Prospective
Réguler l'IA, oui mais autrement…

Pistes de réflexion pour une régulation de l'intelligence artificielle qui privilégient une approche globale et agile pour être mise au service de tous.

L'intelligence artificielle fait peur. Nombreux sont ceux qui veulent qu'on lui donne a minima un cadre éthique voire un cadre juridique. Certains même voudraient la tuer dans l'œuf, avant qu'elle n'existe. Mais qui a déjà rencontré une IA ? Qui sait définir l'IA ? En dehors d'un film de science-fiction ou d'une simple référence à un dictionnaire lambda, l'IA n'est ni un objet, ni un robot, ni un logiciel, ni une plateforme… l'IA n'est rien de tout ça et est tout ça à la fois… L'IA est au plus un concept et au mieux une résultante.

L'IA c'est l'agrégation, voire la fusion, de 3 composantes : algorithmique, apprenante et d'autonomie.

Prenons un exemple simple : « *héberger des amis* ». Par le passé, il fallait aller ouvrir la porte de la résidence à ses amis afin qu'ils puissent entrer, ou laisser la clé chez le voisin. Aujourd'hui, on peut s'équiper d'un digicode et donner le code à ses amis. Demain, la porte saura s'il faut ou non ouvrir aux personnes qui se présentent sans que l'on ait eu à la « *programmer* ». Comme cela est-il possible ? D'abord, la composante algorithmique assignera sa tâche au digicode : ouvrir la porte aux amis, ne pas ouvrir aux autres. Et à la différence d'un système expert, on ne va pas le programmer pour reconnaître qui sont les amis.

En effet, c'est la composante apprenante qui lui permettra de reconnaître qui sont les amis. Le système apprenant (machine ou deep learning) se basera sur tout un ensemble de données pour définir qui sont les amis. L'IA déterminera ses propres critères, c'est-à-dire les modèles qui lui permettront de faire la différence entre « *amis et « pas amis* ».
La composante d'autonomie lui permettra de faire évoluer la liste d'amis et de prendre la bonne décision au bon moment. La porte « *écoutera* » nos conversations : « *Chérie, tu sais que les Dupont viennent ce WE ?*», nos mails : « *Bonjour Eric, on vient ce WE ! N. Dupont !* », nos achats « *Merci Monsieur Dupont pour l'achat de vos deux billets d'avion* ».

Il utilisera pour cela des capteurs et tout un ensemble de technologies comme le traitement automatique du langage naturel, la reconnaissance d'images, la synthèse vocale… pour arriver à déterminer qui sont les amis à qui il va ouvrir la porte vendredi soir. Mais l'IA qui ouvrira la porte n'est pas celle qui vous soignera, qui vous guidera, qui calculera le montant de votre assurance, ou qui répondra aux appels clients les plus courants. L'IA unique n'existe pas !

Ainsi en fonction des tâches assignées à l'IA, les composantes, les données et les technologies utilisées ne seront-elles pas toutes de même nature, ni même leurs combinaisons… Pour revenir à notre propos liminaire « *l'IA n'est ni un objet, ni un robot, ni un logiciel, ni une plateforme* » l'IA est plus complexe et plus interdépendante de son environnement… en cela elle ressemble plus à quelque chose de vivant ou du moins à une version artificielle du vivant.

Si le numérique a créé la dimension virtuelle de notre monde, l'IA va lui insuffler la vie et ce faisant venir impacter nos vies dans le monde réel. Ainsi l'IA agit-elle comme une alchimie. D'où une difficulté majeure : Comment réguler cette alchimie pour faire en sorte qu'elle soit mise au service du progrès de l'humanité ? Pour nous assurer que le discours « *IA for good* » des entreprises technologiques et des startups soit bien une réalité ?

Des régulations impossibles

Différentes approches sont possibles.
Régulation par les acteurs. On analyse les différents acteurs de l'IA, les concepteurs d'algorithmes, de systèmes apprenants, les fournisseurs de data, de technologies, de matériels, les éleveurs d'IA, les opérateurs, l'utilisateur final… Et on établit une nouvelle chaîne de responsabilité. L'expérience du numérique nous montre que dans les mondes virtuels, ces chaînes de responsabilité sont

difficiles à mettre en place et souvent n'évitent pas les dommages. En outre cela conduit à réduire l'IA à la seule mesure de ses résultats, des fautes et des erreurs commises.

Régulation par les composantes. On régule alors les 3 composantes de l'IA : algorithme, système apprenant et système autonome. On règlemente alors par « *silo* » et on perd de vue l'essence même de l'IA, le fait qu'elle est un tout indivisible résultant de la combinaison des composantes. C'est ce qui en fait son caractère unique : tel algorithme, avec tel réseau neuronal, avec tel jeu de data développera tel pattern et prendra une décision plutôt qu'une autre. L'IA ne peut pas être réduite à la somme des technologies qu'elle utilise.

