontrés n'arrivent pas à d'autres. J'ai tendance à privilégier l'ouverture, et c'est l'objectif du Partnership on IA que d'offrir un forum, un espace pour discuter ouvertement, partager les dysfonctionnements et trouver – pourquoi pas – collectivement les solutions à apporter. Etablir des lignes de conduite ne peut avoir qu'un effet bénéfique. »

4. ***La dimension juridique n'est-elle pas essentielle également pour favoriser un usage mieux maîtrisé de la donnée ?***

« C'est une question compliquée à laquelle il n'existe pas de réponse simple.
Certains cadres juridiques sont utiles : ainsi, contraint de mettre en œuvre le RGPD en Europe, Facebook a décidé de l'appliquer dans le monde entier. D'un autre côté, un cadre juridique trop contraignant et prématuré peut limiter l'innovation et tuer dans l'œuf des services qui seraient à terme positifs pour la société.
Pour être optimal, le cadre juridique nécessite une compréhension fine des enjeux, tenants et aboutissants des technologies développées. Or, ce n'est pas toujours le cas, le législateur étant souvent déconnecté de ces problématiques et des questions de technologie.
Une chose est sûre : on ne peut pas tout prévoir a priori et il faut donc faire preuve de prudence, de souplesse et d'agilité pour contrebalancer après coup des problèmes qui peuvent survenir. Comme je le disais plus haut, nous sommes en phase de défrichage, nous explorons des zones grises, dont nous ne comprenons pas tout de suite toutes les conséquences. Il s'agit d'une « danse itérative » qui ne peut être ni tout juridique a priori ni tout correctif a posteriori. Il faut trouver une subtile alchimie entre les deux approches, essayer des choses, voir comment cela fonctionne dans un périmètre restreint avant de déployer plus largement.

Ainsi, au fur et à mesure qu'il a été confronté à des dysfonctionnements, Facebook s'est adapté, en restreignant ses partenariats, en augmentant la modération des contenus, en améliorant ses technologies de reconnaissance d'image pour supprimer autant que possible les contenus illicites avant même leur publication. Cela dit, aucun système de détection ne peut être parfait, et nous devons être ouverts à la critique, agir de manière transparente et corriger les imperfections au fur et à mesure qu'elles se présentent. Cela oblige les entreprises à être moins opaques, à expliquer ce qu'elles font et comment elles fonctionnent, et je pense que c'est une bonne chose. »

5. ***Enfin, et pour conclure, à titre personnel dans le domaine de l'IA ou plus concrètement dans la vie de tous les jours, qu'attendriez-vous d'une initiative telle que celle du Cercle de la Donnée visant à rassembler secteurs public et privé dans une filière d'excellence de la donnée ?***

« Tout d'abord, il me semble qu'un think tank tel que le Cercle de la Donnée a un rôle à jouer en matière d'éducation, de vulgarisation des enjeux liés à ces technologies auprès du grand public, du législateur, des entreprises, du gouvernement. Ces questions relatives à la collecte, l'exploitation, la distribution ou non-distribution des données, à la protection des données à caractère personnel sont complexes et doivent être expliquées.
Les membres du Cercle ont quant à eux tout intérêt à partager leurs bonnes pratiques mais aussi les problèmes rencontrés, comme nous le faisons au sein du Partnership on IA. Ces études de cas permettront à chacun de progresser, d'éviter de commettre les mêmes erreurs. »

PRÉSENTATION de Yann LeCun

Yann LeCun est professeur à NYU et ancien chercheur aux Bell Labs, directeur du centre de recherche en IA de Facebook. Outre ses nombreuses communications dans les plus prestigieux colloques d'IA, et son cours de Deep Learning au collège de France en 2016 en tant que professeur invité, il est l'auteur en 2018 avec Stanislas Dehaene et Jacques Girardon de « La plus belle histoire de l'intelligence ».
En 2019, il reçoit le prestigieux prix Turing avec ses homologues Joshua Bengigo et Geoffrey Hinton pour les travaux de recherche à l'origine du Deep Learning.

INTERVIEW

Guillaume Poupard

DIRECTEUR GÉNÉRAL DE L'AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (ANSSI)

1. ***Pouvez-vous nous rappeler quel est le rôle de l'ANSSI dans un écosystème numérique en évolution tant en France qu'en Europe ?***

« L'ANSSI a été créée il y a 10 ans, à un moment où l'on a pris conscience que les questions de sécurité numérique allaient devenir un enjeu majeur.

Le choix français de créer une autorité unique en charge de la question de la sécurité numérique pour le compte de l'Etat est original et différent des autres pays en termes d'organisation. Ce choix repose sur deux principes très forts :

Premièrement, la séparation de l'offensif et du défensif, qui est un choix structurant, courageux et efficace. Ainsi, l'ANSSI ne s'occupe que de défensif et intègre l'ensemble de ces questions. Nous sommes sur de la prévention, de la sensibilisation, de la détection des attaques avec un côté opérationnel très fort, et sur de la réponse à incident et de l'aide aux victimes. Nous ne sommes pas une agence de renseignement ou d'enquête, nous ne menons pas d'attaque ni de contre-attaque.

Deuxièmement, l'agence est rattachée aux services du Premier ministre, ce qui est un symbole fort et confirme la conviction selon laquelle le sujet « Cyber » ne doit pas être restreint à un domaine particulier. Ainsi, nous ne sommes pas typés « Défense », « Intérieur » ou « Economie ». Cette position interministérielle nous permet de faire des choses en propre et de travailler avec les autres, chacun dans son domaine de compétence.

L'ADN de l'ANSSI, c'est un cœur défensif incluant aussi bien de la technique que de l'opérationnel, qui s'inscrit dans un écosystème, avec pour objectif d'aller aussi vite que les attaquants. Cela met la barre assez haut !

Si je devais décrire cet écosystème, je dirais qu'il se structure en 3 grands pôles :

- Un pôle étatique ambitieux - les différents exécutifs ont toujours réaffirmé l'importance de la sécurité numérique.

- Un pôle constitué par tous ceux qui doivent se protéger, anticiper, réagir. On a fait le choix en France d'une approche par la réglementation. Pour l'ingénieur que je suis, et sans aller sur un terrain politique, il me semble que faire ce choix permet de gagner du temps, de partager une ambition commune, de créer du lien entre les acteurs et de forcer une coopération. Ceci pour éviter d'attendre les catastrophes pour se parler. C'est ce que l'on a fait dès 2013, avec ce qu'on appelle les « opérateurs d'importance vitale » (OIV)[114]. Bien évidemment, les solutions à apporter ne sont pas les mêmes en fonction des acteurs. En ce qui concerne les plus « petits » (PME, collectivités locales), nous travaillons beaucoup avec eux pour les sensibiliser et les aider à anticiper et mieux prendre en compte ces sujets.

- Le troisième pôle est constitué des offreurs de services, produits et solutions en matière de sécurité numérique. Nous nous devons d'avoir une industrie nationale innovante en la matière et l'ANSSI contribue à structurer ce pôle notamment par le biais des Visas de sécurité (certifications et qualifications).

Cet écosystème est efficace si ces trois pôles - Etat, certains opérateurs sensibles, et acteurs privés capables d'apporter des solutions - fonctionnent de manière équilibrée. Cela répond à une question de souveraineté nationale pour la France et d'autonomie stratégique au niveau européen.

Tout cela est très ambitieux évidemment, mais je suis convaincu que c'est tout un écosystème qui doit bouger ensemble sinon cela ne fonctionne pas. »

114 Organisations privées ou publiques, qui exploitent ou utilisent des installations jugées indispensables pour la survie de la Nation.

2. ***Au-delà des aspects réglementaires, quels sont les forums qui existent pour échanger sur ces questions ?***

« Les forums sont multiples. La réglementation notamment fait émerger des communautés. C'est ce qui est en train de se produire avec les opérateurs de services essentiels (OSE)[115], qui sont des acteurs importants pour la société et l'économie. On voit se créer un ensemble assez homogène sur un sujet où la plupart des acteurs comprennent qu'ils ne sont pas en position de concurrence. Le partage est compliqué mais il a un intérêt et l'ANSSI cherche à l'encourager en veillant bien à ce qu'il ne devienne pas une forme de faiblesse.

De la même façon, au niveau national, nous animons la communauté des centres opérationnels qu'ils soient publics ou privés. En effet, c'est le métier et l'intérêt de partager sur les sujets data qui réunit les gens. La frontière entre sphères publique et privée est peu marquée dans le domaine de la sécurité numérique.

