Dossier

IA et droit : dépasser la fiction pour une approche juridique raisonnée

L'Intelligence Artificielle (« IA ») berce nos existences à travers les plus grandes œuvres de science-fiction. L'IA y est présentée comme une menace ou comme une solution pour l'humanité. La remise au premier plan de l'IA grâce aux progrès du numérique a logiquement été accompagnée d'une résurgence de ces réflexes et biais culturels, créant un véritable mythe autour de l'IA.

Cette mystification de l'IA provient d'une erreur d'analyse initiale qui consiste à croire, comme l'a présenté la science-fiction, que l'IA est quasiment omnisciente, généraliste, qu'elle comprendrait par elle-même et qu'elle aurait quasiment conscience de sa propre existence. En somme, l'IA telle qu'elle est fantasmée est une IA « forte » qui ne correspond aujourd'hui à aucune réalité que ce soit au regard du niveau d'avancée des travaux de recherche et développement ou des applications d'IA intégrées aux produits ou services sur le marché.

En effet, l'IA telle qu'elle existe aujourd'hui est loin d'avoir ces caractéristiques. Les IA qui nous entourent au quotidien sont des IA spécialisées, extrêmement performantes dans des domaines très pointus, pour lesquels elles ont été spécifiquement entrainées. C'est ce que l'on appelle des IA faibles. Cette appellation ne doit en aucun cas minimiser les résultats exceptionnels obtenus grâce à ces IA dans des domaines divers tels que la médecine, la mobilité, la finance, l'énergie ou plus généralement toute activité basée sur l'exploitation de données.

Notre réalité est qu'à chaque instant, des algorithmes sondent, calculent et analysent un nombre impressionnant de données, qui serviront à trouver un diagnostic, définir des offres, à améliorer un service ou encore, à proposer un prix.

Face à la montée en puissance des IA et de leur utilisation par divers acteurs économiques et politiques, les questions juridiques et éthiques relatives à cette utilisation se posent. La première question à se poser est d'ailleurs d'examiner la manière dont notre législation actuelle permet d'ores et déjà d'accueillir ces solutions et d'apporter les garanties nécessaires à la sécurité juridique. Ensuite, dans des cas spécifiques, il faut s'interroger sur la nécessité d'adopter des règles spéciales.

Il est donc nécessaire d'anticiper les conséquences juridiques qui découleront de l'utilisation des IA, que ce soit en matière de protection des droits de propriété intellectuelle, de protection des données à caractère personnel, de responsabilités, de mobilité urbaine ou encore de concurrence.

Au sein de l'Union européenne, la Commission développe des mesures pour encadrer les règles en matière de responsabilité et de transparence des IA. Les récents développements autour notamment de la reconnaissance faciale font partie des priorités.

L'heure n'est donc plus à la fiction et au droit prospectif, mais bien à l'analyse concrète des effets des IA sur notre droit et du droit sur les IA. ■

Georgie COURTOIS, Jean-Sébastien MARIEZ et Thierry TITONE
Avocats associés, De Gaulle Fleurance et Associés

SOMMAIRE

RLDA 6781

Intelligence artificielle : quels objets de droit pour quel encadrement contractuel ?

Georgie COURTOIS
Avocat associé De Gaulle Fleurance et Associés

Jean-Sébastien MARIEZ
Avocat associé De Gaulle Fleurance et Associés

Tout d'abord est exposée ici une proposition de modèle d'analyse des composantes d'une solution d'intelligence artificielle, avant de présenter un panorama des problématiques juridiques récurrentes dans le cadre de la sécurisation des rapports transactionnels entre fournisseurs d'intelligence artificielle et clients.(1)

Le regain que l'intelligence artificielle (« IA ») connait depuis quelques années conduit à la multiplication des rapports transactionnels impliquant, d'une part, les fournisseurs de produits ou services informatiques et, d'autre part, leurs clients personnes morales de droit privé ou de droit public.

Dans ce contexte, il est parfois difficile de faire le distinguo entre d'une part, les fournisseurs qui, sous couvert d'IA, proposent en réalité des produits ou services informatiques ne générant pas de spécificités sous un angle juridique (par exemple, un progiciel) et d'autre part, des solutions d'IA à proprement parler qui méritent une attention particulière dès lors que leur encadrement contractuel reste à baliser (solution d'IA).

Dans cette seconde hypothèse, afin de sécuriser autant que possible le rapport contractuel en cause, il est nécessaire de comprendre quels objets de droit composent une IA, afin de déterminer en toute connaissance de cause le régime que les parties souhaitent convenir. À cet égard, la première partie de cet article expose un modèle d'analyse des composantes d'une solution d'IA, ses éléments et leurs interactions.

Sur la base de ce modèle d'analyse, il est ensuite possible d'aborder les problématiques juridiques qui, de manière transversale, doivent être traitées quel que soit le type d'application d'IA en cause. Dans cette perspective, la seconde partie de cet article présente les principales questions qui doivent retenir l'attention des co-contractants : la protection des droits de propriété intellectuel ; la protection des données à caractère personnel ; et la répartition contractuelle des responsabilités(2). Les régulations sectorielles dont l'examen peut s'avérer essentiel ne seront pas abordées ici.

I. – Proposition d'un modèle d'analyse juridique des objets de droit composant une solution « IA »

Afin de sécuriser contractuellement la mise à disposition et l'exploitation d'une solution d'IA, il est nécessaire de s'intéresser d'une part au modèle économique du fournisseur d'IA et d'autre part, au régime qui conduira le sort des objets de droits constitutifs d'une solution IA.

S'agissant d'abord **des modèles économiques** qui peuvent être actuellement rencontrés sur le marché, une première typologie permet de distinguer trois principaux modèles :

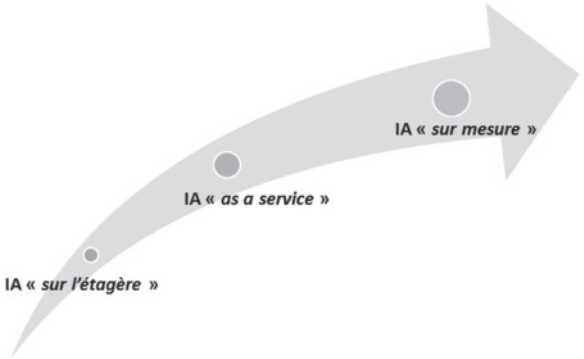
- IA « *sur l'étagère* » : IA, type progiciel, très spécialisée, dont la structure n'évolue pas ou peu au contact

(1) Cet article fait suite à la conférence « *Démystifier et comprendre l'Intelligence Artificielle : conditions nécessaires à une approche juridique sereine et sécurisée* » organisée le 14 mars 2019 par le cabinet De Gaulle Fleurance et Associé. Les auteurs remercient M. Coulaud, Directeur juridique, Microsoft France et M. Hindi, Président fondateur, Snips, pour leur participation ainsi que J. Roussel, avocat et J. Bader, juriste, pour leurs précieuses contributions.

(2) Les régulations sectorielles dont l'examen peut s'avérer essentiel ne seront pas abordées ici.

des données intégrées. La fourniture de ce type de solution d'IA est le plus souvent encadrée par des conditions générales d'utilisation similaires à celles d'un progiciel ;

- IA « *as a service* » : IA mise à disposition sur une plateforme Cloud permettant à l'utilisateur d'exploiter des modèles d'IA (Ex : Microsoft Azure, Google Cloud Platform, Amazon Web Services). La fourniture de ce type de solution d'IA est le plus souvent encadrée par des conditions générales d'utilisation similaires à celles d'un service de Cloud ;
- IA « *sur mesure* » : IA intégrée et développée *ad hoc* dans le cadre d'un projet informatique pour les besoins d'une activité spécifique d'une organisation. Selon son niveau de complexité la fourniture de ce type de solution d'IA devra être encadrée par un contrat *ad hoc* de type projet informatique.



Premier objet, le moteur d'une solution d'IA performante est constitué par la combinaison d'algorithmes auxquels peuvent s'ajouter d'autres technologies (par exemple : logiciel, savoir-faire) : l'algorithme initial. En vue de son exploitation pour une finalité spécifique, ce premier objet doit faire l'objet d'un processus d'apprentissage.

Cet apprentissage implique l'élaboration d'un deuxième objet : un ou plusieurs jeux de données (les données d'apprentissage) dont la nature propre permet de développer, sur la base de l'algorithme initial, un troisième objet : une solution d'IA appliquée à un domaine spécifique et répondant à une fonctionnalité particulière (le modèle).

Ensuite, il est nécessaire d'appréhender **les objets de droit** composant une solution d'IA. Une bonne compréhension des éléments en présence et de leurs interactions est en effet essentielle lorsqu'il s'agit d'encadrer contractuellement un projet d'IA « sur mesure ».

Comme le montre le schéma ci-dessous, une solution d'IA peut être présentée comme étant composée de quatre éléments majeurs :

Résultat de ce processus d'apprentissage, le modèle est alors mis en exploitation pour générer, sur la base de données d'exploitation, un ensemble d'informations présentées sous une forme quelconque, les données de résultat.

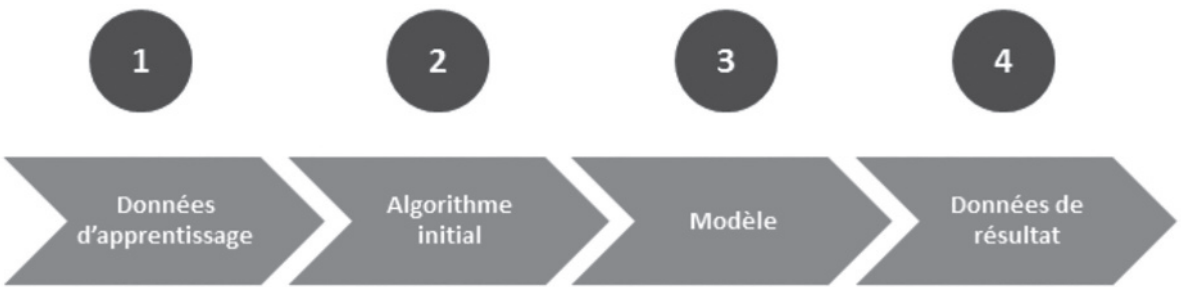
Ces quatre objets peuvent être regroupés en deux sous-ensembles.

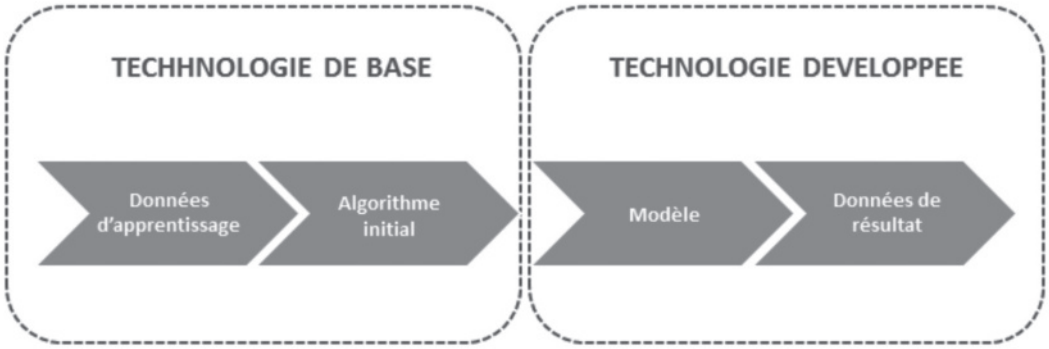
Un premier ensemble regroupe les objets constitutifs des prérequis au développement d'une solution d'IA. Il s'agit des données d'apprentissage et l'algorithme initial, désignés ci-dessous sous l'intitulé technologie de base (*Background technology*). Selon les modèles, ces deux objets peuvent résulter d'apports exclusifs (le fournisseur apporte l'algorithme initial et le client apporte les données d'apprentissage) ou d'apports croisés (l'algorithme initial résulte de la combinaison des algorithmes du fournisseur et de technologies du client ou encore, les données d'apprentissage apportées par le client sont toutefois calibrées par le fournisseur).

Un second ensemble regroupe les objets qui résultent du processus d'apprentissage conduisant au développement du modèle et à l'exploitation de celui-ci pour générer les données de résultat : technologie développée (*Foreground technology*) (v. schéma p. 24).

II. – Encadrement contractuel d'une solution d'IA : points d'attention sur les problématiques récurrentes et recommandations

Une fois bien intégrés les objets de droit composants d'une solution d'IA, il est possible d'analyser toute question juridique susceptible d'être levée dans le cadre de son cycle de vie. La seconde partie de cet article se concentre sur les problématiques récurrentes que les parties à un





contrat de fourniture de solution d'IA ne manqueront pas d'aborder afin de sécuriser leur relation.

A. – Propriété intellectuelle : de la détermination des apports à la technologie de base aux droits d'exploitation de la technologie développée

Pour chacun des objets de droit constitutifs d'une IA (voir ci-dessus I), il est nécessaire de s'interroger sur le meilleur encadrement contractuel susceptible d'apporter un équilibre entre le client et le fournisseur d'IA.

➜ *Technologie de base*

Pour ce faire, dès le stade des « technologies de base», il faut être capable d'identifier précisément les apports (informations, données, technologies…) de chacune des parties et les règles d'utilisation de ces apports.

En premier lieu, le sort des données d'apprentissage du client qui serviront à nourrir l'algorithme doit être précisément encadré. Ces données constituent une partie indéniable du patrimoine du client. S'il fait appel à l'IA, c'est pour extraire de ces données toute leur valeur. Contractuellement, le client autorisera au fournisseur d'IA à accéder, extraire et utiliser ces données dans le cadre du projet les liant, en excluant tout transfert de propriété sur ces données.

En second lieu, le rôle joué par l'algorithme initial est également central. Cet algorithme initial est fourni par le fournisseur d'IA. Souvent composé d'une combinaison d'algorithmes *open source*, il n'en demeure pas moins que la question de sa protection et de sa propriété doit être prévue dans le cadre contractuel. Bien qu'un algorithme ne soit pas protégeable au titre du droit d'auteur par nature[3], les algorithmes sont intégrés à un logiciel qui est susceptible de leur conférer une protection au titre du droit d'auteur des logiciels ou éventuellement à un brevet, sous réserve de satisfaire aux critères de brevetabilité. Dès lors, ces éventuelles licences, leur périmètre d'utilisation et la gestion du savoir-faire associé, doivent être prévus contractuellement entre les parties.

Bien évidemment, une confidentialité particulièrement stricte doit encadrer ces rapports et la fourniture des objets respectifs par les parties.

Après avoir encadré les objets respectifs apportés par les parties dans le cadre du projet IA (« technologie de base »), les parties devront prévoir les conséquences de cette union des apports (« technologie développée »).

➜ *Technologie développée*

Le point essentiel qu'il est nécessaire de prévoir est celui de la propriété et de l'éventuelle réutilisation du modèle entrainé. C'est le cœur même de la spécificité de la contractualisation de l'IA. En effet, le modèle entrainé constitue la fusion des apports respectifs des parties : le modèle ne pourrait exister sans les données d'apprentissage du client, ni sans l'algorithme initial. Mais surtout, en ayant été nourri par les données d'apprentissage, il constitue en quelque sorte une synthèse des données du client ayant servi à son apprentissage, ce dont le client n'a pas forcément conscience. Ces données d'apprentissage, souvent amassées sur de très longues années, ont une valeur particulièrement importante. Le modèle entrainé est donc susceptible d'intégrer des données d'apprentissage dans lesquelles le client a investi énormément de temps et d'argent.

Ces points de négociation sont fondamentaux pour le client et peuvent-être de nature à orienter le choix entre plusieurs fournisseurs d'IA, notamment selon la typologie de projet pour lequel la solution d'IA est développée.

À titre d'exemple, dans un environnement fortement concurrentiel, le client pourrait souhaiter que le modèle entrainé, en ce qu'il intègre ses données d'apprentissage, reste sa seule propriété afin d'éviter, par exemple, qu'un concurrent bénéficie du modèle entrainé grâce à ces données.

Dans d'autres typologies de solution, le fournisseur d'IA pourrait souhaiter réutiliser le modèle entrainé grâce aux données d'apprentissage d'un client auprès de ses

(3) Rapport France IA, mars 2017, Intelligence artificielle et enjeux juridiques, p. 295.

propres clients. Le fournisseur d'IA est même susceptible de mettre en avant son savoir-faire dans un secteur particulier et ses modèles déjà pré-entrainés pour conquérir de nouveaux marchés. Cette autorisation d'utilisation du modèle entrainé peut faire l'objet d'une rémunération du client (si on estime qu'il est copropriétaire du modèle entrainé) ou d'une réduction du prix de la solution d'IA.

Les parties pourront également négocier, à titre d'exemple, une propriété exclusive, une copropriété ou encore une licence d'utilisation du modèle entrainé au fournisseur d'IA pour ses besoins de recherche et de développement, sans qu'il puisse céder le modèle entrainé à des tiers. L'encadrement contractuel devra également prévoir le cas échéant les modalités de dépôt et de cession d'éventuels brevets issus du modèle entrainé.

Enfin, les parties pourront également prévoir le sort des données de résultat issues du traitement par le modèle. Ces données sont de nature à intéresser le fournisseur d'IA pour mieux comprendre le fonctionnement du modèle créé et, partant, celui des autres modèles qu'il développe pour ses autres clients. Bien que la propriété de ces données de résultat au client ne fasse pas de doute[4], ce dernier peut accorder au fournisseur d'IA une licence pour une utilisation limitée en interne.

B. – Responsabilité : recherche d'un équilibre au vu des contributions respectives

La gestion de contours de la responsabilité et ses limitations dans le cadre d'un projet d'IA est complexe. Une solution d'IA est développée le plus souvent pour constituer une aide à la décision. Dès lors, si la solution préconisée par l'IA cause un dommage, toute personne ayant subi un préjudice direct est susceptible d'en demander réparation.

L'origine distribuée des apports respectifs du fournisseur d'IA et du client entraine des conséquences en terme de responsabilité qu'il est nécessaire de prévoir dès le stade de la contractualisation.

À titre d'exemple, la responsabilité du fournisseur d'IA pourrait être engagée dans l'hypothèse où le fait générateur du dommage est lié à un dysfonctionnement de l'algorithme initial qu'il a fourni. Dans cette hypothèse, le client devrait pouvoir être garanti et ne pas subir les conséquences d'un défaut de son fournisseur.

En revanche, la responsabilité du client pourrait être engagée dans l'hypothèse où le fait générateur du dommage est lié à la fourniture de données d'apprentissage biaisées ou défectueuses ayant conduit à l'entrainement défaillant de l'algorithme. Le client est en effet responsable du jeu de données d'apprentissage qu'il décide d'utiliser, tant que le fournisseur n'a pas de contrôle sur ces données. Toutefois, la responsabilité pourrait être distribuée entre le fournisseur et le client, voire peser sur le fournisseur dans l'hypothèse où ce dernier a également pour mission de configurer et de nettoyer le jeu de données fourni par le client. En effet, les projets d'IA contiennent souvent une phase préparatoire de calibration des données d'apprentissage qui seront utilisées pour nourrir l'algorithme. Le fournisseur d'IA est censé aider le client, au moins au titre de son obligation de conseil, pour calibrer les données pour les besoins du projet d'IA.

En tout état de cause, il faut avoir conscience que des difficultés pourront se poser quant à la détermination de la composante à l'origine du fait générateur, cause du dommage. En effet, les solutions d'intelligence artificielle ne sont pas toujours transparentes. C'est notamment le cas des solutions d'intelligence artificielle utilisant la technologie du *deep learning* (apprentissage profond) dont l'utilisation crée un phénomène appelé « boîte noire » : il est possible de comprendre quelles données entrent dans la « boîte » et les résultats qui en sortent, mais sans savoir ni comprendre ce qui se passe à l'intérieur. Dès lors, il est parfois impossible de comprendre les étapes ayant conduit au résultat erroné.

L'enjeu pour le client sera donc de comprendre quelles technologies sont utilisées et les conséquences de leur utilisation afin de pouvoir négocier en connaissance de cause les éventuelles répartitions et limitations de responsabilité avec le fournisseur d'IA. Dans ce cadre, compte tenu de la complexité technologique, il peut être opportun de prévoir en amont un système d'audit et d'expertise de la solution d'IA par un tiers qui sera à même d'apprécier les causes de défaillance potentielles du système.

C. – Protection des données à caractère personnel et Big Data : une réconciliation nécessaire

La question de la protection des données à caractère personnel mérite une attention particulière dans le cadre du développement et de l'exploitation de solutions d'IA. En effet, l'IA et en particulier le *Big Data*[5] se distinguent par une série de caractéristiques aux implications importantes quant au respect des exigences issues de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique (LIL), aux fichiers et aux libertés et du 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 (RGPD).

(4) Une clause permettant la réversibilité pour récupérer l'ensemble des données initiales et des données de résultat est conseillée pour gérer le sort des données à l'issue du contrat.

(5) Ensembles de données très volumineux dont le traitement et l'analyse dépasse l'intuition et les capacités informatiques et humaines classiques.

Au-delà de la nécessité de déterminer contractuellement les responsabilités respectives du fournisseur d'IA et de son client en tant que responsable de traitement, responsables conjoints ou sous-traitants, un certain nombre de points de vigilance doivent nécessairement être abordés par les parties. Sans vocation exhaustive, nous abordons ici les problématiques qui semblent incontournables.

Premier point d'attention à considérer : la notion même de donnée à caractère personnel dans le contexte du *Big Data*. Étant rappelé qu'une donnée est qualifiée de personnelle dès lors qu'elle permet d'identifier un individu directement ou indirectement(6), certaines études soutiennent que la notion d'identification indirecte prend une nouvelle dimension dans le cadre de traitements *Big Data* dès lors que cette technologie induit un risque exponentiel de ré-identification(7). La mise en œuvre de techniques de recoupement massifs et d'agrégation de données, qui, prises isolément sont considérées comme anonymes, permettrait de manière indirecte, dans de nombreux cas, la ré-identification d'individus et donc l'application des exigences issues des textes précités.

Ce constat conduit à une première recommandation pratique : la nécessité de conduire un audit des jeux de données utilisées tant en leur qualité de données d'apprentissage que de données d'exploitation. La raison d'être de cette analyse sera de déterminer l'applicabilité des règles de protection des données à caractère personnel. Trois situations principales peuvent être distinguées. En premier lieu, l'étude permet de confirmer que les jeux de données n'ont pas de caractère personnel et donc d'écarter *a priori* l'application du RGPD et de la LIL. En second lieu, il peut s'avérer que les jeux de données contiennent au moins en partie des données à caractère personnel qui ont cependant été l'objet d'un procédé d'anonymisation. Il s'agira alors de vérifier la robustesse du procédé employé(8) pour écarter tout risque de ré-identification et, par voie de conséquence, l'application des règles issues des textes précités. Dernière hypothèse, l'audit révèle que les jeux de données comportent des données à caractère personnel non-anonymisées. Il s'agira alors de se poser la question de la nécessité d'utiliser des données à caractère personnel. Si l'anonymisation n'est pas adaptée au projet, alors il faudra organiser la mise en conformité de la solution d'IA avec l'ensemble des exigences énoncées par la LIL et le RGPD. Dans chacune de ces situations, l'analyse devra tenir compte du statut des données à la fois au stade du développement de la solution d'IA et au stade de son exploitation qui, si elle induit des recoupements, peut faire émerger un risque de ré-identification n'existant pas *ab initio*. Enfin, il faut souligner que cet audit peut utilement être mis à profit afin, d'une part, de garantir l'intégrité, l'exactitude, la nécessité et la pertinence des données objet du traitement(9) et, d'autre part, mettre en œuvre le principe de protection des données dès la conception *(privacy by design)* et celui de protection des données par défaut *(privacy by default)*(10).

Ensuite, il convient de mettre en regard les principales caractéristiques des traitements reposant sur une technologie *Big Data* avec les règles de protection des données à caractère personnel.

En premier lieu, le *Big data* implique la collecte et le traitement d'autant de données que possible. Comment ménager cet impératif technique avec le principe de minimisation des données issu de l'article 5(1)(c) ?

S'il n'existe pas de réponse tranchée à cette question, une première piste de gestion du risque réside sans doute dans la réalisation de l'audit des jeux de données préconisée ci-dessus. Cette analyse doit permettre d'écarter les données dont le caractère adéquat et nécessaire ne pourrait être démontré. De même, un jeu de données qui révèlerait des inexactitudes devrait faire l'objet d'un nettoyage, en particulier dès lors qu'il pourrait générer des biais dans le fonctionnement de la solution d'IA. Une seconde piste consiste à réaliser une analyse d'impact au sens des articles 35 et 36 du RGPD. Son objet est précisément d'évaluer la nécessité et la proportionnalité des opérations de traitement au regard de leurs finalités afin d'identifier et d'atténuer le risque élevé pour les personnes concernées. Il faut préciser que la réalisation d'une telle analyse est obligatoire dans de nombreuses situations. Par exemple, en cas de traitement à grande échelle de données sensibles au sens de l'article 9 du

(6) RGPD, art. 4(1) « *"données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

(7) Dans ce sens, par exemple : *President's Council of Advisors on Science and Tecnology. Big data and privacy. A technological perspective. White House*, mai 2014 ; C. Zolynski et A. Bensamoun, Actes du colloque Big data et privacy : comment concilier nouveaux modèles d'affaires et droits des utilisateurs ?, Montréal, 15 oct. 2013 : LPA, 18 août 2014.

(8) V. Groupe de travail protection des données, l'article 29, opinion 05/2014 on Anonymisation Techniques, 10 avr. 2014.

(9) RGPD, art. 5(1). : « *Les données à caractère personnel doivent être : […] (c) adéquates, pertinentes et limimtées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ; (d) exacte et, si nécessaire, tenues à jour, toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soit effacées ou rectifiées sans tarder (exactitude)* ».

(10) RGPD, art. 25.

RGPD ou de profilage de personnes sur la base de données provenant de sources externes[11].

En deuxième lieu, le *Big Data* repose sur une exploitation des données ne permettant pas toujours de déterminer la **finalité des traitements** de manière précise, en amont de leur mise en œuvre. En effet, le processus d'apprentissage de l'algorithme initial donne lieu en cours de processus à des calculs et corrélations non anticipées. Ces opérations sont susceptibles de réorienter les finalités du traitement[12]. De prime abord, cette caractéristique semble difficilement réconciliable avec le principe de finalité[13] qui, selon l'article 5 du RGPD, impose de déterminer à l'avance, de manière spécifique, l'objectif ou les objectifs du traitement[14] afin de les porter à la connaissance des personnes concernées[15] dès le stade de la collecte[16].

En pratique, il faut d'abord relever que cette question aura une acuité variable selon le type de solution d'IA dont le développement ou l'exploitation est envisagée. Par exemple, une IA « sur l'étagère » proposant une fonctionnalité spécifique ne semble pas poser de difficulté. De plus, il faut préciser que s'agissant de traitements à des « fins statistiques », le RGPD et la LIL apportent des précisions qui peuvent permettre de diminuer le risque d'incompatibilité avec la finalité initiale[17].

Pour les solutions d'IA plus complexes, la gestion du risque associé à cette question de la finalité doit être abordée sous le double prisme de la notion de traitement ultérieur compatible avec la finalité initiale[18], d'une part, et de l'information des personnes concernées, d'autre part.

Une première recommandation consiste à travailler autant que possible, en amont du traitement, à la détermination de la ou les finalités correspondant au traitement *Big data*. Cette réflexion doit intégrer les finalités susceptibles d'être anticipées *ab initio* ainsi que leur compatibilité avec la finalité initiale. Pour ce faire, il s'agit de se référer au test de compatibilité issu de l'article 6.4 du RGPD[19]. Les critères énoncés par cet article reposent sur le lien suffisant avec la finalité initiale, le contexte et les attentes raisonnables des personnes concernées au stade de la collecte, la nature des données et en particulier leur caractère sensible ou non[20], les conséquences possibles du traitement ultérieur envisagé et les garanties mises en œuvre, y compris, le chiffrement ou la *pseudonymisation*.

Une seconde recommandation concerne la transparence et la loyauté vis-à-vis des personnes concernées. Le niveau d'information fourni par le responsable de traitement participe de la compréhension des finalités du traitement. Ainsi, le contexte du traitement, son objectif, le type de données collectées, leurs destinataires sont autant d'éléments qui doivent entrer en considération afin de déterminer si une finalité nouvelle peut être anticipée par les personnes concernées au titre de leurs attentes raisonnable[21].

En troisième et dernier lieu, selon les technologies mises en œuvre, le *Big Data* se caractérise par une opacité des traitements. Comme exposé précédemment, certaines solutions d'intelligence artificielle utilisant la technologie du *Deep Learning* engendrent, en effet, un phénomène appelé « *boîte noire* ». Cette caractéristique mérite une attention particulière au regard des obligations de transparence et d'explicabilité issues du RGPD. Tout spécialement, s'agissant des applications d'IA en matière de « *prise de décision automatisée, y compris de profilage* »[22], les articles 13 et 14 imposent une information relative à la « *logique sous-jacente* » de la prise de décision automatisée[23]. L'article 47 de la LIL évoque la communication des règles du traitement et de ses principales caractéristiques par celui qui souhaite se prévaloir des exceptions au principe de prohibition des décisions prises sur le seul fondement d'un traitement automatisé de données à caractère personnel. ■

(11) CNIL, Liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données est requise <https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-avec-aipd-requise-v2.pdf>.

(12) N. Forgo, S. Hänold, B. Schütze, *The Principle of Purpose Limitation and Big Data, in New Technology, Big Data and the Law* : Springer, 2017.

(13) Cons. const., 21 fevr. 2008, n° 2008-562 DC et G29, WP203, *Opinion on purpose limitation*, 2 avr. 2013, p. 14.

(14) S. Soltani, « Big data » et le principe de finalité, RLDI 2013/97, n° 3233.

(15) RGPD, art. 13 et 14.

(16) RGPD, cons. 39.

(17) LIL, art. 79 et RGPD, art. 14(5) et cons. 162 : « *[…] Par "fins statistiques", on entend toute opération de collecte et de traitement de données à caractère personnel nécessaires pour des enquêtes statistiques ou la production de résultats statistiques. Ces résultats statistiques peuvent en outre être utilisés à différentes fins, notamment des fins de recherche scientifique. Les fins statistiques impliquent que le résultat du traitement à des fins statistiques ne constitue pas des données à caractère personnel mais des données agrégées, et que ce résultat ou ces données à caractère personnel ne sont pas utilisés à l'appui de mesures ou de décisions concernant une personne physique en particulier* ».

(18) RGPD, art. 5 autorise les traitements ultérieurs dès lors qu'ils sont compatibles avec la finalité initiale.

(19) V. aussi RGPD, cons. 50.

(20) GPD art. 9 et 10.

(21) G29, WP203, *Opinion on purpose limitation*, 2 avr. 2013.

(22) RGPD, art. 22 qui prévoit au bénéfice des personnes concernées, le « *droit de ne pas faire l'objet d'une décision fondée sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire* » et LIL, art. 47.

(23) V. aussi RGPD, cons. 71 : « *En tout état de cause, un traitement de ce type devrait être assorti de garanties appropriées, qui devraient comprendre une information spécifique de la personne concernée ainsi que le droit d'obtenir une intervention humaine, d'exprimer son point de vue, d'obtenir une explication quant à la décision prise à l'issue de ce type d'évaluation et de contester la décision. Cette mesure ne devrait pas concerner un enfant.* ».

RLDA 6782

IA et assurance

Luc GRYNBAUM
Professeur à l'Université Paris Descartes
Avocat Of Counsel De Gaulle Fleurance & associés

Les assureurs peuvent bénéficier de l'IA afin d'améliorer les techniques de souscription, de gestion de sinistre et de lutte contre la fraude. Les assureurs de responsabilité civile des professionnels voient un nouveau marché s'ouvrir : celui de la responsabilité du fait de l'utilisation d'une IA et de la responsabilité du fait d'une IA défectueuse.

Théorisé dans les 1950[1], le concept d'intelligence artificielle a pu se réaliser pleinement grâce à la rencontre du *Big Data* et de l'accroissement des capacités de stockage et de calcul. Aussi, en adoptant la définition de la Commission européenne, peut-on considérer que l'intelligence artificielle (IA) « *désigne les systèmes qui font preuve d'un comportement intelligent en analysant leur environnement et en prenant des mesures avec un certain degré d'autonomie pour atteindre des objectifs spécifiques* »[2]. La même Commission précise que « *les systèmes dotés d'IA peuvent être purement logiciels, agissant dans le monde virtuel (assistants vocaux, logiciels d'analyse d'images, moteurs de recherche ou systèmes de reconnaissance vocale et faciale, par exemple) mais l'IA peut aussi être intégrée dans des dispositifs matériels (robots évolués, voitures autonomes, drones ou applications de l'internet des objets, par exemple)* »[3].

On établit souvent une distinction entre IA faible et IA forte, cette dernière étant capable de produire un comportement intelligent et d'éprouver une conscience de soi. L'IA faible, qui résulte d'algorithmes créés par des ingénieurs, ne peut qu'exécuter des tâches spécifiques. Dans le même esprit, mais plus récemment, une distinction a été opérée entre « *l'intelligence artificielle étroite et l'intelligence artificielle générale* »[4] qui correspond peu ou prou à celle entre IA faible et IA forte. Dans une sorte de situation intermédiaire on peut identifier l'IA en apprentissage profond qui est en mesure d'améliorer ses performances en apprenant au fur et à mesure de sa mise en œuvre.

Si, en France, le rapport Villani[5] a permis une réflexion ordonnée sur les grands mérites du développement de l'IA, c'est au Parlement et à la Commission européenne que reviennent le mérite d'une incitation à une évolution législative à propos de l'IA et des robots qui sont des IA dotées d'une enveloppe physique « *qui agit par le mouvement par et sur le monde réel* »[6].

Pour que le robot soit considéré comme intelligent, le Parlement européen a mis en exergue les critères suivants :

- « *acquisition d'autonomie grâce à des capteurs et/ou à l'échange de données avec l'environnement (interconnectivité) et à l'échange et l'analyse de ces données ;*
- *capacité d'auto-apprentissage à travers l'expérience et les interactions (critère facultatif) ;*
- *existence d'une enveloppe physique, même réduite ;*
- *capacité d'adaptation de son comportement et de ses actes à son environnement ;*
- *non vivant au sens biologique du terme* »[7].

(1) A. Turing, Computing machinery and intelligence, Oxford University Press, vol. 59, n° 236, oct. 1950 ; F. Rosenblatt, *Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms*, éd. Spartan Books, 1962.

(2) Comm. UE, communication, COM(2018) 237 final, L'intelligence artificielle pour l'Europe, 25 avr. 2018, p. 1.

(3) *Ibid*, p. 1.

(4) PE, rés. 12 févr. 2019, sur une politique industrielle européenne globale sur l'intelligence artificielle et la robotique (2018/2088(INI)), n° 116.

(5) Donner un sens à l'intelligence artificielle, 28 mars 2018.

(6) *Ibid*.

(7) PE, rés. 12 févr. 2019, préc.

Enfin la notion d'autonomie, fréquemment évoquée pour caractériser une IA forte a été caractérisée pour le robot comme « *la capacité à prendre des décisions et à les mettre en pratique dans le monde extérieur, indépendamment de tout contrôle ou influence extérieurs* »[8].

Après avoir posé les définitions, dans une approche normative, de l'IA et du robot, il convient de relater les ébauches d'encadrement juridique de ces entités. Dans une première résolution le Parlement européen a considéré qu'il était « *utile et nécessaire de définir une série de règles, notamment en matière de responsabilité, de transparence, et d'obligation de rendre des comptes* », mais « *que ces règles ne doivent pas brider la recherche, le développement et l'innovation dans le domaine de la robotique* »[9]. Puis, la Commission européenne dans une communication du 25 avril 2018 a souhaité qu'il soit établi des lignes directrices concernant l'éthique de l'IA dans le respect des droits fondamentaux, qu'il soit publié un document d'orientation sur l'interprétation de la directive sur la responsabilité du fait des produits défectueux et que les lacunes en matière de responsabilité soient identifiées[10]. Le Parlement européen a repris l'initiative en adoptant une nouvelle résolution dans laquelle il est demandé à la Commission d'améliorer la réglementation en ce qui concerne l'IA[11] tout en constatant qu'un groupe de travail sur la modification de la directive sur la responsabilité du fait des produits défectueux a été installé[12]. Il demande en outre la mise en place de règles éthiques, que le développement de l'IA respecte les règles sur les données personnelles et qu'il soit laissé une place aux citoyens européens qui souhaitent vivre hors ligne[13].

Le secteur de l'assurance peut, comme tous les autres, bénéficier de ces nouvelles technologies et il lui appartient aussi d'apporter une réponse d'accompagnement aux éventuelles responsabilités.

I. – L'assurance bénéficiaire de l'IA

Le secteur de l'assurance peut bénéficier comme les autres services des apports des nouvelles technologies pour renouveler sa pratique. En effet, dans le cadre de la souscription, le *chatbot* intelligent et la technologie *blockchain* sont en mesure d'opérer une nouvelle évolution.

(8) PE, rés. 12 févr. 2019, préc.

(9) PE, rés. 16 févr. 2017, contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL).

(10) Comm. UE, communication préc., p. 20.

(11) PE, rés. 12 févr. 2019, préc., n° 114.

(12) PE, rés. 12 févr. 2019, préc., n° 131.

(13) PE, rés. 12 févr. 2019, préc., n° 138 à 142.

Le *chatbot* permet de mieux orienter le candidat souscripteur à un contrat d'assurance et de dispenser le devoir de conseil renforcé depuis la réforme de la distribution d'assurance[14]. En outre la *blockchain* (sorte de registre étendu de transactions horodatées et classées, distribuées sur un ensemble de machines) offre la sécurité d'une base de données, sécurisée, inviolable et non falsifiable qui n'est pas contrôlée par une personne déterminée.

> *Le secteur de l'assurance peut bénéficier comme les autres services des apports des nouvelles technologies pour renouveler sa pratique.*

L'une des autres applications consiste de la *blockchain* dans l'outil *smart contract*. L'expression constitue à nos yeux un faux ami. Il ne s'agit pas d'une convention née de la rencontre d'une offre et d'une acceptation produisant des effets de droit. Nous sommes en présence le plus souvent, d'un procédé automatique d'exécution d'un contrat cadre plus vaste et/ou préexistant. Par exemple, une assurance retard dans laquelle l'indemnisation serait déclenchée par le chaînage avec le logiciel du transporteur qui enregistre les heures d'arrivée ; ce système de paiement automatisé constituerait un *smart contract* ; de même que le paiement par un régime de base en assurance maladie déclencherait automatiquement le paiement du complément. En outre, l'IA peut aider à la détection des fraudes.

A. – IA et souscription du contrat d'assurance

La première étape pour un assureur consiste à l'identification de son souscripteur (celui qui conclue le contrat) et de son assuré (celui sur qui pèse le risque). L'IA permet déjà de créer des *chatbots* qui orientent le choix du souscripteur en ligne ou par téléphone[15]. Le choix du bon contrat et la réalisation du devoir de conseil par une telle méthode permettent de tracer les échanges et de les enregistrer dans un secteur où l'ACPR est très vigilante.

De surcroît, pour mieux connaître le souscripteur et lui permettre aussi de fournir des informations plus rapidement, il serait possible que ce dernier dispose d'un « jeton » toujours identique sur la *blockchain* avec ses informations identifiantes ; elles pourraient être utilisées pour toutes sortes de services de nature financière. En premier lieu, il faut qu'une telle pratique soit en accord avec l'article 6 du règlement (UE) n° 2016/679 du 27 avril 2016,

(14) C. assur., art. L. 511-1 et s. ; ord. n° 2018-361, 16 mai 2018, transposant la directive distribution d'assurance 2016/97 du 20 janv. 2016.

(15) En respectant les prescriptions de l'art. L. 112-2-1 du code des assurances.

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 entré en vigueur le 25 mai 2018 (ci-après RGDP).

En outre, en matière de garantie IARD portant sur de l'assurance de choses (vol, incendie, dégât des eaux…), si l'assureur veut pouvoir opposer à son assuré ses déclarations préalables pour lui imputer ensuite une mauvaise ou une fausse déclaration, il doit le faire par un questionnaire et non par une simple affirmation préétablie[16]. Les réponses recueillies par le *chatbot* et le « jeton » comportant des informations sur l'assuré, que nous avons évoqué dans la technologie *blockchain*, pourraient être intéressants, mais l'assureur devra continuer de poser systématiquement des questions s'il souhaite des informations plus précises ou renouvelées sur le risque à assurer.

> *Si l'IA est un outil prometteur, elle doit aussi pour l'assureur consister en un nouvel objet à assurer.*

Il est également évoqué, grâce au recueil d'informations par une IA parcourant les données disponibles sur le réseau Internet et à la technologie *blockchain*, la possibilité de mesurer la fiabilité des informations sur un assuré. Cependant, une fois encore la limite de l'usage de toutes donnée quelle que soit sa source réside dans la conformité du traitement des données au RGDP.

Enfin, en matière de conclusion du contrat, il est évoqué les contrats collaboratifs en assurance qui utiliseraient le P2P (*peer to peer*). Cette technique pourrait servir entre assureurs, voire, par l'usage de la DAO (*Decentralized Autonomous Organization*), entre individus non assureurs. Sur ce dernier point toutefois, rappelons qu'il n'est pas possible de développer une activité d'assurance sans agrément en France ou au sein de l'Union européenne[17]. Ce que l'on peut imaginer, c'est que le développement de ces technologies facilite l'entrée de nouveaux acteurs sur les garanties non obligatoires en assurance exploitation et, pour l'essentiel, en complémentaire santé. Ces nouvelles technologies sont également porteuses d'évolution en matière de demande de prestations et de déclaration de sinistre.

B. – IA et gestion des prestations

L'article L. 113-2, 4° du code des assurances impose à l'assuré de déclarer son sinistre. Cette déclaration consiste à porter à la connaissance de l'assureur un fait juridique, ce dernier ne peut donc imposer aucune forme spécifique[18]. L'IA peut donc se déployer librement dans la gestion de sinistre et le règlement des prestations prévues par le contrat.

En premier lieu, le *smart contract*, outil d'exécution du contrat cadre d'assurance, peut devenir le support du déclenchement du remboursement automatique de prestations qui sont commandées par la mise en œuvre d'un régime de base en santé. Cet outil peut également être utilisé pour le paiement de dommages quand des logiciels associés à des capteurs transmettent des informations livrées par un objet connecté. En assurance auto des professionnels de santé, un dépannage ou une mise à disposition d'un véhicule de prêt est tout à fait imaginable.

En assurance vie-décès, la mise en place d'un *smart contract* n'est pas, en revanche, d'emblée convaincante pour verser le capital ou la rente au bénéficiaire, car il convient de bien identifier ce dernier avant de procéder au versement de la prestation. Tout au plus, cela permettrait-il à l'assureur vie de déclencher une alerte avec une obligation de recherche du bénéficiaire.

Par ailleurs, l'IA permet de créer de puissants outils contre la fraude en détectant les anomalies dans les déclarations de sinistres grâce au rapprochement de données propres à l'assuré et de données plus générales collectées grâce au *Big Data*. Par exemple, des informations recueillies par l'assureur sur un réseau social dédié aux carrières professionnelles pourraient être intéressantes comme élément de fait pour prouver une éventuelle fraude de l'assuré ; toutefois la collecte de la preuve doit être loyale[19] et, de nouveau, la collecte des données identifiantes doit être conforme au RGDP.

Si l'IA est un outil prometteur, elle doit aussi pour l'assureur consister en un nouvel objet à assurer.

II. – Assurance et responsabilité du fait d'une IA

Il existe d'ores et déjà en droit une réponse si un dommage était provoqué par le fonctionnement d'une IA ou d'un robot. En effet, un juge qui serait saisi de la réparation d'un dommage du fait d'une IA ou d'un robot serait obligé de statuer sur la demande d'indemnisation en appliquant le droit positif.

On peut alors prendre deux exemples qui pourraient illustrer les solutions applicables en cas de dommage : le *chatbot* intelligent utilisé par un assureur, qui conduirait systématiquement à délivrer un conseil erroné à un sous-

(16) Cass. ch. mixte, 7 févr. 2014, n° 12-85.107, Bull. ch. mixte, n° 1.

(17) C. assur., art. L. 310-1.

(18) Cass. civ. 4 juin 1945, RGAT 1945, p. 151, note A. Besson.

(19) Cass. ass. plén., 7 janv. 2011, n° 09-14.316 et 09-14.667, Bull. Ass. Plén. n° 1.

cripteur ou assuré. Sur quel fondement la responsabilité de l'assureur serait-elle engagée ? De manière plus prospective, un petit robot utilisé dans une clinique, un hôpital ou un EHPAD qui causerait un dommage à un visiteur ; qui en serait tenu pour responsable ?

Le raisonnement par analogie et le mécanisme de responsabilité du fait d'une chose suffisent d'ores et déjà pour appréhender tout dommage provoqué par une chose.

En effet, il convient de rappeler qu'au 19e siècle, il avait été possible d'accompagner l'apparition du machinisme qui provoqua de nombreux accidents du travail en raisonnant à partir de l'ancien article 1385 du code civil. Ce texte prévoyait une responsabilité sans faute du gardien de l'animal qui cause un dommage. La machine ayant remplacé l'animal, il convenait d'appliquer, par analogie, un régime identique aux dommages provoqués par les machines utilisées dans l'industrie ou l'agriculture et plus tard aux véhicules à moteur. Aussi par les arrêts Teffaine de 1896 et Jeand'heur de 1930, la Cour de cassation consacrait-elle un principe général de responsabilité du fait des choses qui rend le gardien de la chose à l'origine du dommage responsable sans faute. Le propriétaire de la chose est présumé le gardien. Plus récemment, il a été adopté un régime de responsabilité du fait des produits défectueux[20] afin de canaliser la responsabilité du dommage causé par le défaut d'un produit vers son fabricant.

Si l'on reprend nos deux cas pratiques : le dysfonctionnement du *chatbot* de l'assureur et le dommage provoqué par le petit robot de l'établissement de santé, il convient d'opérer une distinction entre la situation dans laquelle il y a eu contrôle par l'assureur sur le *chatbot* apprenant (IA) et le robot par l'établissement de santé ou pas[21].

Nous allons d'abord partir de l'hypothèse que le *chatbot* et le robot ont été paramétrés ou commandés par l'assureur ou l'établissement de santé. Ces derniers ont donc eu un pouvoir de contrôle et de direction sur le *chatbot* et le robot. L'assureur et l'établissement de santé se verraient reconnaître la qualité de gardien au moment du dommage et seraient donc tenus pour responsables à l'égard de la victime. Pour le souscripteur qui aurait été mal conseillé par le *chatbot* et le visiteur de l'établissement de santé qui aurait été blessé, la responsabilité du gardien sera fondée sur l'article 1242, alinéa 1er du code civil, qui constitue la base textuelle de la responsabilité du fait des choses.

En revanche, si nous sommes en présence d'une IA forte, ou bien que le dommage ne provient absolument pas du paramétrage par l'assureur ou d'une instruction donnée par l'établissement de santé mais de la conception même de l'IA ou du robot, c'est alors une responsabilité du fabricant qui sera recherchée sur le fondement des articles 1245 et suivants du code civil[22].

On peut étendre la méthode qui consiste à partir du dommage subi par la victime pour remonter au responsable à la situation du véhicule autonome qui provoquerait un dommage. Ce serait alors le régime spécial d'indemnisation des accidents de la circulation instauré par la loi du 5 juillet 1985 qui s'appliquerait ; l'assureur du propriétaire du véhicule assuré serait tenu d'indemniser la victime de l'accident. Cela n'exclut pas ensuite un recours contre le fabricant.

En droit positif, il n'est donc, pour le moment, absolument pas nécessaire de créer une personnalité juridique du robot ou de l'IA[23] afin de faciliter l'indemnisation d'une éventuelle victime. Bien au contraire, la création d'une telle personnalité supposerait d'apporter un actif au patrimoine de cet IA ou de ce robot afin de contracter une couverture d'assurance ou bien de créer une responsabilité du fait d'autrui qui pèserait sur celui qui peut lui donner des instructions. Ces détours sont bien utiles pour le moment. Néanmoins, une adaptation de la directive sur la responsabilité du fait des produits défectueux afin de tenir compte des spécificités de l'IA pourrait s'avérer pertinente. ■

(20) Dir. CE Cons., 25 juill. 1985 ; transposée à C. civ., art. 1245 et s.

(21) G. Courtois, Robot et responsabilité, *in* Les Robots Objets scientifiques, préc., p. 129 et s.

(22) Textes de transposition de la directive sur la responsabilité du fait des produits défectueux du 25 juillet 1985.

(23) *Contra* A. Bensoussan, Essai sur le droit des robots, *in* Les Robots Objets scientifiques, préc., p. 231 et s.

RLDA 6783

Les données publiques au cœur de l'IA et au service de la ville intelligente

Gaïa WITZ
Avocat associé, De Gaulle Fleurance & Associés

Jean-Sébastien MARIEZ
Avocat associé, De Gaulle Fleurance & Associés

Alors que la directive sur l'ouverture des données et les informations du service public vient d'être révisée, Me Witz et Me Mariez proposent un rapide panorama des dispositifs législatifs qui, de la loi pour une République numérique au projet de loi d'orientation des mobilités, ouvrent la donnée publique pour encourager l'émergence de la ville intelligente ; sans manquer de relever les zones de frottement qui ne manquent pas d'apparaître, d'une part, vis-à-vis des droits des opérateurs privés et, d'autre part, des réticences de l'administration elle-même à mettre en œuvre le cadre légal de manière effective.

Depuis quelques années, l'intelligence artificielle pénètre notre quotidien et modifie nos habitudes de vie, que ce soit notre façon de se déplacer, de consommer ou encore de travailler. Ces nouvelles expériences, à travers de multiples applications, dessinent la « *smart city* », la ville intelligente de demain. Parce que la ville est par essence un espace public, la ville intelligente se nourrit de données publiques.

La *smart city* prend des formes très variées : mobilité durable, mobiliers urbains, éco-quartiers et bâtiments intelligents, ou encore équipements connectés de télémesure ou de télé-relève dans les services publics de la distribution d'eau et d'électricité. La ville intelligente passe donc par la dématérialisation et l'évolution des services publics pour s'adapter aux habitudes numériques de consommation et de vie des usagers.

Les collectivités locales françaises sont donc directement concernées par cette transformation : tout d'abord, parce qu'elles sont à l'origine de données publiques qui nourrissent les services tant publics que privés offerts aux usagers ; ensuite, parce que dans l'organisation de leurs activités, elles consomment des données et des applications numériques. De l'autre côté de la chaîne de valeur, on trouve les entreprises qui proposent des services numériques destinés aux activités de service public, et qui vivent, au moins en partie, de commandes publiques.

Nous verrons tout d'abord que le partage et la diffusion en continu des données publiques associées à un encouragement des collectivités à recourir à l'innovation dans l'organisation de leurs activités contribuent à l'évolution numérique des services offerts dans la cité. Cette expansion de la *smart city* n'est toutefois pas sans heurt car la ligne de partage entre données publiques et données privées est parfois difficile à tracer : les opérateurs privés de service public veillent au secret de leurs affaires comme l'administration veille au secret de fabrication de certaines de ses décisions, notamment lorsqu'elles ont trait à des situations personnelles et individuelles.

I. – Le partage et la diffusion des données publiques pour servir la ville intelligente

Très tôt, le législateur français a pris conscience de l'importance et de la valeur des données récoltées, traitées, ou encore produites par les acteurs du secteur public, notamment par l'édition de notes, de documents ou de rapports, et il a donc adopté un cadre permettant leur réutilisation par le secteur privé tout en les protégeant. Avec l'expansion des applications numériques dans l'espace public, il est apparu que les données numériques de l'administration sont, de la même manière que l'étaient autrefois les documents papiers, des données d'importance et d'une grande valeur pour l'économie. Quant à l'administration, elle peut elle aussi être consommatrice d'innovation et ainsi participer à la transformation numérique de la cité.

A. – Le régime des données publiques, carburant de la smart city

La directive dite « ISP »[1] a,, la première, constaté que le secteur public produit et diffuse un grand nombre d'informations qui sont « *une matière première importante pour les produits et les services de contenu numérique* ». Sa version refondue le 20 juin dernier[2], souligne, quant à elle que « *les informations du secteur public constituent une source extraordinaire de données qui peuvent contribuer à améliorer le marché intérieur* ».

Au plan national, la loi pour une République numérique[3] a favorisé l'essor de l'*open data* et l'utilisation des données numériques en élargissant la liste des éléments considérés comme documents administratifs communicables aux « codes sources » : « *Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions, codes sources et décisions* »[4].

Quelle que soit leur forme, un grand nombre des données traitées par l'administration est donc couvert par cette énumération et à ce titre, communicable à toute personne qui en fait la demande.

Plus encore, le principe renforcé par la loi pour une République numérique est désormais celui de la diffusion spontanée par l'administration de certaines de ces données[5]. La loi prévoit même que cette diffusion, lorsqu'elle est effectuée sous forme électronique, doit être réalisée « *dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé* »[6].

Le caractère très large de la liste des éléments qui constituent des documents administratifs et le principe de leur diffusion spontanée par l'administration ont une conséquence directe puisqu'ils ont pour corollaire le principe de la libre réutilisation des informations publiques contenues dans les documents administratifs qui, en conséquence, est lui aussi étendu à d'innombrables données du secteur public.

La réutilisation des informations publiques figurant dans les documents communiqués ou publiés par l'administration est en effet inscrite comme un principe à l'article L. 321-1 du code des relations entre le public et l'administration et il s'applique quelle que soit la nature du demandeur et pour toute finalité, même autre que celle de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus. Bien entendu, ce droit à la réutilisation est encadré par un certain nombre de règles, et la nécessité d'une contractualisation permet notamment de traiter les éventuels droits de propriété intellectuelle détenus par des tiers.

Aujourd'hui, on ne peut que constater l'appétence de certains opérateurs économiques pour certains types de données publiques, ces opérateurs ayant les compétences et les ressources pour valoriser ces données, en développant des applications, des produits et des services numériques qui construisent la ville intelligente. Les données publiques sont donc créatrices de valeur, de projets d'entreprises et d'emplois.

Parce qu'elles constituent une source importante pour la réutilisation, certaines des données traitées par l'administration sont même considérées comme des « super » données dont la mise à disposition a été érigée en mission de service public que la mission *Etalab* a pour rôle de piloter.

Les données de référence sont celles (i) qui constituent une référence commune pour nommer ou identifier des produits, des services, des territoires ou des personnes, (ii) qui sont réutilisées fréquemment par des personnes publiques ou privées autres que l'administration qui les détient, et (iii) dont la réutilisation nécessite qu'elles soient mises à disposition avec un niveau élevé de qualité[7]. Ces données sont entre autres le répertoire des entreprises et de leurs établissements produit par l'INSEE[8], le référentiel à grande échelle, produit par l'IGN[9], ou encore le plan cadastral informatisé, produit par la direction générale des finances publiques.

B. – Les encouragements des collectivités à recourir à l'innovation

La LOM. Outre l'extension du champ de l'*open data* opéré par la loi pour une République numérique, d'autres mesures adoptées par différents textes participent de l'expansion de la *smart city* : sans pouvoir tous les recenser, il faut citer le projet de loi d'orientation des mobilités qui tente d'inscrire des solutions de la *smart city* dans l'ordonnancement juridique en tentant de répondre au défi de la mobilité et ainsi de réduire la fracture entre les territoires. En faisant évoluer l'organisation du service public des transports (notamment en renforçant le couple intercommunalité-région), et en érigeant l'« organisation des mobilités » comme une compétence à part entière, le projet de loi encourage les collectivités et leur donne les moyens d'intervenir de façon plus active encore dans ce secteur d'activités. En l'état du projet, plusieurs dispositions sont consacrées au traitement des données de la mobilité. Les régions et métropoles se voient

(1) Dir. UE et PE Cons. n° 2003/98/CE, 17 nov. 2003, concernant la réutilisation des informations du secteur public.

(2) Dir. UE PE Cons. n° 2019/1024, 20 juin 2019, concernant les données ouvertes et la réutilisation des informations du secteur public (refonte).

(3) L. n° 2016-1321, 7 oct. 2016 pour une République numérique.

(4) Article L. 300-2 du code des relations entre le public et l'administration.

(5) Article L. 311-1 du code des relations entre le public et l'administration.

(6) Article L. 300-4 du code des relations entre le public et l'administration.

(7) Article L. 321-4 du code des relations entre le public et l'administration.

(8) Institut national de la statistique et des études économiques.

(9) Institut national de l'information géographique et forestière.

confier le rôle d'animation de la démarche d'ouverture des données et de transmission des données vers l'interface qui recensera les données de mobilité tandis que l'ARAFER sera chargée de la bonne mise en œuvre de l'accès aux données.

Le partenariat d'innovation. Il faut aussi souligner que le champ de la commande publique a récemment intégré des nouvelles solutions pour faciliter les achats par les collectivités publiques de services et de produits innovants : citons à ce titre le partenariat d'innovation qui a permis d'inclure à la fois une période de « recherche et développement » et l'achat de produits ou services[10].

Flexibilité de la commande publique. Citons encore le décret n° 2018-1225 du 24 décembre 2018 portant diverses mesures relatives aux contrats de la commande publique qui permet aux acheteurs publics pendant trois ans, de conclure des contrats de travaux, fournitures ou services innovants sans publicité et sans mise en concurrence lorsque la valeur du marché est inférieure à 100 000 euros HT.

Ces mesures favorisent l'achat par les collectivités de produits et services innovants si ceux-ci sont susceptibles d'évolution et de développement, et elles participent même, par leurs résultats ou leurs contributions, à faire évoluer le développement de certaines applications pour les rendre encore plus adaptées aux besoins des citoyens et usagers des services publics.

Toutes ces mesures législatives et réglementaires participent bien entendu à l'ouverture des données sans laquelle la *smart-city* ne sera pas possible, mais l'ouverture n'est pas sans rencontrer quelques freins.

II. – La ligne de partage entre données publiques et données privées : un frein au développement de la ville intelligente

La *smart city*, on l'a vu, se fera grâce notamment aux données publiques, mais aussi avec le concours des opérateurs économiques privés qui sont aujourd'hui les principaux initiateurs du développement d'applications facilitant les échanges de produits et de services par la voie numérique. Ce faisant, ces acteurs, lorsqu'ils sont opérateurs de service public, créent eux aussi des données. Il faut alors distinguer celles qui relèvent effectivement de la sphère publique et celle qui relève du savoir-faire de l'entreprise privée. De son côté, l'administration veille, elle aussi, à ne pas diffuser des données notamment dans le cas où des situations personnelles et individuelles sont évoquées. En pratique, on constate donc une zone de frottement entre les données publiques et celles que certains tentent de protéger en considérant qu'elles sont, en quelque sorte, des données « privées ».

A. – Les données des concessions de service public : la frontière entre données publiques et savoir-faire du concessionnaire

L'*open data* s'étend à l'ensemble des services publics de la cité, de sorte que les données publiques produites à l'occasion des activités de service public ne sont pas toutes produites par des opérateurs publics, mais elles le sont aussi par des opérateurs privés chargés de missions de service public (par exemple, les entreprises privées en charge des réseaux de transport urbains, de distribution d'eau, ou d'exploitation d'infrastructures sportives).

En effet, le code de la commande publique[11] introduit un principe selon lequel, lorsqu'un service public est concédé, le concessionnaire doit fournir, au concédant, sous format électronique et dans un standard « *ouvert librement réutilisable et exploitable par un système de traitement automatisé* » les données ainsi que les bases de données qu'il collecte ou produit à l'occasion de l'exploitation du service public. Ainsi, nombre d'informations traitées par des opérateurs privés chargés de mission de service public peuvent elles aussi devenir des informations publiques parce que, par différents biais, elles remontent à l'administration.

En introduisant cette disposition dans le champ très large des concessions, le législateur a couvert de nombreux secteurs d'activité qui font l'objet des traditionnelles délégations de service public. Il fait de ces données qui sont indispensables à la concession et qui deviennent, par là-même, des données publiques, une sorte de nouvelle catégorie des biens de retour[12] qui appartiennent *ab initio* à l'autorité concédante. Ces données publiques sont dès lors diffusables et communicables à tout tiers en faisant la demande y compris le concurrent potentiel du délégataire de service public.

Dans différents secteurs d'activité, la loi a précisé ce que sont les données de la concession. À titre d'exemple, le code des transports[13] fournit la liste des données des services réguliers de transport public de personnes et des services de mobilité qui sont diffusées, par voie électronique, au public et aux autres exploitants, dans un format ouvert

(10) C'est ce type de marché qui semble avoir été retenu par la Communauté de Communes Pays Haut Val d'Alzette pour piloter un projet de « smart city » en Lorraine : associée aux entreprises Capgemini, Bouyges Energies et Services et SUEZ, elle a lancé une politique de transformation du territoire qui s'appuie sur des technologies digitales avancées telles que les objets connectés, l'intelligence artificielle et les services numériques pour offrir de nouveaux services innovants pour l'ensemble des acteurs, usagers, entreprises et partenaires de la collectivité.

(11) Article L. 3131-2 du code de la commande publique reprenant une disposition que la loi pour une république numérique avait introduite à l'article 17 de l'ordonnance n° 2016-65 du 29 janvier 2016 relative aux concessions.

(12) Rappelons ici que les biens de retour sont traditionnellement considérés comme ceux mis à disposition par l'autorité délégante au délégataire ou financés par ce dernier revenant obligatoirement à l'autorité délégante lorsque le contrat de délégation de service public prend fin (v. not. CE, 21 déc. 2012, n° 34.2788).

(13) C. transp., art. L. 1115-1.

destiné à permettre leur réutilisation libre, immédiate et gratuite. On y trouve, par exemple, les données relatives aux arrêts, aux tarifs publics, aux horaires planifiés et en temps réel, à l'accessibilité aux personnes handicapées, à la disponibilité des services, etc.

Sur la base de ces données, dont tout tiers peut demander la communication et la réutilisation, des applications sont ainsi lancées sur le marché par des opérateurs économiques qui se nourrissent de données publiques générées par des opérateurs privés.

Ceci donne lieu à quelques réserves de la part des opérateurs de services pour lesquels l'enjeu de la protection de leur savoir-faire est crucial. Pour certains, la production des données par le service est le fruit d'un réel savoir-faire de l'entreprise, lequel ne peut pas être bradé ni partagé avec tous ses concurrents. L'*open data* se heurte ici au principe du secret des affaires.

B. – Les données publiques confrontées au secret des délibérations de l'administration

Mais la protection de leurs données n'est pas l'apanage des seuls opérateurs privés : l'administration, elle aussi, ne tient pas à partager l'intégralité de ses données. Elle fait parfois de la résistance dans la communication de celles-ci.

Transparence des algorithmes. Ainsi, s'agissant des décisions individuelles créatrices de droits qui peuvent désormais être prises au moyen d'un algorithme, l'administration a été contrainte de divulguer les codes sources du traitement algorithmique, après un contentieux mené par l'union des étudiants de France devant le TA de la Guadeloupe, alors que l'université initialement saisie refusait de communiquer les procédés algorithmiques[14]. L'université des Antilles se défendait en soutenant que ce sont les commissions composées en son sein qui avaient finalement apprécié les vœux exprimés par les candidats à l'entrée à l'université et que les traitements algorithmiques sur lesquels elle s'étaient appuyées ne s'étaient pas substitués à leur appréciation. Les juges du fond ont néanmoins considéré que les règles définissant le traitement algorithmique ainsi que les principales caractéristiques de sa mise en œuvre devaient être communiqués aux intéressés en faisant la demande.

L'université avait également invoqué, en défense, le secret des délibérations, principe auquel, prétendait-elle, la divulgation des règles du traitement algorithmique pouvait porter atteinte. Là encore, les juges du fond n'ont pas retenu cette argumentation et ont retenu que la communication ne devait porter que sur la nature des critères pris en compte pour l'examen des candidatures, leur pondération et leur hiérarchisation, et non sur l'appréciation portée par la commission sur les mérites de chacune des candidatures. De sorte que cette communication n'entravait pas le principe du secret des délibérations.

Cette décision est conforme au code des relations entre le public et l'administration sur l'usage des traitements algorithmiques par l'administration dans la prise de décisions à caractère individuel. Dès lors qu'une telle décision est prise, à l'égard d'un administré, au moyen d'un traitement algorithmique, une mention explicite doit en informer l'intéressé. Les principales caractéristiques de sa mise en œuvre doivent lui être communiquées s'il en fait la demande.

Le Conseil constitutionnel, dans une décision du 12 juin 2018, a ajouté une condition à l'utilisation de ces traitements algorithmiques dans la prise de décisions individuelles en indiquant expressément que la décision administrative individuelle prise sur le fondement d'un algorithme doit pouvoir faire l'objet de recours administratifs[15].

Accès aux données. Dans le secteur juridique aussi l'attente est grande : plusieurs opérateurs se sont lancés dans les services dits de « *legal tech* », avec pour ambition de rendre le droit et la justice plus accessibles aux professionnels juridiques, comme à un public moins averti. La loi de programmation 2018-2022 et de réforme pour la justice[16] a inscrit des dispositions qui doivent permettre à tous l'accès aux décisions de justice au sein du code de l'organisation judiciaire[17] comme au sein du code de justice administrative[18]. Dans le même temps et face aux nombreuses critiques soulevées par ces textes, la loi a multiplié les garde-fous dans le droit à la réutilisation de ce type d'informations publiques : l'occultation de tout élément permettant d'identifier les parties, les tiers, les magistrats et les membres du greffe dont la divulgation serait de nature à porter atteinte à la sécurité ou au respect de la vie privée de ces personnes ou de leur entourage, ou encore l'interdiction de réutilisation des données d'identité des magistrats et des membres du greffe ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées.

L'administration judiciaire qui avait opportunément développé la théorie des documents juridictionnels, par exception aux documents administratifs, pour en soustraire la communication aux personnes en faisant la demande, a réussi une fois encore à restreindre le champ de la communication de ses décisions, sous couvert de la préservation des droits individuels. Les créateurs de services dans le domaine attendent impatiemment les décrets d'application qui permettront de fixer un cadre clair à leur activité… ■

(14) V. TA Guadeloupe, 4 févr. 2019, n° 180.1094, Union nationale des étudiants de France (UNEF) c/ Président de l'université des Antilles.

(15) V. Cons. const., 12 juin 2018, déc. n° 2018-765 DC, Loi relative à la protection des données personnelles.

(16) L. n° 2019-222, 23 mars 2019, de programmation 2018-2022 et de réforme pour la justice.

(17) C. org. jud. art. L. 111-13.

(18) C. just. adm., art. L. 10.

RLDA 6784

Intelligence artificielle et droit de la concurrence

Thierry TITONE
Avocat Associé, De Gaulle Fleurance & Associés

Roxane CHANALET-QUERCY
Avocate, De Gaulle Fleurance & Associés

L'intelligence artificielle, utilisée par les entreprises pour mener des veilles concurrentielles et définir des offres, est une innovation saluée, par principe, par les autorités de concurrence qui y voient un outil de développement de la concurrence. Ces dernières mettent toutefois en garde sur les dérives que l'IA peut engendrer, notamment par des échanges d'informations sur les prix ou des abus de position dominante par la captation et l'exploitation de données.

L'intelligence artificielle (« IA »)(1), couplée aux accès à la *Big Data*, tient déjà pour bon nombre d'entreprises une place stratégique et opérationnelle. Qu'il s'agisse de maintenance industrielle, de services bancaires, de santé ou de distribution de produits, les fournisseurs, distributeurs mais aussi les clients peuvent avoir recours, en pleine conscience ou non, à des outils d'IA pour définir une offre, une action à mener, ou déterminer un prix.

Il est ainsi désormais possible de connaître, en temps réel, le comportement commercial de clients ou de concurrents et d'adapter très rapidement son offre.

De prime abord, l'IA est pro-concurrentielle : l'algorithme de prix va, par exemple, systématiquement ajuster le prix à l'offre et à la demande, assurer aux parties en présence le prix « le plus juste ». L'algorithme de veille concurrentielle va permettre aux entreprises d'avoir une meilleure connaissance du marché, et ainsi d'ajuster leurs offres à celles de leurs concurrents, ce qui peut là encore avoir pour effet d'approcher du « prix parfait ».

Ce caractère pro-concurrentiel de l'IA et de l'exploitation des données a été démontré par les travaux de l'Organisation de coopération et de développement économiques (OCDE) en 2017(2) : grâce à l'IA, les entreprises ont une meilleure connaissance des stocks existants ou des nécessités d'améliorer certains produits, mais aussi de toute la chaîne d'approvisionnement, ce qui aboutit à des innovations permettant de faire baisser les coûts de production ou de livraison.

En aval, l'IA assure aux clients une plus grande accessibilité aux offres, en comparant instantanément l'intégralité ou presque du catalogue produits disponible sur internet(3). Les entreprises, pour capter cette clientèle, ne doivent donc plus miser sur le seul facteur prix, mais sur l'innovation, le caractère durable, ou tout autre élément distinctif parmi la masse d'informations traitées pour le consommateur.

La Commissaire à la concurrence, Margrethe Vestager, a eu l'occasion de souligner que les algorithmes peuvent avoir des effets pro-concurrentiels en aidant les consommateurs à profiter des meilleurs prix, selon les réglages proposés par les entreprises. Elle a ainsi rappelé que « *les autorités de concurrence ne doivent pas systématiquement être suspicieuses à l'encontre*

(1) « *Systèmes qui font preuve d'un comportement intelligent en analysant leur environnement et en prenant des mesures avec un certain degré d'autonomie pour atteindre des objectifs spécifiques* » (Comm. UE, communication, L'intelligence artificielle pour l'Europe, 25 avr. 2018, COM(2018) 237 final ; cité par L.Grynbaum, IA et Assurance, cette RLDA.

(2) OCDE, *Algorithms and Collusion : Competition Policy in the Digital Age,* 14 sept. 2017.

(3) Ces comparaisons instantanées font par ailleurs l'objet de régulations européennes, la Commission européenne souhaitant s'assurer que les géants de l'e-commerce assurent la transparence de leurs algorithmes de comparaison, pour éviter une mise en avant anti-concurrentielle de leurs propres produits ou partenaires (Comm. UE, Proposition de règlement, 26 avr. 2018, promouvant l'équité et la transparence pour les entreprises utilisatrices des services d'intermédiation en ligne, « *Platform To Business (« P2B »)* ».

de toutes les entreprises qui utilisent des systèmes automatisés de fixation des prix[4] ».

L'IA est particulièrement utilisée dans la mise en place de veilles concurrentielles automatisées, permettant aux entreprises d'avoir une vision globale et précise de la concurrence, et ainsi de se positionner vis-à-vis des concurrents, notamment par les prix et les services proposés.

Les veilles concurrentielles ne sont pas nées avec l'IA, et l'Autorité de la concurrence a eu l'occasion de rappeler les critères de veilles licites liées au caractère public et accessible des informations. L'Autorité rappelle qu'il « *appartient à chaque concurrent de mettre en œuvre les moyens qu'il estime nécessaires pour recueillir, hors concertation ou échange d'informations, les éléments d'environnement propres à lui permettre de déterminer en toute indépendance ses prix* [5]».

Dès lors, si les autorités de concurrence admettent que « *la transparence du marché est généralement considérée comme bénéfique aux consommateurs, au moins en théorie, lorsqu'ils accèdent aux mêmes informations que les entreprises* [6]», la transparence peut également avoir pour effet de réduire la concurrence entre les entreprises, même en l'absence d'échange d'informations entre elles[7].

Dans l'affaire de la distribution de carburants sur autoroutes, l'Autorité de la concurrence a sanctionné les entreprises concernées non pas car elles avaient, de façon autonome et parallèle, mis en place une veille concurrentielle, mais parce que des salariés d'entreprises concurrentes en charge des veilles, préféraient communiquer ensemble par téléphone pour mettre en œuvre la veille, sans se déplacer chez les concurrents[8].

La confrontation IA et droit de la concurrence implique donc de s'assurer, et peut-être de démontrer, que les algorithmes programmés pour comparer de façon systématique les prix de concurrents, voire de s'y adapter, ne mettent pas en œuvre une pratique réciproque de surveillance qui pourrait constituer une entente anticoncurrentielle.

La Commission européenne travaille notamment sur la place des IA dans le e-commerce, et reconnaît que les données « *peuvent être une ressource précieuse* » et que « *l'analyse de grands volumes de données peut apporter des bénéfices substantiels sous la forme de produits et de services de meilleure qualité* » [9]. Cependant, la Commission constate également que « *l'importance accrue des données fait état de possibles problèmes de concurrence liés à la collecte et à l'utilisation des données* », en citant notamment les risques d'échanges de données sensibles[10].

L'objectif de cet article n'est pas de tirer la sonnette d'alarme. Cela serait hors de propos. Toutefois, il nous semble utile d'identifier des enjeux actuels soulevés par l'IA au regard du droit de la concurrence notamment concernant l'accord de volontés en matière d'entente, les modalités de preuve ou le renforcement du pouvoir de marché d'acteurs dominants dans le secteur de l'internet et du traitement de données.

I. – IA et ententes

A. – L'IA comme nouvel outil collusif ?

Le risque d'entente anticoncurrentielle résulte d'un accord de volonté entre entreprises, ayant un objet ou un effet anticoncurrentiel[11]. Cet accord de volonté peut prendre une forme expresse ou tacite[12].

Avant que les outils d'IA ne soient particulièrement développés et autonomes quant à certaines de leurs actions ou apprentissages (v. ci-dessous II-B), les autorités de concurrence ont sanctionné des ententes créées par accords de volonté d'entreprises, pour lesquelles l'IA était l'outil, au même titre qu'un téléphone portable ou qu'une

(4) M. Vestager, Algorithms and competition, *Bunderskartellamt*, 18e conférence sur la concurrence, Berlin, 16 mars 2017. Ce même constat est réalisé par l'Autorité de la concurrence et le *Bunderskartellamt*, qui ont annoncé dans un communiqué de presse publié à l'occasion de l'annonce d'une étude conjointe lancée pour mieux comprendre les algorithmes que « *les algorithmes sont sources de nombreuses opportunités pour l'économie, par exemple en favorisant les services innovants, en réduisant les coûts de recherche et en facilitant l'optimisation des stocks* ».

(5) Aut. conc., déc. n° 03-D-17, 31 mars 2003, relative à des pratiques sur le marché de la distribution des carburants sur autoroutes, cons. 101.

(6) Aut. conc., et *Bunderskartellamt*, rapp., 10 mai 2016, Droit de la concurrence et données.

(7) À l'inverse, si les concurrents ne peuvent pas réunir de façon aisée ou fréquente l'information sur les pratiques des concurrents, alors l'Autorité de la concurrence reconnait qu' « *une certaine concurrence par les prix sera possible car chaque [entreprise] pourra espérer qu'une baisse de ses prix dans [son magasin] ne sera pas immédiatement détectée par ses concurrents* » (Aut. conc., déc. n° 03-D-17, précit., cons. 104).

(8) Aut. conc., déc. n° 03-D-17, 31 mars 2003, cons. 102 : « *Loin de se contenter de mettre en oeuvre les moyens qu'elle estime nécessaires au recueil d'informations utiles pour la détermination de ses propres prix, [l'entreprise] accepte que ses employés, aident ses concurrents à établir leurs prix en leur transmettant des informations sur les prix pratiqués dans ses propres stations. Dans un tel cas, la pratique peut avoir pour objet ou pour effet de restreindre le jeu normal de la concurrence par les prix entre les compagnies pétrolières* ».

(9) Comm. EU, rapp. final, 10 mai 2017, relatif à l'enquête sectorielle sur le commerce électronique, pts. 55 et 56.

(10) *Ibid*.

(11) TFUE, art. 101 ; C. com., art. L. 420-1.

(12) La passivité des destinataires de l'invitation à une concordance de volonté peut également être condamné pour entente, v. TPI, 26 oct. 2000, Bayer, aff. T-41/96. Même constat de la Cour de justice de l'Union européenne dans une affaire récente, impliquant un « appel à collusion » du fait de logiciels de prix : CJUE, 21 janv. 2016, aff. C-74/14, Eturas, ECLI:EU:C:2016:42.

salle de réunion, pour faciliter les rapprochements entre concurrents. L'affaire *Topkins*[13], révélée par le gendarme de la concurrence américain, en est une bonne démonstration.

Des fabricants de posters muraux, entre 2013 et 2014, ont échangé des informations sur le prix de vente de leurs produits sur Amazon. Après échanges d'information par voie « classique », les membres du cartel ont mis au point un algorithme de prix capable d'effectuer la veille concurrentielle et la police de prix, en ajustant les prix, si un écart était constaté par « l'outil ».

Les algorithmes étaient donc étroitement surveillés par leurs concepteurs, et leur rôle dans l'entente a pu permette d'établir les faits reprochés, au même titre que s'il s'agissait de notes laissées dans un carnet ou d'emails saisis.

> *L'une des difficultés pour les programmeurs d'outils d'IA serait donc d'anticiper la réaction de l'IA vis-à-vis de l'IA concurrent.*

L'une des difficultés pour les programmeurs d'outils d'IA serait donc d'anticiper la réaction de l'IA vis-à-vis de l'IA concurrent. Selon un exemple récemment cité, il ne sera ainsi pas question d'exiger de l'IA qu'il augmente systématiquement son prix dès qu'il constate un écart avec un prix concurrent sans autre forme d'alerte… au risque de voir le prix augmenter de façon totalement dé-corrélée de l'offre envisagée : le livre *The Making of a Fly* s'est ainsi retrouvé à plus de 20 millions de dollars sur le site de e-commerce Amazon, après que deux algorithmes aient obéis aveuglément à la consigne de leurs programmeurs, qui était de systématiquement assurer un prix plus élevé de 23 % que leur concurrent[14].

Au-delà d'un tel exemple qui illustre surtout une défaillance humaine dans la détermination d'un « ordre » raisonnable pour l'IA, se pose la question du risque de stabilité d'une entente mise en œuvre par le biais d'algorithmes. Si l'IA développe son comportement de façon « raisonnable », la dérive illustrée par cet exemple, sera difficilement détectable du fait notamment d'une programmation humaine « efficace »[15].

Les ententes sont souvent révélées par les demandes de clémence, réalisées lorsqu'une entreprise, pour maîtriser un risque de sanction, décide de dénoncer la pratique aux autorités. L'IA n'aura pas cette crainte, et pourrait continuer à participer à l'entente si par exemple l'équilibre ainsi créé offre le plus de profit à l'entreprise. Une entente *via* des outils d'IA pourrait de ce fait devenir plus stable, et plus durable[16].

Charge reste donc à l'entreprise et aux programmeurs de s'assurer du comportement licite de leur IA, en prenant en compte l'existence et les agissements d'IA concurrentes.

B. – Collusion ou parallélisme de comportement ?

Un autre comportement anticoncurrentiel émerge du fait des IA, et serait plus difficile à déceler pour les autorités de concurrence.

De nombreux algorithmes ont désormais la tâche d'étudier le marché et d'y agir dans un objectif de maximisation du profit de leur « créateur ». Ces « machines autonomes[17] » sont programmées pour s'enrichir tout au long de la vie de l'algorithme. L'IA va apprendre du marché, et s'adapter instantanément à celui-ci.

Plusieurs IA vont se comporter ainsi sur un même marché, et donc apprendre l'une de l'autre, et anticiper les agissements de concurrents sans toutefois jamais perdre leur indépendance puisque, par hypothèse, les IA n'auront pas été programmées pour renoncer à leur autonomie de décision.

Dès lors, au fur et à mesure de leurs actions sur le marché, les prix ou autres critères de différenciation pourraient s'en trouver lissés… Comment alors déterminer, pour une autorité de concurrence, si elle est en présence d'un parallélisme de comportements licite ou d'une collusion illicite *via* l'IA?

Cette situation, qui est déjà largement commentée par la doctrine[18], impliquera des autorités de concurrence qu'elles adaptent leurs modes et moyens d'enquête et de preuve.

Il ne sera, à termes, plus question de découvrir des preuves disséminées par des salariés peu attentifs aux risques qu'ils font prendre à leurs employeurs. Il s'agira de déceler un certain comportement sur le marché, des pratiques collusives, alors que les IA fonctionneraient comme des

(13) *Department of Justice vs Topkins*, 6 avr. 2015, n° CR 15-00201 WHO.

(14) M. Vestager, discours Algorithms and competition, *Bunderskartellamt*, 16 mars 2017.

(15) V. en ce sens, CJUE, 21 janv. 2016, aff. C-74/14, Eturas, ECLI:EU:C:2016:42.

(16) N. Hirst, *When Margrethe Vestager takes antitrust battle to robots*, *Politico*, 28 févr. 2018.

(17) F. Marty, Algorithmes de prix, intelligence artificielle et équilibres collusif, Revue Internationale de Droit Economique, 2017, p. 83-116.

(18) *Ibid* ; *When Margrethe Vestager takes antitrust battle to robots*, Nicholas Hirst, Politico, 28 févr. 2018 ; *Cartels by Robots – Current antitrust law in search of an answer*, Intereulaweast Vol IV (2) 2017, *Faculty of Law of the Charles University*.

« boîtes noires » en principe indépendantes, rendant l'action collusive *via* l'algorithme difficile à retracer[19].

Les enquêteurs seront peut-être amenés à rechercher une « preuve négative »[20], c'est-à-dire effectuer la démonstration que, dans une configuration de marché concurrentielle, le parallélisme de comportements ne pourrait s'expliquer que par une concertation tacite entre les entreprises *via* le déploiement et l'utilisation d'IA[21].

Une autre approche serait la mise en place de contrôles *ex ante* des IA sur les marchés, et une régulation des IA, au même titre que le contrôle des concentrations. Le droit de la concurrence aurait alors vocation à anticiper des effets structurels de l'IA sur certains marchés et tout naturellement sur les marchés de l'internet ou de l'accès aux données.

II. – IA et abus de position dominante

A. – Marché oligopolistique et abus d'exploitation

En matière d'IA et de risques d'abus de position dominante, nous pensons assez naturellement à la capacité de certaines entreprises qui, du fait de leur pouvoir de marché et de leurs accès « facilités » à d'énormes bases de données (les GAFA, notamment), peuvent influencer la structure de marchés existant sous forme d'oligopole[22]… et donc potentiellement d'y commettre des abus d'exploitation.

Les données prennent ici toute leur importance, puisque c'est notamment par l'étude des données que l'IA s'améliore et devient plus performante. Une entreprise maîtrisant un grand nombre de données, la matière première, bénéficiera donc d'une IA performante sur le marché.

À titre d'exemple, la doctrine cite le cas d'IA capables de déterminer le prix d'un produit non plus en fonction du marché, mais en fonction des habitudes du consommateur. L'IA peut donc opérer par différenciation tarifaire et déterminer si tel consommateur, compte tenu de ses revenus, doit payer un produit à « bas prix », et répercuter la marge manquante sur un consommateur identifié comme habitué à payer un prix plus élevé sur internet. En procédant de la sorte, l'entreprise en position dominante s'accapare le surplus de consommateurs qui n'auraient pas nécessairement pu s'offrir le produit au prix de marché[23].

> *De nombreux algorithmes ont désormais la tâche d'étudier le marché et d'y agir dans un objectif de maximisation du profit de leur « créateur ».*

Le prix ne serait donc plus corrélé, dans cet exemple, au marché, aux innovations, ou à la valeur intrinsèque du produit, mais dépendrait, par la mise en œuvre d'IA, des capacités contributives du consommateur et, surtout, du pouvoir de marché du vendeur par sa capacité d'analyse des données par « son » IA.

B. – IA et accès aux données : la théorie des facilités essentielles

Nous identifions enfin un dernier enjeu lié à la capacité d'entreprises disposant d'un fort pouvoir de marché notamment les GAFA, à créer des cercles d'exclusion des néo-entrants, en bloquant l'accès aux bases de données relatives en particulier aux consommateurs.

Cette pratique semble être au centre des préoccupations de la Commission puisque c'est l'accès à ces mêmes données qui permettent aux opérateurs de mieux anticiper les besoins du marché[24].

Cette inquiétude a notamment été soulignée par les autorités, française et allemande, à l'issue de leurs travaux en 2016 : « *lorsque l'accès à un large volume ou à une importante variété de données est un facteur de compétitivité sur le marché, leur collecte peut constituer une barrière à l'entrée si de nouveaux entrants ne sont pas en mesure de collecter ou d'acheter le même type de données, en termes de volume et/ou de variété, que les entreprises déjà en place* »[25] .

(19) OCDE (2017), *Algorithms and Collusion : Competition Policy in the Digital Age*.

(20) Rapport annuel - Étude Thématiques de l'Autorité de la concurrence 2006, p. 79.

(21) « *Dès lors, dans la plupart des cas, l'existence d'une pratique ou d'un accord anticoncurrentiel doit être inférée d'un certain nombre de coïncidences et d'indices qui, considérés ensemble, peuvent constituer, en l'absence d'une autre explication cohérente, la preuve d'une violation des règles de la concurrence* » (CJUE, aff. C-204/00, 7 janv. 2004, Aalborg Portland e.a. c/ Commission, ECLI:EU:C:2004:6, pts 55 à 57.

(22) Sur les trois critères habituellement retenus par la CJUE pour définir une position dominante collective, v. not. TUE, 6 juin 2002, T-342/99, Airtours, ECLI:EU:T:2002:146, cons. 54 et s.

(23) F. Marty, Analyse présentée dans Algorithmes de prix, intelligence artificielle et équilibres collusif, Revue Internationale de Droit Économique, 2017, p. 83-116.

(24) À ce titre, la Commission européenne a ouvert le 16 juillet 2019 une enquête préliminaire contre AMAZON afin de déterminer si l'utilisation par cette dernière de données sensibles provenant de détaillants indépendants qui vendent sur sa place de marché enfreint les règles de concurrence de l'UE, comp., communiqué de presse, 17 juill. 2019.

(25) Aut. de la concurrence et *Bunderskartellamt*, 10 mai 2016, Droit de la concurrence et données.

La « théorie des facilités essentielles », définie dans l'arrêt *Microsoft* du Tribunal[26], implique qu'une entreprise dominante peut être tenue d'ouvrir l'accès à certaines informations, données ou IA, pour permettre à des concurrents d'être présents sur le marché.

Les données sont donc encore au cœur de l'utilisation des IA, puisque, ayant accès aux données, les GAFA peuvent utiliser toutes les capacités des IA et renforcer leurs positions de marché.

Consciente de cet enjeu, la Commission s'est inquiétée des accès aux données post-concentrations, notamment lorsque les GAFA font l'acquisition de plateformes ou d'application à fort potentiels en matières de données. Lors du contrôle de l'opération Apple/Shazam[27], la Commission a été attentive à ce que l'opération n'ait pas pour effet de permettre à Apple de cibler, *via* les données, les clients des concurrents et à sa capacité, *via* les habitudes d'écoute des utilisateurs, à détourner les clients de ses concurrents en cessant d'émettre des recommandations les concernant depuis l'appli Shazam.

Autre facette de l'IA, elle est également perçue comme un outil de détection des pratiques anticoncurrentielles notamment par les États[28] et les autorités administratives qui se penchent sur la question de la « régulation par la donnée »[29]. Les autorités publiques étudient la possibilité d'utiliser l'IA pour collecter, exploiter et publier des données pour amplifier leur capacité d'action : « *la régulation par la donnée permet ainsi une responsabilisation plus importante des acteurs, une capacité renforcée d'analyse du régulateur et une information accrue des utilisateurs et de la société civile* »[30].

L'IA serait donc un outil de développement et de protection de la libre concurrence, tant du point de vue de l'entreprise, créatrice et utilisatrice de l'IA, que de celui des autorités de contrôle qui disposeraient à leur tour d'un IA « régulateur » ou enquêteur. ■

(26) Comm. UE, COMP/C-3/37.92, n° 2007/53/CE, 24 mars 2004, JO 2007, L 32, p. 23 ; confirmé pour partie par TPI, 17 sept. 2007, aff. T-201/04, Microsoft c/ CEE, ECLI:EU:T:2007:289.

(27) Comm. UE, 6 sept. 2018, aff. M.8788, Apple c/Shazam.

(28) Aut. conc., communiqué,18 juill. 2019, G7/Accord commun droit de la concurrence et économie numérique.

(29) Aut. conc., AMF, ARAFER, ARCEP, CNIL, CRE et CSA, rapp., 8 juill. 2019, La régulation par la donnée.

(30) Aut. conc., communiqué, 8 juill. 2019, Coopération entre régulateurs.