Régulation par l'objet. Il s'agit là du travail classique du juriste qui va donner une définition juridique de l'IA et bâtir un cadre juridique ad hoc. Or, si l'on s'en tient à la définition actuelle de l'IA « *l'ensemble de théories et de techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence* [1]»on comprend bien que la régulation va être difficile. Le CESE (Conseil économique social et environnemental) ne fait pas mieux, l'IA aurait pour but d' « *automatiser les comportements intelligents* », entre autres la capacité de raisonner, de collecter des informations, de planifier, d'apprendre, de communiquer, de manipuler, de signaler et même de créer, de rêver et de percevoir [2]». Ainsi tous les algorithmes, toutes les data, toutes les technologies entrent-ils dans la définition de l'IA, ce qui est irréaliste et serait une entrave à son développement. C'est réduire l'IA dès sa conception, en prévention de risques non prévisibles voire fantasmés.

Régulation par les finalités. Le tout nouveau règlement sur les données personnelles[3] nous rappelle fort à propos que le droit peut aussi réguler par les finalités. C'est-à-dire, ce pour quoi l'on fait les choses. C'est la finalité du traitement de données personnelles qui fonde les obligations. Ce type de raisonnement législatif n'est valable que dans un monde numérique statique où le collecteur de données sait ce qu'il va faire de ses données. Ce n'est pas le cas de l'IA puisque les jeux de données serviront à différents systèmes apprenants qui auront différentes fonctionnalités sans que l'on sache a priori ce qui servira au final dans la décision prise par l'IA.

Là encore une telle solution réduirait le développement potentiel de l'IA.

Régulation de la résultante. C'est l'option prise actuellement par le Parlement européen en faveur d'une immatriculation des robots et la création de la personnalité juridique de l'IA. Le Parlement européen[4] veut réguler l'IA en l'incluant dans une enveloppe corporelle qui serait le robot qui a la capacité : « *d'acquisition d'autonomie grâce à des capteurs et/ou à l'échange de données avec l'environnement (interconnectivité) et l'analyse de données ; d'apprentissage à travers l'expérience et l'interaction ; d'adaptation de son comportement et de ses actes à son environnement.* »

La solution européenne est très anthropo-centrée. L'IA serait, comme nous, limitée à son enveloppe corporelle. C'est ignorer que l'IA est avant tout une intelligence en réseau et qu'il n'existe pas, sauf preuve contraire, de « *personnalité collective* ». Que même une IA consciente n'aura pas de forme d'individualité telle que nous la connaissons. Toutes les « *Samantha 2000* » resteront en réseau. En détruire une ne détruira pas Samantha, qui est et restera une intelligence artificielle qui vit et est nourrie par la dimension virtuelle de notre monde. La régulation de l'IA serait inefficace.

Trop réguler, pas assez protéger, la question de la régulation reste entière mais ne peut plus être négligée compte tenu des avancées technologiques et de l'impact sociétal de l'IA. Comment alors construire un cadre qui puisse embrasser la complexité d'une technologie vivante ? Un cadre qui soit suffisamment agile comme le préconise le lanceur d'alerte Christopher Wylie ? Lequel ne voit pas en quoi le RGPD va éviter un prochain Cambridge analytica.

Une régulation par les « Grands principes de l'IA »

Ce papier n'a pas pour prétention d'avoir trouvé la pierre philosophale. Il permet surtout de fermer des pistes. Mais se limiter à ce simple constat n'est pas très constructif.

Au plan juridique, l'IA n'est pas une simple révolution, c'est une disruption juridique. Il bat en brèche les modèles statiques de régulation. L'IA nous oblige donc à repenser notre façon de réguler et de privilégier une approche globale et agile.

Pour répondre à ce double impératif, il y a lieu de se concentrer sur l'esprit de la loi et non sa lettre. De ne plus raisonner en termes de règles et de normes mais plutôt à la manière d'Aristote puis du Droit romain qui distinguait le jus de la Lex.

S'il doit y avoir un droit de l'IA, alors il convient sans doute de se limiter à de grands principes à l'instar des 3 lois d'Asimov. Mais les lois d'Asimov sont bien trop limitées pour constituer un corpus permettant d'atteindre l'objectif de cette régulation : la confiance !

Lister ces grands principes n'est pas si compliqué… Il suffit de se poser la question de ce que nous voulons et ce que nous ne voulons pas de l'IA.