A l'échelle européenne, nous avons mis en place un réseau entre les Etats, dont les échanges vont au-delà des espérances, preuve que cela répond probablement à un vrai besoin. Notamment, un groupe informel s'est constitué dans le cadre de l'élaboration de la directive network and information security (NIS) concernant des mesures destinées à assurer un niveau de sécurité élevé dans l'Union[116]. Il vise à échanger sur la base du volontariat sur la façon dont les questions de sécurité nationale sont prises en compte dans l'ensemble des Etats membres. Ainsi, des pays qui ont commencé un peu plus tôt comme la France, peuvent partager leur expérience avec les autres. Ce n'est pas de la philanthropie, c'est bien un intérêt partagé. Rester focalisés sur le périmètre national ne sera en effet pas suffisant s'il existe des zones de non droit en matière de sécurité numérique et c'est donc bien le niveau de sécurité de toute l'Europe qu'il faut développer.

A l'échelle mondiale, une coopération se met en place, plus facilement avec certains pays qu'avec d'autres bien sûr. Nous croyons beaucoup à l'Appel de Paris, porté par le Président de la République le 12 novembre 2018 pour la confiance et la sécurité dans le Cyberespace. Ce n'est pas idéaliste, c'est même plutôt intéressé : il s'agit de reconnaître que si les tensions continuent à monter entre les grands blocs, à un moment, les dommages vont devenir inacceptables. Et il faudra bien se poser des questions sur la façon dont on veut que le cyberespace fonctionne. »

3. ***Comment se fixe-t-on des règles pour faire en sorte que cet espace numérique, ce bien commun, ne soit pas uniquement un champ de bataille ?***

« J'ai l'habitude de décrire cet espace numérique comme étant très multi-échelle, or les échelles ne s'opposent pas les unes aux autres, elles se complètent. Ainsi, il existe un échelon national, qui est très fort, un échelon européen qui fonctionne, est indispensable et en phase de développement. Et puis un échelon international qui est majeur parce qu'autrement c'est l'aspect conflictuel qui prendra le dessus… »

4. ***La vision du Cercle de la Donnée est que la data est au cœur de l'économie aujourd'hui et le sera encore plus demain. Quel rôle peut jouer l'ANSSI dans ce contexte-là ?***

« En ce qui concerne la donnée « cyber », strictement liée à la sécurité nationale, très technique et spécifique, relative à la connaissance des attaques, il s'agit de la partager avec le plus de personnes possible, en évitant que les attaquants en fassent partie. Vous comprenez bien que cette donnée ne peut pas être totalement « open », et cela complique la donne. Mais on a absolument besoin de partager cette donnée avec tous ceux à qui elle peut bénéficier, et ils sont nombreux, pour éviter des attaques lourdes, complexes et dommageables pour les victimes.

Concernant la donnée en général, c'est une toute autre question. La donnée est devenue une sorte de matière première, convoitée, que certains n'hésitent pas à voler (je pense notamment aux vols de données de santé à Singapour ou en Norvège, sûrement destinées à alimenter une intelligence artificielle). Il faut avoir conscience que nous vivons dans un monde partiellement hostile. Cependant, face à ce risque, réagir en se renfermant, en gardant les données pour soi, en refusant de les partager, n'est pas la bonne solution. Les données de santé sont un exemple intéressant car elles sont sensibles mais peuvent également permettre des innovations, par exemple contre le cancer.

L'enjeu est de trouver un juste équilibre, qui protège la donnée tout en permettant son utilisation. »

115 https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/faq-operateurs-de-services-essentiels-ose/

116 « Network and Information Security », ou « NIS », 2016/1148 du 6 juillet 2016, directive sur la sécurité des réseaux et des systèmes d'information, https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

5. ***Croyez-vous en la professionnalisation du numérique, à l'instar de ce qui existe dans le secteur de la santé justement, avec un accès permissionné et une réglementation stricte qui permettent d'exploiter la donnée sans anonymisation avec un niveau de sécurité acceptable, et, à la clé, des bénéfices réels ?***

« A mon sens, l'anonymisation ne fonctionne pas. On peut y avoir recours de manière micro, sur des données avec peu de champs mais pas sur des traitements complexes ou des croisements de données.
La vraie question est la suivante : comment casser l'idée communément admise et faussement intuitive que la donnée doit être amenée et transmise à ceux qui en ont besoin ? Pourquoi les Intelligences artificielles ne se déplaceraient-elles pas ? Pourquoi ne fonctionnerait-on pas avec des accès permissionnés ? Après tout, quand nous apprenons nous-même, nous nous déplaçons.
Depuis des années, on s'escrime à vouloir désensibiliser des données, qui, au final, ne valent plus grand-chose pour les transmettre. (Pourquoi ne pas imaginer des sentinelles des données, gardiens du temple, qui décideraient d'ouvrir ou non la porte aux intelligences artificielles qui en demanderaient l'accès ?) On pourra ainsi mieux contrôler qui vient et qui ne vient pas. Et ne donner que le résultat du « machine learning » et non pas la source. »

6. ***Devant l'accroissement de la menace dans le secteur du Numérique, l'ANSSI a-t-elle les moyens de couvrir ce périmètre et comment voyez-vous l'avenir pour faire face à ces grands enjeux ?***

« Il ne faut jamais demander à un directeur s'il a assez de moyens (rires).
Bien sûr, nous avons besoin de moyens en propres mais la solution est de partager le sujet avec ceux qui sont et seront acteurs, les aider à décrypter, les accompagner. Il faut travailler ensemble, expert et acteurs, publics et privés.
L'important est de normaliser le risque cyber, de faire en sorte qu'il soit traité comme les autres risques. L'échec complet serait de voir que la sécurité numérique en France se résume seulement l'ANSSI, car en réalité, c'est bien l'affaire de tous. »

7. ***Comment le Cercle de la Donnée peut-il contribuer aux missions de l'ANSSI ?***

« Comme je vous le disais, nous ne sommes pas une « Cyber Agency » et à ce titre, nous ne sommes pas là pour protéger le contenu (la donnée en elle-même), mais bien pour protéger le contenant (les systèmes d'information).
Aussi, l'approche du Cercle de la Donnée, qui s'intéresse au contenu, vu par le prisme des aspects métier, de façon pluridisciplinaire me semble tout à fait complémentaire de ce que nous faisons à l'ANSSI. »

PRÉSENTATION de Guillaume Poupard

Guillaume Poupard est ancien élève de l'École polytechnique, promotion X92. Ingénieur de l'armement en option recherche, il est titulaire d'une thèse de doctorat en cryptographie réalisée sous la direction de Jacques Stern à l'École normale supérieure de Paris. Il est également diplômé de l'enseignement supérieur en psychologie.
Il débute sa carrière comme expert puis chef du laboratoire de cryptographie de la Direction centrale de la sécurité des systèmes d'information (DCSSI). Il rejoint en 2006 le ministère de la défense, toujours dans le domaine de la cryptographie gouvernementale puis de la cyberdéfense.
En novembre 2010, il devient responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la Direction générale de l'armement (DGA). Le 27 mars 2014, il est nommé directeur général de l'Agence nationale de sécurité des systèmes d'information. plus belle histoire de l'intelligence ».

CONTRIBUTEURS DE CETTE ÉTUDE

- Matthieu Bourgeois
  Avocat, spécialiste en Droit des nouvelles technologies

- Carole Chartier
  Juriste Nouvelles technologies

- Caroline Fauveau
  Compliance Officer

- Marine Frouard
  Juriste, expert en Protection des données à caractère personnel

- Sara Gomes da Silva
  Juriste Digital & Propriété intellectuelle

- Marie-Charlotte Grasset
  Responsable Juridique Digital et Data

- Emmanuel Leprat
  Chief Data Officer

- Jérôme Loncelle
  Expert Data et IA

- Denis Pélanchon
  Cybersécurité et Computer Forensics

- Franck Régnier-Pécastaing
  Conseil expert en Gouvernance des Données

- Christophe Richard
  Médecin

Conception et réalisation :
INTERSECTION
CONSEIL & CRÉATION

Le Cercle de la Donnée est un think tank indépendant réunissant des spécialistes de la donnée, soucieux d'excellence et d'éthique et s'intéressant aux usages de la donnée, au-delà de la seule dimension technologique.
Le Cercle de la Donnée veut faire émerger et transmettre les bonnes pratiques, approfondir les multiples expertises, briser les classiques cloisonnements professionnels et ainsi contribuer à la structuration d'une filière de la donnée, basée sur l'excellence, l'éthique et l'interdisciplinarité.
Il est soutenu par des partenaires qui partagent les valeurs du Cercle, dont fait partie MarkLogic, éditeur de logiciel.

Merci également à Doshas Consulting, cabinet de conseil spécialisé pour les acteurs de la Santé, de l'Assurance et de la Protection Sociale, pour son soutien à la diffusion de cette étude.

En Savoir + : https://www.linkedin.com/company/cercledonnee/

Pour agrandir le Cercle et/ou participer à ses travaux : **contact@lecercledeladonnee.org**