Ce que nous voulons :

- une IA transparente : l'IA doit reposer sur un principe fondamental, celui de l'information ;
- une IA neutre : l'IA doit être au service de l'individu et non l'asservir ;
- une IA pour tous : l'IA doit être un droit opposable et exempt de toute forme de discrimination ;
- une IA universelle : l'IA ne doit être mise en œuvre que pour le bien commun ;
- une IA loyale : l'IA doit être exempte de toute manipulation individuelle ou collective ;
- une IA digne : une IA qui ne juge pas l'humain ou qui, si elle le juge doit être combinée avec d'autres facteurs humains ;
- une IA verte : l'IA doit être économe en matière première et limiter son empreinte sur l'écologie ;
- une IA citoyenne : une IA qui laisse aux citoyens le débat et les choix politiques.

Ce que nous ne voulons pas :

- une IA imposée : il faut donc consacrer un droit à refuser l'IA ;
- une IA cachée : il importe que les individus soient conscients de la mise en œuvre d'un process d'IA ;
- Une IA manipulatrice : l'IA doit être une IA « *for good* » ou ne pas être.

Cette liste a vocation à s'enrichir des différents travaux d'éthiques qui sont menés çà et là.

Une régulation par les grands principes aurait également l'avantage de pouvoir être adoptée sans grande difficulté au niveau mondial. Car méfions-nous des régulations nationales, l'IA de par sa dimension transnationale ne pourra pas être régulée localement. Une telle approche présenterait l'avantage de pouvoir être mise en œuvre rapidement.

Le process engagé par l'UE a certes le mérite d'exister, mais il s'inscrit dans une démarche temporelle qui n'est pas celle imposée par les développements exponentiels de l'IA. Enfin, cette approche permettrait d'éviter les régulations sectorielles comme c'est le cas pour la blockchain. Aujourd'hui, nombre de secteurs professionnels s'interrogent sur l'IA à l'instar du CSPLA (Conseil supérieur de la propriété littéraire et artistique). Si l'approche est très intéressante gardons-nous qu'elle aboutisse à une régulation sectorielle éclatée.

Une déclinaison in situ

Mais soyons clairs, une régulation par de grands principes ne suffit pas, elle est bien trop élastique, interprétative et donc par nature permissive. Il faut donc combiner les grands principes avec une contrainte de mise en œuvre.

Comment atteindre cet objectif : très simple… imposer à tous les acteurs de l'IA (des concepteurs aux utilisateurs) de décliner in situ les grands principes ainsi adoptés.

Chaque entreprise qui fournirait ou utiliserait l'IA aurait alors pour obligation de décliner, en fonction de son environnement, de ses fonctions, de ses objectifs et de ses cas d'usages, les grands principes à travers un engagement formel dont le non-respect serait juridiquement sanctionné. Il ne s'agirait plus d'une soft law basée sur des chartes plus ou moins éthiques, mais d'une régulation bâtie sur le modèle des règles d'entreprises contraignantes.

Ces BCR for IA (Biding corporate rules for IA) pourraient alors faire l'objet au besoin d'une validation ou d'un contrôle par des tiers indépendants à l'instar des procédures de certification ou de labélisation. Elle pourrait aussi faire l'objet de contrôle par des autorités désignées à cet effet, sur le modèle de la régulation des grands pans du droit comme le sont pour l'heure la Cnil, l'Arcep ou encore le CSA.

Avec l'IA, l'objectif ne doit pas être d'appliquer la loi mais de la respecter…

Prologue…

Il est usuel de terminer un article par une conclusion… mais pouvons-nous valablement conclure une histoire qui ne fait que commencer ! On ne peut parler que d'un « *prologue juridique* », une pièce très modeste à l'édifice qui consistera nécessairement à réguler l'IA. Car clairement, il ne saurait être question de laisser le secteur de l'IA s'autoréguler, l'IA y perdrait.

Inversement, il faut savoir choisir la bonne voie. En matière juridique il n'existe que deux voies : la régulation de contrôle ou la régulation de développement. La régulation de contrôle consiste à encadrer une technologie et généralement d'en brider le développement. La biométrie en est l'exemple parfait qui est une technologie particulièrement intéressante bridée par un cadre juridique suspicieux. A l'opposé, la réglementation peut supporter le développement d'une technologie en fixant un cadre qui soit favorable au déploiement et même à l'expérimentation.

Gageons, pour l'IA et pour tous les bénéfices que nous pourrions en retirer que la régulation sera une régulation du possible et non une régulation de l'interdit…

Affaire à suivre.

Isabelle GALY
Experte en écosystème numérique

Eric BARBRY
Avocat associé, Cabinet RACINE

Notes

(1) *Définition de Wikipédia*

(2) *AVIS du Comité économique et social européen sur « L'intelligence artificielle – Les retombées de l'intelligence artificielle pour le marché unique (numérique), la production, la consommation, l'emploi et la société » 2016*

(3) *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE)*

(4) *Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique*