



ALGORITHM DATA
ETHICS LABEL

VADE-MECUM SUR LE TRAITEMENT, DES DONNEES NUMÉRIQUES

Réflexions et bonnes pratiques éthiques

Écrit par l'équipe de direction d'**ADEL**
Avec la participation des membres de son Comité d'experts indépendants,
ainsi que d'autres spécialistes du numérique de la société civile

Février 2018

CITATIONS

« L'information est partout,
au bout des doigts »
[Bill Gates](#)

« Le savoir est la seule matière
qui s'accroît quand on la partage »
[Socrate](#)

« L'anonymat est devenu
algorithmiquement impossible »
[Arvind Narayanan](#)

« J'espère que les principes
que j'ai posés dans cet ouvrage
pourront être de quelque utilité
à cette manière de philosopher,
ou à quelques autres plus véritable,
si je n'ai pas touché au but. »
[Isaac Newton](#)

AVANT-PROPOS

Cet ouvrage constitue un recueil de réflexions des acteurs de la société civile sur le sujet des bonnes pratiques éthiques autour du traitement des données numériques. Il est important d'indiquer que ces opinions personnelles engagent uniquement les auteurs, et non la structure ou l'institution à laquelle ils sont rattachés.



Jérôme BERANGER
CSO et co-fondateur d'ADEL

Avec l'avènement des Nouvelles Technologies de l'Information et la Communication (NTIC) autour des *Big Data*, il apparaît difficile de trouver un équilibre entre la disponibilité des données médicales, leur confidentialité et leur protection. Dès lors, il devient essentiel d'établir une réflexion éthique sur des processus de Sourcing, de contrôle, de traitement et d'encadrement de ces métadonnées afin de conserver une place prédominante à la confidentialité et la confiance auprès des acteurs du numérique, et ainsi contribuer à donner une certaine maîtrise des risques et des déviations. Dès lors, il faut apporter du sens aux données, aux algorithmes et à leurs usages, afin de faire naître une véritable valeur ajoutée aux NTIC qui envahissent notre société. Cela passe obligatoirement par l'élaboration, la construction et le développement d'une éthique algorithmique. Car, à notre sens, écrire et penser l'avenir d'une éthique algorithmique puis quantique, c'est la rendre tout simplement possible !



Cédric VILLANI
Mathématicien - Médaille de Fields 2010 / Député

La convergence historique entre biologie, mathématique et informatique apporte avec elle des promesses considérables, et donc des menaces tout aussi considérables. Dans ce contexte il est plus important que jamais de s'interroger sur l'éthique scientifique et de l'aborder aussi bien en théorie qu'en pratique, structurellement et dans les détails. Confidentialité des histoires individuelles, protection contre les conflits d'intérêt, ... toutes ces questions sensibles sont renouvelées et accentuées par la montée en puissance des technologies de l'information !



Gilles BABINET
Digital Champion pour la France

Mettre l'éthique au cœur de la modernité ; s'en servir comme d'un axe pour permettre à la révolution digitale de se déployer dans l'univers de la santé me semble être une approche pertinente autant qu'utile. Toute la difficulté consiste de ne pas adopter de posture manichéenne : trop de conservatisme nous empêchera de rentrer dans cette révolution tandis qu'une logique d'innovation débridée pourrait nous faire perdre une partie de ce qui nous caractérise en tant qu'humanité. L'éthique, qui privilégie une vision d'ensemble, et non pas le point de vue du juriste contre celle de l'innovateur me semble répondre à ces défis.

TABLE DES MATIERES

Citations	3
Avant-propos	4
Table des matières	7
Introduction	8
Chapitre I : La révolution numérique : entre espérances et inquiétudes	10
1. Philippe De Lorme : Mutation numérique = promesses et exigences	14
2. Dr François Teboul : Le traitement des données de santé au coeur de toutes les attentions	18
3. Karine Lazimi Chouraqui : La révolution numérique recompose le monde de l'assurance	24
4. Vincent Trély : Ethique et données de santé à l'ère du dataïsme	28
5. Sophie Floreani : L'Humain au coeur du digital	34
6. Alban van Landeghem : Vers une plus grande prudence scientifique autour du traitement des données numériques...	38
Chapitre II : La «datasphère» et ses applications numériques	42
1. Alban Jarry : L'homme bionique et numérique est-il déjà au milieu de nous ?	46
2. Valéry Ravix : Objets connectés : devenir et conséquences des données collectées	50
3. Dr Loic Etienne : L'Intelligence Artificielle en médecine	54
4. Dr Joël Colloc : De l'Intelligence Artificielle mimétique aux systèmes autonomes : quels objectifs et quels enjeux éthiques ?	62
5. Sajida Zouarhi : Ethique et TIC, la <i>Blockchain</i> comme outil de gouvernance des données	68
Chapitre III : Le droit et la réglementation autour du traitement des données numériques	74
1. Me Jeanne Bossi Malafosse : La protection des données personnelles s'invite au coeur de la stratégie des organisations	78
2. Me Lina Williatte : Le cadre légal et réglementaire : les exigences du Règlement européen du 27 avril 2016 et la loi française pour une République numérique du 7 octobre 2016	80
3. Emmanuelle Rial-Sebbag : Objets connectés utilisés pour la santé : une nécessaire clarification réglementaire	88
4. Hugues Le Bars : Gouvernance des données, RGPD et éthique pour le futur	94
5. Pr. Solange Ghernaoui : Homo Numericus et hyperconnectivité, résister à la colonisation numérique, produire du bien commun	98
Chapitre IV : Les pistes de réflexions éthiques pour tendre vers une confiance numérique	110
1. Christine Balagué : De l'éthique des algorithmes et de l'intelligence artificielle	114
2. Florence Picard : Une éthique du numérique centrée sur les citoyens et orientée vers des solutions techniques	118
3. Benoit Dos : Vers une voie européenne de la révolution numérique ?	124
4. Jean-Sébastien Vayre : La socialisation algorithmique	132
5. Quentin Bériot : Cibler l'action de prévention : condition sine qua non de son efficacité	138
6. Dominique Pon et de Serge Maîtrejean : Le projet Eternesia : vers un humanisme numérique, un patrimoine commun et une mémoire de l'humanité	144
Conclusion	148
Remerciements	150

INTRODUCTION

L'accroissement des données brutes produites par les particuliers, les entreprises, les institutions publiques et les acteurs scientifiques offre de nouvelles perspectives de monétisation, d'analyses et de traitement. Les *Big Data* induisent une transformation majeure dans l'usage du numérique par les entreprises de tous les domaines économiques. Ces derniers ont des répercussions considérables en termes de développement, de recherche ou d'amélioration des services, de leur gestion, et de création d'emploi. Ceci aboutit donc à une société dans laquelle les Nouvelles technologies de l'information et de la communication (NTIC) jouent un rôle majeur et central.

Dans les débats éthiques qui en découlent, des tensions transparaissent entre la morale de conviction à la morale de responsabilité, l'individuel et le collectif, contribuant au dysfonctionnement stratégique, organisationnel et gouvernemental de notre société. À cela on peut ajouter une révolution technologique de l'information avec le développement des NTIC. Désormais, une « intelligence des données » apparaît comme la réponse stratégique pour la gestion de l'usage et la déviance de ces dernières.

Cependant, une telle révolution comporte également des risques éthiques autour des données à caractère personnel comme l'intégrité, la fiabilité, la sécurité, le respect de la vie privée et des libertés individuelles, la réputation, la régulation, etc.

Dès lors, l'exploitation des *Big Data* est un sujet sensible, du fait que ces dernières touchent directement à l'intimité de chaque personne. Les situations dans lesquelles se posent de difficiles problèmes de choix stratégiques en matière de gestion de la donnée personnelle sont chaque jour plus nombreuses. La numérisation croissante des données numériques, la capacité sans cesse accrue à stocker des données numériques, l'accumulation d'informations en tous genres qui en découle, contribuent alors à apporter certaines craintes et incertitudes en raison de ses usages multiples (voire complexes), de ses impacts difficilement mesurables touchant des populations très différentes, et de son information parfois hors de contrôle.

L'éthique ne peut constituer une réponse absolue, elle n'est pas une science exacte qui, par l'intermédiaire de théorèmes et d'axiomes, aboutirait à une vérité universelle. Elle ne peut qu'espérer y tendre afin d'établir un rapport de confiance entre les entreprises utilisatrices des données numériques et la société. Sa finalité est d'apporter des orientations qui ne recherchent pas un consensus mais révèlent des antagonismes existants. Ainsi, les divergences d'avis illustrent bien les difficultés auxquelles vont être confrontés les professionnels du numérique et l'ensemble de la société.

C'est à partir de ce contexte, que la société ADEL (*Algorithme Data Ethics Label*) a souhaité réaliser cet ouvrage intitulé : « *Vade-mecum* sur le traitement des données numériques » en laissant la parole à ses membres de son Comité d'experts indépendants, ainsi qu'à d'autres spécialistes du numérique de la société civile.

Dès lors, ce livre blanc nous amène à nous questionner sur les valeurs de la société et les principes éthiques impliqués dans la conception et l'utilisation des NTIC. L'une des questions majeures que soulève cet ouvrage est de savoir comment la modernisation technologique de l'usage des données numériques peuvent s'accompagner d'une sensibilisation éthique dessinant un Système d'Information (SI) à visage humain ? Quelles sont les répercussions d'un SI sur les mentalités et valeurs sociales des acteurs du numérique, d'un point de vue structurel, technologique, stratégique, méthodologique, organisationnel, relationnel ou culturel ? Nous pourrions alors replacer cette réflexion éthique dans la perspective d'une évolution des NTIC, à l'heure à la fois des développements technologiques récents et des nouveaux outils associés aux *Big Data*, ainsi que des nouvelles organisations qui sont en train de se mettre en place. C'est à partir des interrogations suivantes que notre ouvrage s'appuiera afin de développer une réflexion transversale et éthique, successivement sur la révolution numérique, la « datasphère » et ses applications numériques, le cadre juridique, et les idées pour tendre vers une confiance numérique de la société.

Enfin, en mettant en évidence une trame de fond basée sur une réflexion nouvelle éthico-technique, ce livre blanc ADEL souhaite apporter les premiers éléments d'un plan d'évolution contribuant à des changements sensibles des mentalités, de la manière de travailler ainsi qu'une transformation stratégique et organisationnelle à « visage humain » des Big Data et des technologies qui leurs sont associées. Le but étant de trouver une certaine cohérence et sens dans ce paysage en perpétuelle évolution technologique afin d'apporter la meilleure prise en charge possible pour le patient. Enfin, cet ouvrage a pour vocation de sensibiliser l'ensemble des acteurs de la société civile et de promouvoir une culture orientée vers l'implication, l'appropriation et la responsabilisation autour du traitement des données numériques.

Chapitre I :
La révolution numérique :
entre espérances et inquiétudes



Le monde d'aujourd'hui correspond à un univers où l'information numérique est omniprésente, ouvrant ainsi des perspectives sur la réalité que nous n'avons jamais eues auparavant. On assiste, désormais, à l'émergence de processus de «datafication» qui consiste à tout numériser et à mesurer afin d'en ressortir des données que ce soit pour des écrits, des localisations, des actes individuels, voire des empreintes. Une telle révolution numérique contribue à transformer notre écosystème en apportant :

- la possibilité d'analyser des quantités gigantesques de données croissantes,
- l'acceptabilité de l'approximation et du désordre,
- la recherche des corrélations plutôt que des causalités.

On peut remarquer que cette notion de « corrélations » issue de la biologie est employée depuis longtemps en économie.

Les *Big Data*, qui apparaissent aujourd'hui comme un moyen à la fois d'optimiser les processus et de participer au diagnostic et à la dispensation des soins, déboucheront de toute évidence sur une métamorphose, non seulement du système de santé tel que nous le connaissons aujourd'hui, mais encore de la médecine. Ainsi, nous rentrons dans l'ère postindustrielle. Dans un monde où les données se démultiplient, où les perceptions vont devenir infinies, et où tout deviendra une somme de singularités, les structures essaient de comprendre comment extraire de la valeur de toutes ces données qu'ils récupèrent. Cette nouvelle masse de données inédite crée de nouveaux savoirs. Cela modifie le paradigme même du traitement algorithmique des données, des acteurs du numérique, et de leurs rapports avec l'ensemble de notre société, provoquant un climat instable où s'entremêlent à la fois un sentiment d'espérance et d'inquiétude.

1 / MUTATION NUMÉRIQUE = PROMESSES ET EXIGENCES



de Philippe De Lorme

Directeur d'hôpital honoraire
Président de la Commission Internationale du CATEL
Administrateur de Formatic Santé
Représentant National au Conseil d'Administration de l'ISFTeH

Je commencerai mes propos par une anecdote vécue cet été qui m'a interpellé quand, naviguant dans une région de France largement fréquentée par une population estivale essentiellement d'origine britannique, je constate que mon GPS se met à converser avec moi en langue anglaise. Bien qu'au fait en continu des enjeux phénoménaux des *Datas* et de notre écosystème global de plus en plus digitalisé, on ne peut que s'interroger sur la protection de nos libertés individuelles et sur notre extrême vulnérabilité ne faisant que renforcer ce sentiment de défiance contextuellement généralisé.

L'actualité géo-économico-politique internationale en apporte la preuve régulièrement *via* les *Ransomware* survenus au printemps 2017 bloquant entreprises et commerce mondial, citons aussi les conséquences d'ordre géo-diplomatiques issues de l'affaire du Qatar et de l'Arabie Saoudite en juin dernier menant à un *Blackout* total du premier par le second et suivi par d'autres dont il s'est avéré que l'affaire était « numériquement » manipulée.

Ainsi, doivent se poser de multiples interrogations sur la gouvernance globale de nos (des) données numériques dont nous sommes propriétaires que nous confions « aveuglement » sans aucun contrat de bail à des « boîtes noires propriétaires » sans garanties aucune quant à leur protection cyber-sécurisée et à leur utilisation finale. Ce sujet préoccupe nombre de continents et pays, dont l'UE, dans toutes ses composantes techniques, juridiques et éthiques.

La révolution numérique que nous traversons impacte politiquement nos civilisations et exacerbe nos propres contradictions entre ce qui relève de la propriété privée et du bien commun et *de facto* notre regard sur nos chaînes de valeurs.

Se référant à la définition de la gouvernance issue du Larousse, « qui désigne l'ensemble des mesures, des règles, des organes de décision, d'information et de surveillance qui permettent d'assurer le bon fonctionnement et le contrôle de nos organisations » quelle qu'elles soient ;

« Il est grand temps de s'interroger sur le pouvoir des algorithmes¹ issus de puissants systèmes experts menaçant nos arbres décisionnels et éthiquement notre libre arbitre. »

En matière de santé, on peut aisément en mesurer les conséquences pour les décideurs/managers institutionnels et les personnels de santé en termes d'aide au diagnostic et de suivi thérapeutique, surtout dans nos contextes visant l'efficacité et à tracer et coordonner intelligemment les usages et au mieux l'organisation des parcours de soins de patients (que nous sommes tous en devenir) à prendre en charge territorialement.

En d'autres termes, vers quel type « d'humanisme numérique » tendons nous ? Où désirons nous aller ? Ceci dans un cadre de mobilité technologique tout azimut et d'une temporalité accélérée n'autorisant pas le temps nécessaire pour modéliser culturellement, intellectuellement et cérébralement de façon performante et pertinente nos organisations. A ceci, se superpose une nouvelle « révolution culturelle Internet », issue des dispositifs technologiques dits « *Blockchain* » redistribuant une nouvelle gouvernance Internet qui ne sera pas sans poser de nouvelles interrogations sur nos gouvernances digitales, dont le monde de la santé ne sortira ni indemne ni fortement impacté. (Cf. Tryptique recherche / développement / innovation / suivi de pathologies chroniques, etc.). Sont à craindre l'émergence de nouvelles fractures numériques. *Machine Learning*, *Deep Learning*, le développement d'ordinateurs cognitifs associant auto-apprentissage et Intelligence Artificielle (IA) / systèmes experts, les progrès de l'informatique quantique, le développement de la génomique personnalisée, les résogiciels ... autant de révolutions issues d'innovations formidables tendant vers des cultures collaboratives, certes, mais qui vont dessiner ainsi peu à peu de nouvelles gouvernances et de nouveaux arbres décisionnels et *de facto* notre futur proche environnement managérial.

Qui va décider en fin de parcours ? Comment ? Qui va avoir le courage de stopper peut-être un enchaînement de circuits décisionnels immaîtrisables mettant en jeu le bien commun ?

Par ailleurs, la nécessité d'intégrer et encore des normes et standards interopérables partagées² du fait de nos mobilités va impacter le monde économique-sanito-médico-social avec toutes ses conséquences métiers / compétences / formation / l'emploi / les organisations sans omettre leur dimension éthique.

¹ Les algorithmes hiérarchisent des données selon des impératifs économiques et non de connaissance pure, d'après Bernard Stiegler dans « Mémoire et oubli ».

² Par exemple : application de la directive UE transfrontalière, le futur dossier patient européen partagé.

« Se posent d'ores et déjà des problématiques de responsabilisation et de régulation, quelle sera ou devra être la place de la puissance publique et de l'État ? Du droit face aux applications *Blockchain*, dont les applications en santé se développent ? Quels contrôles ? De la place qui sera faite aux usagers ? Et du devenir de nos démocraties ? Etc. »

En dehors de déclarations d'intentions aussi respectables soient-elles, nos institutions de santé sont-elles prêtes à affronter et s'approprier ces profondes et vertigineuses mutations algorithmo-technico-sociétales en termes de gouvernance numérique ?

Les récents rapports du CERNA (Commission de réflexion sur l'Éthique de la Recherche en sciences et technologies du Numérique d'Allistene), ou encore de Bercy (Transalgo)³ nous interpellent et nous obligent à s'interroger dès maintenant sur ces sujets⁴. Citons, le risque d'opacité des données, leur qualité, leur incomplétude qualitative et leur vulnérabilité potentielle, leur explicabilité, leur exploitation, l'équilibre à trouver entre le respect des libertés individuelles et la sécurité des données de plus en plus cryptées, les risques de discrimination induits, un contrôle par la puissance publique balbutiant ...

En outre, de façon non exhaustive, tout ceci invite à débattre des quelques propositions suivantes :

- **Informer** : ne pas sous-estimer le pouvoir de la culture, de l'accès aux connaissances et à l'information tout en adaptant ses modalités de transmission et respectant les publics auxquels on s'adresse. Ceci ne peut s'effectuer sans investissements au niveau des territoires en infrastructures le permettant. (Cf. Université des déserts médicaux sept 2017).

- **Rassurer** : dans notre monde disruptif « algorithmique » croissant voire « outrancier », de défiance et de doutes, il convient aux responsables quel qu'ils soient, d'une part, de mesurer l'importance visionnaire et humaniste de nos chaînes de valeurs, et d'autre part, « allier le pessimisme de l'intelligence à l'optimisme de la volonté »⁵. L'avènement des « *Blockchain* » représente d'ores et déjà un véritable challenge.

- **Former** : et encore former plus que jamais. Nos institutions de formations, toutes filières de métiers confondues, doivent s'approprier et décliner pédagogiquement avec toute l'intelligence et pertinence nécessaire leurs programmes. Anecdotiquement, une lettre ouverte datant de 2 ou 3 ans rédigée conjointement par des directeurs de grandes écoles, d'universités, de grandes structures de formation nommément reconnues dans notre hexagone ... de professeurs et d'anciens élèves ou en fin de cycles, alertait le MESR (Ministère de

l'Enseignement Supérieur et de la Recherche) sur l'inadéquation des programmes enseignés, déconnectés des réalités du terrain pour des candidats destinés à exercer des fonctions de responsabilités une fois affectés. Parmi les priorités, dont celle du CERNA, mettre l'accent sur la formation de la culture et à l'analyse de la donnée, sa valeur et son usage. Créer et cibler de nouveaux métiers tels que des *Data Scientists*, des *Data Protection Officer*, des responsables sécuritaires et architectes réseaux, Citant Thomas L. Friedman, éditorialiste⁶, « on n'a pas d'autre option que de travailler à muscler la résilience des sociétés » qui dépend à 90% de l'optimisation de l'apprentissage, et d'insister sur la responsabilité qui pèse sur nos systèmes éducatifs et de formation, et, « si une société ne construit pas de sol sous les pieds de ses membres, ils seront nombreux à vouloir édifier des murs ».

- **Accepter** : « Le monde n'est pas seulement en train de changer à toute vitesse, il se reconstruit en profondeur et se met à fonctionner différemment dans de multiples domaines à la fois »⁷. Nous avons besoin plus que jamais de philosophes, de sociologues pour nous éclairer de par leurs démarches de pensées au sein de nos organisations.

Enfin, revenant à la gouvernance globale du monde de la santé, de nouvelles stratégies managériales de nos organisations (Cf. Méthode Agile) sont à mettre en oeuvre de toute urgence, afin de lever nos « peurs » sous-jacentes. Cela passe notamment par une identification et un accompagnement de compétences employables et adaptables couplée d'une culture d'ouverture nécessaire facilitant la compréhension de ce monde changeant, prometteur, exigeant et complexe, mais néanmoins passionnant.

ACCEPTER est à mettre au centre d'un triangle dont les angles sont : **INFORMER, RASSURER, FORMER.**

Citant à nouveau B. Stiegler, une thérapeutique antidote au numérique afin de lutter contre le défaitisme et le refus du progrès, serait constituée « par des savoir-vivre, des savoir-faire et des savoirs spirituels ».

³ <https://www.inria.fr/actualite/actualites-inria/transalgo>

⁴ Notons que la mise en application du nouveau règlement européen relatif à la protection des données personnelles sera effective le 25 mai 2018.

⁵ Selon Antonio Gramsci – écrivain et philosophe italien – dans la lettre destinée à son frère Carlo qu'il a écrite en prison.

⁶ Dans l'ouvrage intitulé : « *Merci d'être en retard* », aux éditions St Simon.

⁷ De Th. L. Friedman dans l'ouvrage intitulé : « *Merci d'être en retard* », aux éditions St Simon.

2 / LE TRAITEMENT DES DONNÉES DE SANTÉ AU COEUR DE TOUTES LES ATTENTIONS



de Dr François Teboul

Médecin Urgentiste,
Directeur médical - Visiomed

Il m'a fallu du temps et de la réflexion avant de commencer à distinguer une différence entre « résoudre un problème » et « couvrir un besoin ». Elle peut paraître ténue mais à bien y réfléchir, elle me semble aujourd'hui fondamentale. Cette anamorphose qui permet, en somme, de faire un pas de côté, pour voir la situation autrement permet aussi, parfois, d'arrêter de se mettre le doigt dans l'oeil jusqu'au coude. Ces notions très employées dans le monde de l'innovation, de la transformation digitale, des *Start-ups*, des *Fab-labs*, ... font appel, fondamentalement, à la relation entre le fournisseur et l'utilisateur, avec comme objet la solution proposée.

Prenons la phrase « ma solution répond à un besoin » : Dans cette situation j'ai donc un fournisseur qui dit à son client qu'il lui propose une solution qui répond à un besoin, qu'il a, même si le client ne le sait pas lui-même. Cette notion de « besoin » contenant en elle déjà l'objectif qu'il se serait fixé.

Mais comment ce besoin a-t-il été défini ? Là, réside la première question d'importance. Qui a dit que ce besoin est bien réel ? Qu'il l'a été ou qu'il l'est toujours ? Comment a-t-il été établi ? Par qui ? Bien souvent, une fois que ce besoin est admis par le client ou l'utilisateur, on entre alors dans une compétition dans laquelle les différents acteurs du marché vont chercher à le couvrir le mieux possible et de mieux en mieux. Et dans cette course à la performance, nous risquons, nous, d'oublier quel était l'objectif fixé.

Ce « besoin » me semble être, en partie au moins, un reliquat du millénaire précédent, ayant émergé du monde du marketing des années 1970 pour lequel créer un besoin a permis et permet toujours aujourd'hui de vendre. Dans la séquence : « J'ai un besoin donc je veux. En tout cas il me manque quelque chose si je ne l'ai pas ».

Des méthodes plus modernes comme le *Design Thinking*, propose au contraire d'oublier un moment le besoin pour revenir à l'objectif. Et, pour définir cet objectif, d'analyser le problème ... Quel est le problème qui se pose aux utilisateurs ? Et du coup, comment régler ce problème ? Quelle solution y apporter ? Finalement on

en arrive, là encore, à exprimer des besoins mais qui découlent des problèmes rencontrés et ainsi deviennent des notions beaucoup plus dynamiques : les solutions proposées, les besoins exprimés devant être confrontés régulièrement, de façon itératives et incrémentales, aux problèmes rencontrés, à la « réalité » des utilisateurs. Des sociétés comme Google ont même dépassés l'idée de fournir des solutions, en procurant plutôt des usages à leurs clients et en les analysant.

« La donnée de santé doit avant tout être créée, de bonne qualité. »

En Côte d'Ivoire, nous participons avec l'UNFM, à un très beau programme dans lequel le CADA⁸ dépiste et suit des milliers de patients diabétiques au sein de l'Institut National de Santé Publique (INSP) d'Abidjan. Nous allons, cette année, commencer l'équipement de centres ou dispensaires plus éloignés qui permettront de télé-suivre ou de télé-consulter les patients à distance. Cette solution répondant aux problèmes suivants : les patients doivent parfois faire 2 jours de transport en bus, en dormant sur des bancs pour aller voir leur diabétologue pour une simple consultation de dépistage ou de suivi.

Avant d'introduire des notions plus complexes comme l'utilisation d'objets connectés, de faire du partage ou de l'exploitation de données, nous avons avant tout consacré plus d'une année, à installer un Dossier Patient Informatique, à s'assurer de la conduite du changement et de son adhésion (Cf. Approche métier) puis avons continué vers une solution plus aboutie. Aujourd'hui l'INSP a pu devenir l'un des premiers centres de toute l'Afrique à transmettre des données à un registre épidémiologique international diabéto-pédiatrique (SWEET⁹).

A contrario, j'ai eu l'occasion, lors de ma dernière visite, de discuter avec des membres du monde académique qui ont exprimé leur besoin de faire des analyses épidémiologiques à grande échelle et qui ont décidé d'investir dans de gros entrepôts avec des logiciels capables de manipuler des milliards de données, sauf, qu'aucun hôpital n'est équipé de Dossier Informatique, donc aucune donnée n'est générée ... Cela rappelle un peu le DMP ! Le premier problème est donc d'être capable de générer de la donnée de bonne qualité et de la standardiser, le second est de le partager et de la *Data-miner*. Peu importe ce que le client veut, ce qu'il exprime comme besoin, il ne pourra régler ces problèmes que l'un après l'autre ...

⁸ Centre Anti Diabétique d'Abidjan (Dr F. Aka).

⁹ <http://www.sweet-project.org/>

« Des besoins exprimés, dépassés par l'évolution des problèmes. »

Le dogme actuel dominant dans le domaine de la protection des données de santé est la réalisation de « coffres-forts numériques » dans lesquels sont stockées toutes les données sensibles des utilisateurs (patients). Et l'on voit, là encore, depuis des années, une course en avant de la part des industriels et des pouvoirs publics pour créer des entrepôts de plus en plus sécurisés. Ces entrepôts coutent très chers et consomment une bonne partie de la matière grise des entrepreneurs, pouvant même constituer une barrière à l'entrée sur ce marché. Le raisonnement admis est donc le suivant : « J'ai besoin de mettre toutes mes données à l'abri dans un coffre-fort dans lequel personne ne pourra accéder sans ma clé privée, donc sans mon consentement ». Mais se souvient-on encore d'où vient ce besoin ? Quels sont les problèmes sous-jacents ? Pourquoi vouloir rendre mes données inaccessibles ? Si je les mets sur le cloud c'est avant tout parce que j'ai envie ou besoin de les partager.

Très souvent, un des arguments avancés est qu'il s'agit d'empêcher, par exemple, les assureurs d'utiliser les données personnelles pour faire varier le coût des mutuelles en fonction de l'état de santé d'un individu. Par exemple, le taux de cholestérol pour un prêt, pour une assurance santé complémentaire, le génotype de mon hépatite C pour le remboursement du médicament. La réponse classique est de mettre cette information dans l'un de nos coffres forts numériques.

Dans le cas de l'hépatite C, je vous conseille d'aller vous promener sur des *forums* publics¹⁰ où vous verrez dans la section forum (publique) que les patients, *via* leurs pseudos, partagent énormément d'informations (génotype, traitements, etc.) car ils ont bien compris que la transparence était un atout pour une meilleure prise en charge. D'ailleurs, les sites communautaires du type *patientslikeme.com* aux USA ou *Careny.com* en France ont fait de cette transparence et de ce partage d'informations sensibles entre patients leur fonds de commerce.

Dans le cas du taux de Cholestérol, on sera rapidement capable de répondre assez simplement à cette question en analysant des données non confidentielles et en établissant des corrélations (Cf. *Deep Learning* et *Smart* ou *Big Data*), créant des modèles prédictifs qui, connaissant la marque de votre dentifrice et de votre plat surgelé préféré, sauront prédire à 99,5% votre taux de cholestérol. Si l'assureur est capable, en exploitant des données non confidentielles, parfois sans aucun rapport, de « deviner » les données que vous cherchez à lui masquer, que ferons-nous de tous ces entrepôts de données sécurisés qui nous auront coutés des centaines de millions d'euros ? Et surtout, la question se pose de savoir quelle valeur accorder, finalement, à rendre toutes ces données confidentielles ?

¹⁰ <http://www.hepatites.net/index.php?name=PNphpBB2&file=viewtopic&t=24531> ou site www.soshepatites.org

« Des objectifs parfois contradictoires. »

En tant qu'urgentiste, dans la vie réelle, le vrai problème, peut-être même le seul vrai problème qui se pose est d'accéder aux données du patient (ses antécédents, traitements habituels, allergies, dernières consultations, etc.) : « Un homme, 89 ans, suivi depuis 20 ans dans le même hôpital arrive aux Urgences en grande détresse. Je suis remplaçant cette nuit-là dans l'hôpital que je découvre pour la première fois (désertification médicale oblige). Le patient a du mal à s'exprimer en Français. Il me faut ma carte CPS associée à celle de l'établissement. Et puis, sa carte vitale. Puis je cherche le mot de passe pour ouvrir le logiciel (la fameuse clé privée) qui est d'habitude gravé au cutter sur la table. Au final, au bout d'une dizaine de minutes, je laisse tomber, parce que le patient est en train de crever... Je vais devoir le soigner sans aucune information, alors que je suis convaincu qu'une ribambelle d'externes et d'internes ont bien consciencieusement remplis et classés des milliers de documents ».

Moi-même, qui a longtemps été un patient, comme cet homme de 89 ans, j'ai souvent eu envie de hurler : « Partagez mes données, mettez-les sur Facebook, publier les dans le Monde ou le Figaro mais accéder à mes p... d'informations ! ». En tant que patient ou que médecin, la protection des données peut donc apparaître comme une entrave à l'objectif principal de l'information de santé : celui d'être partagée.

Il ne faut pas non plus être naïf ; Il faut bien entendu trouver un moyen de se protéger de l'usage abusif de nos données de santé mais tout est là : il faut se rappeler du problème que l'on essaye de régler et auditer si la solution que l'on propose, le solutionne toujours. Si la réponse est non, alors il ne faut probablement pas insister mais réfléchir et en penser de nouvelles. Avoir le courage de faire face au problème réel même si cela signifie que pendant un temps on n'a pas de solution satisfaisante à proposer.

« La technologie quantique rend la cryptographie classique obsolète. »

Nous avons vu que dans le cas des données de santé, la solution admise de « coffre-fort digitale » peut entraver le partage des données et ne permet pas nécessairement de résoudre les véritables objectifs que l'on a pu se fixer. Au-delà de ces considérations, la solution du coffre-fort numérique est basée sur le principe de la factorisation (problème qui consiste à trouver, pour tout nombre entier n , les deux nombres premiers p et q tels que n soit égal au produit de p par q). C'est sur la quasi-impossibilité de résoudre ce problème (pour un nombre n suffisamment grand) que repose le fameux système de cryptographie RSA¹¹. Or dès 1994, un mathématicien américain du nom de Peter Shor a inventé un algorithme qui, implanté dans un ordinateur quantique, serait capable de résoudre n'importe quelle factorisation. Pour donner un ordre d'idée il faut 100 000 ans pour un ordinateur classique actuel pour factoriser un nombre RSA de 1024 bits

¹¹ D'après les initiales de leurs inventeurs Ronald Rivest, Adi Shamir et Leonard Adleman.

alors qu'il faudrait seulement 5 minutes, et quelques calculs, pour un ordinateur quantique de 5100 qubits (l'ordinateur classique en ayant environ 35 milliards...)¹². Même si nous n'y sommes pas encore, l'ère du cryptage quantique a commencé¹³ et à cause d'elle, la cryptographie classique vit probablement ses derniers jours.

« L'éthique comme solution. »

Technique obsolète, objectifs contradictoires, solution désuète ou carrément hors sujet, à des problèmes mal identifiés : on en est là et pourtant on continue ... Nous sommes au cirque, on vient de voir des éléphants et des acrobates. La scène est dans l'obscurité absolue et le brouhaha de la salle s'estompe. Silence. Dans un coin de la scène, un lampadaire s'allume progressivement et éclaire sous lui quelques mètres carrés de sable. Un clown, apparaît. De toute évidence, il cherche quelque chose par terre. Il scrute le sol, en silence, absorbé et continue de faire le tour de ce tout petit espace éclairé. Il se baisse, gratte le sol, fait semblant de soulever quelques pierres. Plusieurs longues minutes passent, quand, subitement la voix d'un autre clown que l'on ne voit pas se fait entendre et demande :

« Qu'est-ce que tu fais ?

- Ça ne se voit pas, je cherche... J'ai perdu une pièce de 5 francs et du coup, maintenant, je la cherche.
- Et tu l'as perdu où ?
- Ben, là-bas... Le clown fait un grand geste et pointe au loin.
- Pourquoi tu la cherches ici, alors ???
- Ben enfin ?! C'est parce qu'ici il y a de la lumière. Là-bas, je n'y vois rien ... »

Pour moi, cette scène, ce souvenir d'enfance illustre parfaitement la situation du traitement des données médicales. On comprend aisément que la politique puisse parfois se résoudre à augmenter la puissance du lampadaire... mais l'Éthique ne devrait-elle pas être celle qui rappelle qu'il ne sert à rien de chercher ici, uniquement parce qu'il y a de la lumière.

La politique est souvent en retard sur les mœurs. Et les mœurs, en retard sur la technologie et le champ des possibles. Restreindre le champ des possibles c'est restreindre notre capacité à véritablement et durablement changer notre vision sur les objectifs. Comme on dit : « On n'a pas inventé l'ampoule électrique en faisant de l'amélioration continue sur la bougie ... ».

¹² Introduction à l'informatique quantique, Y. Leroyer, document de cours de l'école ENSEIRB-MATMECA.

¹³ http://www.lemonde.fr/asi-pacifique/article/2016/08/17/la-chine-fait-un-saut-quantique-dans-le-cryptage-de-ses-communications_4983720_3216.html

3 / LA RÉVOLUTION NUMÉRIQUE RECOMPOSE LE MONDE DE L'ASSURANCE



de Karine Lazimi Chouraqui

Fondatrice - Cabinet LCK Assurances
www.assurancesfinances.com

« Le numérique ... l'Intelligence Artificielle (IA), une rupture avec le passé qui recompose notre monde au quotidien. »

J'ai fait mes premiers pas sur le Web en 1994 ... époque où nous attendions 10 minutes pour voir une page html s'afficher si elle contenait une image ... certains en parlent encore tellement cela semble la préhistoire aujourd'hui. Depuis, la sémantique a bien évolué et on parle de numérique, de digital et d'IA.

Vous le savez, le numérique et surtout le mobile est bien une rupture avec l'ensemble de la chaîne de valeurs et recompose notre société, notre quotidien, la transforme avec une nouvelle culture et un nouveau regard sur le monde. C'est donc une rupture avec le passé dans la relation que l'on a présentement avec les autres tant à titre privé mais également dans notre façon d'exercer notre métier au quotidien.

Comment réussir à être dans le monde tel qu'il évolue aujourd'hui ? Un monde où nous sommes tous(tes) hyper connecté(e)s (*Smart Cities*, domotique, objets connectés, tablettes, smartphone ...). Comment les citoyens vont-ils s'approprier ce monde et comment vont-ils intégrer ces nouveaux paramètres dans leurs relations de tous les jours ?

Le citoyen est ultra-connecté, mobile et de plus en plus réactif, la société se doit de s'adapter à un univers qui est de plus en plus numérique avec des interactions immédiates avec le mobile (Cf. Réseaux sociaux, apps, etc.). Les citoyens dans la mobilité souhaitent interagir avec les autres (à titre privé ou professionnel) n'importe quand et n'importe où. Dans ce contexte, le mobile transforme complètement les usages. Il a ouvert le champ des possibles pour être en lien avec les autres au quotidien. Les citoyens interpellent les marques, les institutions sur Internet, sur les réseaux sociaux et c'est aux entreprises, aux institutionnels d'adapter l'ensemble de la chaîne de valeurs pour entrer en contact avec eux par le canal qu'ils ont utilisé.

« Ces interactions obligent le système à repenser chaque métier en obligeant tous les interlocuteurs à mettre réellement le citoyen au cœur de leurs préoccupations sans leur laisser le choix. »

La façon dont nous construisons nos relations de confiance avec les clients change. Comment allons-nous construire un lien, une relation de confiance entre citoyens, avec les entreprises, avec les institutionnels ? Une révolution silencieuse se passe sous nos yeux.

Le mobile nous permet d'échanger des milliards de données sur notre famille, nos loisirs, nos pratiques de consommation. Nous vivons dans une époque où la vie privée n'a pas la même valeur aujourd'hui qu'il y a 30 ans. Dans la mesure où les citoyens diffusent leurs données et qu'ils donnent leur accord (parfois à leur insu) pour qu'elles soient transférées, il devient très difficile de revenir en arrière.

« Et si le règlement général sur la protection des données à caractère personnel (RGPD), qui doit entrer en vigueur en mai 2018, était une opportunité pour toutes et tous (citoyens, clients et entreprises) ? »

Savez-vous comment les données des clients générées sont conservées et gérées ? Le règlement RGPD va, d'une part, renforcer les droits des personnes sur la protection de leurs données, et d'autre part, simplifier pour les entreprises les procédures de gestion des données. Les clients vont avoir de nouveaux droits à savoir : être informés de manière honnête et transparente sur le traitement de leurs données, un droit d'accès à leurs données, un droit de rectification, un droit de portabilité des données et un droit à l'oubli. Des procédures de gestion des données deviennent indispensables pour éviter tout problème. En focalisant sur l'assurance, plus le client va communiquer des données à son assureur, meilleure sera la couverture. L'assureur sera donc en mesure de proposer un contrat adapté avec des garanties spécifiques. La contrepartie sera de bien respecter ces droits. Par ailleurs, dans l'univers de l'assurance, l'IA pourrait faire apparaître la différenciation du risque selon les assurés. L'assureur a un rôle de vigie et doit le garder dans le monde de demain pour éviter un bouleversement de nos valeurs. Nous sommes dans un cycle normal de l'humanité qui suit le cours de son évolution ... Comment faire pour contrôler, réguler ces algorithmes face à de grands détracteurs ? Comment réguler ces usages, ces techniques ? Quelles seront les implications de ces techniques et de ces outils que nous souhaitons appliquer dans nos cultures et dans nos sociétés ? Comment faire en sorte en tant qu'assureur de conserver un rôle de vigie avec bienveillance ? Les algorithmes vont envahir notre vie parce qu'ils sont efficaces. Il va falloir choisir la façon dont nous souhaitons les voir évoluer. Pourrons-nous en tant que citoyen choisir la société dans laquelle nous souhaitons vivre demain ?

L'idée n'est pas de faire un procès à la technologie mais bel et bien d'étudier comment nous allons accompagner ce changement qui s'accélère très vite, sans le subir. L'enjeu est de politiser ces sujets et de faire en sorte que nous puissions avoir une technologie qui soit humaniste.

« N'oublions pas que ces mêmes algorithmes soignent le cancer et surveillent les espions. »

La mise en place des règles relatives aux données, avec une forte volonté de protéger les individus, est indispensable. Ce n'est pas au monde technologique industriel de décider du cadre de l'action et de la condition humaine, mais aux citoyens, librement, par la délibération et par la contradiction, de décider du cours de leur destinée.

Les entreprises exploitant des données personnelles doivent donc faire de leur mieux pour se conformer aux nouvelles règles, même si celles-ci sont parfois floues. Nous ne serons jamais à 100% conformes, il faut l'admettre et avancer progressivement. La mise en application des nouvelles règles devrait donc conduire les organisations à revoir leur gouvernance sur les sujets de données, tout en étoffant les équipes dédiées à ces problématiques de plus en plus centrales. Outre l'évolution de la gouvernance, c'est aussi l'occasion de remettre à plat toutes les pratiques de l'entreprise et de se pencher sur la question de l'éthique ... Un mal pour un bien ... ?

Si les entreprises font l'effort de repenser leur façon de gérer les données de leurs clients, en leur permettant de se les réapproprier et d'en garder le contrôle, plutôt que de donner le sentiment de les leur confisquer, ceux-ci seront plus disposés à les partager et, surtout, à fournir des données fiables à forte valeur ajoutée pour l'entreprise. La connaissance client essentielle pour les entreprises, sera ainsi nettement améliorée.

« Il est évident qu'il faut voir ici une opportunité pour les entreprises à réinventer leur rapport aux données personnelles et leur façon de présenter la collecte et l'utilisation des données aux clients, qui ne demandent en réalité, comme dans toute relation économique, qu'à comprendre en quoi cela leur sera profitable réellement. »

Selon le Parlement Européen, « le traitement des données à caractère personnel devrait être conçu pour servir l'humanité ». Ce n'est qu'à cette condition que les entreprises parviendront à lever les obstacles et vaincre les réticences qui freinent encore la digitalisation de nos économies. Instaurer un climat de confiance entre les personnes et les entreprises sur le terrain des données personnelles, sera le meilleur retour sur investissement qu'obtiendront les entreprises qui anticiperont dès à présent le tournant induit par la GDPR.

Si la protection des données personnelles est un point d'attention premier, il est essentiel de surveiller de près, les différentes expérimentations et les idéologies. Si nous prenons le secteur de l'assurance, nous arrivons à une hyperpersonnalisation des produits. Le concept de mutualisation dans l'assurance tend à disparaître. Y a-t-il des domaines et des limites à ne pas franchir ? Allons-nous pénaliser des

individus aux comportements « dangereux » pour leur santé ? Allons-nous isoler des groupes d'individus atteints de maladies chroniques ou génétiques ? Allons-nous privilégier les personnes qui font des efforts pour mener une vie saine ? Les nouvelles technologies bouleversent le secteur de l'assurance bien établi depuis longtemps et apportent des éléments de réflexion nouveaux. Différentes voies sont possibles pour le futur de l'assurance et certaines sont plus limites que d'autres.

L'assureur transforme son modèle économique autour de la prévention pour devenir l'assureur de demain. Des investissements considérables (hommes, infrastructures et technologies) sont mis à disposition pour diminuer les risques. Plus le niveau de prévention est élevé, plus le risque d'accident est faible et donc plus la cotisation d'assurance devrait diminuer.

Un challenge : préparer l'économie et la société numérique française telle que nous la souhaitons, plus ouverte, tournée vers l'innovation mais aussi protectrice en particulier des données personnelles. Il faut que le numérique puisse bénéficier à tout le monde. Le numérique aujourd'hui touche tout le monde, l'univers économique, social, environnemental, sociétal. Un énorme travail de vulgarisation, de pédagogie est à prévoir. Nous vivons une révolution industrielle et sociétale. Il nous appartient d'être acteur et de coconstruire avec les politiques et les industriels la société actuelle et future dans laquelle nous souhaitons évoluer. Nous sommes toutes et tous concerné(e)s par l'IA. Nous devons accompagner l'Humain dans le monde d'aujourd'hui et de demain, et aider à anticiper les risques, pour faire en sorte d'y vivre le mieux possible et que chacun y trouve sa place.

4 / ÉTHIQUE ET DONNÉES DE SANTÉ À L'ÈRE DU DATAÏSME



de Vincent Trély

Président Fondateur - APSSIS
CEO - Cabinet Vincent Trély Consultants

Objets de santé collecteurs et communicants (Cf. *Healthcare IoT*), homme augmenté, macro et micro organisations de santé connectées, création de valeur par la donnée de santé et appétits générés : quel est l'avenir de nos données de santé à caractère personnel ? Comment penser l'évidente « nouvelle confidentialité » basée sur un nouveau socle éthique ? Quelles sécurités sont indispensables à la confiance et peut-être au modèle gagnant / gagnant envisageable ?

Gilles Babinet¹⁴ parle de l'ère numérique comme « d'un nouvel âge de l'humanité », et nous invite à « penser l'Homme et le Monde autrement ». Nous allons devoir réviser notre rapport à la donnée, quelle que soit sa qualité. Le Professeur Guy Vallancien¹⁵, dans son ouvrage « La Médecine sans Médecins », propose une vision prospective de la santé si réaliste qu'elle inquiète. Les *Big Data*, les *Learning Machines* qui diagnostiquent mieux que les Docteurs, les dispositifs médicaux non plus « implantés », mais « embarqués » et bourrés d'électronique vont nous faire vivre plus longtemps en meilleure santé.

Et nous, les Homo-Sapiens, se rêvant Homo Deus, comme nous invite si brillamment à le concéder Yuval Noah Harari¹⁶, au centre d'un système théoriquement conçu pour nous servir, à la fois sources intarissables d'informations de plus en plus précises et usagers compulsifs, quelles négociations allons-nous entamer avec le XXI^e siècle pour fixer les clauses du contrat qui va lier notre plus profonde intimité au « super système » global ? Comment vont se définir les espaces privés et ceux dont nous céderons les détails ? Pour quels usages et pour servir quels objectifs ? Et quels modèles d'éthiques, inexorablement universels, allons-nous substituer aux imperfections des lois ?

La sécurité des Systèmes d'Information de Santé (SIS) et le pacte de confiance entre le citoyen et toute forme de « collecteur », est au coeur des débats depuis environ 5 ans. Les technologies numériques offrent de vraies révolutions

positives dans nos existences et le futur de notre santé en est parsemé. Je suis non seulement certain de l'intérêt à court terme des technologies numériques de santé, embarquées jusqu'en nous-mêmes, mais également optimiste sur la capacité de nos sociétés à en séparer l'ivraie du bon grain. Ce n'est pas pour autant que je me sens naïf, ni dépassé ou débordé par la célérité d'un phénomène sans précédent.

Un « *Business* » de 10 milliards de clients-patients en 2050¹⁷, tous soucieux de leur longévité et de leur bien-être, ne laisse personne indifférent ! Ce « *Business* » a ses particularités. La santé n'est pas un processus industriel comme les autres, même si l'on voudrait parfois l'y assimiler, sans grand succès. Il possède une variable humaine majeure qui change tout. Quoique l'on fasse, il existe une limite d'optimisation que la technologie n'absorbera pas tout de suite : le lien. Ce lien est d'ordre scientifique, déontologique, éthique et juridique. Ce lien est aussi et surtout celui des sens et du verbe.

Nos ancêtres hébreux disaient : « Honorez le médecin avant que vous n'ayez besoin de lui ». Le dicton perdure et l'on n'imposera pas grand-chose aux médecins et aux professionnels de santé, qui se feront certes de plus en plus rares et spécialisés au sein de systèmes de santé en large partie automatisés, robotisés et pilotés par une algorithmique complexe. Ils conserveront un pouvoir central, et accompagneront l'évolution de leur métier vers de plus en plus d'ingénierie. Il convient de les former très vite et beaucoup mieux aux usages sains et valides des technologies numériques, de leur offrir l'opportunité du refus motivé ou de la co-conception initiale des environnements fonctionnels.

« Les médecins seront alors un premier rempart éthique éclairé contre les excès du dataïsme¹⁸. »

Comment gérer un SI ultra communicant en assurant sa sécurité, au sens DICP (Disponibilité – Intégrité – Confidentialité – Preuve)¹⁹, le respect des normes et des lois, et donc les libertés individuelles ? Comment envisager l'interconnexion de dossiers médicaux, de dispositifs technologiques (scanners, IRM, pacemakers, pompes à insuline ou à morphine connectés et pilotés à distance, applications techniques et fonctionnelles dans le Cloud), d'accès certifiés et de possibilités d'actions par des milliers de profils utilisateurs (du patient au médecin, des acteurs médico-sociaux aux constructeurs d'objets et éditeurs de logiciels), l'ensemble au sein d'un espace de confiance ? Les réflexions en cours sont abondantes et plutôt bien coordonnées : on trouve du réalisme technique et un travail de fond sur l'éthique, dont la CNIL²⁰, le CNOM²¹, le Ministère des Solidarités et de la Santé, l'ANSSI, l'ASIP Santé, l'ANAP, la HAS et l'APSSIS sont les principaux producteurs.

¹⁴ Gilles Babinet - *L'Ère Numérique, un nouvel âge de l'humanité*, éditions Le Passeur, janvier 2014.

Gilles Babinet - *Big Data, penser l'homme et le monde autrement*, éditions Le Passeur, février 2015.

¹⁵ Guy Vallancien - *La médecine sans médecin ? Le numérique au service du malade*, Paris, Gallimard, 2015.

Guy Vallancien - *Homo Artificialis, plaidoyer pour un humanisme numérique*, Paris, éditions Michalon, 2017.

¹⁶ Yuval Noah Harari - *Sapiens : Une brève histoire de l'humanité*, Paris, Albin Michel, 2015.

Yuval Noah Harari - *Homo Deus : Une brève histoire de l'avenir*, Albin Michel, 30 août 2017.

¹⁷ https://fr.wikipedia.org/wiki/Population_mondiale

¹⁸ Dataïsme : la religion des données. Yuval Noah Harari – « *Sapiens : Une brève histoire de l'humanité* », Paris, Albin Michel, 2015 et « *Homo Deus : Une brève histoire de l'avenir* », Paris, Albin Michel, 2017.

¹⁹ https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_de_l'information

²⁰ Cahier IP 2 – 2013 ; https://www.cnil.fr/sites/default/files/typo/document/CNIL_CAHIERS_IP2_WEB.pdf

²¹ « De la e-santé à la santé connectée » - 2015 <https://www.conseil-national.medecin.fr/node/1558>

« Il s'agit du second rempart éthique, essentiellement axé sur les volets juridiques, étatiques et européen, fragilisé par la mondialisation et le caractère planétaire des interactions numériques. »

Les SIS sont en pleine mutation, impulsée par le programme Hôpital Numérique et le nouveau programme e-Hôp 2.0, par les fusions des systèmes d'information des établissements dans le cadre de la réforme des GHT (plus de 1300 SIH à 135 SIS de GHT) et par les obligations de qualité des SI imposés par la HAS, la PSSI-MCAS, la PGSSI-S et la certification HDS. 2018 et la mise en oeuvre du Règlement Général européen sur la Protection des Données (RGPD) parachèvera cette lourde charge de mise en conformité des SIS, avec, comme conséquence directe, une externalisation d'une large partie de ceux-ci vers des opérateurs privés dont la sécurité et la protection des données constituent le coeur de métier. Il s'agit de la troisième vague d'informatisation des établissements de Santé, après les fonctions administratives et de support, puis les fonctions médicales avec les DPI, les PACS, les progiciels de Laboratoire, de prescription médicamenteuse, de blocs opératoires, de management des urgences ... De grands projets régionaux et nationaux poussent cette modernisation, avec des progiciels en réseaux, des messageries médicales sécurisées, des déploiements d'outils de télémédecine.

Le développement massif de la chirurgie et de la médecine ambulatoires, objectif réaffirmé en octobre 2017 par Madame Agnès Buzyn, Ministre des Solidarités et de la Santé²², l'impulsion donnée à la télémédecine « qui va être mise au coeur des politiques publiques » (Olivia Grégoire, Députée LREM lors d'une conférence le 3 novembre 2017)²³ et le design des parcours de soins nécessitent la mise en réseau d'un ensemble hétérogène de professionnels de Santé : Médecins, Hôpitaux, Libéraux, Pharmaciens, Maisons médicales, Psychologues, Personnel soignant ... Le système est donc intrinsèquement communicant ou cherche à l'être, quelle que soit la qualification des communications ! La complexité de l'ensemble est redoutable. La mise en réseau et la circulation de nos données de santé ne peuvent se faire que sous contraintes sécuritaires majeures. Et il y a, à ce stade, encore un long chemin à parcourir.

Depuis une dizaine d'années, en France et à l'étranger, les dangers, longtemps évoqués, sont matérialisés et les prises de conscience se font, avec brutalité. Vols de données de santé et mise en vente de celles-ci, chantage à la disponibilité de matériels médicaux critiques, actes de malveillances à conséquences vitales, fuites d'informations de santé et conséquences juridiques et humaines, détections de failles de sécurité majeures font partie de la vie des structures de santé et alimentent les médias hebdomadairement. Le darknet permet l'accès à des services de vente d'ordonnances et d'arrêts maladie « officiels », pour quelques euros, et plusieurs dizaines de bases de données médicales sont en vente, proposant des volumes compris entre 100 000 et plusieurs millions de

²² http://www.lemonde.fr/sante/article/2017/10/05/buzyn-fixe-l-objectif-de-70-de-la-chirurgie-realisee-en-ambula-toire-en-2022_5196776_1651302.html

²³ <http://www.latribune.fr/entreprises-finance/industrie/chimie-pharmacie/nous-allons-mettre-la-telemedecine-au-coeur-des-politiques-publiques-756673.html>

dossiers médicaux partiels d'individus. Il existe une cotation du dossier médical, régulièrement évaluée sur une fourchette allant de 35\$ à 250\$. Voler des dossiers de santé numériques est donc une activité criminelle lucrative.

Les systèmes numériques médicaux produisent des peta octets et bientôt des hexa octets (10 puissance 18) de données. Tout est en train d'être stocké sur des infrastructures techniques complexes, virtualisées, redondées, parfois chiffrées. Celles-ci sont partout : au coeur des 1389 Centres Hospitaliers (CHR / CHU, CH, autres établissements publics)²⁴, des 7394 EHPAD²⁵, des centaines de cliniques du secteur privé, des milliers d'autres entités de soin de type USLD, SSR, laboratoires de biologie et d'anatomo-cytopathologie, centres d'imagerie, mais aussi dans les ordinateurs de nos médecins généralistes, sur des plates-formes régionales ou territoriales de santé (Dossier Communicant de Cancérologie, d'hématologie, d'imagerie...), dans des applications médicales diverses, tournant sur des supports multiples, associées à des objets connectés ou communicants de santé. La diversité et l'éparpillement des données, avec un contrôle d'usage quasi impossible pour le moment, posent un réel problème.

Tout va circuler, dialoguer et calculer de plus en plus vite, pour notre plus grand bien-être. Nous aurons d'ici à 20 ans une dizaine d'applications et d'objets communicants directement liés à notre santé, en mode gadget, en mode dispositif médical ou en mode « imposé » par notre mutuelle, voire par la sécurité sociale, pour le calcul du bonus / malus lié à la prise en compte personnalisée de notre santé.

Le marché du *Big Data*, c'est 60% de croissance par an, avec 55 milliards de dollars en 2016 évalués par le Gartner Group et 4,4 millions d'emplois induits.

« Selon une étude menée par MarketsandMarkets, le marché du *Big Data* pourrait atteindre une valeur de 66,79 milliards de dollars en 2021²⁶. »

Le *Business* a donc démarré mais il n'est ni patient, ni philanthrope. En 2016, plus de 295 000 applications médicales et dites « de bien-être » étaient en téléchargement sur les stores²⁷, pas moins de 73 millions d'objets connectés de santé étaient recensés et des centaines d'autres déferlent sur un marché mature et très dynamique (prévision à 161 millions d'objets santé pour 2020)²⁸. Patients-clients mais aussi toute une génération de médecins avides de technologies élevés dans le numérique en font usage quotidiennement. Les SIS vont devoir s'adapter vite, rester robustes tout en accueillant l'irréversible modernité. La vigilance et l'acculturation des usagers, qu'ils soient professionnels de santé, patients ou simples citoyens, sont primordiales.

Par ailleurs, la circulation massive d'images médicales pour avis ou diagnostic

²⁴ <http://drees.solidarites-sante.gouv.fr/etudes-et-statistiques/publications/panoramas-de-la-drees/article/les-etablis-sements-de-sante-edition-2017>

²⁵ <https://www.insee.fr/fr/statistiques/2569388?sommaire=2587886>

²⁶ <http://www.lebigdata.fr/marche-big-data-atteindra-67-milliards-de-dollars-2021>

²⁷ <http://research2guidance.com/product/mhealth-app-developer-economics-2016/>

²⁸ <https://www.sfrbusiness.fr/room/internet-des-objets/objets-connectes-nouveaux-partenaires-sante.html>

complémentaire via les réseaux de *Smartphones* tous constructeurs et tous opérateurs, hors de tout processus sécurisé, est un exemple de mésusage. L'usage massif d'applications médicales issues des stores et utilisées par la nouvelle génération de Médecins, souvent hors de tout contrôle des Directions informatiques, et sans avoir pris connaissance des complexes conditions générales d'usages internationales des éditeurs, en est un autre. Objets de toutes origines, sociétés récentes et peu identifiées, conditions générales d'usage des éventuelles données collectées opaques, qualité du développement des applications inconnue, labellisation non opérationnelle, sont autant de questions cruciales qu'il est temps de se poser.

Vous aurez donc compris que pour ajouter à la complexité initiale, l'apparition rapide et massive d'objets connectés de santé et leur appropriation tant par les patients que par les professionnels de santé, relance avec force le dossier sécurité, sous tous ses aspects : techniques, territoriaux, juridiques et pose des questions morales. Albert Einstein prévenait : « Le monde que nous avons créé est le résultat de notre niveau de réflexion, mais les problèmes qu'il engendre ne sauraient être résolus à ce même niveau ». Il ajoutait : « Il est hélas devenu évident aujourd'hui que notre technologie a dépassé notre humanité ».

De plus, selon les études (Gartner et IDC), il est attendu entre 80 et 200 milliards d'objets connectés à horizon 2020²⁹. Comment construire un usage sage, raisonné et conscient de ces nouveaux objets ? Comment classer ce qui aura vraiment un impact positif sur le parcours de soins et ce qui relèvera du gadget ? Comment les Médecins vont-ils accorder, ou non, leur confiance à ces outils, et avec quelles garanties ? Et la nouvelle génération, s'en préoccupe-t-elle, finalement ? Et qui va payer ?

Ce sont des questions cruciales dont les réponses vont fonder les modalités d'un usage pour longtemps, avec une irréversibilité évidente des options prises en début de processus. La philosophie humaine et l'évolution des sociétés vont également réviser de fond en comble le concept de confidentialité³⁰. Les nouvelles générations, et mêmes les plus anciennes, abordent très facilement leurs problèmes de santé, sur les réseaux dits sociaux, sur les forums spécialisés, laissant partout la trace de leurs pathologies ou de leurs petites souffrances quotidiennes. Ces données sont massives, produites chaque jour, directement par les patients, conscients ou inconscients de dévoiler eux-mêmes, entièrement ou par petites briques, leur dossier médical, de façon quasi irréversible. Nos données personnelles circuleront, seront analysées, traitées, pour apporter en permanence les bonnes réponses à nos désirs. En ce qui concerne la santé, il en sera de même. L'objet connecté de santé est le dernier rempart avant le corps connecté, nouvel essor que nous préparent les nanotechnologues : des microrobots qui nous répareront en temps réel et qui sont déjà bien réels au sein des programmes de nanorobotique. L'ignorance relative aux conséquences de

l'usage est le principal débat, il est d'ordre éthique, et l'éducation des populations est la seule réponse connue. Nous avons tous une responsabilité à prendre et à assumer concernant le contenu de notre futur, la recherche de l'équilibre entre le bien et le mal étant toujours le cœur de la question.

« Les citoyens-patients constitueront le troisième rempart éthique, en tant qu'usagers exigeants et souhaitons-le, éclairés. »

²⁹ <http://www.gie-gers.fr/objets-connectes-une-revolution-dans-lindustrie-de-la-sante/>

³⁰ Adieu confidentialité – DH Magazine N°151 – 2ème trimestre 2015 ; p. 62.

5 / L'HUMAIN AU COEUR DU DIGITAL



de Sophie Floreani

CEO - ARA & CO³¹, Innovation Managériale
et Transformation Digitale,
Conférencière, Formatrice et Enseignante

Un nouveau monde et un changement de paradigme :

La société dans laquelle nous vivons n'a plus rien à voir avec celle de mes parents ou de mes grands-parents. Pourtant issue de la Génération X, je fais désormais partie de la Génération C : Génération Connectée, autrement définie ainsi : la génération Y (*Digital Natives*) plus ceux de la Génération X qui sont *Digital Addict*. Avec 3, 8 Milliards d'individus connectés à Internet dans le Monde³², nous sommes passés dans l'ère digitale. Cette dernière bouleverse nos modes de vie, nos modes de consommation, nos modes de travail. Elle nous ouvre un boulevard sur l'information et la communication et modifie radicalement nos modes de fonctionnement. En somme, nous vivons autrement et nous avons intérêt à nous adapter pour profiter de ce qu'elle peut nous offrir et de nous permettre d'offrir aux autres.

Le digital rend à chacun sa souveraineté³³. Car finalement, il répartit le pouvoir en cassant les silos et les monopoles du savoir et de l'information. L'individu n'est plus seulement considéré au quotidien que d'un seul point de vue : consommateur, fournisseur, parent, homme ou femme. Il est considéré dans sa globalité. Nous sommes entrés dans une ère de changement permanent, de disruption, où les maîtres mots de la survie sont réactivité, adaptabilité et donc innovation.

Le succès des plateformes Internet et de l'économie collaborative montre les bouleversements induits dans l'économie et dans nos modes de vie. Les « disrupteurs » comme Uber, Airbnb, Amazon ou Netflix en sont la preuve vivante. Nos usages changent et nous sommes chaque jour plus nombreux à y participer. Dans les pays développés, qui n'a jamais utilisé le Web pour réaliser un achat, chercher une information, ou réaliser une démarche administrative ? Le phénomène se mondialise et par exemple, le téléphone portable est devenu omniprésent dans le quotidien des Africains à des fins d'utilisation de messagerie et de réalisation de paiements.

³¹ www.ara-and-co.com

³² Blog du Modérateur août 2017.

³³ Expression de Thierry Jadot dans son livre « la fin des Rentiers » (Débats publics – Novembre 2016).

Vigilance et Éthique :

« Le point fondamental de cette révolution numérique, c'est de rester dans l'Humain et les valeurs afférentes que sont l'éthique, l'équité, le respect, la confiance, la bienveillance. »

Comment ne pas risquer de dévier vers la course au pouvoir et au profit en utilisant la nouvelle arme que sont devenues les *Datas*. Que penser des monopoles détenus par les grands acteurs du numérique, les fameux NATU (Netflix, Airbnb, Tesla et Uber) et les GAFAs (Google, Apple, Facebook et Amazon) ?

Comme dans toute (r)évolution économique et sociétale, il y a des bénéfices et des inconvénients. Car nos modes de vie moderne nous mènent lors de chacune de nos connexions sur Internet à y laisser nos données de nature personnelle ou professionnelle. Tous les utilisateurs des réseaux sociaux et d'Internet alimentent eux-mêmes, par un libre consentement, le vaste empire de connaissances de la Toile. Il est important que l'internaute en soit bien conscient car ses données seront reprises par de multiples acteurs ; de même le contenu de ce que vous publiez peut-être repris par n'importe quelle personne privée ou entreprise³⁴ ; ce qui explique les publicités « ciblées » qui s'affichent sur l'écran lors d'une connexion.

Les entreprises, lorsqu'elles vous demandent de remplir vos données ou vous proposent des cadeaux dans le cadre d'une opération commerciale ou d'un devis en ligne en font de même. C'est une façon de mieux connaître ses clients ou ses prospects, pour proposer un service ou produit qu'elles imaginent correspondre davantage à vos attentes.

Danger ou opportunité ?

Je fais partie de celles qui considèrent que toute évolution est une opportunité à condition d'être vigilants au maintien des valeurs humaines et notamment, dans le cadre de l'utilisation des données, de l'éthique.

Il est donc indispensable et non négociable, si l'on veut maintenir ces valeurs, d'utiliser les données au bénéfice de l'Humanité : au sens des avantages qu'on peut apporter à l'Humain en général via l'amélioration de sa qualité de vie, voire de sa vie.

L'utilisation d'algorithmes dans la santé semble ainsi promettre des avancées considérables, quant à la possibilité de certains algorithmes d'anticiper des risques de cancers ou autres maladies graves en fonction du mode de vie d'une personne et de ses antécédents génétiques. Oui mais ... qui les utilise et dans quel but réel ? Ainsi, quelle certitude a-t-on que l'assurance qui va couvrir un client sur la base d'algorithmes et de l'utilisation des données numériques le fait dans un objectif bienveillant ? L'important est de s'assurer que les valeurs profondes et incarnées de l'entreprise - utilisant des données - respecte la dignité Humaine et considère chaque personne d'une manière équitable, sans risquer de tomber dans l'iniquité de traitement et une nouvelle forme de discrimination.

³⁴ Twitter met en place de nouvelles conditions d'utilisation à compter d'octobre 2017, à savoir : « Twitter, ou ces autres sociétés, organisations ou personnes privées, pourront utiliser ainsi le Contenu que vous aurez soumis, publié, transmis ou de quelque autre façon mis à disposition via les Services sans que vous puissiez prétendre à une quelconque rémunération au titre de ce Contenu ».

« L'idée d'un label peut être un élément de réponse ; encore faut-il valider l'indépendance de ce label et considérer les critères à partir desquels il est construit. »

L'Humain dans tout ça ?

Quand on voit comment l'utilisation des données peut améliorer notre vie, on a tous envie d'y aller, tant que cela reste pour notre bien-être. Car le digital remet l'Humain au centre. Au centre de quoi, direz-vous ? Au centre de tout ! De la société, de l'entreprise, de l'économie, de nos vies ! Le digital, en renversant le pouvoir établi, démocratise l'information et la communication, et permet une liberté d'expression. Il remet chaque personne en capacité d'être acteur dans la société ; le pouvoir des pétitions pour empêcher ou protester contre une loi, un jugement, une décision gouvernementale n'est plus à démontrer. Les manifestations traditionnelles de rue, où chaque manifestant est physiquement présent sont de plus en plus relayées par le Net, accessibles au plus grand nombre. Le site *change.org* en est une parfaite démonstration.

De plus en plus, les instances politiques se mettent à l'écoute des concitoyens en leur demandant leur avis et des propositions par des sites de consultations en ligne, permettant ainsi de cocréer des mesures réellement efficaces car adaptées aux besoins. La Toile permet de trouver des emplois d'une manière « augmentée ». Je fais partie d'un collectif bénévole sur Twitter intitulé *#i4emploi* qui a permis à environ 200 personnes de trouver un travail par un simple retweet des membres du collectif ! Les possibilités de recrutement sont élargies pour les demandeurs d'emplois : ainsi la dynamique start-up COOP-TIME recrute par cooptation *via* les réseaux sociaux. Pour chaque emploi trouvé, le *coopteur* reçoit 700 € et le demandeur d'emplois a trouvé un travail !

En dehors de l'environnement économique, le digital est également une opportunité dans la vie de tous les jours, dans les relations humaines personnelles. Jusqu'à il y a quelques mois, j'avais encore ma grand-mère italienne de 105 ans. Etant éloignée de moi, nous échangeons par l'intermédiaire du portable d'une de ses auxiliaires de vie des petits films sur WhatsApp. Quelle joie pour chacune de nous de pouvoir se voir, se parler ... alors où se trouve le point d'équilibre entre le fait de laisser des données sur le Net et le bonheur, pour les êtres humains que nous sommes, d'une telle facilité de communication ? Quel est le *delta* entre l'inconvénient de libérer ses données et le bénéfice que l'on retire de l'usage d'Internet ? Quel coût et quelle valeur réelle représentent l'utilisation d'Internet pour les parents d'un enfant malade qui parviennent à financer une prise en charge médicale pour leur enfant, grâce à un site de *Crowdfunding*, sans lequel ils n'auraient pas pu le soigner ?

En conclusion, il me semble essentiel de vivre en phase avec notre société digitale, donc nécessairement en laissant nos données lorsque nous utilisons Internet, cependant en toute conscience et en demeurant vigilants sur les informations que nous libérons pour le plus grand nombre.

« Le plus beau métier d'homme est le métier d'unir les hommes avait dit Antoine de Saint Exupéry. Osons considérer que le digital est une formidable opportunité pour l'être Humain, à condition de faire des données un usage utile au bénéfice de l'Humanité. »

6 / VERS UNE PLUS GRANDE PRUDENCE SCIENTIFIQUE AUTOUR DU TRAITEMENT DES DONNÉES NUMÉRIQUES ...



d'Alban van Landeghem

Pharmacien Industriel

De l'antiquité à nos jours, la prise en charge du patient n'a cessé d'évoluer, vers une connaissance toujours plus approfondie de la pathologie. L'invention du stéthoscope, par René Laennec en 1815³⁵, la découverte de la structure de l'ADN par Watson et Crick en 1953³⁶, ont chacune transformé, à leur époque, de manière spécifique, la prise en charge médicale. Cette accélération de la connaissance, a été mue par le progrès des technologies, mais aussi la recherche constante de la vérité et des connaissances³⁷. Un exemple de cette recherche est la théorisation, dans les années 1980, de la médecine basée sur les faits³⁸. En ce début du XXI^{ème} siècle, la médecine connaît une nouvelle révolution, avec l'avènement de l'exploitation massive des données de santé³⁹. Que cela introduit-il ? Quel est le statut actuel de ces données ? Quel sera l'impact pour la médecine ? Que cela va-t-il apporter à la dyade patient-professionnel de santé ? À quels risques les patients devront-ils faire face ? Quelles recommandations adopter pour la gouvernance de ces données ?

C'est un fait : les capteurs ont envahi les sphères individuelles et industrielles. Désormais les professionnels de santé libéraux, mais aussi les établissements publics hospitaliers génèrent des quantités de données tout au long du parcours de soin du patient. L'exploitation de ces dernières et leur croisement constituent un changement de paradigme dans l'approche diagnostique et médicale⁴⁰. Ces masses de données, sont telles, que seule une automatisation validée et soigneusement conçue, deviendra désormais capable de procurer une lecture synthétique, en renseignant le professionnel de santé, tout en contribuant à sa prise de décision⁴¹. Il en découle que le patient court le risque, avec ou contre sa volonté, de se retrouver assimilé, voire réduit à « son équivalent » en données de santé⁴².

³⁵ Source Internet : https://fr.wikipedia.org/wiki/René_Laennec

³⁶ Source Internet : https://fr.wikipedia.org/wiki/Acide_desoxyribonucléique

³⁷ « Tous les hommes aspirent à la connaissance », Aristote, *Métaphysique*, I, 1.

³⁸ Source Internet : https://fr.wikipedia.org/wiki/M%C3%A9decine_fond%C3%A9e_sur_les_faits

³⁹ Colloque *Big Data* et Santé, 2016. Source internet : <http://solidarites-sante.gouv.fr/actualites/evenements/article/colloque-big-data-en-sante-quels-usages-queles-solutions>

⁴⁰ ASIP Santé 2013. Source Internet : <http://www.esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-1>

⁴¹ *La médecine sans médecin*, Guy Vallancien, Gallimard, 2015, p.203

⁴² *Big Data Privacy : the datafication of personal information*, Mai JE (2016), *The Information Society*, 32 (3), 192-199.

Cette nouvelle approche, introduit un défi éthique⁴³, affectant l'intimité même de chaque individu, et à plus large échelle, sa sphère de libertés⁴⁴.

Face à ces changements majeurs, la Commission Européenne a délivré depuis le 27 avril 2016, un nouveau règlement concernant le traitement des données à caractère personnel. La nature des données de santé a même été clarifiée par ce règlement⁴⁵ et ces dernières sont désormais définies comme : l'ensemble des données se rapportant à l'état de santé d'une personne qui révèlent des informations sur son état de santé physique ou mentale, passé, présent ou futur. Cette définition, en demeurant très large, concrétise un cadre d'actions pour tous les acteurs, qui participeront aux traitements de données. Leur catégorisation bien-être, génomique ou autre, procurera des restrictions particulières le cas-échéant. Jusqu'à présent, la réponse Française et Européenne demeure de sanctuariser les données de santé, d'une manière similaire à celle du traitement réservé pour les organes.

Tous ces nouveaux usages liés à l'exploitation massive des données, auront un impact majeur sur l'exercice de la médecine, comme les autres progrès technologiques en ont eu avant. En 1997, Jean-François Mattei⁴⁶ écrivait : « Si l'instrument est le prolongement des sens du médecin, il ne doit pas s'y substituer, ni même les occulter... Il ne faudrait pas que l'apport indiscutable des nouvelles méthodes d'exploration fasse passer au second plan le dialogue avec le patient...Le médecin, super spécialiste...ne peut se limiter à une connaissance partielle et ponctuelle de l'homme, sauf à se laisser entraîner dans une médecine déshumanisée, qui oublierait délibérément cet ensemble harmonieux du corps et de l'esprit, fondement de la nature humaine et de son caractère sacré ».

Ainsi, la relation patient-professionnel de santé se retrouvera modifiée, mais, cette dernière ne sera pour autant pas renversée. En effet une grande part de la relation médecin-patient s'opère en dehors de la donnée et demeurera subjective et non quantifiable⁴⁷.

Dans ce concert, le patient apparaît toutefois très vulnérable et n'a pour lui que la confiance qu'il accorde dans le système de soins. Or ce dernier laisse actuellement transparaître des failles, liées essentiellement à une absence de recul sur le sujet de l'exploitation massive des données de santé. En effet, une faiblesse de la sécurisation des données, ou une exploitation frauduleuse de ces dernières, portent directement atteinte à la dignité du patient⁴⁸. Dans certains cas, ces données sont spécifiquement sensibles, *a fortiori* s'il est question de données génomiques, qui par nature constituent une signature unique, par définition jamais anonyme.

⁴³ Rapport du Comité International de bioéthique (CIB), *Big data* et Santé, 2016

⁴⁴ *Big Data and due process : toward a framework to redress predictive privacy harms*, Crawford K & Schultz J, 2014, MIT, Centre for Civic media

⁴⁵ Règlement Européen Avril 2016. Source Internet : <http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR>

⁴⁶ *De la médecine à la santé*, Flammarion 1997. Jean-François Mattei

⁴⁷ *L'empathie dans la relation médecin-patient*, 2002, Vannotti M, n°29, p213-237

⁴⁸ Source Internet : http://solidarites-sante.gouv.fr/IMG/pdf/5-_avis_citoyen_big_data_en_sante.pdf

« Dans un récent essai sur les données génétiques⁴⁹, la CNIL concluait : c'est pourquoi l'extrême sensibilité des données génétiques, les « convoitises » multiples dont elles font l'objet et l'importance des enjeux éthiques sous-jacents justifieraient l'adoption d'une convention bioéthique internationale assurant une réelle protection de ces données au plan mondial. À cet égard, l'Europe pourrait donner l'exemple. »

Il semble que cette remarque soit frappée de bon sens. Enfin l'exploitation des données massives introduit un nouveau défi, celui de la vérité. Les critères de modélisations algorithmiques ne sont absolument pas comparables aux critères de véridiction scientifique. La répliquabilité des opérations algorithmiques, par exemple, est quasiment impossible dans un contexte dans lequel les jeux de données sont en expansion continue⁵⁰.

Par ailleurs, le traitement des données massives doit être considéré dans le contexte de sa finalité, à savoir, de permettre une compréhension rapide des ensembles et de déduire un comportement analysé sur des échantillons de sous-populations prélevés dans une masse. Ces calculs sont obtenus par l'élaboration de corrélations. Or les liens constitués par ces corrélations, ne préjugent pas de la nature de ces liens. Entre corrélation fortuite et causalité efficiente, il existe un écart, que le récipiendaire des résultats obtenus devra garder en mémoire, avant de ne tirer des conclusions trop hâtives.

En conclusion, si la valeur positive de l'exploitation des données massives apparaît évidente, la nature extrêmement complexe de sa mise en oeuvre (mathématique mais aussi technique) appelle à la prudence. Albert Einstein ne disait-il pas : « Le progrès technique est comme une hache qu'on aurait mis dans les mains d'un psychopathe ».

« Sans sombrer dans une crainte paralysante, il semble urgent qu'au niveau international une gouvernance s'organise. »

Ainsi, des réflexions qui mèneraient à la création de standards de qualité sur la sécurisation des données de santé, sur l'exploitation bénéfique de ces dernières par les établissements dont l'objet moral est dédié à la santé, au profit du plus grand nombre, auraient très certainement la vertu de rassurer les utilisateurs et les communautés scientifiques. Sans cela, il apparaît évident, que les autorités de santé réagiront⁵¹ dès la première déviation, qui souhaitons-le, préservera les patients d'un trop grand dommage collatéral ...

« Sciences sans conscience n'est que ruine de l'âme. » Rabelais

⁴⁹ *Les données génétiques*, CNIL, La Documentation Française, 2017.

⁵⁰ *Des données et des hommes, Droits et libertés fondamentaux dans un monde de données massives*, 2016, Rouvroy A, Conseil de l'Europe.

⁵¹ Epître de Saint-Paul aux Galates, 3.16-22 « Alors pourquoi la loi ? Elle a été ajoutée en vue des transgressions ».

Chapitre 2 : La « datasphère » et ses applications numériques



D'une manière générale, la technologie permet à l'Homme, en lui procurant des outils toujours plus performants, de construire un univers socio-économique propre et d'innover par rapport à cette construction. Les nouvelles technologies favorisent la circulation d'une information multiforme : celle-ci nécessite moins de place et devient plus facile à déplacer, à partager, voir même à vendre. Des codes morse en passant par des fils télégraphiques, nous sommes désormais propulsés dans l'ère du numérique où jpeg et mp3 se côtoient dans les réseaux de l'Internet où l'information est devenue plus que jamais immatérielle. Conformément à la loi de Moore (1985), la technologie permet désormais de traiter des millions d'informations en quelques instants. Chaque jour, nous semons sur la toile des dizaines de petites pierres numériques qui dessinent et consolident un peu plus l'édifice des *Big Data*. Comme une « pyramide du savoir » surgissant un beau jour dans le désert égyptien, voici un nouvel univers en train d'éclore sous nos yeux. Et contrairement aux monuments des pharaons, ce secteur croît de manière exponentielle et sans limites.

Ainsi, depuis une vingtaine d'années, la croissance constante des NTIC dans la société contribue à apporter un nouvel espace d'accès aux données numériques pour les citoyens. Avec la croissance d'internet, de l'usage des réseaux sociaux, de la téléphonie mobile, du *Cloud Computing*, des objets connectés et communicants, l'automatisation des échanges de données, l'information est aujourd'hui plus abondante que jamais et sa croissance est chaque jour plus rapide. L'informatique des *Big Data* se renouvelle tous les jours pour traiter une énorme quantité de données, souvent non structurées, en des temps record. Cela se traduit par le développement inéluctable des écosystèmes et technologies numériques à venir (*Big Data*, Intelligence Artificielle (IA), plateforme, IoT (*Internet of Things*), *Blockchain*, système biométrique, réalité virtuelle voire augmentée, Nanotechnologies, Biotechnologies, Informatique et sciences Cognitives (NBIC), informatique quantique, bio-impression tridimensionnelle, etc.). Ceci aboutit donc à une société dans laquelle les NTIC jouent un rôle majeur et central notamment dans notre société numérique. C'est pourquoi, il est essentiel de s'intéresser avant tout à l'environnement où se génère et se propage l'information (appelé aussi «datasphère»). Cette infosphère représente un espace numérique constitué par un patrimoine persistant et volatile dans un espace géographique souvent indéterminé. Elle est par essence un environnement intangible et immatériel, ce qui ne le rend pas pour autant moins réel ou moins primordial. A cette «datasphère» est reliée l'ensemble des logiciels et autres outils technologiques gérés par ce responsable ainsi que l'ensemble de leurs utilisateurs légitimes.

Elle se compose d'un ensemble de sujets et d'objets qui gravitent autour des dispositifs informatiques. Elle comprend également toutes les données appartenant à un individu (ou personne morale) et toutes les données qui le concernent, mais qui sont en dehors de son centre de gravité (sécurité, politique, etc.). En conséquence, ces NTIC et leur environnement digital suscitent des questionnements à la fois d'ordre technique, organisationnel, stratégique, économique, moral, voire sociétal. Autant de questions qui nous amènent tout naturellement à réfléchir sur les changements environnementaux nécessaires à apporter afin de tendre vers un fonctionnement optimal des NTIC.

1 / L'HOMME BIONIQUE ET NUMÉRIQUE EST-IL DÉJÀ AU MILIEU DE NOUS ?



d'Alban Jarry

Président Délégué - École Polytechnique d'Assurances

Jamais, je n'avais imaginé rencontrer un héros des temps modernes capable d'être un cobaye en se faisant implanter un système révolutionnaire dans sa boîte crânienne pour de nouveau entendre. Jamais, je n'avais imaginé que le transhumanisme était déjà au cœur de nos vies et pouvait en transformer positivement certaines. Jamais, je n'avais imaginé que l'un des cinq sens pouvait renaître grâce aux inventions et interventions humaines. Jamais, je n'avais imaginé que grâce au numérique et aux réseaux sociaux, j'aurais pu me lier d'amitié à un homme bionique et découvrir sa force et son courage.

Réparer des sens ?

En prenant le risque de devenir complètement sourd, pour le reste de sa vie, Guillaume Rovere⁵² a montré par son courage que les techniques modernes pouvaient aussi offrir une seconde naissance et permettaient une re connexion avec le monde de l'écoute. Par un boîtier électronique, et numérique, le pouvoir de l'audition est ainsi réapparu chez lui. La technologie a montré les bienfaits qu'elle pouvait apporter. L'opération n'a pas été sans douleurs, et l'appareillage a failli être rejeté après l'opération par ce corps qui décide finalement de tout ! Depuis, un homme bionique s'est dévoilé et a accentué la perception positive que pouvaient procurer les nouvelles technologies lorsqu'elles étaient employées à bon escient. Cela fait de nombreuses années que les appareils numériques sont venus substituer certaines déficiences du corps humain. Aux Etats-Unis, déjà plus de 1 500 personnes physiquement sourdes bénéficient de cette technologie. Un autre appareil a sauvé tant de vies : le pacemaker. Une fois connecté, ces objets servent aussi à collecter des données pour veiller au bien de ces personnes et améliorer leur santé.

Limiter les risques :

Néanmoins, face au développement des piratages sauvages, ces objets ne sont pas à l'abri d'interventions externes et malveillantes. Guillaume a ainsi été victime

d'un vol. Le boîtier qui active l'appareil devenu interne lui a ainsi été dérobé. Peut-être aussi est-il possible de capter toutes les conversations qui lui parviennent électriquement. Un pacemaker peut être transformé à distance. Tel le Yin et le Yang, le numérique a ainsi parfois 2 faces et selon l'emploi qui en est fait le bénéfice peut aussi s'inverser.

C'est au milieu des années 70 que le grand public a probablement pris conscience des nombreuses possibilités que pourrait un jour apporter la science pour transformer un corps humain. Le célèbre Steve Austin, l'homme qui valait 3 milliards, est ainsi devenu le symbole de cette mutation qui allait se produire et des facultés qui pouvaient être accentuées. Ce héros de la télévision préfigurait certains pouvoirs hors normes que l'Homme pourrait démultiplier. Steve Austin pouvait aller plus vite que tout le monde, avoir une force disproportionnée ou être capable de voir plus loin. Alors que le numérique ne cesse de s'étendre et que la bascule dans une nouvelle ère de la maîtrise du corps humain a commencée, la science-fiction dévoilait que le futur était à portée de doigts. Que la digitalisation de l'espèce humaine était inexorable.

Trouver une éthique :

Cette ère de l'ultra collecte d'information dévoile de nouvelles formes de risques et de dérives possibles de l'humanité. Par l'intermédiaire de l'ultra connaissance, il est envisageable d'utiliser ces données et d'en détourner leur usage initial. De ne pas utiliser le transhumanisme dans un but de guérison mais dans une finalité de pouvoir ou de domination. Dans ce monde de l'interconnexion où tout circule, l'humanité doit réfléchir à la protection qu'elle associe à ces nouveaux usages, à ce qu'elle autorise ou non. La transparence de la destination est primordiale pour maîtriser les risques associés à un usage dévoyé des *Datas* et des technologies. La sécurité doit être suffisante pour anéantir la tentation de la fraude. Aujourd'hui, le risque est important que certains se permettent d'entendre ce qui ne doit pas être entendu et d'utiliser ce qui devrait rester confidentiel.

« En inventant le code binaire, il y a quelques années, l'Homme n'avait certainement pas envisagé qu'il deviendrait lui-même une suite de 0 et de 1 et que tous ses faits et gestes pourraient devenir une mine d'or pour lui-même ... et pour d'autres. »

La prévention au cœur de la vie :

La santé est devenue un secteur incontournable de la collecte des données et de l'utilisation des technologies du numérique. Depuis longtemps le dossier médical s'est numérisé et ne cesse de s'enrichir pour prévenir. Avec l'essor des capacités de stockage, de captation et d'analyse des données, de nouveaux parcours de soins, pour limiter les maladies, deviennent possibles. D'un mode curatif, la gestion de la

⁵² [Transhumanisme] J'ai été réparé en 30mn chrono ! <https://www.linkedin.com/pulse/transhumanisme-jai-%C3%A9t%C3%A9-r%C3%A9par%C3%A9-en-30mn-chrono-guillaume-rovere>

santé devient anticipative et participative car ces nouveaux services permettent à chaque assuré de mieux se connaître, de s'auto surveiller. Par une multitude d'objets, par un usage différent des mobiles ou des ordinateurs, le temps réel devient la norme. Ce temps que les *Datas* cherchent à repousser. Pour certains, la dépendance vis-à-vis de cette la connaissance de soi peut devenir obsession. À chaque usage des limites doivent se trouver.

Une collecte perpétuelle :

Face à cette industrialisation rapide, de nombreux acteurs se sont intégrés dans la chaîne de traitement et de collecte des données de santé.

« La mise en place rapide de règles éthiques doit accompagner ce mouvement car peu de données sont plus précieuses que celles qui concernent l'intimité de chacun. »

La connaissance du comportement ne doit pas se transformer en traque permanente. Afin d'assurer la pérennité du système et de l'offre, il est primordial d'offrir un service en adéquation avec la valeur des informations véhiculées tout au long de la chaîne et de limiter l'usage à ce qui apporte réellement de la valeur. À chaque instant, les règles du jeu de l'utilisation doivent être connues car l'ère de l'ultra connaissance ne peut se passer d'une ultra transparence. Dans cette quête perpétuelle, aucune limite n'est pour le moment connue et seules les réglementations sur l'usage des données personnelles mettent un cadre à ces utilisations.

2 / OBJETS CONNECTÉS : DEVENIR ET CONSÉQUENCES DES DONNÉES COLLECTÉES



de Valéry Ravix

Responsable informatique - Espace Ethique Méditerranéen

Les objets connectés ont envahi notre quotidien depuis quelques années déjà. Selon l'IDC⁵³, le nombre d'objets connectés en 2020 avoisinera les 30 Milliards. *Via* cette technologie, circule une quantité importante de données qui peuvent être assimilées à des données personnelles. Avant de discuter du devenir de ces données, j'essayerais de définir ce que sont les objets connectés.

Qu'appelle-t-on Objet Connecté ?

Il n'existe pas actuellement de définition officielle pour un objet connecté. Néanmoins, nous pouvons le définir de la façon suivante : il s'agit d'un objet physique fabriqué par l'homme qui possède la capacité de communiquer avec un système connecté (un autre objet ou autre). Cette définition masque tout de même la complexité de l'objet connecté que l'on va approfondir *via* le schéma d'une pyramide à quatre niveaux⁵⁴.

1° niveau : Les capteurs

L'objet connecté doit au départ capter des informations qui peuvent être très variées (pression, vitesse, température, composés chimiques, orientation, etc.). Les capteurs doivent collecter des informations les plus justes et les plus reproductibles possibles. La qualité de cette captation va induire la qualité des données et des décisions qui vont en découler. En informatique, il y a un adage classique « *Garbage In, Garbage Out* » (GIGO) que l'on pourrait expliciter de la façon suivante : si une donnée est mal renseignée et quel que soit la qualité des algorithmes de traitement, les décisions prises en fin de traitement ont de fortes probabilités d'être très éloignées de la réalité.

2° niveau : Agrégation des données

Une fois les données collectées, que celles-ci le soient directement dans l'objet ou pas, il faut pouvoir les combiner avec d'autres données. Cette agrégation permettra d'apporter une plus-value aux informations ainsi recueillies. C'est la

quantité et la qualité des données collectées qui fait l'intérêt majeur des objets connectés.

3° niveau : Analytique des objets

Cette étape va transformer une information brute en une information structurée. Celle-ci est essentielle pour mettre en place des actions ou des décisions résultant de l'analyse de ces informations.

Pour effectuer ce traitement, il faut compiler de nombreuses données provenant de nombreux objets connectés arrivant en un flux continu. Cette analyse se rapproche de celle effectuée lors d'un traitement *Big Data*. En effet, les termes qui spécifient les *Big Data* sont similaires à ceux utilisés pour l'analyse de données venant des objets connectés :

- Volume ;
- Vitesse (il s'agit du flux continu d'informations) ;
- Variété (il s'agit de la variété des capteurs et des données générées par ces derniers).

Ce traitement n'est pas une finalité pour l'objet connecté mais seulement une étape intermédiaire.

4° niveau : Action cognitive

La prise de décision ou l'action induite par l'analyse des données peut se réaliser par des humains directement ou à l'aide d'algorithmes décisionnels. Du fait de la quantité d'informations à exploiter, la majorité des actions est effectuée par des algorithmes décisionnels (avec parfois le contrôle de personnes qualifiées). Cette prise de décision peut fortement varier en fonction des capacités attribuées aux objets connectés. Nous pouvons définir 4 niveaux de capacités, du plus faible au plus important sachant que le niveau supérieur nécessite les capacités des niveaux inférieurs.

- **Niveau 1 : Le Monitoring.** C'est le cas des objets connectés les plus simples. Par exemple un compteur de pas. L'objet doté de capteurs renvoie peu d'informations qui sont traitées de façon très simple.
- **Niveau 2 : Le contrôle.** Il existe pour ce niveau un contrôle des fonctions de l'objet et un paramétrage de la part de l'utilisateur. On peut prendre comme exemple une balance connectée ou un traceur d'activités. Le traceur d'activités *via* ses capteurs et le paramétrage de l'utilisateur pourra, par exemple, calculer le nombre de calories dépensées. L'utilisateur pourra donc adapter son activité ou son régime alimentaire pour avoir une action sur son poids.
- **Niveau 3 : L'optimisation.** L'objet connecté devient plus performant grâce à la présence d'algorithmes décisionnels plus complexes. Cela permet l'optimisation du fonctionnement de l'objet. On peut prendre

⁵³ IDC : *International Data Corporation*. Premier groupe mondial de conseil et d'études sur les marchés des technologies de l'information.

⁵⁴ Dossier : Les objets connectés page 388 à 414. Dalloz IP/IT Numéro 9 septembre 2016.

comme exemple la nouvelle génération de véhicule électrique qui grâce aux différents capteurs embarqués et au traitement des différentes données est capable d'optimiser son autonomie énergétique et d'anticiper la maintenance technique nécessaire.

- **Niveau 4 : L'autonomie.** Il s'agit d'objets connectés autonomes capable de prendre en compte l'environnement pour prendre de lui-même les meilleures décisions. L'exemple le plus connu est la voiture autonome qui représente bien les capacités actuelles des objets connectés.

L'impact des Objets Connectés sur la société ?

Après cette définition de l'objet connecté, je me propose d'évoquer le devenir des données collectées et les conséquences liées au traitement de ces dernières.

Les objets connectés interagissent avec notre environnement afin de nous aider à des prises de décisions ou à effectuer des actions. Suivant le degré de complexité de l'objet connecté⁵⁵, les actions ou les prises de décisions induites n'auront pas les mêmes conséquences. Excluons pour la suite les objets connectés entièrement autonomes, pour nous consacrer aux objets induisant une décision ou une action pour l'utilisateur. Ces dispositifs après captation des données proposent à l'utilisateur des actions à effectuer. Dans le cas de données apparentés à des données de santé (rythme cardiaque, dépenses caloriques, etc.), la qualité des capteurs et des algorithmes de traitement peut donner des informations différentes à l'utilisateur qui devra prendre ou pas des décisions. Comment celui-ci va réagir ? Est-il en capacité de comprendre et de faire preuve de discernement face à ces informations ? L'on voit bien que face à cet afflux d'informations, l'utilisateur doit être en état de comprendre le fonctionnement de l'outil technologique mis à sa disposition ainsi que les conséquences éventuelles qui peuvent découler de ses actions. Prenons deux exemples pour illustrer mon propos.

Un système GPS avec qui vous partagez vos données (géolocalisation, habitude de trajets, etc.) pourra vous conseiller sur le meilleur itinéraire à prendre en fonction de la circulation et cela en temps réel. Suivant votre décision (choix de l'itinéraire proposé ou choix de l'itinéraire habituel), vous pourrez arriver en retard ou non, mais l'impact d'un mauvais algorithme reste mineur.

Un objet connecté utilisé pour le diabète⁵⁶, non apparenté à un dispositif médical⁵⁷, peut engendrer des dysfonctionnements et présenter une fiabilité et une qualité de mesure faible. Lors de cette utilisation, les informations fournies par l'objet peuvent être inexactes et induire des actions néfastes pour l'utilisateur.

À travers ces deux exemples, on observe bien que suivant le contexte et la nature des informations fournies par l'objet, l'utilisateur doit posséder un regard critique et éclairé sur l'information divulguée par l'objet.

Concernant le devenir des données, les *Data* générées relèvent généralement des données personnelles. La loi protège les utilisateurs en encadrant le traitement de

ces données générées. Néanmoins, nous faisons parfois preuve de légèreté lors du partage potentiel de nos données avec les fabricants d'objets connectés. Il est vrai que le partage est parfois nécessaire si l'on souhaite profiter de l'ensemble des fonctionnalités offertes par le constructeur. J'illustrerais ce propos par un exemple concret de partage de données personnelles. De nombreux trailers utilisent des montres GPS pour gérer leur effort et leurs entraînements. Ces objets indiquent la vitesse et la distance parcourue. En vous connectant à l'interface du constructeur (après création d'un compte et acceptation de leur politique de confidentialité), vous disposez d'outils complémentaires pour l'analyse de vos performances (dénivelé, rythme cardiaque, etc.). De ce fait, vos données personnelles alimentent la base de données du constructeur qui dispose de l'ensemble de vos informations. Ces informations à forte valeur ajoutée (détermine un profil utilisateur très précis bien que spécifique) peuvent être transférées à des tiers par le constructeur. Ce type de transfert est toutefois indiqué dans les déclarations de confidentialité. Vous pouvez masquer vos données (suppression par l'utilisateur) mais la suppression de votre compte reste une étape plus difficile. En général, cela passe par l'envoi d'un *e-mail* demandant la suppression du compte mais le constructeur se réserve le droit de refuser de supprimer tout ou partie de vos informations personnelles !

Pour conclure, on peut constater que ces technologies génèrent un flux massif de données, le plus souvent, à caractère personnel. Il ne s'agit pas d'être technophobe ou technophile mais de faire preuve de discernement lors de l'utilisation de ces différents objets connectés.

3 / L'INTELLIGENCE ARTIFICIELLE EN MÉDECINE



du Dr Loic Etienne

CEO - Medical Intelligence Service

Les facettes de l'intelligence humaine sont très variées, à la fois d'ordre physique, psychiques, émotionnelles, voire mystique, et ses domaines d'application ne se limitent pas à la mémoire, au calcul, à la manipulation des concepts et de toute autre forme d'intelligence que l'on peut apprécier dans l'art, la philosophie, et la création dans tous ses aspects. L'intelligence humaine est possiblement infinie, et sans doute non compréhensible si l'on en croit le théorème de Gödel⁶⁰ qui dit que pour comprendre un système, il faut s'en extraire. Pour comprendre l'intelligence humaine, sans doute faudrait-il en confier l'examen à une intelligence sensiblement différente de la nôtre.

Parmi ses multiples créations, l'homme au long des siècles a tenté de mimer le fonctionnement de son intelligence pour le soulager de tâches présentes ou à venir. Et de fait, grâce à l'Intelligence Artificielle (IA) et à la maîtrise des matériaux, en particulier les nanotechnologies, les robots dédiés à des tâches précises sont et seront plus efficaces que l'être humain dans ce domaine de compétence qui leur est dédié. On sait maintenant concevoir des robots capables de se déplacer dans un terrain inconnu et totalement aléatoire (une forêt sous la pluie, la planète Mars, etc.) avec autant de dextérité sinon plus qu'un être humain. Cela tient à la sensibilité de ses capteurs et à la finesse de réaction des moteurs qui animent ses diverses articulations. Est-ce pour autant une preuve d'intelligence ? Assurément non. C'est une simple capacité d'adaptation à un milieu.

D'autres voies ont été explorées, dans un domaine qu'on pourrait appeler de « l'intelligence pure », consistant à réaliser des activités purement intellectuelles de l'ordre du raisonnement. On s'est attaqué dès le XVIII^e siècle à la réalisation d'un joueur d'échec, cette discipline étant considérée comme l'un des panthéons de l'intelligence humaine. À notre époque, et grâce à l'informatique, cette démarche a donné naissance à *Deep Blue* qui battu Kasparov aux échecs, ou à *AlphaGo* de la société *DeepMind* qui a battu le champion de Go en 2016. Il ne s'agit pas seulement d'une puissance de calcul du meilleur coup à jouer,

⁶⁰ Cf. https://fr.wikipedia.org/wiki/Théorèmes_d'incomplétude_de_Gödel

mais également d'une vision stratégique, et d'une capacité à déjouer le bluff et les pièges tendus par l'intelligence humaine à l'intelligence artificielle. Gagner aux échecs ou au Go est certes une performance intellectuelle, mais seulement appliquée au domaine pour lequel on l'a programmé. L'homme reste encore le maître, mais depuis les années 2010 sa raison vacille, avec dans le collimateur l'angoisse que ces machines intelligentes un jour le surpassent.

Dès 1950, la question éthique a été posée par Asimov⁶¹ qui a en quelque sorte fixé les règles de cohabitation entre l'homme et les machines que celui-ci créé. On sent déjà poindre le vent du boulet, celui d'une intelligence créée par l'homme qui se retournerait contre son créateur. Carl 500, l'ordinateur de 2001 Odyssée de l'espace, reste encore un fantôme destiné à nourrir nos angoisses d'êtres humains dépassés par leur propre création. Mais de fait, cette intelligence nous menace-t-elle ?

Assurément non, si on estime que la machine devrait avoir pour cela une conscience d'elle-même, de son devenir, de sa sécurité et de sa perpétuation, et considérer que l'homme qui l'a créé soit devenu un ennemi. On peut raisonnablement estimer qu'on en est loin. Mais assurément oui si on considère que toutes ces notions (devenir, sécurité, perpétuation, etc.) sont programmables. Doter une machine d'une conscience artificielle n'est pas hors de portée.

Le problème qui émerge depuis 2016, c'est que l'on sait de façon très claire, et en particulier dans le domaine de la santé, que la numérisation du vivant, est un extraordinaire outil pour récupérer des données, les agréger, les partager, les faire examiner par des outils d'intelligence artificielle (*le Deep Learning*), et finalement apporter à l'homme des informations dont il ne pouvait pas soupçonner l'existence. Arrêtons-nous sur ce point dans le domaine de la médecine et faisons un bref retour en arrière : on peut faire l'approximation que la médecine occidentale a véritablement commencé avec le Siècle des Lumières et la pensée scientifique, puis avec Claude Bernard (qui a défini la notion fondamentale du déterminisme en médecine), la physiopathologie, puis dans les années 40 avec les premiers antibiotiques, la première greffe rénale en 1959, avec après, la propulsion vertigineuse des examens complémentaires (biologie, imagerie, immunologie, etc.) qui nous ont permis d'ordonner et de classer les maladies.

« Fort de ce passé récent, on peut imaginer que notre progression dans la connaissance sera exponentielle, au point de nous présenter comme évolution possible le transhumanisme. »

Sans entrer dans la polémique à ce sujet, on voit qu'un certain plafond de verre, du domaine de l'éthique, est potentiellement en passe d'exploser si le

⁶¹ Cf. https://fr.wikipedia.org/wiki/Isaac_Asimov

transhumanisme devient une réalité. Pour s'en convaincre, il suffit de constater que la quasi-totalité des questions éthiques qui alimentent les polémiques ont trait à la santé (PMA, GPA, fin de vie, euthanasie, génome, thérapie génique, etc.). Tous ces problèmes éthiques sont devenus d'une actualité brûlante parce qu'ils concernent la vie humaine, le seul souffle intangible auquel chaque individu reste accroché durant toute son existence !

J'en reviens à l'IA appliquée à la médecine. Rien de ce que l'homme peut imaginer en médecine ne peut se faire sans capteurs, sans données numérisées (mesures et contexte) et sans outils informatiques pour les analyser. On se trouve donc au cœur de l'univers des données, ce qu'on appelle les *Data*. Plongée dans le noir de la méconnaissance et des fantasmes, notre société se fait peur avec *Big Brother*, les *Big Data*, les données de santé, imaginant des monstres surgis d'appétits financiers capables par là même d'asservir les individus aux assureurs, aux politiques et aux laboratoires pharmaceutiques. Peut-être est-ce pour l'instant une peur excessive, mais « la peur n'exclue pas le danger ». Or le danger est bel et bien là, tapi dans l'ombre et prêt à bondir si des barrières éthiques ne sont pas dressées, destinée à faire obstacle à l'invasion dans nos vies d'univers fantasmatiques décrits entre autres par Orwell et Huxley qui sont bel et bien à nos portes !

L'IA a-t-elle une autonomie créatrice ? En d'autres termes, si l'IA est capable d'analyser, d'évaluer, de mesurer, voire de comprendre et d'apporter des solutions, ce sera pour l'instant dans l'univers existant, un monde connu, mesurable reportable, et transmissible sans équivoque. Mais cette IA sera-t-elle en mesure d'inventer, avec tout ce que cela suppose d'intuition, de vision claire de concepts immatériels, voire de récupération de données oniriques, mystiques, intrinsèquement puisées dans la vie de l'inventeur, puisant ses sources dans des tréfonds de son inconscient, ce que fait l'être humain quand il crée un objet nouveau ou qu'il développe une idée nouvelle ? Wagner, Debussy, Van Gogh, Kafka, Einstein... tous ces génies créateurs ont pu faire bouger les lignes par des pensées disruptives, issues d'expérience, de vécu personnel et d'intuition. L'IA aura-t-elle cette autonomie et cette individualité créatrice ? On peut actuellement penser que non ! Mais rien n'est moins certain. On a demandé à des programmes d'IA d'inventer des slogans ou des maximes : les résultats obtenus étaient soit décalés au point de n'avoir aucun sens, soit porteurs de pensées mortifères ou racistes. L'IA laissée seule face au fonctionnement aléatoire des données qu'elle a ingérée, reste pour l'instant une pâle figure d'intelligence. Mais on ne peut d'un revers de main en évacuer la possibilité.

Deux domaines échappent (pour l'instant) totalement à l'IA : la puissance du cerveau émotionnel⁶², et ce qu'on pourrait appeler l'expérience mystique. Qu'on admette ou non la réalité et l'existence de cette dernière, la moindre des logiques

scientifiques est de mettre dans toute équation la variable Epsilon, qui reste inexpugnable de toute expérimentation ou raisonnement tant qu'on n'a pas fait la preuve de son inexistence. Si on dit que $A = B + C$, c'est vrai au sens des mathématiques, mais au sens de la physique, de la chimie ou de la médecine, il serait en toute logique scientifique raisonnable de dire que $A = B + C + \text{Epsilon}$, avec Epsilon comme étant tout ce qui sort de notre simple représentation du réel. Et en médecine, la part d'Epsilon est considérable ! Elle est faite de notre inconscient, de nos talents individuels incompréhensibles, et de tout ce qui est n'est pas insérable dans nos outils de mesure car ils font appel à l'émotion et à la transcendance.

L'éthique en médecine est tout aussi complexe à définir car elle est culturelle - si profondément humaine ! - elle est confrontée à un univers aux limites inconnues (le cerveau et le corps humain), et totalement soumise aux soubresauts de l'inventivité humaine et de son *alter ego* désormais indissociable : l'IA. Tout se passe comme si nous avions inventé un scorpion, et que nous refusions de lui accorder une place dans le lit où nous dormons. Il y a en effet de quoi cauchemarder !

Ces éléments (intelligence et éthique) étant sommairement posés, on peut se demander finalement en quoi consiste l'IA en médecine.

D'abord la compréhension de la nature humaine et de l'histoire de chaque patient. Ne serait-ce que sur ce point, l'IA est confrontée à la complexité : celle du patient qui parle, qui écoute, qui manipule, qui ne dit pas tout, qui oublie... toutes données difficilement accessibles à l'IA, mais que le médecin réel sait déceler grâce à son expérience, son intuition, et son talent personnel à repérer chez son patient les éléments de communication non verbale. Mais comme on le verra plus loin, l'IA étant liée à sa capacité d'apprentissage, de reconnaissance de formes, de sons et de mouvements, on peut raisonnablement penser que l'IA saura faire la même chose.

Ensuite la capacité de recueil des données : même si l'on exclue la complexité du langage et l'incertitude de la valeur accordée aux mots (l'anamnèse), on se trouve confronté à la valeur que l'on accorde aux données des capteurs, de la même façon qu'on peut remettre en cause la valeur de l'examen clinique d'un médecin par rapport à un autre (ce qu'on appelle des données « opérateur-dépendant »). Il est vraisemblable que d'ici 5 ans, la finesse des capteurs, sera beaucoup plus fiable que les données d'examen clinique recueillies par les yeux, les oreilles et les mains des médecins.

Et enfin, la capacité d'interprétation de ces données, ce qu'en médecine on appelle le « diagnostic » ou la « décision ». Et là, il est clair que la machine du fait de sa mémoire prodigieuse et sans cesse en mouvement sera bien plus efficace que le meilleur des Docteurs House !

⁶⁰ Cf. https://fr.wikipedia.org/wiki/Théorèmes_d'incomplétude_de_Gödel

« On peut donc admettre que dans un futur proche, les systèmes d'IA seront capables de comprendre, de recueillir les données et de les interpréter. »

Mais au-delà : quel crédit apporter à toutes les préconisations de ces systèmes ? C'est le rôle de la certification (le Marquage CE). Tout système informatique d'ici 3 ans devra être certifié selon les directives européennes de mai 2017. On entend par là que chacun de ses rouages doit avoir été testé, mesuré, évalué et corrigé selon des normes précises, des protocoles et des tests cliniques. Grâce à cette rigueur scientifique, on évacuera bien des systèmes prétendument d'IA bancals ou sans utilité.

Comment définir les tâches actuelles de l'IA ? Je les exprimerai selon trois objectifs :

« Comprendre pour Agir, Apprendre pour Évoluer, Inventer pour Survivre. »

Objectif 1 : Comprendre pour Agir.

La compréhension d'une situation est fondée sur l'interrogatoire (l'anamnèse), on y rajoute les données des capteurs (ce que le médecin fait avec l'examen clinique), et on aboutit à des hypothèses diagnostiques lesquelles sont confirmées ou infirmées par les examens complémentaires (imagerie, biologie). Ce raisonnement est tenu par des algorithmes. La solution d'IA MEDVIR⁶³ est en mesure d'évoquer 750 diagnostics courants, dont 350 en urgence, et de proposer une décision. La barrière éthique se situe dans le fait que ce n'est pas la machine qui applique cette décision, mais bel et bien un être humain, en l'occurrence un médecin, la machine étant là seulement en tant qu'aide à la décision. De la même façon, Watson⁶⁴ en oncologie est en mesure de comprendre de façon sémantique le cas d'un patient et de rechercher dans la littérature qu'il a ingurgitée, la solution thérapeutique la mieux adaptée. Ce travail de super documentariste ne rend pas pour autant Watson décisionnaire de l'action à entreprendre. Ces deux exemples d'IA montrent que de la compréhension à l'action, il y a un plafond de verre à ne pas franchir : le médecin réel doit rester l'ultime décisionnaire.

Objectif 2 : Apprendre pour Evoluer.

L'apprentissage est une donnée essentielle de l'intelligence, car c'est grâce à cette capacité qu'elle deviendra jour après jour plus « sachante ». L'IA doit pour cela recueillir la confirmation ou l'infirmité de ses hypothèses. Une infirmité l'obligera soit à revoir ses algorithmes, soit à modifier les données discriminatives qui ont gouverné son raisonnement. L'intelligence humaine est alors nécessaire pour guider les pas de l'IA. En revanche, une confirmation, permettra à l'IA de créditer son raisonnement d'un « bon point » et d'en stocker les éléments dans sa mémoire. C'est cette lente et progressive acquisition qui permet un auto-apprentissage à chaque expérience positive, ce que fait le système MEDVIR.

⁶³ www.mis-medvir.fr

⁶⁴ [https:// www.ibm.com/watson/](https://www.ibm.com/watson/)

La question qui se posera sera de se demander à partir de quand ces expériences positives permettront à l'IA d'être autonome et d'utiliser ses expériences positives comme critères de décision. Par exemple si on a pu montrer avec une probabilité raisonnable, que le diagnostic A était très probable si le patient possédait les symptômes X, Y et Z, (ce qu'on appelle en médecine un syndrome) alors on peut estimer qu'on peut laisser l'IA raisonner toute seule face à ce diagnostic A. Et donc à terme, on peut envisager comme possible que la somme des expériences positives soit suffisante pour laisser la machine raisonner en toute autonomie, ce qui nous ramène en termes éthiques à la limite fixée par l'objectif 1.

Mais une autre forme d'apprentissage existe également, qui consiste à apprendre ce qui est encore inconnu et que la machine aurait compris. C'est ce qu'on espère avec les *Big data* : on analyse avec du *Deep Learning* toutes les données d'où qu'elles viennent, et on espère trouver en les examinant avec des algorithmes des corrélations que nos cerveaux humains ne peuvent réaliser. Il y a là, de mon point de vue un leurre lié au « bruit informatique ». Pour donner une image, c'est un peu comme si on espérait en enregistrant tout le bruit fait par les centaines de milliers de personnes présentes lors de l'élection du Pape, comprendre le sens de la conversation entre deux personnes au beau milieu de la foule. Cette prouesse serait possible si on éliminait le bruit tout autour. C'est ce que font les *Smart Data*, qui sont des « *Big Data* qualifiées » : on recueille des données en très grand nombre, mais celles-ci ont été contextualisées et qualifiées (horaire, lieu, contexte et symptomatologie du patient), ce qui permet d'éliminer le bruit informatique. C'est ce qui a pu commencer à être fait sur le site E-docteur.com qui a recueilli 650.000 questionnaires entièrement remplis en 2016 qui ont été horodatés et géolocalisés. Le nombre de données est insuffisant pour parler de *Smart Data*, mais si on possédait 1000 fois plus de questionnaires de ce type, sans doute pourrait-on découvrir des associations de symptômes qui feraient émerger une nouvelle connaissance.

Et là en terme éthique se pose la problématique des données de santé. Ce type de données sensibles nous confronte à la question de la propriété⁶⁵ de nos Data. Sans aller trop loin dans le raisonnement, je pense que nous ne sommes pas propriétaires de nos données, nous en sommes seulement dépositaires, car si nous pouvons dire que les 12/8 de tension nous concernent en propre, ils n'ont été possibles à recueillir que grâce à l'invention du tensiomètre en 1896. L'inventeur, le médecin italien Scipione Riva-Rocci aurait pu prétendre à une propriété puisque c'est lui qui a généré cette mesure avec son appareil. Pour donner une autre image, l'appartement que nous avons acheté et dont nous nous estimons propriétaire a appartenu auparavant à d'autres, et appartiendra à d'autres après nous. Nous sommes donc des sortes d'occupants autorisés et limités dans le temps, les « dépositaires d'un droit transmissible ». Et si on considère comme plus acceptable ce terme de dépositaire d'un droit transmissible, on peut imaginer

⁶⁵ Cf. <http://www.zeblogsante.com/sommes-nous-totalement-proprietaires-de-nos-donnees-de-sante/>

qu'à partir du moment où l'individu est protégé (des spams, des publicités, des contrats d'assurance, etc.), alors cette donnée doit être partageable et donc transmissible pour que la recherche médicale progresse.

« Sans « partage éthique de la connaissance », avec son corolaire qui est la « monétisation éthique de la connaissance », il n'est pas de Big ou de Smart Data possibles, pas d'évolution possible de l'intelligence, et donc non réalisation de l'objectif 2. »

Il y a urgence à faire bouger les lignes juridiques sur ce point.

Objectif 3 : Inventer pour Survivre.

C'est ce qui a permis à l'être humain d'avoir toujours survécu dans un environnement hostile auquel il n'était pas préparé. Et c'est ce que nous faisons chaque jour lorsque notre organisme invente des anticorps pour lutter contre tel ou tel nouveau virus. L'invention est la forme suprême de l'intelligence, puisqu'elle est capable à partir de rien ou presque, de fabriquer quelque chose qui n'existe pas. Si on parle des *Data*, la découverte de corrélations entre des événements ou des symptômes disjoints est une véritable invention capable de découvrir de nouvelles maladies ou de nouvelles explications aux événements que nous ne comprenons pas. Les machines sont donc là pour nous aider à inventer, sous notre contrôle, ce qui nous renvoie aux principes d'Asimov. Seront-elles pour autant capables d'inventer de par leur propre réflexion ? Vraisemblablement oui à terme. Et c'est là que se pose la véritable question éthique du monde 4.0 : des machines autonomes et intelligentes, munies de capteurs affranchis de toute limitation de transmission de l'information, et dialoguant entre elles à notre insu, aux mains de puissances informatiques qui pourront rationnellement décider de notre légitimité à survivre. Le monde 4.0, celui des IoMT (*Internet of Medical Things*) interreliés et communiquant est le véritable enjeu.

« Si nous ne prenons pas garde à border éthiquement le monde 3.0 actuel (les machines intelligentes sous le contrôle humain), alors le plafond de verre éthique aura explosé et nous ne pourrons plus rien y changer. Notre survie sera alors guidée par la rationalisation des machines intelligentes de notre vie, de notre survie et donc possiblement de notre disparition. »

En conclusion, l'IA hors du contrôle des humains dans un monde 4.0 non éthique a toutes les chances de nous amener à notre disparition, ou *a minima* à une nouvelle forme d'esclavage technologique. Je terminerai en citant Stephan Hawking en 2014 : « Je pense que le développement d'une intelligence artificielle complète pourrait mettre fin à l'humanité ». *Dont Acte !*

4 / DE L'INTELLIGENCE ARTIFICIELLE MIMÉTIQUE AUX SYSTÈMES AUTONOMES : QUELS OBJECTIFS ET QUELS ENJEUX ÉTHIQUES ?



du Dr Joël Colloc

Professeur des Universités - Université du Havre
Normandie Université, IDEES Le Havre UMR CNRS 6266

Histoire et évolution du paradigme d'Intelligence Artificielle (IA) :

L'histoire de l'intelligence artificielle (IA) se déroule parallèlement à celle de l'informatique durant le 19ème et le 20ème siècle. Elle débute avec les travaux d'Ada Lovelace (1815-1852) qui développa le premier algorithme sur la machine analytique de Charles Babbage (1791-1871). Ce dernier eut l'idée d'incorporer les cartes du métier à tisser de Joseph Marie Jacquard (1801) qui est considéré comme la première machine programmable. Un peu plus tard George Boole inventa la logique binaire (1815-1864) et Lewis Carroll (Charles Lutwidge Dodgson) publia un traité de logique symbolique en 1896. Ces travaux précurseurs donnèrent naissance au début du 20ème siècle aux premiers ordinateurs avec la machine de Turing proposée par Alan Mathison Turing (1936) qui, en collaboration avec Alonzo Church, Stephen Cole Kleene et Kurt Gödel et quelques autres, fondèrent les principes de la calculabilité. À cette époque McCulloch et Pitts établirent également la théorie des automates et les bases des premiers neurones artificiels. Dans la continuité de la machine de Turing, John Von Neumann⁶⁶ proposa en 1945 l'architecture générale des ordinateurs que nous utilisons toujours aujourd'hui. Par la suite, le développement exponentiel des machines durant la fin du 20ème siècle, celui des réseaux avec l'avènement d'Internet, de l'approche orientée objet dans les années 1980 constituèrent le support des systèmes à acteurs puis des systèmes multi-agents proposés dans les années 1990 pour mener aujourd'hui au développement de systèmes multi-agents autonomes distribués sur la toile ou embarqués dans des robots. L'histoire de l'informatique se déroule donc sur un peu plus de deux siècles de 1801 à nos jours.

« L'idée de créer des machines autonomes remonte sans doute à l'antiquité grecque avec les automates fabriqués par Héphaïstos relatés notamment dans l'Iliade⁶⁷. »

⁶⁶ Chazal Gérard Théorie générale et logique des automates John Von Neumann.

⁶⁷ Marcinkowski A., Wilgaux J. Automates et créatures artificielles d'Héphaïstos : entre science et fiction, Techniques & Culture, 43-44 | 2004, DOI : 10.4000/tc.1164

Ces automates étaient mécaniques, comme par exemple le canard de Vaucanson élaboré par Jacques de Vaucanson en 1738 et exposé au palais royal en 1744 qui constitua indéniablement un des premiers robots.

Les spécialistes considèrent que l'IA est née en 1956 durant une école d'été au «Dartmouth Collège», Hanovre, New Hampshire aux Etats-Unis autour de chercheurs de disciplines très diverses mathématiciens, logiciens, biologistes, psychologues, physiciens, neuropsychiatres : Ray Solomonoff, Marvin Minsky, John McCarthy, Nathaniel Rochester (IBM) et Claude Shannon, Herbert Alexander Simon, Allen Newell, Cliff Shaw, John Nash, John Holland, Nathaniel Rochester, Oliver Selfridge, Trenchard More ... avec comme objectif le développement du programme cognitiviste. C'est John McCarthy qui aurait utilisé le terme d'« Artificial Intelligence » pour la première fois, l'année précédente pour frapper les esprits et obtenir une subvention de la part de la NSF⁶⁸. En 1956, l'objectif était de créer une réplique de l'intelligence humaine en s'inspirant du fonctionnement du cerveau humain. Tous ces chercheurs ont été des pionniers et publièrent des travaux considérés comme séminaux de la nouvelle discipline AI appelée en France l'IA. L'essor des premiers calculateurs à transistors et le développement des réseaux de neurones artificiels ouvrirent des perspectives de la création à terme d'un cerveau artificiel qui devait dépasser les capacités humaines. Toutefois, cet objectif s'est révélé rapidement très complexe surtout en regard des connaissances de l'époque concernant la physiologie et du fonctionnement du cerveau. Ce désenchantement conduisit aux années noires de l'IA. Ces limites amenèrent à renforcer l'étude du fonctionnement du psychisme et du fonctionnement du cerveau comme l'a proposé Marvin Minsky dans son ouvrage « The society of Mind » (1986) et de nombreux travaux dans le champ des sciences cognitives et les neurosciences étudièrent l'élaboration des connaissances et les modes de raisonnement afin de les mettre en oeuvre dans la résolution de problèmes concrets plus ou moins difficiles. Les travaux de Jean Piaget⁶⁹ ont joué un rôle important dans ce domaine.

L'IA mimétique :

Ces limites de l'IA conduisirent à fixer des objectifs plus pragmatiques et faisables constituant à mimer les actions des spécialistes d'un domaine scientifique dans la résolution de problèmes en médecine, en économie, en géologie, en gestion, en agriculture et généralement dans tous les domaines où une expertise est disponible ... De 1964 à 1985, les ambitions de l'intelligence artificielle se réduisirent à la réalisation de systèmes experts exploitant des systèmes à base de connaissances. Le premier d'entre eux a sans doute été Dendral qui a été proposé pour l'identification de composants en chimie organique par Edward Feigenbaum, Bruce Buchanan⁷⁰ et Joshua Lederberg (prix nobel de chimie 1958) (Buchanan et al., 1989). Il sera suivi assez rapidement par le système expert

⁶⁸ Ganascia Jean-Gabriel, L'intelligence artificielle, idées reçues, ed. Le Cavalier Bleu, 2007, 127 p.

⁶⁹ Piaget J., 1967. « La psychologie de l'intelligence », ed. Armand Colin, 192p., ISBN : 2-200-32214-3.

⁷⁰ Buchanan Bruce G., Sutherland G. and Feigenbaum E.A. Heuristic DENDRAL : A Program for generating Explanatory Hypotheses in Organic Chemistry, "Machine Intelligence 4, B. Meltzer and D.Michie, ed., American Elsevier, New York, 1969.

MYCIN (projet mené de 1972-1976) par B.G Buchanan ⁷¹ et E.H. Shortliffe ⁷², pour le diagnostic et traitement des maladies infectieuses. Ces systèmes étaient fondés sur la logique formelle et une ou plusieurs bases de règles de production déclenchées et enchaînées par un programme appelé moteur d'inférence chargé d'effectuer des déductions successives et de proposer et expliquer des conclusions utiles à la prise de décision dans des domaines complexes. MYCIN était capable de fournir le cheminement logique des conclusions qu'il propose, le diagnostic et le choix d'un traitement antibiotique. Ce type de système pragmatique rencontra un vif succès et conduisit à la naissance d'une nouvelle branche de l'informatique appelée ingénierie de la connaissance et au métier de cognicien qui était chargé de recueillir et d'exprimer les connaissances sous la forme de règles logiques en interrogeant les experts humains d'un domaine : des médecins dans cet exemple. En France, à cette époque, l'IA devint une nouvelle branche de l'informatique, les pionniers furent Jacques Pitrat ⁷³, Jean-Louis Laurière ⁷⁴, Suzanne Pinson ⁷⁵, Alain Colmerauer ⁷⁶, Henri Farreny ⁷⁷, Olivier Gascuel ⁷⁸, Henri Prade ⁷⁹, Alain Bonnet, Jean-Paul Haton et Jean-Michel Truong Ngoc ⁸⁰ et bien d'autres. Plusieurs milliers de systèmes experts médicaux furent développés dans le monde, notamment en France : SAM ⁸¹, SPHINX ⁸², SUPER ⁸³, SIAMED ⁸⁴, TROPICAID ⁸⁵. J'ai effectué une étude sur un échantillon de 110 systèmes expert médicaux (entre 1964-2000) qui montrait que la plupart des spécialités médicales étaient concernées et qui recensait les modèles de connaissance utilisés ⁸⁶. La plupart des applications

portaient sur le diagnostic, le pronostic, la thérapie des pathologies, la prise en charge des patients et les études épidémiologiques des maladies. L'IA mimétique permet de nombreuses réalisations utiles aux hommes et à la société dans des domaines très variés comme la géologie, l'agriculture, l'archéologie, la gestion, la biologie ...

L'IA autonome distribuée sur le réseau Internet :

À partir de modèles orientés objets qui furent proposés pour décrire les objets, les utilisateurs et leurs interactions au sein d'un système, Carl Hewitt aux USA proposa un modèle d'acteurs et le langage Planner tandis qu'en France, Jean-Pierre Briot et Pierre Cointe proposèrent la plate-forme de langage acteurs *Actalk* fondée sur le langage objet *Smalltalk*. Ces travaux constituèrent les débuts des systèmes coopératifs qui mirent en oeuvre des entités logicielles capables de coordonner ensemble leurs actions dans le temps, de manière synergique afin de parvenir à un objectif. L'Intelligence Artificielle Distribuée (IAD) débuta avec les travaux de Reid. G. Smith ⁸⁷ sur les protocoles de négociation de contrat entre agents dans sa thèse en 1978. Dans la continuité, furent développés les premiers agents et systèmes multi-agents (SMA) qui constituèrent les descendants des langages acteurs tout en étant dotés d'une autonomie de décision et d'action. En France, Jacques Ferber ⁸⁸ fut le précurseur des SMA dès 1990 et les acteurs devinrent des agents. Aujourd'hui, on distingue d'une part les systèmes multi-agents réactifs qui organisent la coopération de très nombreux agents réactifs, mais frustrés dans leurs capacités de perception et d'actions et de communication au sein de leur environnement. Ils réagissent à des stimuli et développent des actions coordonnées comme les insectes sociaux (fourmis, abeilles...) en vue d'atteindre un objectif global qui se construit par leurs interactions et leurs ajustements mutuels afin de produire une intelligence collective émergente ⁸⁹.

Les applications sont nombreuses : la simulation de transports en logistique, de diffusion d'épidémies, de la propagation de nouvelles espèces animales ou végétales dans l'environnement... D'autre part les systèmes multi-agents cognitifs mettent en oeuvre des agents cognitifs plus sophistiqués qui possèdent une connaissance interne réflexive chargée de décrire leurs aptitudes (les actions qu'ils savent réaliser). Les plus évolués sont dotés d'une autonomie de décision, de capacités de négociation et de communication et surtout de celle de fixer par eux-mêmes leurs objectifs sans intervention humaine et de concrétiser leurs intentions sous la forme d'actions qu'ils souhaitent réaliser au sein de leur environnement en vue d'agir sur lui et d'atteindre leurs objectifs. Il s'agit de systèmes multi-agents cognitifs autonomes. Les principales applications concernent la robotique, la coopération de systèmes d'aide à la décision multi-experts, multi-domaines tactiques et stratégiques (par exemple en économie gestion) ou qui utilisent différents modèles d'apprentissage et de raisonnement comme les algorithmes génétiques, les réseaux de neurones, la logique floue ...

⁷¹ Buchanan Bruce. G., Shortliffe E.H. Rule-Based Expert Systems, The Mycin Experiments of the Standford Heuristic Programming Project. Addison Wessley, 1984, 748 p.

⁷² Shortliffe Edward H. MYCIN : A rule-based computer program for advising physicians regarding antimicrobial therapy selection,. Ph. D. dissertation, Standford University (reprinted with revisions in 1976).

Shortliffe Edward H. Computer-Based Medical Consultations : MYCIN, Elsevier-North Holland, New York, 1976.

⁷³ Pitrat Jacques, La genèse des systèmes experts, Bull INRIA, 1984, n°97, 2-8. Et, Pitrat Jacques, Métaconnaissance, Futur de l'Intelligence Artificielle, Hermès, 1990.

⁷⁴ Laurière Jean-Louis Un langage et un programme pour énoncer et résoudre les problèmes de combinatoire, Thèse d'état paris VI, 1976.

Laurière Jean-Louis Intelligence Artificielle, résolution de problèmes par l'homme et la machine, ed. Eyrolles, 1986, 473p.

⁷⁵ Pinson Suzanne, Représentation des connaissances dans les systèmes experts, RAIRO, Informatique, 1981, 15 :4, 343-367.

⁷⁶ Colmerauer Alain, Précédences, analyse syntaxique et langages de programmation, Th d'état, Grenoble, 1967.

⁷⁷ Farreny Henri, Les systèmes experts principes et exemples, ed. Cepadues, Toulouse, 1985, 254 p.

⁷⁸ Gascuel Olivier, SAM : Un système expert dans le domaine médical, Thèse 3e cycle, Paris VI, Nov 1981.

⁷⁹ Prade Henri Modèles mathématiques de l'imprécis et de l'incertain en vue d'applications au raisonnement naturel, Thèse d'état, Toulouse, 1982.

⁸⁰ Bonnet Alain, Haton Jean-Paul, Truong Ngoc Jean-Michel, Systèmes experts Vers la maîtrise technique, InterEditions, Paris, 1986, 288 p., ISBN 2-7296-0144-9.

⁸¹ Gascuel Olivier, SAM : Un système expert dans le domaine médical, Thèse 3e cycle, Paris VI, Nov 1981.

⁸² Fieschi Marius, Aide à la décision en médecine : le Système SPHYNX. Application au diagnostic d'une douleur épigastrique. Thèse de médecine, Marseille, 1981.

Fieschi Marius, Intelligence artificielle en médecine, des systèmes experts, Masson, 1986, 240 p.

⁸³ Fontaine Dominique, Le Beux Pierre, An Expert System for Rubella Consultation. MEDINFO 83, 1983. 6.

Le Beux Pierre, Les systèmes experts en médecine, Thèse de médecine, Université Paris 6, 1983, 127p.

⁸⁴ Colloc Joël, Informatique Médicale (SIAMED) Application : Logiciel original d'antibiothérapie médicale Thèse de médecine, Université Lyon 1, 1985, 229 p.

⁸⁵ Auvert Bertran, Aegerter Pierre, Gilbos Valery, Benillouche E., Bourtin P., Desve G., Landre M-F, Bos D. TROPICAID : Un système expert sur ordinateur portatif pour l'aide à la décision en médecine dans les pays en développement, In 6e Journées Int. Les Systèmes Experts & leurs applications, Avignon, 1986, Vol 1., pp.109-112.

⁸⁶ Colloc Joël, Les apports réciproques de la modélisation objet et de la connaissance médicale, Habilitation à diriger des recherches, Université Lyon 1, 2000 T1 243 p., T2 108 p.

⁸⁷ Smith R.G. 1979. The Contract Net Protocol : High Level Communication And Control In A Distributed Problem.

⁸⁸ Ferber Jacques, Carle P. Actors and Agents as Reflective Concurrent Objects : A Mering IV perspective, Proceedings of the 10th workshop on Distributed Artificial Intelligence, Bandera, Oct 1990.

⁸⁹ Drogoul Alexis De la simulation multi-agent à la résolution collective de problèmes une étude de l'émergence de structures d'organisation dans les systèmes multi-agents, Thèse Paris 6, 1993, 214p.

Ces systèmes multi-agents autonomes permettent de renouer avec l'objectif initial de l'IA des années cinquante qui est de constituer le psychisme artificiel des robots autonomes, de plus en plus anthropomorphiques avec l'intention première d'apporter une aide désirée ou non, donc acceptée ou non acceptée par l'utilisateur et ce éventuellement à son insu.

L'IA autonome : une informatique mondiale sans utilisateur :

Ce que nous appelons le numérique couple aujourd'hui le réseau de communication Internet qui a envahi toutes les activités personnelles humaines (domotique, achats, communication, smartphone, sphère personnelle privée, travail, loisirs et intime comme la santé, la famille, les comptes bancaires, etc.) et les systèmes d'IA qui organisent l'indexation automatique des connaissances et des données de tous les usagers qui fréquentent le réseau.

Les communications entre personne se font aujourd'hui principalement par le truchement des smartphones (SMS, Chat, Tweets, e-mail, réseaux sociaux) et de moins en moins directement de bouche à oreille. Au passage, les données sont stockées de manière plus ou moins permanente sur d'immenses serveurs sur lesquels nous n'avons aucun accès ni contrôle. Les rapports sociaux en sont profondément modifiés. Les objets connectés, la domotique, les véhicules intelligents, bientôt autonomes, recueillent déjà automatiquement nos données tout en nous fournissant des services dont il devient impossible de se passer et qui nous sont imposés. Autrefois, il suffisait de débrancher l'ordinateur, de jeter le *Smartphone*, mais aujourd'hui cela devient impossible sous peine de ressentir brutalement une grande infirmité et de se trouver exclu de la société⁹⁰. Actuellement, les relations humaines ne peuvent plus s'exprimer sans l'utilisation d'un dispositif numérique *Smartphone*, tablette ou ordinateur connecté par Wifi à Internet. Aujourd'hui les agents autonomes (*Chatbots*) simulent sur Internet le comportement d'utilisateurs humains, ils deviennent de plus en plus sophistiqués et donc plus difficiles à différencier des acteurs humains (Cf. Test de Turing). Ils permettent de profiler les utilisateurs de tous systèmes numériques qui échangent ses données sur Internet⁹¹. Comme ils sont reproductibles autant de fois qu'on le veut, ces agents autonomes peuvent envahir Internet, influencer les opinions et coordonner des attaques en saturant des serveurs.

« L' « *Affective Computing* » est la branche de l'IA destinée à doter les robots d'émotions artificielles. Les progrès de la réalité virtuelle ont pour conséquences de déconnecter définitivement les hommes de leur environnement réel et de les faire vivre dans un monde parallèle totalement manipulable par les géants du Web. »

Les jeux et à la réalité virtuelle constituent une nouvelle drogue numérique dont l'addiction représente un danger considérable pour l'humanité car elle permet une

⁹⁰ Ganascia Jean-Gabriel, L'intelligence artificielle, idées reçues, ed. Le Cavalier Bleu, 2007, 127 p.

⁹¹ Colloc Joël, Santé et *Big Data* : l'Etat et les individus, impuissants face aux pouvoirs des réseaux L'Espace Politique, 2015, 26, 2015-2.

manipulation à grande échelle de la population et particulièrement des plus jeunes qui perdent tous repères sociaux avec des conséquences psychologiques sur leur comportement dans la société. Les systèmes multi-agents autonomes peuvent être dotés d'une conscience artificielle fondée sur des émotions et de nombreux agents en interactions. Ils disposent de capacités de compréhension langagière, de moyens de communication et d'un accès aux données et connaissances sur Internet⁹². Leur mode de pensée artificielle est différente de la pensée humaine mais ils communiquent entre eux à votre insu et indépendamment de tout utilisateur humain.

En conclusion, les systèmes multi-agents autonomes constituent une nouvelle forme d'IA reproductible distribuée et ubiquitaire dont les agents relèguent l'utilisateur humain au rang de simple sujet d'observation dont il convient de mesurer l'activité, de profiler le comportement en vue de le contrôler et de l'influencer dans ses choix et décisions. Les données le concernant peuvent être échangées et conservées à son insu pour des utilisations qui échappent à sa connaissance. Progressivement, ce sujet perd toute liberté d'agir en dehors du réseau numérique tant il est asservi par les services qui lui sont proposés et qui lui deviennent indispensables. Une panne d'ordinateur et de *Wifi* provoque un handicap immédiat dans de plus en plus d'actes de la vie courante. Les consommateurs assujettis et dépendants de services n'en ont pas conscience car cette inféodation au numérique est progressive, insidieuse, généralisée et elle est revêtue des habits de la normalité (tout le monde est concerné). Les rares réticents aux numériques sont perçus comme asociaux, infirmes ou subversifs à la modernité et sont donc exclus d'une société où ils n'ont plus leur place où toutes les perceptions et les rapports à la réalité sont filtrés et contrôlés par les systèmes autonomes.

« L'avenir de l'humanité réside sans doute dans sa capacité à conserver une pensée humaine et une communication interhumaine⁹³. »

Lorsqu'ils sont embarqués dans des robots ou des dispositifs mécaniques comme des drones, les systèmes autonomes peuvent constituer des armes redoutables des robots tueurs avec toutes les utilisations déviantes que l'on peut imaginer⁹⁴. Ces systèmes donnent un pouvoir d'oppression considérable à ceux qui possèdent les moyens d'acquérir et de dominer ces technologies par rapport à l'immensité des sujets qui sont soumis à une nouvelle forme de dictature numérique. Les systèmes proposés par l'IA doivent rester soumis aux seuls besoins désirés et exprimés par les utilisateurs. Ces systèmes ne doivent pas imposer aux utilisateurs des services qui portent atteinte à leur liberté de décider de leur vie à leur place pour des raisons économiques ou sous le prétexte de leur procurer un supposé bien-être.

⁹² Cardon Alain, Conscience artificielle & systèmes adaptatifs, ed. Eyrolles, 2000, 380p. Et, Cardon Alain, Un modèle constructible de Système Psychique. Automates Intelligents, 2011.

⁹³ Colloc Joël, L'éthique des systèmes d'information autonomes vers une pensée artificielle in Les Cahiers du Numérique Enjeux du *big data* et identifications des données médicales, Vol 12, n°1-2/2016, 187-2011.

Colloc, Joël Une approche orientée objet pour l'élaboration d'applications médicales Thèse informatique et automatique appliquées, INSA de Lyon, 0054, 1990, 390 p.

⁹⁴ Conn Ariel, 2017, Newsletter of the Future of Life Institute, Leaders of Top Robotics and AI Companies Call for Ban on Killer Robots, <https://futureoflife.org/2017/08/20/leaders-top-robotics-ai-companies-call-ban-killer-robots/>

5/ ETHIQUE ET TIC, LA BLOCKCHAIN COMME OUTIL DE GOUVERNANCE DES DONNÉES



de Sajida Zouarhi

*Blockchain Architect, PhD Student in Computer Science
Founder of the Kidner Project,
President – eHealth & Blockchain Think Tank*

Le Token : de la Propriété comme monnaie d'échange à la gestion d'Accès comme ressource :

Il est intéressant lorsqu'on étudie les données de se pencher sur la notion de propriété. Contrairement à certains objets du monde physique, il n'y a pas de réponse simple à la question : « à qui appartiennent les données ? ». Quand un utilisateur produit des données avec un objet connecté (par exemple de type *Fitness*) et que celles-ci sont remontées sur la plateforme de l'équipementier qui ensuite les utilise « à des fins d'amélioration du service » ou plus simplement en le revendant à des tiers, s'agit-il des données de l'utilisateur en train d'être vendues à des tiers sans son consentement ? Ou est-ce la façon normale de procéder et devons-nous l'accepter ?

Dans ce cas on note que l'équipementier a participé à la création de la donnée (sans son objet connecté pour capturer cette donnée, elle n'existerait pas), et que l'utilisateur a également été acteur de la création de la donnée (sans son utilisation de l'objet et sans ses signes vitaux, la donnée n'aurait pas existé).

Aujourd'hui les données sont utilisées comme monnaie d'échange. C'est par exemple le cas lorsqu'on demande à l'utilisateur ses données en échange de l'accès à un service « gratuit ». On ne compte plus les exemples de cette pratique qui a connu un essor considérable durant les deux dernières décennies (Facebook, Twitter, Instagram etc.). Les données utilisateurs sont aussi le carburant des plus gros systèmes de service actuels : réseaux sociaux et publicités, services de recommandation (vente de produits), services de mise en relation (applications comme Uber) qui s'épanouissent par-dessus ces écosystèmes de données. En somme, sans les données des utilisateurs ces systèmes ne seraient que des coquilles vides.

« On constate que la propriété d'une donnée (par essence numérique ou digitale) a peu à voir avec la propriété d'un objet physique dans le monde réel. »

Au quotidien quand un utilisateur possède un objet (une voiture ou un bijou précieux), il possède également un titre de propriété qui le prouve (une facture ou pour certains objets de valeur un certificat) et au quotidien l'objet est soit au côté de son utilisateur, soit dans un espace auquel il a accès. Dans le monde virtuel c'est bien plus compliqué étant donné que l'utilisateur ne stocke pas lui-même ses objets virtuels (données) dans une base de données privée, et que jusqu'à présent il n'existe aucune attestation prouvant qu'un utilisateur est à l'origine de ses données.

Au contraire, ces dernières sont éparpillées dans des *Datacenters* (entrepôts de données) sous la responsabilité de multinationales. Si quelqu'un souhaite accéder, vendre ou analyser ces données, de quels moyens concrets et réalistes l'utilisateur dispose-t-il aujourd'hui pour l'en empêcher ? Le sujet important est donc ici de donner à l'utilisateur le moyen de reconquérir ses données.

Il se trouve que la *Blockchain* est un moyen de choix pour y parvenir si tant est que les mentalités évoluent avec la technologie comme outil.

« Aujourd'hui la *Blockchain* nous laisse imaginer un monde où l'on pourrait rester propriétaire de nos données tout en les mettant à disposition d'autres personnes, une sorte d'usufruit virtuel. L'utilisateur-propriétaire pourrait produire des données et décider qui y aura accès. »

C'est dans la *gestion de l'accès* que l'on retrouvera finalement l'essence de ce qu'on appelle la *propriété*. Être propriétaire d'un bien signifie avoir pleins pouvoirs sur l'usage qui en est fait, il est donc possible avec des systèmes *Blockchain* d'atteindre ce degré de souveraineté de l'utilisateur. On peut citer comme exemple le système *uPort* « *Self-sovereign Identity* ». Il s'agit d'un projet *Blockchain* de gestion de l'identité qui permet notamment de générer des attestations sur l'identité d'une personne ou d'une donnée mais aussi sur des *Claims* (revendications) permettant par exemple de prouver qu'une personne et une donnée sont liées.

Imaginons une plateforme médicale utilisée pour réaliser des études longitudinales sur des données de patients. Chaque utilisateur pourra alimenter cette plateforme *via* son dossier médical dont il est désormais propriétaire et ainsi améliorer la pertinence du système de santé dans son ensemble. Aujourd'hui les systèmes sont en silos et les données sont « propriétaires » (détenues par des institutions ou des laboratoires) ce qui rend difficile l'analyse de données à grande échelle et sur de longues durées. Une plateforme médicale telle que décrite ci-dessus permettrait aux initiatives de médecine préventive et personnalisée de réellement progresser pour le bénéfice de tous.

On peut également imaginer une monétisation de l'accès aux données *via* le concept de *Market Place* (bourse) de données - qui aujourd'hui bien qu'existantes dans certains secteurs sont souvent caduques faute d'avoir atteint une masse critique intéressante. De telles *Market Place* pourront concurrencer directement

les GAFAs tout en incluant l'utilisateur dans la création de valeur générée grâce à ses données et en proposant une plus grande traçabilité et transparence dans les flux de données. Prenons un exemple, une entreprise développe un algorithme et ce dernier apprend des données de 100000 utilisateurs qu'il a trouvés sur une *Market Place* alimentée par des milliers d'utilisateurs. Ce faisant, l'algorithme devient plus performant et propose un service à très forte valeur ajoutée (recommandation personnalisée, mise en relation pertinente etc.). L'entreprise va donc gagner beaucoup d'argent grâce à ce service et on pourrait considérer qu'une partie est bien sûr le dû de l'entreprise qui a mis en place le service et financé la R&D, et que l'autre serait logiquement à redistribuer aux 100000 utilisateurs ayant, par leurs données, contribué au succès et à la pertinence de cet algorithme. C'est ici que la notion de « Token » citée dans le titre intervient. Ce cryptojeton virtuel peut représenter bien des choses : un droit d'accès, une unité de ressource, un objet virtuel, une action d'une entreprise, une dette etc. Les Tokens possèdent les propriétés de base de la monnaie : c'est une unité de compte, une réserve de valeur et un intermédiaire dans les échanges. De plus, le Token n'est pas duplicable et il est impossible de dépenser deux fois un même jeton.

Il est l'outil idéal, apporté par la *Blockchain*, à la problématique de propriété et de gestion d'accès et de ressources. On peut donc imaginer que lorsque l'entreprise a acheté des droits d'accès à certaines données sur la *Market Place*, elle a payé ses droits en tokens qui sont allés dans le compte de chaque utilisateur concerné par la requête (la *Market Place* maintient donc un *Mapping* entre les données et les comptes utilisateurs). Par la suite on peut imaginer que ces Tokens aient un prix fixe déterminé par la plateforme selon un cours (offre / demande) comme une sorte de cryptomonnaie de la donnée.

Enfin, il est essentiel de voir que la *Blockchain* seule ne suffit pas. En effet, ce n'est pas une solution miracle aux problèmes techniques ou de gouvernance. Avec la *Blockchain* on ne peut réussir à mettre tout le monde d'accord ou à sécuriser des données. En revanche elle offre un fabuleux *moyen* d'y parvenir.

De plus dans la plupart des cas d'utilisation de la *Blockchain*, on se rend compte qu'il faut la compléter par d'autres briques technologiques pour qu'elle accomplisse la fonction qu'on lui prête et que le service escompté soit effectivement rendu. Par exemple une *Blockchain* ne peut s'engager sur la véracité des données que l'on y stocke, elle ne fait pas de tri. En revanche une fois la donnée stockée, la *Blockchain* pourra préserver son intégrité en empêchant quiconque de modifier son contenu et pourra fournir la preuve non-répudiable de l'état d'une donnée à un instant t. Toutes les briques technologiques utilisées dans les premières *Blockchains* étaient disponibles dans le monde informatique depuis plusieurs décennies. C'est donc en l'association astucieuse de ces technologies que réside la réelle innovation *Blockchain*. La *Blockchain* est plus une nouvelle façon de procéder qu'une nouvelle technologie. Il est certain que ce nouveau paradigme sera adopté dans la plupart des systèmes informatiques de demain pour leur

conférer des propriétés fortement en demande telles que la transparence, la fiabilité, l'intégrité, la provenance, la traçabilité, etc.

Le *Smart Contract* : une réponse à la complexité kafkaïenne de nos systèmes actuels ?

Le monde *Blockchain* évolue très vite et se dote de plusieurs sous-éléments dont il est important de saisir le rôle. Précédemment, nous avons introduit la notion de Token, il convient maintenant de parler des *Smart Contracts* et de leur potentiel. En effet, la *Blockchain* constitue actuellement un moyen de renverser certains rapports de force qui ont cours depuis plusieurs décennies voire des siècles. L'un des outils pour y parvenir est indéniablement le *Smart Contract*. Les *Smart Contracts* sont des programmes informatiques qui, une fois déployés sur un réseau de type *Blockchain*, permettent d'embarquer une logique métier et de l'exécuter avec la garantie que ses termes et conditions sont infalsifiables.

L'inversion du rapport de force que la *Blockchain* permet va faire émerger de nouvelles chaînes de valeur dans la plupart des industries. On peut le voir déjà dans le secteur de l'Assurance avec le produit Fizzy, développé par Axa, qui propose à ses souscripteurs d'être indemnisés directement et automatiquement en cas de retard de leur vol. L'époque où les assureurs gagnaient de l'argent en comptant sur la lourdeur des processus de remboursement pour décourager une majorité de clients à réclamer leur dû serait-elle en train de toucher à sa fin ?

Les industries les plus impactées par cette transformation sont bien celles où la valeur repose davantage sur une activité d'intermédiaire ou de tiers que sur une activité humaine ou sur une expertise difficilement automatisable. Pour citer un exemple français, prenons le métier de Notaire. Un métier reposant beaucoup sur l'authentification d'actes (signature avec un sceau) et la conservation de documents. Il est aisé de voir comment tout ceci peut être réalisé avec une *Blockchain* et comment ce métier, s'il ne disparaît pas totalement, devra se transformer en se focalisant sur la partie humaine des activités, le reste pouvant être automatisé et revenir à un coût plus faible pour le client.

La chaîne de valeur est donc bousculée et pour s'en donner une idée, il suffit de s'intéresser à l'émergence des économies sociales et solidaires ou, dans ce domaine *Blockchain*, à l'émergence de DAOs (*Decentralized Autonomous Organizations*). Ces dernières peuvent être définies comme des organisations fonctionnant grâce à un programme informatique qui fournit des règles de gouvernance transparentes et immuables à une communauté. Il n'y a pas d'autorité centrale comme dans les organisations actuelles. Les décisions sont prises collectivement et les bénéfices sont redistribués.

On voit déjà des alternatives à Uber ou à Amazon émerger de communautés *Blockchain*. Après tout, une DAO comprenant des acteurs du monde du transport à la personne et des particuliers pourrait mettre au point les règles d'une

application comme Uber, financer son développement par *Crowdfunding* classique ou ICO (*Initial Coin Offering*), celle de Tezos par exemple a levé 233 millions de dollars, et laisser la DAO gérer les affaires courantes en étant sûr de la légitimité de l'opération et en gardant un contrôle commun sur les prix et les marges. Encore une fois ce n'est ni l'argent, ni la technique qui manque mais bien un outil de gouvernance et le fait de savoir que c'est *possible*. La valeur créée par un réseau d'acteurs pourra donc se redistribuer horizontalement, des acteurs « non desservis » précédemment (les utilisateurs par exemple) pourront désormais en avoir leur juste part. La valeur cessera d'emprunter la voie à sens unique de nos économies traditionnelles.

Le magazine The Economist titrait en 2015 « *The trust machine* » en référence à la *Blockchain*.

Une interprétation courante est donc de se dire que la *Blockchain* se substituera à la confiance traditionnelle entre les acteurs. Sur le *Bitcoin* c'est certainement vrai, sur d'autres applications plus complexes du monde réel ce n'est pas le cas.

« Avec la *Blockchain*, la confiance ne disparaît pas : elle change de nature. »

La confiance n'est plus binaire : confiance aveugle ou suspicion automatique. Elle devient modulable au niveau le plus fin : choix des noeuds qui constitueront le réseau *Blockchain*, choix de leur rôle (noeuds avec pouvoir de validation des transactions ou non), choix des données auxquelles ces noeuds auront accès etc. Ainsi, le temps où, pour accéder à un service, on devait accepter une confiance totale et non modulable sera révolu avec l'apparition de services déployés sur des *Blockchains* ou via l'usage de DAPP (Applications Décentralisées), ces applications dont l'infrastructure repose sur une *Blockchain*.

La confiance traditionnelle est donc amenée à disparaître au profit de la confiance numérique. Dans certains secteurs contraints au niveau légal tel que le domaine de la Santé, on voit qu'une grande part du process reste entre les mains des êtres humains (soignants, patients) auquel on fait confiance (de manière paramétrable car il est toujours possible d'intégrer des garde-fous). Cela est tout à fait normal, et ne revient pas à une « recentralisation » des systèmes. La *Blockchain* ne pourra jamais être un substitut au système de santé, mais elle peut le rendre plus efficace, plus économe et plus pertinent. Elle peut généralement être utilisée comme :

- un outil technique (base de données décentralisée avec caractéristiques de transparence, de sécurité, d'automatisation),
- un outil de facturation et de remboursement simplifié (grâce aux *Smart Contract*),
- un outil de gouvernance (décentralisation, diminution des silos, les mêmes règles sont appliquées partout sans possibilité de corruption).

Revenons sur la gouvernance : dans la plupart des projets qui échouent le problème n'est pas technique mais humain. Plus précisément, on observe que les acteurs n'arrivent pas à se mettre d'accord sur les processus de fonctionnement ou de contrôle, ils n'arrivent pas à se projeter ensemble (et avoir confiance en cette projection), et quand ils imaginent des cas de litiges futurs (comptable, légal ou autre) ils ont du mal à savoir s'il y aura une justice ou si les autres acteurs pourraient se liguer contre un acteur. Souvent dans ces cas-là, ils feront appel à des tiers de confiance qui parfois n'ont d'autre valeur ajoutée que celle d'être un tiers, et donc par définition d'être neutre dans les litiges et impartial dans leur résolution. La *Blockchain* apporte des alternatives à ces tiers. Cette technologie transforme et améliore la plupart des composantes de notre économie traditionnelle : les intermédiaires, les médiateurs, les monnaies d'échange, le troc, les bons, les certificats, etc.

On peut désormais créer fort simplement une monnaie ou représenter unitairement une ressource ou un service grâce aux Tokens. Concernant les intermédiaires humains et les tiers de confiance, la *Blockchain* peut jouer ce rôle. Par exemple entre un acheteur et un vendeur qui ne se font pas confiance, un *Smart Contract* peut bloquer les fonds de l'acheteur en attendant la bonne réception du produit puis transférer ces fonds au vendeur. En cas de litige, des médiateurs prédéfinis interviennent et peuvent débloquent la situation dans un sens ou dans l'autre (en votant pour le remboursement de l'acheteur ou pour le paiement du vendeur avec des systèmes de *multisignatures*).

Enfin, la *Blockchain* n'est pas « intelligente », tout ce qui est décrit précédemment correspond à ce que nous - ensemble et non pas individuellement - pouvons en faire pour créer des meilleurs services.

Ainsi, la façon dont nous utiliserons la *Blockchain* dans les prochaines années fera la différence entre réussir à passer dans une nouvelle ère où la confiance numérique n'est pas un *Buzz Word* mais bien le socle de notre civilisation, ou échouer et refaire - mais sous un nom plus attrayant- les mêmes systèmes qui ont fait tourner notre économie et qui ont régi les interactions commerciales durant les derniers siècles en excluant certains pour enrichir d'autres.

Chapitre 3 :
Le droit et la réglementation
autour du traitement
des données numériques



Le traitement des données numériques est en mesure de constituer pour les entreprises un vaste champ de développement et de création de valeur. Ces systèmes algorithmiques dont disposent les entreprises créent des perspectives nouvelles et peuvent leur permettre de réinventer leurs activités *via* de nouvelles offres et produits, l'amélioration de celles et ceux qui existent déjà, l'établissement de liens plus forts avec leurs clientèles, et l'amélioration de leurs résultats commerciaux. Désormais, l'information est de plus en plus l'objet d'obligations. convoitée, elle devient aussi la cible des malfaiteurs entraînant des enjeux juridiques toujours plus importants.

Ce virage technologique soulève toute une série d'interrogations : dans quelle mesure et selon quelles conditions peut-on admettre que les données issues du corps humain puissent faire l'objet d'une monétisation ? Qui est le véritable propriétaire des données ? L'utilisateur dispose-t-il d'un contrôle réel ? Est-il informé de la revente possible de ses données ? Comment contrôler et maîtriser les données émises ? Doit-on les classer et les catégoriser ? Doit-on avoir peur de l'exploitation des données à caractère personnel ? Que faire de ces informations ? Où sont-elles réellement stockées ? Comment le cadre légal peut-il prévenir les abus et lutter contre l'utilisation dommageable des données personnelles sans paralyser la croissance de l'économie numérique ? Comment empêcher l'exploitation d'« anomalies profitables » chez les personnes sans freiner les progrès liés aux NTIC ? Ainsi, le besoin d'établir un cadre législatif clair et précis sur l'usage des données numériques apparaît comme indispensable pour ne pas basculer dans une psychose autour des *Big Data*.

C'est dans ce contexte de méfiance et d'inquiétude que sera mis en application, le 25 mai 2018 prochain, le Règlement européen sur la protection des données (RGPD). Ce dernier imposera des obligations spécifiques autour de la donnée numérique auprès de tous les organismes qui traitent des données personnelles, directement ou indirectement (pour le compte d'un autre organisme), dans le cadre d'un service ou d'une prestation. Sont notamment concernés :

- les prestataires de services informatiques (hébergement, maintenance, ...),
- les intégrateurs de logiciels,
- les sociétés de sécurité informatique,
- les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données,
- les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients.

1 / LA PROTECTION DES DONNÉES PERSONNELLES S'INVITE AU COEUR DE LA STRATÉGIE DES ORGANISATIONS



de Me Jeanne Bossi Malafosse

Avocat associée / Responsable du département
Données Personnelles - DELSOL Avocats

Le nouveau Règlement européen sur la protection des données personnelles va incontestablement bouleverser la façon d'appréhender le sujet de la protection des données. Aujourd'hui, sa mise en application prochaine est surtout évoquée à travers le prisme des nouvelles responsabilités qui vont peser sur les responsables de traitement. Conséquence du principe dit d'*Accountability* qui imposera demain à tous les acteurs d'être en mesure de démontrer à tout moment leur conformité aux principes de protection des données personnelles, sous peine d'encourir des sanctions dont le montant financier est sans commune mesure avec ce qui prévalait jusqu'à présent (près de 4 % du chiffre d'affaires mondial d'un organisme en cas de violation des droits).

Cette prise de conscience - soudaine pour certains - du sujet de la protection des données personnelles peut paraître surprenante alors que la loi Informatique et Libertés date de 1978 et que, sur le plan européen, la Convention du Conseil de l'Europe du 28 janvier 1981 est un texte de référence.

Les enjeux de la protection des données personnelles ont jusqu'à présent davantage été vécus comme un sujet d'éthique qui, aidé en France par une autorité de protection des données - la CNIL - au travail très didactique et pédagogique au surplus peu tournée vers la sanction, a permis en pratique à beaucoup d'acteurs, essentiellement du secteur privé, d'éviter de s'intéresser au sujet.

Le développement massif du numérique au cours des dernières années dans tous les secteurs et la présence ubiquitaire de la donnée ont transformé l'environnement et c'est dans ce contexte que le Règlement européen du 27 avril 2016 intervient pour devenir demain la loi nationale commune à tous les pays de l'Union Européenne dans le domaine de la protection des données personnelles. La donne change et avec elle la façon d'appréhender le sujet.

En effet, la protection des données personnelles passe d'un sujet d'éthique dont les règles étaient respectées de façon très disparate par les acteurs à un sujet proprement juridique composées de règles à respecter et dont la violation n'a

rien à envier désormais aux sanctions que l'on peut connaître et appliquer en droit de la concurrence ou dans le cadre des réglementations anti-corruption par exemple.

Certains mettent en avant le fait que ce changement de paradigme contribue à retirer au sujet son caractère noble, matière liée au respect des droits de l'Homme qui serait désormais cantonnée à une vision économique, utilisée par certains dans un but purement mercantile pour valoriser leur capital informationnel et algorithmique.

« La donnée personnelle et le capital informationnel d'un organisme ont indéniablement acquis une valeur économique qu'ils n'avaient pas auparavant. »

En imposant par des contraintes plus fortes le respect des principes de protection des données, la matière s'invite désormais, à l'égal des autres, dans la gestion des projets au quotidien.

Demain, il ne s'agira plus de s'interroger sur la nature des formalités préalables à accomplir auprès de la CNIL, question très réductrice mais longtemps seul intérêt des acteurs pour la matière, mais de s'inquiéter dès le départ de la façon d'assurer le respect des principes de protection des données, ce qui impose de rentrer dans le fond d'un sujet dont l'appréciation était jusqu'ici surtout le fait de la CNIL.

À chaque acteur dorénavant d'assurer effectivement en pleine responsabilité le respect des droits des personnes dont il traite les données, d'analyser le bon niveau de risque pour les droits et libertés fondamentaux afin de mettre en place la sécurité adaptée.

Le sujet ne pourra dès lors plus être ignoré ou réduit à une formalité administrative mais deviendra une matière incontournable au même titre que le respect d'un budget ou l'allocation des ressources.

De la même façon que le respect des règles de concurrence ou de celles relatives à la lutte contre la corruption est devenu, grâce au cadre européen, un sujet essentiel et pris en compte à tout moment par les organisations avec le risque de très lourdes condamnations, de même l'évolution de la prise en compte des principes de protection des données personnelles deviendra demain une préoccupation permanente.

En rendant le sujet incontournable sous peine de sanctions sévères, le Règlement européen peut contribuer à mobiliser l'ensemble des acteurs et à généraliser des pratiques plus respectueuses de la protection des données.

2 / LE CADRE LÉGAL ET RÉGLEMENTAIRE : LES EXIGENCES DU RÈGLEMENT EUROPÉEN DU 27 AVRIL 2016⁹⁵ ET LA LOI FRANÇAISE POUR UNE RÉPUBLIQUE NUMÉRIQUE DU 7 OCTOBRE 2016⁹⁶



de Me Lina Williatte

Professeur de droit - Université Catholique de Lille
Avocat Au Barreau de Lille - Cabinet WT AVOCATS

Nul ne contestera que ces dernières années, il a été observé une accélération de la production législative à la fois nationale et supra nationale relative à l'exploitation de la donnée ; ce constat est révélateur des enjeux que représente aujourd'hui le traitement de la donnée numérique. Que ces enjeux soient économiques, financiers, sociétaux et juridiques, la donnée est, incontestablement, au cœur des préoccupations quotidiennes des entrepreneurs. À juste titre, car bien loin de n'être qu'une information brute, son traitement peut être la source d'une violation grave des droits fondamentaux des personnes. C'est pourquoi, un cadre normatif est indispensable.

En France, c'est la loi informatique et liberté du 6 janvier 1978⁹⁷ qui a posé les principes fondamentaux applicables au traitement informatique des données personnelles. Cette loi a été modifiée une première fois par la loi du 6 août 2004⁹⁸, dont l'objet principale était de transposer en France, la Directive européenne du 24 octobre 1995⁹⁹. Cette même directive faisait suite à une recommandation du Conseil de l'Europe qui avait clairement affirmé la nécessité d'harmoniser les dispositions des Etats membres en matière de traitement des données afin de limiter les entraves à leur libre circulation au sein de l'Union européenne. En dépit de ces textes, des pratiques différentes ont été constatées au sein des pays européens, certains Etats s'étant révélés plus permissifs que d'autres, des facilités de développements sont dénoncées par des acteurs contraints par une norme nationale plus stricte en la matière.

Il a fallu attendre la Charte des droits fondamentaux de l'Union européenne pour que soit inscrit le droit à la protection des données personnelles dans la législation européenne¹⁰⁰. Adopté par la conférence inter gouvernementale de Nice, le Traité

de Lisbonne lui confère ainsi une portée contraignante¹⁰¹. L'ensemble ayant été consacré par le Règlement européen 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 données¹⁰².

« La valeur juridique d'un règlement européen est plus contraignante de celle d'une directive européenne. »

En effet, si une directive fixe un cadre souple permettant aux Etats membres qui se sont engagés à l'appliquer, à s'en inspirer pour légiférer sur leur territoire, le Règlement européen est plus opposable. Dès lors, la marge d'interprétation et d'appréciation d'Etat est beaucoup plus restreinte, si bien que la loi nationale devant être adoptée en application dudit règlement est de nature soit à le compléter soit à le préciser mais en aucun cas à le contredire. C'est l'essence même du texte de la loi pour une République Numérique de 2016. Dès lors, s'il l'on peut affirmer que désormais le cadre légal français et européen convergent sur le socle fondateur de la protection des données personnelles, il doit être souligné que demeure des particularités propres à l'Etat français.

Cadre général :

Préalablement, il doit être rappeler que contrairement à nos voisins d'Outre Atlantique, soumis à la Common Law, en Europe et donc en France, aucun droit de propriété n'a été reconnu sur la donnée. En effet, la donnée n'est juridiquement pas qualifiée de « chose ou d'objet », elle ne peut dès lors bénéficier des prérogatives accordées habituellement aux propriétaires. Sont donc exclues, toutes possibilités de revendiquer un droit de propriété sur la donnée et partant un quelconque droit d'achat ou de vente.

« Selon la vision européenne, la donnée est une émanation de la personnalité juridique d'une personne physique. Elle relève de la catégorie des droits subjectifs. A l'instar, de l'identité de la personne, elle bénéficie de la même protection juridique que les informations relevant de la vie privée des personnes. »

Le droit à la protection de la vie privée des personnes est l'un des droits les plus protégés de notre système normatif. Consacré par l'article 12 de la Déclaration universelle des droits de l'Homme et repris à l'article 8 de la Convention européenne des droits de l'homme, en France, il est contenu à l'article 9 du Code civil qui s'est vu reconnaître en 1995, une valeur constitutionnelle¹⁰³.

⁹⁵ Règl. 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.

⁹⁶ N°2016-1321. JO du 8 octobre texte n°1.

⁹⁷ Loi n°78-17.

⁹⁸ Loi n°2004-801.

⁹⁹ Directive 95/46/CE sur la protection des données personnelles.

¹⁰⁰ Charte des droits fondamentaux de l'Union européenne 18/12/2000. JO des Communautés européennes C 364/1

¹⁰¹ Traité sur l'Union européenne et Traité sur le fonctionnement de l'Union européenne qui a adopté le traité de Lisbonne signé le 13 décembre 2007 publié au Journal officiel n°C326 du 26/10/2012, p.0001 - 0390.

¹⁰² N°2016/679. JOUE n°L119 du 4 mai 2016, p.1. Ce règlement directement applicable dans la législation interne aux Etats membres abroge la directive 95/46/CE jugée obsolète.

¹⁰³ Cons. Const. 18 janv. 1995, n°95-352 DC. JO 21 janv. 1995.

Dès lors, toute récolte, traitement, exploitation, cession, circulation, etc. d'une donnée personnelle est soumise à l'information préalable et au consentement de la personne dont elle est issue.

- Qualification de la donnée :

L'application de ce principe implique dès lors que la donnée est une donnée personnelle, de nature à identifier la personne. Partant la donnée anonyme ne nécessite pas, pour son traitement, le consentement de la personne dont elle émane. Encore faut-il, cependant, être en mesure de pouvoir qualifier la donnée de « donnée anonyme ». Une affirmation, dont il semble aujourd'hui qu'elle ne pas soit aisée, tant la performance des solutions et outils informatiques mettent à mal toute hypothèse d'anonymisation absolue. C'est pourquoi, le juriste recommande de faire de l'information et du consentement de la personne, un principe applicable à tout traitement, même si celui-ci ne concerne que des données dites anonymisées.

« En tout état de cause, la charge de la preuve du consentement appartient au responsable de traitement. »

La demande de consentement doit être présentée sous une forme qui la distingue des autres questions que le responsable de traitement pose potentiellement et doit être formulée sous une forme compréhensible, accessible et en des termes clairs et simples. Par ailleurs, le consentement ainsi recueilli doit avoir été donné librement c'est-à-dire sans contraintes, sans manipulations, sans fausses informations à l'instar du prestataire qui conditionne, la fourniture d'un service, ou l'exécution d'un contrat au consentement de la personne au traitement de ses données, alors même que ledit traitement n'est pas nécessaire à la réalisation de la prestation vendue ou à l'exécution du contrat.

- Cas particuliers :

Tenant à la personne concernée :

Il s'agit principalement de faire état de la situation de l'enfant mineur. Le Règlement européen n'a pas interdit le traitement de la donnée les concernant. Néanmoins, il a posé quelques limites destinées à le sécuriser.

Ainsi, le traitement des données à caractère personnel d'un mineur est licite dès lors qu'il est âgé d'au moins 16 ans. En deçà, le consentement des titulaires de l'autorité parentale est requis. Il appartient au responsable de traitement d'apporter la preuve du respect de ces conditions.

Tenant à la qualification de la donnée :

Si le traitement des données personnelles est autorisé, dès lors que la personne informée, y consent. Le principe est inversé lorsque le traitement porte sur des données personnelles dites sensibles. Sont qualifiées de sensibles : toutes données

qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ainsi que le traitement des données génétiques, biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le traitement des données dites sensibles est interdit. Ce principe est assorti d'exceptions prévues à l'article 9 paragraphe du RGDP ¹⁰⁴. Parmi elles, le consentement explicite de la personne concernée au traitement de sa donnée pour des finalités autorisées par l'Union européenne. Cependant, la CNIL, autorité de surveillance, doit préalablement, au lancement du traitement, autoriser son traitement. En d'autres termes, le consentement de la personne n'est pas une condition suffisante en soit, il faut impérativement pour le traitement des données sensibles, déposer une demande d'autorisation auprès de la CNIL qui ne l'accordera que, sous réserve notamment d'une garantie de protection de la vie privée de la personne et de la légitimité du traitement ainsi que sa finalité.

Droits de la personne concernée : principes fondateurs du traitement de la donnée personnelle :

La donnée fait partie de la vie privée de la personne. Dès lors les droits qui lui sont rattachés sont assortis de la même protection. Cette protection implique le respect d'un nombre certains d'exigences que le responsable de traitement doit garantir. Ainsi, la personne dont les données sont traitées doit être informée :

- De l'identité et des coordonnées du responsable de traitement, de son représentant ou le cas échéant, du délégué à la protection des données (DPO ¹⁰⁵) ;
- Du droit d'accès aux données traitées, du droit de rectification, du droit à l'effacement, du droit d'opposition, du droit à la limitation du traitement, du droit à la portabilité des données ;
- Des finalités du traitement, de la durée de conservation des données, de l'existence d'une prise de décision automatisée, y compris un profilage ;
- Des destinataires des données, si un transfert de données vers un pays étranger (Europe ou hors Europe) va être effectué ;
- Du droit d'introduire une réclamation auprès d'une autorité de contrôle (...).

- *Un droit à l'information pour ...*

La personne qui consent au traitement de sa donnée doit, pour délivrer un consentement éclairé, être informée des finalités dudit traitement. Bien que d'apparence aisée à réaliser, cette exigence n'est pas, sur le terrain, facilement tenue. En effet, les responsables de traitement et/ou les porteurs de projet ne pensent pas suffisamment en amont les potentiels de leur projet. Si bien qu'au moment de son déploiement, ils utilisent les données pour une finalité autre,

¹⁰⁴ RGDP : Règlement européen sur la protection des données.

¹⁰⁵ Obligatoire à compter de mai 2018.

qu'ils ne pensent jamais bien différentes de celle qui avait été consentie par la personne concernée. Bien que justifiable, juridiquement ce comportement s'analyse comme une défaillance, de nature à faire rentrer en responsabilité, le responsable de traitement. Par ailleurs, ce droit à l'information concerne également le droit pour toute personne de connaître la destination finale de ses données et particulièrement si ces dernières vont être amenées à passer les frontières de la France, de l'Europe ou au-delà. Soit le transfert des données est envisagé en dehors des frontières Françaises mais au sein de l'Union Européenne. L'obligation pour les Etats européens d'être en conformité avec le RGDP au plus tard en mai 2018 est de nature à sécuriser la protection des données des personnes dès lors que lesdites données sont traitées dans un pays qui s'est engagé au même niveau de protection que celui de la France. À cette fin, un Comité européen de la protection des données est institué principalement pour veiller à l'application cohérente du règlement au sein de l'Union.

Soit le transfert des données est envisagé en dehors des frontières de l'Europe. Ce transfert n'est possible que si la Commission européenne a constaté par voie de décision que le pays tiers en question assure un niveau de protection adéquat. En l'absence de décision de conformité de la Commission, le responsable de traitement ou le sous-traitant ne peut transférer les données vers un pays tiers que s'il a prévu des garanties appropriées à la protection des droits des personnes. Ces garanties peuvent être un instrument juridiquement contraignant et exécutoire entre les autorités, des règles d'entreprises contraignantes, des clauses types de protection des données adoptées par la Commission ou par une autorité de contrôle nationale approuvée par la Commission européenne, un code de conduite ou un mécanisme de certification.

- *Un droit d'accès à la donnée pour ...*

À tout moment, la personne a le droit d'obtenir du responsable de traitement toute information qui lui permette de faire valoir ses droits. En l'occurrence, il s'agit ici de vérifier le caractère transparent et loyal du traitement. C'est ainsi que la personne est en droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données la concernant, dès lors qu'elles s'avèrent inexactes. Elle peut également obtenir la limitation du traitement lorsqu'elle conteste l'exactitude des données la concernant, ou lorsqu'elle identifie un traitement illicite. Elle peut exiger également l'effacement des données soit parce qu'elles ne sont plus nécessaires eu égard à la finalité du traitement, soit parce que la personne a retiré son consentement et/ou s'oppose au traitement de la donnée, soit parce que le traitement s'avère être illicite. Néanmoins, la personne peut se voir refuser l'exécution de ce droit lorsque le traitement de la donnée répond à des impératifs d'intérêt public ou à l'exercice du droit à la liberté d'expression et d'information ¹⁰⁶.

- *Un droit à la portabilité des données pour...*

Il s'agit d'une des nouveautés du RDGP. Le droit à la portabilité implique que toute personne dont la donnée est traitée de manière informatisée, est en droit de récupérer les données qu'elle a fourni au responsable de traitement et ce dans un format structuré, couramment utilisé et lisible par machine. Ce droit n'est cependant applicable qu'au traitement informatisé qui suppose en amont le consentement de la personne (à l'exclusion donc des traitements informatisés répondant à une mission d'intérêt général ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement).

La responsabilisation du responsable de traitement (le principe d'Accountability) :

Bien qu'auparavant basé sur un système de respect des obligations légales qu'il appartenait aux instances nationales de contrôler (en l'occurrence pour la France : la CNIL) de vérifier et de sanctionner, le cas échéant ; le RGDP modifie le postulat et met en responsabilité en amont du projet, le responsable de traitement. Désormais, il appartient à ce dernier de mettre en oeuvre un traitement des données en conformité avec les exigences normatives et de déceler ses éventuelles failles, de les déclarer et d'y appliquer des mesures correctives.

« Dès lors, le responsable du traitement doit procéder à un auto diagnostic, sur la base d'une analyse d'impact, de son système de traitement de données à la fois sur sa sécurité mais aussi sur sa légitimité. »

Dans l'hypothèse où le traitement présenterait un risque élevé, le responsable du traitement doit présenter à la CNIL des mesures visant à le réduire. À défaut, la CNIL peut l'accompagner pour une mise en conformité, le cas échéant des sanctions peuvent être prononcées. Sur ce point, le RGDP a également innové.

Le paragraphe 3 de l'article 17 du RGDP prévoit précisément que le droit à l'effacement ne s'applique pas si le traitement est nécessaire a) à l'exercice du droit à la liberté d'expression et d'information, b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'Etat membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement, c) pour des motifs d'intérêt public dans le domaine de la santé publique (...), d) à des fins d'archivistiques dans l'intérêt public (...), e) à la constatation, à l'exercice ou à la défense de droits en justice.

Ainsi, si un responsable du traitement ou un sous-traitant viole délibérément ou par négligence les obligations qui lui incombent, le montant total de l'amende administrative peut s'élever jusqu'à 10 000 000 EUR ou, dans le cas d'une entreprise, jusqu'à 2% du chiffres d'affaires annuel mondial total de l'exercice précédent. Cette sanction peut s'élever jusqu'à 20 000 000 EUR ou pour les entreprises

¹⁰⁶ Cardon Alain, Conscience artificielle & systèmes adaptatifs, ed. Eyrolles, 2000, 380p. Et, Cardon Alain, Un modèle constructible de Système Psychique. Automates Intelligents, 2011.

jusqu'à 4% du chiffre d'affaires annuel mondial de l'exercice précédent dès lors que la violation est relative au principe de base d'un traitement et notamment les conditions applicables au consentement et aux droits des personnes. La sévérité de la sanction démontre la résolution du législateur européen de faire respecter le cadre légal du traitement informatisé des données. Un cadre qui *in fine* consacre deux principes nouveaux :

- le principe d'*Accountability* pour le responsable de traitement, qui désormais est responsabilisé de la licéité, la légitimité et la sécurité de son traitement de données, non seulement vis-à-vis de l'autorité de contrôle (la CNIL), mais aussi à l'égard de la personne dont il traite la donnée.
- le principe de l'*Empowerment* des personnes dont la donnée est traitée. En consacrant un socle protecteur de droits, le législateur a ainsi permis à la personne concernée d'exercer un contrôle sur le traitement de ses données. Ce contrôle, à pour viser de le responsabiliser dans la gestion de sa donnée.

Les particularités de la loi française :

La loi pour une République Numérique du 7 octobre 2016 prise en application du Règlement européen de 2016 a bien entendu repris dans son objet le contenu du RGDP, d'ailleurs sur certains aspects, elle est allée plus loin. Ainsi, elle reconnaît à tout citoyen un droit à la libre disposition de ses données numériques personnelles qui se décline en plusieurs mesures concrètes : le droit à l'oubli numérique pour le mineur : ainsi un mineur peut obtenir plus facilement et plus rapidement l'effacement d'un contenu en ligne le concernant.

« **Le droit à la mort numérique : chaque citoyen aura le droit d'exprimer de son vivant ses volontés sur la conservation et la communication de ses données après son décès ou demander leur effacement.** »

Ainsi que l'application stricte de la règle des correspondances privées qui interdit tout accès par une personne non autorisée au contenu du correspondance quel que soit son vecteur ou la technologie de l'information utilisée (mails, etc.). Force est de constater que nous sommes à l'aune de la construction d'un Droit du traitement des données informatisées. Un droit que l'on conseillera aux entrepreneurs de maîtriser avant le déploiement de leur projet car l'expérience démontre en la matière que tout incident consécutif au non-respect du cadre normatif applicable au traitement de la donnée est à l'origine d'un préjudice d'image qui fait basculer la relation de confiance de l'entreprise avec ses clients en relation de défiance. Une bascule dont il est difficile *a posteriori* de se remettre.

3 / OBJETS CONNECTÉS UTILISÉS POUR LA SANTÉ : UNE NÉCESSAIRE CLARIFICATION RÉGLEMENTAIRE



d'Emmanuelle Rial-Sebbag

Docteur en Droit de la santé, HDR - Directrice de Recherche Inserm, UMR 1027 Inserm / Université Paul Sabatier, Toulouse ; Responsable de l'équipe «Trajectoires d'innovations en santé : enjeux bioéthiques et impact en santé publique»

Les Objets Connectés (OC) vont-ils révolutionner notre santé ? Il est coutume de lire bien souvent que l'avènement de nouvelles technologies dans le domaine de la santé s'assimile à un progrès pour les usagers. Dans le cadre des OC, une meilleure maîtrise de ses paramètres, un recueil en temps réel de ses informations, un outil « *User-Friendly* », sont autant d'arguments avancés par les fabricants pour accélérer leur développement. Toutefois ces OC, difficiles à définir, répondent globalement à une demande sociale héritée du « santéisme » et du mouvement de la quantification du soi et se doivent aussi de répondre à plusieurs critères d'exigence que ce soit en termes de sécurité du produit ou encore d'utilisation des informations collectées.

Les objets connectés saisis par le droit :

À ce jour il n'existe pas de définition juridique des OC. Ces derniers se définissent plutôt sur le plan technique comme « des dispositifs connectés à l'Internet pouvant collecter, stocker, traiter et diffuser des données ou pouvant accomplir des actions spécifiques en fonction des informations reçues »¹⁰⁷. Il faut retenir de cette proposition que non seulement sont concernés des objets, tels que des *Smartphones*, montres, tablettes, outils de mesure, mais aussi des applications mobiles et des programmes informatiques, ce qui en fait une catégorie des plus hétérogène. La difficulté juridique de leur catégorisation consiste justement à correctement identifier ceux qui sont utilisés dans le cadre du système de santé et délivrent à ce titre des informations personnelles de santé et ceux qui sont utilisés dans le cadre du bien-être et délivrent des informations personnelles qui ne seront pas systématiquement considérées au regard du droit comme des informations de santé. Cette catégorisation représente la première étape dans la régulation de ces objets et des informations qu'ils délivrent permettant dès lors de leur appliquer un régime juridique tant pour leur production que pour leur utilisation.

¹⁰⁷ Haute Autorité de santé, Evaluation et amélioration des pratiques - Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth), octobre 2016. Disponible à cette adresse https://www.has-sante.fr/portail/upload/docs/application/pdf/2016-11/has_ref_apps_oc.pdf

Les objets connectés, outils de réponse à une demande sociale :

Les difficultés de catégorisation juridique n'ont pas freiné le développement commercial de ces objets qui représentent un marché non-négligeable au sein de ce qu'il est aujourd'hui convenu de nommer la e-santé¹⁰⁸ ou la santé mobile¹⁰⁹. La particularité de ce marché est d'être destiné à tous les utilisateurs dont tous ne sont pas des patients. En effet, les OC peuvent être non seulement mobilisés dans le cadre d'une prise en charge médicale pour des actions de prévention ou de surveillance mais également dans le cadre du bien-être et de l'automesure. Le mouvement d'automesure, ou encore du « *Quantified Self* » s'est largement développé ces dernières années au nom d'une revendication sociale visant à maîtriser ses paramètres de santé. En effet, que ce soit *via* une montre connectée ou d'autres capteurs, les individus sont techniquement en capacité d'avoir accès directement aux mesures de leurs paramètres physiologiques afin d'améliorer leurs performances, de surveiller leurs données de santé ou encore d'adapter leur style de vie. Les données générées ici sont diversement qualifiées au regard du droit (*infra*) mais ont comme point commun d'être directement accessibles aux personnes qui les génèrent, l'interprétation éventuelle par un tiers (professionnel de santé) n'étant qu'une possibilité dans le cas des OC utilisés dans le contexte médical.

« Ainsi, ces objets répondent à une revendication sociale de maîtrise de ses données de « santé », leur utilisation se démocratise (notamment en raison de l'accessibilité en termes de prix et leur vente commerciale libre), ils permettent de constituer des communautés d'utilisateurs (notamment dans le cadre du *running*) et font donc dorénavant partie intégrante de la vie d'un grand nombre d'utilisateurs. »

Toutefois leur fabrication et leur utilisation doit répondre à des critères de sécurité, de fiabilité et de respect des règles en vigueur en ce qui concerne la protection de la vie privée.

La sécurité des objets connectés :

Les OC, dès lors qu'ils sont fabriqués pour être mis à la disposition du grand public, doivent, avant leur commercialisation, faire l'objet de procédures garantissant leur sécurité. Dès lors que le dispositif et le logiciel assurant son fonctionnement présentent une finalité médicale l'OC doit être qualifié de dispositif médical (DM) au sens de la réglementation européenne¹¹⁰. Le règlement illustre différents

¹⁰⁸ La e-santé peut se définir comme « tout ce qui contribue à la transformation numérique du système de santé, voire au-delà du seul secteur santé, du médico-social », in « Santé connectée de la e-santé à la santé connectée », le livre blanc du Conseil national de l'Ordre des médecins, janvier 2015

¹⁰⁹ S'entend des « pratiques médicales et de santé publique reposant sur des dispositifs mobiles tels que téléphones portables, systèmes de surveillance des patients, assistants numériques personnels et autres appareils sans fil », Organisation mondiale de la santé, mHealth – New horizons for health through mobile technologies, Global Observatory for eHealth series – Volume 3, p.6

¹¹⁰ Au sens du Règlement (UE) 2017/745 du Parlement européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, le règlement (CE) n° 178/2002 et le règlement (CE) n° 1223/2009 et abrogeant les directives du Conseil 90/385/CEE et 93/42/CEE un dispositif médical s'entend de « tout instrument, appareil, équipement, logiciel, implant, réactif, matière ou autre article, destiné par le fabricant à être utilisé, seul ou en association, chez l'homme pour l'une ou plusieurs des fins médicales précises suivantes (...) », article 2

cas dans lesquels la qualification de DM s'impose et c'est donc bien la finalité médicale qui est le critère principal qui doit être employé pour déclencher les procédures d'évaluation préalable à la mise sur le marché¹¹¹ d'un OC. Dans tous les autres cas l'OC ne sera pas qualifié de DM mais simplement de produit ce qui ne l'exonère pas du respect d'un certain nombre de procédures visant à garantir sa fiabilité. Notamment s'applique dans ce contexte la Directive générale relative à la sécurité des produits¹¹² ainsi que le droit commun applicable en matière de vente.

« Dès lors le fabricant d'un OC non destiné à une finalité médicale devra se tourner vers des référentiels afin de garantir la sécurité de son produit avant sa commercialisation. »

Dans le contexte de la santé la Haute Autorité de santé a justement rédigé un référentiel pour la mise sur le marché des OC n'étant pas qualifié de DM destiné aux fabricants¹¹³. Si ces critères semblent bien délimiter les deux champs entre DM et non DM, il est en pratique bien difficile de tracer une ligne franche entre eux. En effet, les stratégies commerciales pourraient assez facilement, favoriser le développement d'un produit sur le terrain non médical afin d'éviter la lourdeur des procédures attachées aux DM. Un même objet pourrait ainsi voir sa finalité médicale « détournée » au profit d'une finalité de bien-être jouant ainsi sur la porosité entre données de santé et donnée de bien-être.

La sécurité des informations personnelles :

Les données délivrées par les OC sont des données personnelles au sens de la loi¹¹⁴ et de la réglementation européenne. En effet l'article 4 du Règlement européen relatif à la protection des personnelles¹¹⁵ indique que doit être considérée comme personnelle « 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 ».

Donc toute information produite par le biais d'un OC tombe sous le coup de cette réglementation qui en impose la confidentialité. Le Règlement oeuvre en faveur de la protection de l'utilisation de ces données par des tiers mais ne s'immisce

111 Le Règlement impose le respect de procédures strictes mises en oeuvre par des institutions dédiées, en France l'Agence Nationale de sécurité des produits de santé.

112 Directive 2001/95/CE du Parlement européen et du Conseil du 3 décembre 2001 relative à la sécurité générale des produits.

113 Haute Autorité de santé, Evaluation et amélioration des pratiques - Référentiel de bonnes pratiques sur les applications et les objets connectés en santé (Mobile Health ou mHealth), op. cité.

114 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés révisées.

115 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE

pas dans l'utilisation qui peut en être faite par le sujet lui-même. En d'autres mots, ces données ne peuvent être utilisées que par des tiers autorisés à cet effet mais leur diffusion ou partage reste libre pour la personne dont elles sont issues, c'est une protection vis-à-vis de l'utilisation par des tiers.

Parmi ces données personnelles il en est certaines qui sont particulièrement protégées dont les données concernant la santé. Ces dernières sont entendues comme « les données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ». Par nature ces données tombent sous le coup d'une interdiction de traitement assortie d'un certain nombre d'exceptions permettant le suivi médical et le traitement des patients.

Ces données sont donc considérées comme particulièrement sensible au regard de leur utilisation par des tiers. Cependant l'application de ces dispositions dans le cadre des OC reste controversée. En effet une interprétation large de ces dispositions devrait permettre d'inclure toutes les données collectées par des OC au sein des informations concernant la santé ceci indépendamment du fait que le dispositif soit un OC de bien-être ou un OC médical (DM). Une lecture plus fine du Règlement incite cependant à en avoir une interprétation plus restrictive puisque le considérant 35 dudit Règlement indique que « les données à caractère personnel concernant la santé devraient comprendre l'ensemble des données se rapportant à l'état de santé d'une personne concernée qui révèlent des informations sur l'état de santé physique ou mentale passé, présent ou futur de la personne concernée. Cela comprend des informations sur la personne physique collectées lors de l'inscription de cette personne physique en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services au sens de la directive 2011/24/UE du Parlement européen et du Conseil (9) au bénéfice de cette personne physique; un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l'identifier de manière unique à des fins de santé; des informations obtenues lors du test ou de l'examen d'une partie du corps ou d'une substance corporelle, y compris à partir de données génétiques et d'échantillons biologiques; et toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic *in vitro*. ».

« Cette disposition orienterait donc vers une adéquation entre données concernant la santé et données médicales et tendrait donc à exclure de ce champ les données de bien-être qui resteraient uniquement des données personnelles et seraient donc régies par un système de protection plus souple. »

Cette interprétation pourrait, elle aussi, être discutable car à la lecture de ce considérant c'est finalement l'utilisation médicale qui semble être le critère d'application et on peut facilement imaginer qu'une donnée générée dans le contexte du bien-être (exemple : fréquence cardiaque) puisse être par la suite utilisée dans le contexte médical et donc être considérée comme une donnée concernant la santé.

Vers une clarification du régime des OC :

Après cette analyse succincte des enjeux juridiques soulevés par l'utilisation des OC, on ne peut que constater la nécessaire clarification de leur réglementation. Les divers outils proposés pour encadrer ces nouveaux objets montrent finalement leur limite notamment du fait qu'ils ne s'adressent pas de manière spécifique à la régulation des OC. Leur application par analogie semble parfois artificielle et finalement n'embrasse pas l'ensemble des pratiques contemporaines autour des OC.

« Il semble donc nécessaire de proposer des instruments adéquats sinon spécifiques qui devront bien évidemment assurer la fiabilité et la sécurité de ces objets, clarifier l'utilisation des données produites notamment par les entreprises commercialisant les OC (ou sont stockées ces données, qui peut y avoir accès, peuvent-elles être utilisées pour d'autres fins comme la recherche, etc.) et assurer la sécurité et l'intégrité des données personnelles produites (qu'en est-il du consentement des personnes pour leur (ré)utilisation par des tiers ?). »

Nous ne pouvons qu'appeler de nos vœux une discussion de fond de l'ensemble des parties prenantes sur les conséquences sociétales de ce qu'il est coutume d'appeler la « révolution numérique ».

Remerciements : ce texte fait suite à une étude réalisée par Morgane Roques, Florence Taboulet et Emmanuelle Rial-Sebbag (UMR 1027, Inserm, Université de Toulouse, Paul Sabatier, Toulouse) dans le cadre du projet Agence nationale de sécurité du médicament et des produits de santé (2016-2018) : Quantification du soi (P. Ducournau & E. Rial-Sebbag).

4 / GOUVERNANCE DES DONNÉES, RGPD ET ÉTHIQUE POUR LE FUTUR



de Hugues Le Bars

Chief Data Officer (CDO) / Membre fondateur -
International Society of Chief Data Officers (ISCDO)

Au sein de toute organisation, la gouvernance du traitement des données ne doit pas être menée par ceux qui l'exploitent. Qu'est-ce que cela signifie ? Les acronymes anglo-saxons sont légion quand il s'agit de désigner les disciplines du traitement de données numériques et certains désignent des expertises identiques. Simplifions, afin non pas de rendre le sujet plus simple mais bien de le rendre accessible. Pour toute organisation, la discipline mère est désignée par l'EIM (*Enterprise Information Management*), celle-ci porte sur la définition et la mise en place des organisations, de règles, du choix des technologies ainsi que les personnes et processus dans le but de maximiser les investissements consentis dans l'exploitation de la donnée reconnue comme un capital.

« **Gouvernance des données et management des données. Un duo de disciplines distinctes, nécessaires et inséparables.** »

Cela rassemble les activités de mission et de contrôle qui sont naturellement séparées et respectivement portées par les disciplines filles *Data Management* (DM), qui traite les données afin d'atteindre des objectifs et *Data Governance* (DG), qui garantit le bon respect des règles de l'exploitation des données.

L'une ne va pas sans l'autre, s'il est naturellement nécessaire de savoir collecter, préparer, cataloguer, analyser les données, il est aussi nécessaire de bien connaître les obligations réglementaires ainsi que les règles métiers associées. Un exemple trop bien connu est celui de la qualité des données ; un bon moyen de le constater est d'expérimenter rapidement le non-respect de cette recommandation. Par exemple essayez-vous à une collecte de données en silos afin de les rassembler dans un « *lac* » puis les exploiter sans gouvernance. Les problèmes de format, définition, se manifesteront très vite, et le *Data Management* vous fera rapidement comprendre qu'il manque ce que l'on nomme *Data Governance*.

Les données, traitées en temps réel ou à l'état d'historique de la vie l'entreprise ont une valeur, les possibilités d'exploitation sont telles que l'on veillera à déduire les premiers choix à partir de la stratégie de l'entreprise formulée par le comité exécutif ainsi que les objectifs et défis formulés par ses leaders business. La

gouvernance de la donnée est permanente et en cela fait l'objet d'un programme, succession de cycles répétés, et non pas d'un projet qui par définition a une fin. Ceci amène à considérer le démarrage d'un tel programme comme celui d'un modèle économique, c'est-à-dire évaluer votre organisation, sa maturité, questionner les défis économiques à relever. Des réponses, découleront naturellement une liste ordonnée des premières actions à mener en matière de communication interne et conception d'un référentiel d'exécution. À cette fin, disposez d'un sponsor au *Comex* et d'une équipe de 5, 6 personnes nanties des expertises gestion de projet, méthodes, procédures, qualité de données, applications. Une première étape consistera à formuler une vision de ce que doit être la gouvernance des données, la seconde est sa mise en place qui déclenchera un programme d'intendance de la donnée (*Stewardship*). Voici pour la gouvernance des données moteur de règles internes au service de votre modèle économique.

Le Règlement Général de Protection des Données personnelles : opportunité ou contrainte ?

Les règles et obligations n'émanent pas seulement de la gouvernance interne d'une organisation, elles sont aussi à l'initiative du législateur. Le 25 mai 2018, le Règlement Général de Protection des Données personnelles (RGPD) entre en vigueur dans tous les pays de l'union Européenne. Sans entrer dans le détail de ses 99 articles, il faut retenir que ce règlement vise à protéger les données personnelles de tout résident européen dans le monde en imposant aux entreprises le principe de consentement du résident/client européen (et non pas citoyen), son droit à l'oubli, et la portabilité de ses données personnelles.

On ne manquera pas de s'étonner de l'utilisation très fréquente du terme « *Data Privacy* » alors que l'enjeu est celui de la protection et pas seulement la vie privée. Une rapide recherche dans le document de référence est révélatrice de cet étrange abus de langage, le terme « *Data Privacy* » n'apparaît dans aucun des chapitres de la version anglaise du RGPD (GDPR : *General Data Protection Regulation*). Puisque les anglicismes semblent malgré tout inévitables, j'invite le lecteur à distinguer « *Data Privacy* » et « *Data Protection* » déjà différenciées dans les étapes dites de « *Privacy Impact Assessment* » (PIA) et « *Data Protection Impact Assessment* » (DPIA).

Une gouvernance d'entreprise est alimentée par un ensemble de règles, le RGPD n'est finalement qu'un ensemble de règles parmi d'autres.

« **Il est naturel d'accueillir ce règlement comme une contrainte lorsque l'on déroule un modèle économique « *Data Driven* » où l'acquisition et l'exploitation de données personnelles constituent un véritable Graal.** »

Toute contrainte est une opportunité d'amélioration, et le RGPD en est clairement une à différents égards pour peu que l'on accepte de l'internaliser dans les modèles économiques à définir ou redéfinir. Nous avons précédemment abordé la gouvernance des données comme une gouvernance de valeur, le cas RGPD est bien

une aubaine, celle bien motivante de démarrer votre programme de gouvernance des données. Tout comme la « *Data Governance Team* » précédemment décrite, démarrez une « *GDPR Team* » en prenant soin d'y inclure un expert sécurité et un expert juriste.

Gouvernance, expertises et sensibilités invitées :

Le RGPD amène la gouvernance des données à interpellier le seul ordre commercial qui sert le modèle économique de toute entreprise. Sciences et techniques développées dans le domaine du traitement des données, et initialement appliquées à internet, apportent leurs contributions aux sphères justice, démocratie, santé, défense, environnement, soit le bien public géré par l'Etat. Les deux instances, entreprise et Etat, expérimentent respectivement leurs défis, trouver le temps et les marges de manoeuvre nécessaires à une « transformation digitale » du premier, augmenter la vitesse des réformes du second. Pour ces seules contraintes qui s'imposent au présent, sciences et techniques sont invoquées. Rappelons qu'elles se distinguent par les valeurs pour lesquelles elles procèdent et que les sciences n'endossent pas la responsabilité des applications techniques découvertes et exploitées dans la sphère économique. Un exemple, celui de l'alliance des techniques de *Cloud Computing* avec celle de la science des données révèle une « technoscience » d'une puissance phénoménale de portée immédiatement mondiale.

Cette même technoscience des données, que nous exploitons tant qu'il est possible d'innover et produire, induisent des effets globaux sous l'impulsion de l'exigence de « scalabilité » de tout modèle économique. Les données décrivant des humains aux rôles multiples tels que citoyen, parent, employé, client sont associées à celles de biens et services marchands, objets connectés, puis livrées aux algorithmes traqueurs de valeur, ces mêmes algorithmes qui préfigurent les intelligences artificielles de demain.

Nous comprenons ces valeurs dans la résolution de problèmes du présent. Qu'en est-il des impacts à long terme pour les futures générations ? La philosophe américaine Hannah Arendt, dans son ouvrage *Condition de l'homme moderne*, développe le concept de *Homo Faber* qui fabrique des outils alors que l'Homo sapiens fait preuve de sagesse. Rien de manichéen dans la description, nous tâchons de trouver des compromis sans compromission entre les deux postures avec un avantage manifeste pour le *Faber*.

« **Gouvernants, experts, sensibilités que nous sommes quotidiennement et à tour de rôle, ne peignons-nous pas, à l'échelle globale, à nous accorder sur les problèmes à résoudre et l'ordre dans lequel il faut les aborder ?** »

La genèse du RGPD a connu les frictions du « *Safe Harbor* » et du « *Privacy Shield* » avec les Etats-Unis, rien de grave, c'est culturel...et les seuls gouvernants et experts n'ont certainement pas abouti à un RGPD mondial. La gouvernance

des données semble sommée d'inclure ce type de réflexion sur la valeur ; s'il est bien question de dire, faire et raconter, il s'agit aussi rendre des comptes (principe d' « *Accountability* »).

Perspectives au-delà du présent. Nécessité d'une éthique responsable pour le futur :

Tout est numérique et rien n'échappe au phénomène « Big Data » dont la vocation première est (ou était) d'asservir la technologie aux activités de tri, filtrage, agrégation, groupage de l'information. A nous, humains le pouvoir de décider, en temps-réel s'il vous plait. Les pionniers Alan Turing, John McCarty, Marvin Minsky ont posé les jalons de l'Intelligence Artificielle (IA) à présent championne d'échecs et de go. La technologie de décision automatique est en marche et y faire barrage relèverait du voeu pieu, et il n'est nullement question de poser un quelconque moratoire scientifique, technologique. Ce qui est faisable peut être fait, le possible devient probable. Nous avons bien conscience de la puissance dont nous disposons, une puissance phénoménale depuis peu puisque nous commençons à prendre conscience des influences globales et à long terme de nos actions au présent. Penser au long terme c'est repenser notre responsabilité envers nous-mêmes, la nature et les générations futures, celles qui n'existent pas encore.

« **La gouvernance des données numériques est aussi une gouvernance pour le futur qui exhorte à revoir les dimensions de l'éthique d'aujourd'hui.** »

Pratiquer l'heuristique d'une peur fondée comme l'explique le philosophe Allemand Hans Jonas dans son ouvrage monument *Le Principe responsabilité* n'a rien de pusillanime : Eviter l'angoisse là où elle est de mise, ce serait de l'anxiété. Ce qui est bon pour l'humanité d'aujourd'hui peut ne pas l'être pour celle de demain.

5 / HOMO NUMERICUS ET HYPERCONNECTIVITÉ, RÉSISTER À LA COLONISATION NUMÉRIQUE, PRODUIRE DU BIEN COMMUN



du Pr. Solange Ghernaouti

Directeur du Swiss Cybersecurity Advisory & Research Group / Présidente de la Fondation SGH – Cybermonde / Associate Fellow Geneva Center for Security Policy / Membre fondateur de Heptagone Digital Risk Management & Security

John Conally, secrétaire d'Etat au Trésor américain du président Nixon affirmait : « Le dollar c'est notre devise, c'est votre problème », à l'heure de l'hyperconnectivité, cette maxime paraphrasée « les *Datas* sont notre monnaie, c'est votre problème » pourrait être celle des acteurs hégémoniques d'Internet qui imposent leur vision du monde qu'ils ont colonisé.

« Le numérique, réactualise le mythe du feu de Prométhée à l'heure du Cyberspace, « toute innovation technique est à double face selon le changement qu'elle opère dans la distribution et l'exercice du pouvoir, elle enlève le pouvoir à certains pour le donner à d'autres, en changeant la réalité pour tous »¹¹⁶. »

C'est effectivement ce qui se passe avec la maîtrise des données par des entreprises hégémoniques du Net. Connectés, les internautes se laissent déposséder de leurs données qui sont sources de profit et de pouvoir pour les entités qui maîtrisent les services et les technologies.

Les processeurs, nouveaux vecteurs des cyberattaques

L'article du 21 décembre 2017 publié par l'agence Bloomberg « *How Tech Companies Own Your Day* »¹¹⁷, illustrés de nombreux tableaux et graphiques, met en évidence les multiples dépendances de nos activités quotidiennes à des fournisseurs tels que Google, Apple, Samsung, Microsoft, Amazon, ou encore Facebook. Force est de constater que la vie cachée des données des internautes échappe à leur compréhension et à leur maîtrise. Sommes-nous en mesure de reprendre le contrôle de nos données et des équipements technologiques qui composent notre environnement et nous déterminent ?

¹¹⁶ R. Berger, S. Ghernaouti, « Technocivilisation : pour une philosophie du numérique » Focus Sciences, PPUR, 2010

¹¹⁷ <https://www.bloomberg.com/graphics/2017-how-tech-owns-your-day/>

Ce constat de dépendance, dont nous sommes les témoins et les acteurs, est aggravé, par la prise de conscience de la dépendance du numérique aux concepteurs et fabricants d'équipements comme nous l'a dramatiquement rappelé l'actualité du 3 janvier 2018 qui a mis en évidence la fragilité du monde numérique sur lequel nous bâtissons notre société. En effet, Google rendait public des vulnérabilités (Spectre et Meltown), liées à des failles de l'architecture et du mode de fonctionnement d'une large gamme de processeurs Intel, ARM et AMD. Elles permettent de développer des attaques pour dérober des données et porter atteinte à la confidentialité des informations traitées par ces processeurs. Le cas est emblématique de par l'ampleur et le nombre de systèmes concernés y compris dans domaines d'utilisation très sensibles (armement, défense, diplomatie, gouvernement, santé, finance, ...).

Il ne s'agit pas d'un problème de logiciel ni de sécurité informatique, mais d'un défaut de conception des processeurs dont les vulnérabilités, si elles sont exploitées (mais peut être le sont-elles déjà puisque ces failles existent depuis longtemps ?), conduisent à un problème de sécurité informatique majeur. Ce qui est fondamentalement nouveau est que le processeur, le cerveau de l'ordinateur, est devenu le vecteur de cyberattaques. C'est un peu comme si on avait construit une maison, avec du béton qui ne s'avère ne pas être du béton armé. La bâtisse risque de s'effondrer même si elle possède des solutions de sécurité comme une porte blindée ou des barreaux aux fenêtres. Car ces solutions de sécurité ont été installées pour répondre à un problème de sécurité particulier et non pour pallier des défauts de conception de la maison ou de ceux liés à un choix de composants matériels manquant de robustesse. Ceci indépendamment du fait que la maison, avec ses solutions de sécurité, ait été vendue très cher à son propriétaire. Peut-on vivre avec ce risque d'effondrement et ce manque de confiance ?

« En faisant le choix de privilégier les performances des processeurs au détriment de leur sécurité et fiabilité, concepteurs et fabricants de processeurs informatiques n'ont pas voulu payer le prix de la sécurité, mais nous allons tous payer celui de l'insécurité. »

Cyber-insécurité, défauts de conception et usages abusifs, détournés et criminel de l'informatique a fait la une du quotidien indien *The Tribune (voice of the people)* le 4 janvier dernier, qui informait du piratage informatique de la plus grande base de données d'identification biométrique du monde concernant plus d'un 1 milliard d'indiens (la base Aadhaar concerne 99% des personnes de plus de 18 ans en Inde)¹¹⁸. En effet, le gouvernement indien a instauré depuis 2009, l'identification des résidents par un numéro unique à douze chiffres auquel est associé leurs données personnelles et biométriques. L'agence UIDAI (*Unique Identification Authority of India*), qui dépend du ministère de l'électronique et des technologies de l'information, en a la responsabilité. Cette base permet entre autres, de créer des cartes d'identités, des passeports, d'ouvrir des comptes bancaires, de payer

¹¹⁸ <http://www.tribuneindia.com/news/nation/rs-500-10-minutes-and-you-have-access-to-billion-aadhaar-details/523361.html>

des factures, de réaliser des contrôles d'accès et d'authentification par empreintes digitales ou scan de l'iris, d'obtenir des cartes SIM pour la téléphonie mobile, des Apps ou encore pour certains, de la nourriture.

Objets connectés et hyperconnectivité, catalyseurs d'insécurité et d'atteinte à la vie privée

Ce défaut de prise en compte des exigences de la sécurité informatique dans la conception des systèmes existe également dans la majorité des objets connectés à Internet et des logiciels d'application, qui privilégient la mise rapide sur le marché de produits qui n'intègrent pas de sécurité pour des raisons de performance, de convivialité ou de coût. La sécurité coûte cher et personne, à moins qu'elle n'y soit contrainte, ne souhaite supporter le coût de la sécurité informatique. Au final c'est souvent l'utilisateur final et la société tout entière qui en supporteront les coûts réels. Ce qui a été une fois de plus confirmé à la fin de l'année 2017 par l'annonce d'une vulnérabilité des routeurs Huawei, qui équipent de nombreux réseaux de télécommunication, qui a permis de créer des réseaux de *Botnet* d'objets connectés pilotés pour réaliser des cyberattaques en déni de service distribué (il s'agirait des variantes Satori et BrickerBot du botnet Mirai découvert en 2016).

Il est désormais nécessaire et urgent de pouvoir utiliser des services et des équipements qui aient été conçus en intégrant les exigences de la protection des données et de la sécurité au plus tôt de leur cycle de vie et de faire de la sécurité « *by Design* » et de pouvoir opérer des contrôles de la qualité de la sécurité de ces éléments avant leur mise sur le marché, de manière analogue à ce qui est réalisé dans les processus de validation des médicaments avant leur commercialisation.

L'Homo numericus, un changement de paradigme, des questions fondamentales non - résolues

Avec le tout numérique, l'hyper-connectivité permanente, l'automatisation à outrance et la globalisation des échanges, nous ne vivons plus avec l'ordinateur, mais nous apprenons à vivre dans le monde de l'ordinateur en intégrant les contraintes technologiques, en les subissant un peu à l'instar du tabagisme passif. Plus nous sommes connectés (*On Line*), plus notre existence devient une existence hors sol, retranchée du vivant, déconnectée de la réalité du vivant. Plus les mondes virtuels nous paraissent plus vivants que le monde réel et plus nous devenons absents au monde. Plus les technologies semblent combler nos attentes avec des services personnalisés, plus les algorithmes se substituent à l'action humaine dans des processus de prise de décision et de réalisation, plus nous pouvons ressentir nos faiblesses humaines. Ainsi, nous intégrons de manière subliminale parfois, que l'humain devient superflu. Sommes-nous déjà entrés dans l'ère de l'obsolescence programmée de l'humain ? Voulons-nous devenir des zombies pilotés par des *e-trucs* et des *Smart* choses qui tend à nous rendre transparents, dénués de tout libre arbitre ? Sommes-nous aveuglés par des

mirages technologiques, endormis par des divertissements addictifs, séduits par la facilité du « sans effort » et d'un certain confort que procurent les technologies du numérique qui nous assistent en permanence ?

Saurons-nous en mesure de résister au pouvoir totalitaire d'un modèle de société du tout numérique et du tout connecté tout le temps ?

« **Modèle imposé, que nous acceptons implicitement, auquel nous nous soumettons et que nous contribuons à développer par nos usages numériques et par notre autorisation sans limite de durée et d'usage de l'exploitation de nos données. Modèle basé sur l'exploitation des données fournies par l'utilisateur mais aussi collectées et générées à partir de traitements informatiques à son insu. Modèle qui empêche de penser et de réaliser des modèles alternatifs, puisque notre imagination a aussi été colonisée par les technologies.** »

Saurons-nous transformer les progrès technologiques en progrès social et politique ? Serons-nous suffisamment courageux, rigoureux et exigeants pour être en mesure de reprendre notre liberté et notre vie privée afin de ne pas être asservis par des technologies et par ceux qui les conçoivent, les fabriquent, les mettent en oeuvre et les gèrent ? Serons-nous capables de décider de notre destin d'humain avant que le point de non-retour ne soit atteint ? Pour que l'utopie de la société de la connaissance, ne se transforme pas en réalité de techno-crétins, disciples dociles, aliénés par des techniques qui les dépassent mais parfois satisfaits par des perfusions de flux numériques et une servitude volontaire.

De nouveaux risques liés à l'intelligence artificielle

En offrant de nouveaux possibles, les avancées technologiques façonnent l'évolution de nos comportements, tout en créant de nouvelles habitudes et dépendances. Opportunités pour certains, risques pour tous, forgent le changement de société dont nous sommes témoins et acteurs. Avec la convergence des nanotechnologies, des biotechnologies, de l'informatique et des sciences cognitives, nous sommes passés à l'ère des technosciences. Le vivant et le non-vivant, interconnectés par un Internet de toutes choses, sont des sources inépuisables de données et de génération de flux informationnels. Le corps, le cerveau humain, les mouvements, les comportements, les sentiments ou les émotions sont un minerai informationnel capté et traité en permanence par des opérations arithmétiques et logiques. Les fournisseurs de technologies considèrent l'individu comme un système d'information, un objet. Connecté, il participe bon gré, mal gré à l'exploitation de ses données. Il alimente un marché *a priori* sans limite. Il favorise à son insu l'apprentissage des machines, le développement d'algorithmes prédictifs, de systèmes d'aide à la décision, d'intelligence artificielle ainsi que le courant transhumaniste. Ainsi, il contribue à la délégation de ses responsabilités et de ses

libertés à des ordinateurs avec lesquels il interagit mais aussi qui peuvent agir pour lui, le remplacer, l'influencer, le surveiller, le contrôler.

La possibilité de l'amélioration artificielle des capacités humaines physiques et cognitives laisse entrevoir un horizon d'êtres hybrides issus de l'électronique et du biologique. Utiliser des technologies à des fins non thérapeutiques, c'est considérer l'humain comme une chose à améliorer. Le risque que cette transformation artificielle soit réalisée dans un cadre normatif des manières d'être, de penser et d'agir, imposé par des acteurs hégémoniques des technosciences et fervents adeptes de l'ultralibéralisme, n'est pas négligeable. Dès lors, l'individu pourrait se retrouver amputé de ce qui fait sa condition humaine, de sa personnalité, de ses forces et faiblesses. L'expression d'humain augmenté est alors un abus de langage car il s'agit d'un humain transformé, standardisé, voire simplifié, mais surtout un humain piloté et contrôlé, via les technosciences, par des entités licites ou illicites qui les contrôlent. En effet, le risque de détournement, d'usage abusif, criminel et terroriste des objets connectés, équipements électroniques, systèmes informatiques et réseaux de télécommunication est réel, comme en témoigne le nombre d'incidents de sécurité plus ou moins graves révélés en permanence et affectant tous types d'infrastructures, y compris celles critiques ou a priori hautement protégées.

« L'expression d'humain augmenté est un abus de langage car il s'agit d'un humain transformé, standardisé, voire simplifié, mais surtout un humain piloté et contrôlé, via les technosciences, par des entités licites ou illicites qui les contrôlent. »

L'humain doit-il être modifié, éventuellement augmenté par la technique ? À partir de quelle technologie, quantité de technologies ou degré de d'intégration de celle-ci dans le corps peut-on encore définir un être comme étant humain ? Est-ce que la frontière de la peau permet de faire la différence dans l'hybridation du biologique et du technique ? L'effraction corporelle est-elle nécessaire ou doit-on déjà considérer une personne dépendante aux objets technologiques et connectée en permanence, comme un mutant, un primitif du futur ... ?

Complexité et perte de contrôle, la fuite en avant technologique

S'il est difficile aujourd'hui de maîtriser la cybersécurité, de réduire les vulnérabilités, de lutter contre la cybercriminalité, d'éviter les dérives comme par exemple la surveillance de masse, la fin de la vie privée, du libre arbitre, de l'autonomie ou de la démocratie, de réguler ou encore d'instaurer les niveaux de confiance nécessaires au bon fonctionnement de la société, qu'en sera-t-il demain avec des systèmes encore plus complexes, plus miniaturisés et invisibles, plus intriqués, interconnectés et interdépendants, plus «intelligents»? Comment sécuriser toute la chaîne des acteurs, systèmes, processus, algorithmes, services liés aux *Big Data*, à l'intelligence artificielle, à l'Internet de toutes choses ? Comment s'assurer de la sécurité, de la fiabilité, de la sûreté de tous les composants et

de toutes leurs interrelations, durant tout leur cycle de vie (développement, fabrication, implantation, gestion, utilisation, élimination) ?

La complexité des environnements technologiques mis en place est devenue telle que l'humain ne peut penser pouvoir la maîtriser qu'en ayant recours à encore plus de données, plus d'algorithmes, de processeurs interconnectés et de traitements. Cette fuite en avant est paradoxale puisqu'il ne les maîtrise pas, ne les comprend pas, mais est enclin à leur accorder sa confiance et à se soumettre à eux. Dans tous les cas, la question centrale demeure : qui sera en mesure de contrôler ces nouvelles infrastructures technologiques ?

Enjeux de société et bien commun à l'heure de la mondialisation

Les sciences du vivant et de l'ingénierie soulèvent des enjeux sociétaux et défis idéologiques pour tous, comme c'est déjà le cas avec l'usage des drones tueurs qui pourraient devenir autonomes et décider de tuer sans contrôle humain. Il est urgent, hors des injonctions d'innovation et des discours messianiques qui accompagnent le développement des technosciences, de débattre de ces questions afin de contribuer à la définition du bien commun et du bien vivre avec les technologies sans en être esclave. C'est à ce prix que l'humain pourra conduire de façon éclairée et responsable le développement d'une techno-civilisation ouvrant la voie à un humanisme renouvelé et au service des générations futures. Notre devenir ne doit pas être la résultante de logiques financières et de puissance hors de contrôle, ni dépendre de dictatures technico-économiques. Celles-ci ignorent le principe de précaution et sont rarement synonymes de progrès social et politique.

Internet, fruit d'une évolution technologique inscrite dans un contexte géopolitique et économique particulier a donné naissance au cyberspace. Cet environnement numérique, qui prolonge notre réalité physique et quotidienne, est structuré par les technologies de l'information et de la communication, par les services offerts et les usages que nous en faisons et par les acteurs qui les fournissent. Comme la terre, la mer, l'air ou l'espace, le cyberspace est un environnement commun qui doit être partagé et régulé. Depuis ses origines, différents mécanismes mis en place en marge des institutions internationales, permettent la coordination globale de son développement technique.

« Dans la mesure où l'Internet possède une couverture mondiale et que les cyberattaques ne s'arrêtent pas aux frontières nationales, les accords régionaux ou bilatéraux sont insuffisants. Le cyberspace requiert des mesures de coordination, de coopération et de législation effectives au niveau local, tout en étant compatibles au niveau international. La question actuelle est de savoir comment mettre en place de telles règles et sous l'égide de quelle(s) institution(s) ? »

Seule une approche multi-gouvernementale d'envergure internationale s'inscrivant dans le cadre des Nations Unies semble capable de définir et de mettre en place un tel instrument de régulation supranationale. À défaut, on peut craindre que l'anarchie ou la loi du plus fort ne s'impose dans le cyberspace. Au vu de l'importance en nombre et en intensité des cyberattaques pratiquées par toutes sortes d'acteurs indépendamment de leurs motivations, il devient urgent de spécifier les pratiques inacceptables et de fixer les responsabilités de chacun.

À l'instar de la Déclaration de Genève sur les Droits de l'Enfant de 1924, il serait souhaitable qu'il existe un texte de référence qui reconnaîtrait et affirmerait l'existence de droits spécifiques aux internautes et préciserait la responsabilité des acteurs du cyberspace à l'égard de l'humanité et des générations futures. Paraphrasant la Déclaration de 1924, une Déclaration de Genève du Cyberspace, pourrait par exemple réaffirmer dans son préambule, que « les hommes et les femmes de toutes les nations reconnaissent que l'humanité doit donner au cyberspace ce qu'elle a de meilleur, affirmant leurs devoirs, en dehors de toute considération de race, de nationalité, de croyance ».

Une telle Déclaration servirait de socle à un futur Traité International du Cyberspace, lequel constituerait l'instrument juridique permettant de poursuivre les délits, quel que soit leur lieu de réalisation ou leur origine (ce qui n'est pas le cas actuellement). Ainsi, les cyberattaques portant atteinte à la vie humaine, aux droits fondamentaux, à la paix, à la sécurité des nations ou à la stabilité des États, deviendraient punissables par le droit international, même si elles ne sont pas répréhensibles à un niveau national, par exemple si elles émanent de « paradis digitaux »¹¹⁹. Un tel traité autoriserait la poursuite des responsables des cyberattaques quelle que soit leur localisation géographique.

Ces recommandations et constats ont déjà été effectués, par un groupe d'experts à l'issue de l'initiative du *Global Cybersecurity Agenda (GCA)* de l'Union Internationale des Télécommunications débutée en 2007¹²⁰. Ainsi, sous l'égide et du juge norvégien Stein Schjolberg, *Chairman* et de la professeure suisse Solange Ghernaoui *Work Area Leader* du GCA, des publications internationales¹²¹ déterminantes et fondatrices ont vu le jour et se sont enrichies depuis. Ces initiatives doivent encore être complétées et finalisées dans le cadre des Nations Unies. Elles doivent notamment être portées par la communauté internationale afin de traduire une volonté politique et économique forte, seule capable de motiver un engagement réel de tous les États. Un simple document ne peut à lui seul freiner les conflits dans le cyberspace, néanmoins il serait déterminant pour accentuer la prise conscience des États, pour préciser les lignes directrices

¹¹⁹ Par analogie aux paradis fiscaux, les paradis digitaux désignent des pays où la réglementation et les mesures de lutte contre la cybercriminalité sont faibles voire inexistantes.

¹²⁰ <http://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>

¹²¹ Stein Schjolberg & S. Ghernaoui « *A global treaty on cybersecurity and cybercrime; A contribution for peace, justice and security in cyberspace* », first edition, 2009. <http://www.cybercrimelaw.net/Cybercrimelaw.html>

S. Schjolberg « Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace » (10th Edition, June 2015)

http://www.cybercrimelaw.net/documents/Draft_Treaty_text_on_International_Criminal_Tribunal_for_Cyberspace.pdf

S. Schjolberg, S. Ghernaoui « A Geneva Convention or Declaration for Cyberspace: A global framework on cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace » VFAC Review, No. 12, October 2016, Korean Institute of Criminology. <https://eng.kic.re.kr>

du développement du cyberspace et de son écologie, et pour développer des mesures de confiance. Identifier les limites des pratiques acceptables encouragerait la dénonciation des usages abusifs et détournés des technologies de l'information constituerait un premier pas vers plus de stabilité et de sécurité *On Line* comme *Off Line*.

Il serait dommage de laisser aux seules mains des géants de l'informatique et de l'Internet, le soin de fixer les règles du jeu et du contrôle du cyberspace. Une grande confusion règne dans les démarches, finalités et motivations des acteurs, notamment depuis que Microsoft a demandé en février 2017 que les civils soient mieux protégés dans le cyberspace. C'est à San Francisco lors d'une grande messe commerciale de la sécurité¹²², que Brad Smith, responsable juridique de Microsoft, a proposé une Convention Digitale de Genève¹²³ basée sur la Convention de Genève de 1949 relative à la protection des civils en temps de guerre¹²⁴.

S'il est évidemment louable de voir les géants digitaux comme Microsoft se préoccuper de la cybersécurité mondiale, il est permis de questionner leur légitimité et leur indépendance quand ils proposent leurs bons offices pour définir les règles globales de la gouvernance du numérique. Le fait que ces multinationales se posent comme gendarmes du monde digital, ou comme leurs assistants, d'égal à égal avec les États et les Organisations Internationales crée des situations à très haut risque de conflit d'intérêt. Le risque est d'autant plus grand que les enjeux commerciaux sous-jacents sont gigantesques et que les géants digitaux sont déjà en confrontation avec des États sur des questions liées à la confidentialité des données qu'ils possèdent sur des personnes qui intéressent les instances de justice et police. Entre droits des citoyens et des consommateurs, droit des entreprises et droit des États, le contexte est aussi complexe qu'explosif. Tous les discours ne peuvent faire oublier la réalité économique et les stratégies d'emprise des géants de l'informatique et des télécoms. Leur pouvoir économique et leur puissance politique sont à la mesure des enjeux économiques et géo-stratégiques associés au monde numérique. Nous devons composer avec eux, les consulter, mais pas nous laisser imposer leurs réglementations. Dans le digital, comme dans tant d'autres domaines, c'est au politique de réguler les multinationales et non aux multinationales de dicter la régulation aux politiques. Le concept de neutralité, sonne faux lorsque qu'il est avancé par des fournisseurs en laissant croire que la technologie est neutre, alors que les infrastructures, les algorithmes, les services et les données sont créés, imposés et contrôlés par des multinationales qui n'ont d'autres buts que le profit, la croissance, la domination monopolistique et la pérennisation de celle-ci.

Résister à la colonisation numérique

De l'ère de la société de l'information promue par le sommet mondial de la société de l'information (Genève, WISIS 2003) nous sommes passés à celle d'une société

¹²² <https://www.rsaconference.com/events/us17>

¹²³ <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0001eqppgm6p5ezju-jk1fpzx0tj59>

¹²⁴ <https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf>

de la surveillance généralisée, rendue possible par l'usage extensif du numérique, ère pilotée par des entités à la volonté hégémonique affichée. En effet, nous vivons à l'ère de la «colonisation numérique». Comme aux siècles passés, le processus de colonisation consiste à dépouiller les colonisés de leurs ressources et de transformer en profit, tout en les maintenant en état de dépendance et d'infériorité.

Aujourd'hui, les ressources sont nos données. L'histoire se répète avec la conquête des cyber-territoires et le pillage des données fournies par les utilisateurs du numérique ou capter et générer à leur insu. La colonisation, c'est la soumission du plus faible au plus fort, esclavage, travail gratuit, prise en otage des ressources du pays, imposition des règles de comportement, des prix ... Force est de constater que nous participons, à bien des égards aujourd'hui à notre colonisation numérique par des fournisseurs de services qui font travailler «au noir» les individus à la production des données, en échange d'un service dit gratuit afin que ces acteurs hégémoniques en position de monopole les transforment en gains financiers. Si un service est gratuit, cela signifie que l'utilisateur le paye en nature avec ses données et qu'il en est de ce fait dépossédé.

Les fournisseurs ont tous les droits – y compris ceux de modifier de manière unilatérale les conditions d'utilisation. En face, les utilisateurs n'ont aucun droit et encore moins de choix, car il y a de moins en moins de possibilité de pouvoir s'en passer, certaines applications ou services sont devenus obligatoires et se sont substitués à toutes alternatives.

« C'est totalement paradoxal : le consommateur est nu, transparent, et ceux qui possèdent et maîtrisent ses données sont totalement opaques. On ne connaît rien de leur processus internes, comment ils stockent les données, comment ils les traitent, la durée de stockage, la finalité des traitements ... Il faut imposer à ces sociétés de la transparence, les obliger à rendre des comptes, se donner la possibilité d'effectuer des audits. »

Une évolution non naturelle

L'innovation technologique n'est pas une évolution naturelle, contrairement à ce que les sociétés hégémoniques du Net¹²⁵ souhaiteraient nous faire croire afin d'annihiler notre éventuel désir de résistance ou de contestation. En fait, rien n'est naturel car les choix technologiques sont conduits par des logiques économiques contextuelles (capitalisme, ultra libéralisme d'origine Nord-américaine), que c'est le progrès technologique, que l'on ne peut arrêter, que ce sont les consommateurs qui le veulent. Ceci est faux, il suffit pour s'en convaincre d'apprécier les ressources et les budgets alloués par ces acteurs à la communication d'influence, au *Marketing*, au *Lobbying*. Les internautes ont été rendus addictes à des services dont l'utilité est de les garder captifs, dociles et tenus en laisse électronique en

¹²⁵ Il s'agit notamment des GAFAM (Google, Amazon, Facebook, Apple, Microsoft) et NATU (Netflix, AirBnB, Tesla, Uber)

permanence. Aucune campagne de sensibilisation ou d'éducation aux risques de perte de maîtrise de leurs données et à leurs conséquences n'a été réalisée.

Ces compagnies transnationales basées aux USA que sont les GAFAM et les NATU représentent les compagnies les plus importantes, les plus grandes, les plus dominantes du monde. Leur principal objectif est de tirer profit d'un marché mondial et de l'économie globale tout en empêchant la compétition ou la survenue de nouveaux acteurs. Leur pouvoir économique leur permet d'acheter les bonnes idées, la concurrence potentielle de nouveaux entrants. Ils utilisent tous les moyens à disposition pour défendre leurs droits et les règles du marché afin de favoriser leur croissance comme les règles du commerce international tout en limitant le pouvoir des pouvoirs publics, des gouvernements d'intervenir, de réguler leur comportement pour l'intérêt public, pour cela ils détournent les processus démocratiques traditionnels. Ils détournent les règles à leurs seuls avantages et imposent leur vision du monde / les règles du jeu de l'économie numérique à leurs seuls avantages. C'est pour cette raison que les notions de protection des données personnelles, d'intimité numérique (*Privacy*) leur pose problème car c'est un frein à l'exploitation, à la circulation sans limite, sans restriction, des données. Aux USA, une donnée est considérée comme une valeur marchande comme une autre, pas en Europe pour ce qui concerne les données personnelles. Ils oeuvrent pour limiter les obligations des gouvernements et se décharger de leur responsabilité envers les pays, les populations de devoir partager, redistribuer les bénéfices.

Les avancées technologiques qu'ils produisent ne sont pas partagées mais imposées pour maintenir dans un état de dépendance tous les autres acteurs, indépendamment de leur culture ou besoins spécifiques. Au lieu d'apprendre à pécher et à construire à l'ère numérique, de développer l'économie numérique tous ont besoin les populations pour subvenir à leurs besoins particuliers, les entités hégémoniques du Net et les maîtres de la mondialisation numérique définissent à la place des acteurs locaux, leurs besoins et leurs donnent des boîtes noires à utiliser, sans jamais donner les clés de la maîtrise de celles-ci et de celle de la gouvernance des cyber-risques et de la cybersécurité, tout en les convainquant qu'il n'y a pas d'autres solutions possibles !

Refuser une soumission docile, briser un cercle non vertueux

Catalyseur du bouleversement sociétal en cours, Internet ne complète pas les services traditionnels, mais se substitue à eux. Les services imposés aux internautes par souci de rationalité économique offrent une relative facilité d'usage, mais sans garantie de sécurité. Cette industrie repose sur quelques fournisseurs hégémoniques d'Internet qui ont construit leur pouvoir économique et politique par le numérique, auquel nous nous soumettons avec docilité et parfois délectation. Ces firmes bénéficient généralement d'aides de l'Etat du pays dans lequel elles s'implantent. Pour ce dernier, le retour sur investissement n'est souvent que très marginal du fait de l'optimisation fiscale et de la concurrence déloyale. La valeur créée ne profite pas aux ressortissants du pays car les

acteurs économiques locaux classiques ne peuvent être compétitifs. Ainsi à l'ère numérique, ceux qui possèdent et maîtrisent les données sont en mesure d'en exploiter les richesses et d'en tirer des bénéfices. Répondre à la question de savoir à qui appartiennent les données est complexe et soulève des questions d'ordre politique, économique, juridique, technologique et sociale. Toutefois, elle trouve une réponse pragmatique dans les conditions d'utilisation des services, que les personnes acceptent – souvent sans les lire ou les comprendre. Les fournisseurs ont tous les droits – y compris ceux de modifier de manière unilatérale les conditions d'utilisation, les utilisateurs ont aucun droit !

La maîtrise des données passe également par celle des infrastructures matérielle et logicielle de captation, de transfert et de traitement des données (téléphones intelligents, tablettes, divers capteurs comme Amazon Echo ou Google box, Google glass, Apple TV, montres connectées, infrastructures de communication, ...). Être au plus proche de l'utilisateur, non seulement sur les lieux professionnels mais aussi dans l'intimité des foyers, des chambres à coucher, au plus proche de la personne (dans sa poche) mais aussi dans son corps ...

Par ailleurs, plus le service est personnalisé, plus l'utilisateur est captif du fournisseur de service et dépendant de ce dernier. Il nous appartient de casser ce cercle non vertueux du développement du numérique et de son économie, de résister à la soumission technologique pour sauvegarder une certaine liberté et indépendance de penser, d'agir et d'être. Nous devons désormais apprendre à résister à la puissance du tsunami numérique *Made In Silicon Valley* qui est en train de nous submerger sous couvert d'humanisme revisité et de pseudo-évangélisme techno-centré. Affirmons haut et fort notre souhait que la fin de la vie privée, que la transparence totale, mais unilatérale et que la surveillance de masse ne soit pas la norme du XXI^e siècle. Nous ne pouvons ni accepter, ni contribuer au pillage de nos données, devenir les fossoyeurs de notre vie privée, de notre travail, de notre économie, de notre culture et modèle social sous prétexte d'innovation technologique.

Chapitre 4 :
Les pistes de réflexions éthiques
pour tendre vers une confiance
numérique

Ethics



Y a-t-il une éthique propre au numérique ? Cette question revient régulièrement et fait débat, tellement il apparaît non naturel d'associer une science humaine à une science technologique que presque tout oppose. Et pourtant, le numérique crée de toute part des injonctions contradictoires qui ont par conséquent des répercussions éthiques spécifiques aux NTIC. Si les *Big Data* sont éthiquement neutres, leurs usages ne sont pas. Des comportements singuliers naissent des usages de ce nouvel espace-temps que génère le numérique. Les NTIC sont un phénomène culturel voire anthropologique. Ils produisent de nouveaux comportements, de nouvelles visions du monde, et de nouvelles normes sociales.

On peut prendre l'exemple, de l'anonymisation qui pose la question de la responsabilité des personnes dont l'invisibilité peut dédouaner de certaines règles de bienséance. L'instantanéité et l'ubiquité que permet l'Internet, répercutent nos actes de paroles et de pensée de manière conséquente et irréversible. Désormais, l'éthique et la technologie ne doivent plus être mises en relation selon un dispositif à deux étapes. Les questions éthiques doivent faire partie intégrante de leur mission et ainsi construire une réflexion éthique orientée. Dès lors, on ne parle plus d'une approche interdisciplinaire mais plutôt d'une fusion aboutissant à une véritable éthique du numérique où la question des implications sociales et morales s'intègre dans les NTIC. Dans ces conditions, il devient essentiel d'établir des attentes et des préconisations éthiques spécifiques au monde numérique et de réifier des nouveaux systèmes de valeurs d'éthique et de droit, en gardant toujours en tête cette question : est-ce que le numérique peut induire un risque de mésusages de nos comportements éthiques ?

D'autre part, en éthique, le terme de « valeur » est de l'ordre du devoir-être. C'est un étalon de mesure qui permet de jauger les faits. Il indique des idéaux à poursuivre. Ce mot a une connotation générale et dynamique ; il a d'abord une évocation philosophique avant d'avoir une retombée éthique. Un des fondements de l'éthique est cette impérativité à faire appel à la rationalité des acteurs. Cette idée se structure via une entente dans la coordination, l'échange et le partage entre les protagonistes. Chaque personne contribue à la recherche d'une intercompréhension de la situation à analyser. Cela présuppose donc un certain consensus et solidarité entre les interlocuteurs qui partagent une même finalité. Si l'éthique est déjà par nature complexe à définir, sa mise en perspective avec le numérique relevait d'un autre défi. L'éthique demande une vision, un dessein, une ambition qui se concrétise dans une orientation.

Par ailleurs, toute technologie définit une relation entre les êtres humains et leur environnement, tant humain que physique. L'idée d'une dynamique technologique suivant sa propre trajectoire reste très forte. L'héritage de McLuhan selon lequel les technologies se développent et ont une répercussion sur la société demeure prégnant. Les NTIC ont le pouvoir d'hypnotiser la société, du fait que toute nouvelle technologie diminue donc l'interaction des sens et de la conscience, et plus précisément dans le domaine nouveau des innovations où se produit une sorte d'identification du sujet et de l'objet. Aucune technologie ne peut être considérée comme purement instrumentale. Ceci est particulièrement pertinent lorsqu'il s'agit de grands SI automatiques, mis au point pour contribuer à la gestion et l'intégration des grandes organisations, comme les structures de santé. Dans ces conditions, les *Big Data* apparaissent principalement comme un système social, avec ses caractéristiques psychologiques, sociologiques et éthiques. L'écart entre l'espace d'action et de représentation de l'action s'est fortement réduit. Une ambiguïté s'installe entre action réelle du numérique et représentation d'elle-même, ou entre mouvement continu et gestion discrète de ce mouvement. Dès lors, le numérique est un lieu où la liberté semble être sans limites, du fait que tout est dans la continuité du mouvement. En même temps, ce mouvement est finalement discret et donc facilement contrôlable. Par conséquence, l'éthique du numérique doit essayer de penser le rapport entre geste et cristallisation du geste. C'est à partir de cette approche que notre réflexion éthique doit commencer sa démarche et poser les principes éthiques spécifiques à l'action digitale afin de tourner vers une plus grande confiance numérique.

1 / DE L'ÉTHIQUE DES ALGORITHMES ET DE L'INTELLIGENCE ARTIFICIELLE



de Christine Balagué

Professeur à l'Institut Mines Télécom-TEM, Titulaire de la Chaire réseaux sociaux et objets connectés, membre de la Cerna (Comité d'Éthique de Recherche sur le Numérique d'Allistène), membre du bureau de Dataia, institut de Convergence interdisciplinaire sur les données, ex-Vice-présidente du Conseil National du Numérique.

Quelques éléments de contexte :

L'un des grands enjeux sociétaux du numérique durant la métamorphose digitale de nos sociétés et de nos économies durant les vingt-cinq dernières années porte sur les données personnelles et le respect de la *Privacy*, qui a abouti en Europe à l'élaboration du GRDP, nouveau règlement européen qui va rentrer en vigueur en mai 2018, auquel les différents acteurs économiques doivent se soumettre en adaptant parfois en profondeur leur stratégie digitale. La question du respect des données personnelles dans une société numérique a ainsi bien avancée jusqu'au stade de la régulation. Plus récemment, un nouvel enjeu a émergé : l'éthique, la redevabilité et la transparence des algorithmes à l'ère de l'Intelligence Artificielle (IA). Nos vies et journées sont en effet de plus en plus dépendantes d'algorithmes : réveil le matin à une heure optimale grâce à un objet connecté, déplacement vers le lieu professionnel *via* un algorithme minimisant le temps de transport (de type Waze ou RATP), moteur de recherche sur Internet (Google, Bing, Qwant), traduction de texte (Google traduction), achat de produits sur un site de E-commerce (comme Amazon), recommandation de restaurant (comme La fourchette), utilisation d'Uber pour y aller, Trip Advisor et ses recommandations pour préparer ses vacances, réservation de vols *via* Orbitz ou Expedia optimisant les réponses selon différents critères (bas prix, vols directs, etc.), réservation de logement *via* AirBnB, recommandation d'activité physique *via* une montre connectée, ou d'un film pour le soir avec Netflix, et on pourrait en citer bien d'autres, touchant à des sujets plus sensibles comme la santé (algorithmes prédictifs donnant une probabilité d'avoir telle ou telle pathologie). L'enjeu de l'éthique des algorithmes est d'autant plus important aujourd'hui que l'intégration de l'IA dans les produits et services grand public explose dans tous les secteurs économiques.

Quels sont donc les problèmes posés par les algorithmes ?

« Le premier problème est l'opacité des traitements algorithmiques pour l'utilisateur final, et les effets potentiels de manipulation associés. »

Le cas des moteurs de recherche est révélateur : lorsque plusieurs utilisateurs effectuent la même requête, les résultats peuvent être différents, car des critères personnels sont intégrés à l'algorithme classant les liens qui apparaissent sur la page *Web* de l'utilisateur. Les chercheurs Epstein & Robertson en 2015 ont montré qu'un moteur de recherche peut faire bouger de 20% les intentions de vote des indécis lors d'élections présidentielles en fonction du classement des informations qui apparaissent lors d'une requête. Jesse Hirsh en 2016 affirmait que la transparence des algorithmes est un prérequis pour la démocratie.

« Le deuxième problème posé par les algorithmes est la diffusion massive de fausses informations (*Fake News*), en particulier sur les réseaux sociaux, dont le métier est de sélectionner par des algorithmes (souvent de *Deep Learning*), l'information vue par des millions d'utilisateurs sur leur page du réseau social. »

Les chercheurs Allcott et Gentzow ont montré en 2017 que lors de la campagne présidentielle américaine, les *Fake News* favorisant Trump se sont diffusées 30 millions de fois, celles favorisant Clinton 8 millions de fois, et qu'un adulte américain moyen a vu une ou plusieurs *Fake News* dans les mois avant l'élection, la moitié de ceux qui s'en souvenait les croyant vraies. Le rapport *Fake News Machine*¹²⁶ paru en 2017 révèle qu'on peut manipuler une élection avec 400 000 dollars aujourd'hui, en mettant en place un système de diffusion massive de fausses informations sur les réseaux sociaux.

« Le troisième problème posé par les algorithmes est la bulle de filtrage et l'enfermement créée par l'algorithme du réseau social Facebook, qui limiterait l'accès des individus à la diversité d'opinion. »

La chambre d'écho est le phénomène suivant lequel les individus sont plus amis sur Facebook avec des personnes qui leur ressemble (homophilie), Facebook favorisant ainsi les échanges avec des individus ayant la même opinion. La bulle filtrante est directement liée à l'algorithme de Facebook qui filtre l'information vue par les utilisateurs quotidiennement, les critères d'affinité, de type d'action et de récence favorisant un enfermement dans une bulle informationnelle donnée. Comme le résume Matthew Hughes, journaliste *The Next Web*, « comme la plupart des gens, je vis dans une bulle que j'ai créée, où les seules perspectives que je croise sont similaires aux miennes ». L'impact de la bulle filtrante de Facebook a

¹²⁶ Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin (2017). *The Fake News Machine How Propagandists Abuse the Internet and Manipulate the Public*, Trendlabs research paper, Trend Micro.

généralisé de nombreux débats aux Etats-Unis et en Europe sur le rôle de Facebook dans la campagne présidentielle américaine.

« Les algorithmes posent un quatrième problème actuellement, car ils peuvent être source de discrimination et de biais. »

La chercheuse Grazia Cecere, économiste à Télécom École de Management, en créant une publicité sur les STEM (Sciences, Technologie, Education, Mathématiques) sur un réseau social, a montré en 2017 que l'algorithme discriminait selon le genre, puisque la publicité était davantage distribuée aux hommes qu'aux femmes. Dans le cadre de recherche d'emploi ou du secteur de l'assurance, cette discrimination est illégale. Les biais des algorithmes peuvent provenir quant à eux de bases de données au départ qui ne sont pas de qualité (surpopulation d'une catégorie d'individus, données manquantes, etc.), ou de choix délibérés des concepteurs des algorithmes. Il a déjà été montré que les algorithmes peuvent construire des régimes de puissance et de connaissance, et être utilisés pour séduire, discipliner, décider, réguler et contrôler. Un algorithme biaisé peut aussi donner un résultat inattendu, comme le récent exemple testé par Facebook de *Chatbots* négociant entre eux qui aurait inventé un nouveau langage, ou les dérives racistes d'un autre *Chatbot* sur Twitter.

Face à ces enjeux, les questions d'éthique, de redevabilité et de transparence des algorithmes a émergé dans différents pays. Aux Etats-Unis, des rapports du bureau officiel de la Maison Blanche en janvier et Mai 2016 ont soulevé les potentielles conséquences des traitements algorithmiques. Un partenariat entre plusieurs grands acteurs américains (Facebook, Google, Amazon, IBM, etc.) s'est développé pour réfléchir sur la question de l'éthique dans les méthodes d'algorithmes de type *Deep Learning*, *Machine Learning* et plus largement de l'IA. La France n'est pas en retard sur ce sujet. Le rapport Ambition Numérique du conseil national du numérique rendu au premier ministre Manuel Valls en 2015 soulevait ces questions. La loi pour une république numérique du 8 octobre 2016 impose la transparence des algorithmes dans le secteur public et la loyauté des plateformes numériques. Le Conseil Général de l'Économie (CGE) a rédigé le rapport « Modalités de régulation des algorithmes de traitement des contenus » et la plateforme *TransAlgo* a été lancée, visant à développer des technologies, des méthodes, une culture et un savoir-faire pour le développement d'algorithmes responsables et éthiques. Le lancement de l'Institut de convergence *Dataia* montre également une forte ambition de la France sur ces sujets, au travers de ce programme interdisciplinaire sur 10 ans, dont l'objectif est de systématiser les réflexions et intégration de l'éthique, de responsabilité et de transparence dans l'IA.

2 / UNE ÉTHIQUE DU NUMÉRIQUE CENTRÉE SUR LES CITOYENS ET ORIENTÉE VERS DES SOLUTIONS TECHNIQUES



de Florence Picard

Docteur en Mathématiques / Actuaire / Présidente - EPA

Mes convictions sont nourries par les expériences pratiques d'amis entrepreneurs du Machine Learning et de l'Intelligence Artificielle (IA), et par les réflexions des chercheurs sur les sciences du numériques (ceux du CERNA, Serge Abitboul, Raja Chatila, ... ainsi que celles de Gilles Babinet, Gilles Dowek, Jean-Gabriel Ganascia, Daniel Le Métayer, Michel Serres, etc.

Dans mon métier d'actuaire, appliquant les mathématiques des probabilités et des statistiques au domaine de l'assurance, j'ai toujours vécu en compagnie des données. À l'époque (pas si lointaine), elles étaient soigneusement collectées, sagement rangées dans des bases de données et faisaient l'objet d'études statistiques, avec mesures d'erreur, et de modélisations basées sur des lois de probabilité. L'utilisation des données était un « métier », avec méthodes, bonnes pratiques et déontologie partagées.

À mon niveau, l'éthique se résumait à des principes simples acceptés par toute la communauté des mathématiciens : utiliser des données pertinentes pour le sujet d'étude (sans les trier pour éliminer celles qui pourraient perturber un résultat espéré), fournir seulement des résultats fiables selon les méthodes adaptées reconnues, et présenter honnêtement ces résultats sans abuser des présentations visuelles et des couleurs qui faussent l'objectivité et orientent la lecture.

Aujourd'hui, l'omniprésence des données et la puissance technologique des ordinateurs mettent les données à la portée de tous dans un mélange déroutant de transparence et d'opacité, d'ouverture et de quasi monopoles. Ouverture, car l'*Open Data* donne accès, pour tout le monde, à des données clé, qui auraient autrefois été réservées aux spécialistes des statistiques, rompus à l'utilisation des données et aux dangers d'une utilisation ou d'une présentation malhabile des résultats. Mais opacité, car, en général, chacun de ces citoyens ignore tout des algorithmes sur lesquels il s'appuie au quotidien pour prendre des décisions et agir dans la vie courante : il ne sait rien du code, des données utilisées et des choix de valeurs qui ont procédé à l'écriture de ces algorithmes par les géants qui les mettent gracieusement à notre service.

« Dans le monde numérique, quelle éthique pour guider nos actions ? Qui en décide ? A qui appartient-il d'ériger les principes de l'éthique numérique ? »

Avant l'ère numérique, l'éthique était un sujet de haut niveau, traité par les plus hautes instances, qui s'appuyaient sur des experts des domaines concernés : CCNE (Comité Consultatif National de l'Éthique) pour la santé, la fin de vie, la génétique, experts pour l'éthique de la Défense, de l'énergie, etc. Ces sages éclairés décidaient après mure réflexion de ce qu'il convenait de faire et de ne pas faire sur ces grands sujets de société et chacun les appliquaient ensuite à son niveau.

Aujourd'hui, cela est encore en partie vrai pour ces grands sujets sociétaux qui concernent la santé et les biens communs, même si les citoyens expriment de plus en plus fréquemment leur avis sur les réseaux sociaux et, *via* des pétitions, pèsent parfois avec force, sur les décisions. Pour plusieurs raisons, le bon usage du numérique ne peut plus être un sujet du seul ressort de ce haut niveau d'instances :

- les choix éthiques du numériques sont très fréquents et relèvent souvent de petites décisions de la vie quotidienne des individus,
- la technologie numérique ne permet pas toujours de dissocier facilement la décision éthique et l'action et pose donc le sujet au niveau de l'acteur, notamment du codeur d'algorithmes, et pas à celui des instances dirigeantes,
- l'autonomie relative des algorithmes, et souvent leur opacité, nécessitent que des choix éthiques soient opérés au niveau de leur conception technique et que des avancées soient opérées en matière de sciences fondamentales de logique mathématique.

Les choix éthiques sont faits le plus souvent par les individus, dans la vie quotidienne :

Dans la période récente, de grands choix de société relatifs au numérique n'ont pas été faits par les Etats, mais par les citoyens et par les plateformes : séduits par des services gratuits très utiles et performants, les citoyens ont fourni aux plateformes toutes leurs données de vie privée, alimentant ainsi un nouveau modèle économique disruptif.

Du fait de la puissance de ré-identification du *Big Data*, par ses choix individuels, le consommateur a aussi décidé pour les autres, sans vraiment s'en rendre compte. C'est le cas par exemple quand il partage des informations sur ses amis ou sa famille (par exemple via adresse gmail, compte FaceBook, etc.) sans leur demander leur avis. Il ne s'agit pas de grands choix réfléchis. Ce sont des micros choix individuels de tous les jours : « liker » ou être « follower », passer par des plateformes pour réserver un restaurant ou le faire directement, choisir Uber ou pas, évaluer par note la qualité d'une personne (chauffeur ou personnel d'un

hôtel), choisir tel moteur de recherche qui pratique le profilage, ou tel autre qui ne stocke pas les informations que vous lui donnez sur vous, mettre ou pas les photos de sa famille et ses amis sur les réseaux sociaux sans les en informer, etc. Mais en fait, s'ils ne sont pas conscients, et s'ils ne se situent pas dans un cadre éthique, tous ces choix individuels nous conduisent sans pilote vers une société que nous n'avons pas choisie explicitement, et que peut-être nous ne souhaitons pas. Ils peuvent nous conditionner, normer nos comportements et nous enfermer en nous-mêmes, dans les profils dans lesquels les algorithmes nous ont catégorisés.

Le numérique a écrasé les hiérarchies et a placé le citoyen peu informé, seul, face aux plateformes et aux réseaux sociaux. Les Etats s'évertuent, *via* les CNIL et les réglementations, à tenter de limiter les risques d'impact de ces bouleversements en matière de discriminations, de liberté et de financement des politiques publiques *via* l'impôt (dont la levée va se compliquer dans cette nouvelle économie numérique sans frontières). Mais le poids économique transfrontière des grands du numérique (GAFAM) relativise celui des Etats.

« C'est au niveau où sont opérés la plupart des choix numériques de la vie courante, au niveau de l'individu, que se joue l'éthique du numérique. »

Une éducation à cette nouvelle responsabilité est indispensable, mais sera longue et difficile, dans un monde où la technologie va très vite, sans laisser beaucoup de temps pour la réflexion et la compréhension des enjeux.

Décision et action sont moins souvent dissociés qu'auparavant :

Dans le monde professionnel, la numérisation imbrique plus étroitement qu'auparavant décision et action. C'est la même personne qui décide et agit. Auparavant, des directives opérationnelles pouvaient être données aux collaborateurs et leur application pouvait être contrôlée par les hiérarchies. La compétence technique des responsables le permettait. Aujourd'hui, l'évolution rapide des technologies rend les expertises très rapidement obsolètes et amène à remplacer l'obéissance à des règles par une démarche individuelle d'adhésion à un objectif et des valeurs.

Les pyramides hiérarchiques sont écrasées : le Directeur tape lui-même ses instructions par mail ou dans un réseau social interne à l'entreprise, modifie lui-même ses réservations de train ou d'avion sur son *Smartphone* ou à une borne, confectionne lui-même ses slides de présentation à un Conseil, etc.

Concernant des sujets plus complexes, la technologie est devenue si pointue et évolutive que le Directeur n'est plus compétent pour donner bon nombre d'instructions techniques. C'est celui qui fait qui sait.

« Dans cette complexité inaccessible de l'extérieur, au coeur de son action, le codeur est souvent seul face à ses choix et le seul capable d'apprécier si ce choix est éthique ou pas. »

C'est le cas par exemple pour la quantité de données qu'il va utiliser pour procéder au traitement qu'il a à effectuer : bien réfléchir aux données réellement utiles, coder l'algorithme en conséquence, constitue une démarche éthique, soucieuse de la protection des données et de leur confidentialité, dont, bien souvent, personne d'autre que lui n'aura connaissance et ne saura l'apprécier.

De même, énoncer les résultats d'une étude fondée sur des données qui sont le reflet d'une actualité plus ou moins récente, sans prendre en compte des dynamiques, ou des corrélations avec d'autres éléments non étudiés, peut conduire à alimenter des stéréotypes en matière de sexe, religion, origine, etc.

La masse des données ne dispense pas de veiller à leur représentativité. Il faut en tenir compte, tout comme il faut veiller dans la présentation de résultats mathématiquement exacts à anticiper les interprétations rapides erronées qui peuvent en être faites, qui peuvent amener discriminations, atteinte à l'image, aux libertés, voire même conduire à l'exclusion.

Les algorithmes auto-apprenants ont une certaine autonomie qu'il faut s'efforcer de contrôler :

Une autre raison qui rend incontournable que l'éthique ne soit plus seulement le sujet des grandes instances, mais celui des codeurs et des utilisateurs, réside dans la relative autonomie des algorithmes auto-entrepreneurs (appelés souvent *Machine Learning*), en particulier ceux des apprentissages profonds (*Deep Learning*).

Ces algorithmes sont programmés par des humains pour affiner leur fonctionnement en fonction de leur expérience, c'est-à-dire des situations de données dans lesquelles ils ont été placés. Ils ne répondent plus seulement à des règles logiques simples définies dans l'espace mathématique des états, comme c'est le cas dans la programmation informatique traditionnelle. Ils agissent, certes selon les instructions données par le codeur, mais de façons différentes en fonction de leurs apprentissages et des données qu'ils ont rencontrées. Le chemin qu'ils suivent pour tirer parti de l'expérience qu'ils ont acquise dépend bien sûr des instructions données par les humains qui les ont conçus. Mais il n'est pas toujours traçable. L'explication des résultats devient alors impossible.

« Or l'éthique exige de pouvoir expliquer les résultats et le pourquoi des décisions qu'ils génèrent. Les solutions sont donc forcément techniques, même si elles s'appuient sur un corpus de valeurs partagées. »

Ainsi, il appartient aux *Data Scientists* et aux chercheurs de trouver les méthodes technologiques pour introduire au sein des algorithmes des moyens de rendre compte des chemins choisis, par exemple des sortes d'observateurs capables de raconter ce qui se passe dans le fonctionnement opérationnel de l'algorithme en situation. Il s'agit aussi de mieux guider les algorithmes dans leur chemin, en fonction de valeurs éthiques socialement partagées, gérées par un système logique dynamique.

Cette relative autonomie de certaines catégories d'algorithmes pose donc le problème des capacités technologiques face à l'acceptabilité des résultats par les individus. Cette nécessité de contrôle du fonctionnement des algorithmes dans chaque situation de données, pourrait être facilitée par des avancées en matière de recherches : anthropologie, et sciences sociales bien sûr, mais aussi en science de la logique, essentiellement la logique de l'action, science moins mature que celle de la logique des états, habituellement utilisée en informatique. Les chercheurs de cette discipline pointue de mathématique fondamentale et informatique théorique pourraient ainsi contribuer de façon déterminante à l'établissement de cette nouvelle éthique numérique qu'il nous faut construire au plus près des acteurs et des utilisateurs.

C'est donc l'ensemble de la société qui doit définir l'éthique du numérique : les hautes instances pour porter les valeurs communes, les individus qui doivent devenir conscients des nouveaux enjeux des technologies numériques, les professionnels des algorithmes qui doivent être guidés dans leur travail au plus près de l'action, et les chercheurs en science logique pour traduire en code la complexité des hiérarchies de valeurs, pas toujours rationnelle, des sociétés humaines.

3 / VERS UNE VOIE EUROPÉENNE DE LA RÉVOLUTION NUMÉRIQUE ?



de Benoit Dos

Directeur Général - Ecole Polytechnique d'Assurances (EPA)

La « révolution numérique » marque, comme son nom l'indique, l'entrée dans une nouvelle période de l'Histoire : en effet, bien plus qu'un « phénomène de mode » associé à l'invention et à l'utilisation par la population de nouvelles technologies, il s'agit d'une véritable « révolution industrielle » qui non seulement a des conséquences sur l'organisation du travail et des rapports sociaux en général, mais qui amène (ou doit amener) aussi l'humanité à se poser des questions sur son *avenir* et sur le *sens* du monde qui est en train de se construire¹²⁷. Car la « digitalisation » est un processus qui a pour double caractéristique de s'étendre, à une vitesse fulgurante, à l'échelle mondiale (tous les individus ou presque sont donc concernés par ce phénomène¹²⁸), et d'être associé à un développement de la connaissance techno-scientifique tel que la production, l'assimilation et l'utilisation de ce nouveau savoir ne devient humainement plus possible ni gérable... C'est pourquoi l'Intelligence Artificielle (IA), que l'on pourrait définir comme « la mise en réseau de machines auto-apprenantes au sein d'un système mondial organisé selon un schéma neuronal », est un élément central, pour ne pas dire le « pilier », de la révolution numérique : en effet, sans IA, impossible de gérer la complexité abyssale du nouveau modèle de civilisation qui est en train de se construire.

¹²⁷ La question du sens de la révolution digitale est actuellement pleinement débattue au sein-même de la Silicon Valley, comme le révèle cette citation d'un article intitulé « Intelligence artificielle ou intelligence collective ? », paru dans Les Echos du 4 septembre 2017 :

« La controverse estivale entre Elon Musk, le flamboyant patron de Tesla et Space X, et Marc Zuckerberg, le fondateur et CEO de Facebook, au sujet des dangers et opportunités de l'intelligence artificielle (IA) a quelque chose de bienvenu. Elle signale que les géants de la nouvelle économie ne forment pas un bloc monolithique dont la seule préoccupation serait de faire naître au forceps une nouvelle société numérique, sans qu'on s'arrête un instant sur le sens de cette révolution en cours.

Elle pose au fond une question politique : comment réguler ce qu'on ne comprend pas ? Parle-t-on, comme le Big Data, d'un outil au service de la prise de décision - publique, privée, commerciale... ? Ou bien faut-il voir dans l'IA un nouvel acteur qui décidera en lieu et place d'untel, ce qui implique de réfléchir à sa gouvernance ? Ces questions sont majeures car elles concernent la capacité des citoyens consommateurs à évaluer l'action publique et à faire des choix avisés, ou encore notre capacité collective à réguler les effets de l'intelligence artificielle. Devrons-nous tous être experts en code ou en algorithmique pour être des citoyens éclairés ? ».

¹²⁸ « Selon des estimations datant de juillet 2016, le monde comptait 3,4 milliards d'internautes. » (Source : <http://www.journaldunet.com/ebusiness/le-net/1071539-nombre-d-internautes-dans-le-monde/>)

« 7,4 milliards d'abonnements mobiles étaient souscrits à fin 2016, selon les estimations de l'International Telecommunication Union, pour un taux de pénétration de 99,7% » (Source : <http://www.journaldunet.com/ebusiness/inter-net-mob/1009553-monde-le-nombre-d-abonnes-au-telephone-mobile/>).

Or, cette cohabitation de plus en plus importante entre l'homme et la machine a, ces dernières années, inéluctablement donné lieu à des débats philosophiques portant sur des questions d'ordre anthropologique : « Qu'est-ce que l'Homme ? », « La machine pourra-t-elle un jour être dotée de conscience ? », etc. Ces questionnements qui, hier, pouvaient sans doute être perçus comme très éloignés de notre vie quotidienne, et donc comme l'apanage de quelques êtres « dont la tête était dans les nuages et dont les pieds ne touchaient pas terre », sont aujourd'hui devenus absolument essentiels pour que l'humain puisse trouver sa place dans la société digitale qui est en train de naître : par conséquent, la « révolution numérique » a aussi eu pour effet de remettre en question les fondements philosophiques de la pensée éthique traditionnelle.

Ces dernières années, les énergies des acteurs du numérique (*Start-up*, entreprises engagées dans la « transition digitale », écoles et organismes de formation, etc.) ont essentiellement été investies dans la résolution des questions d'ordre technique associées à la « révolution numérique ». Autrement dit, beaucoup d'artisans du « nouveau monde » se sont penchés sur la problématique du « Comment implémenter les nouveaux outils digitaux ? ». En revanche, moins nombreux ont été les entités et les individus qui ont pris le temps de s'interroger sur le sens que l'on veut donner à la nouvelle civilisation qui est en train de naître, et qui se sont donc intéressés à la question du « Pourquoi ce nouveau modèle ? Quel modèle de société veut-on développer ? ».

Comme Internet¹²⁹ est un outil qui a été développé aux Etats-Unis, ce sont essentiellement les écoles de pensée américaine qui ont décrit le sens qu'elles comptaient donner à la révolution numérique. Parmi ces deux écoles de pensées, deux font particulièrement entendre leur voix : le « transhumanisme » et le « libertarisme ». Mais l'Europe, s'inspirant de sa tradition humaniste, ne pourrait-elle pas contribuer au débat sur le sens à donner à la « révolution numérique » ? Et n'y aurait-il pas une voie vers un « humanisme numérique européen » ?

L'éthique au centre du modèle de civilisation européen :

L'Europe a toujours mis l'éthique au centre de son modèle de civilisation. Mais qu'est-ce que l'éthique ? L'éthique est une discipline philosophique née en Grèce Ancienne (dont Platon et Aristote ont été deux éminents représentants) qui s'interroge sur la finalité dernière de l'existence humaine. Ainsi, la question sous-jacente à la réflexion éthique est la suivante : « Qu'est-ce qu'une vie humaine réussie ? ». Formulée dans des termes plus contemporains, la question devient : « Qu'est-ce qui donne sens à la vie humaine ? ».

À cette question, les philosophes de la tradition européenne apporteront des réponses différentes : Aristote dira que c'est le *bonheur* qui donne sens à l'existence

¹²⁹ Réseau dont la construction a été inspirée par les travaux du mathématicien Norbert Wiener sur la « cybernétique ».

humaine (resterait alors à préciser ce qu'Aristote entend par « bonheur » ...), tandis que Kant affirmera, vingt siècles plus tard, que c'est, non pas le bonheur, mais la *liberté* qui représente l'idéal vers lequel l'Homme doit tendre pour accomplir sa destinée.

Mais quel que soit le « contenu » que les différents penseurs de la tradition philosophique de notre continent aient pu donner au sens ultime de l'existence humaine (bonheur, liberté...), l'on constate que leur réflexion éthique est basée sur une même conception anthropologique. Voici comment l'on pourrait résumer cette conception : « *L'homme est doté d'une nature qui sommeille en lui à l'état de puissance. Il doit faire éclore cette nature en la développant et en l'exerçant en acte. C'est là le sens de la vie sur Terre.* ».

« Dit dans des termes contemporains, c'est dans le développement personnel et spirituel que réside le sens de l'existence terrestre. »

Ainsi, Aristote plaçant le bonheur dans l'exercice des vertus, c'est en développant ses qualités vertueuses, inhérentes à sa nature, que l'homme pourra trouver le bonheur et donc vivre une vie pleinement humaine : le sens de l'existence terrestre est donc de devenir courageux, tempérant, généreux... (vertus éthiques) et d'exercer sa faculté de contemplation de ce qu'il appelle le « Premier Moteur », la « Cause de toutes les causes » (vertu intellectuelle ou « spirituelle »). Chez le Stagirite, c'est le sage qui incarne le modèle de l'homme heureux.

Kant place quant à lui le sens de la vie humaine dans l'effort de l'homme pour atteindre la « liberté ». Rappelons que Kant pose deux ordres au fondement du Monde (« Monde » qui est lui-même une construction de l'esprit, en tant qu'« Idée de la Raison ») : l'ordre de la « Nature », régi par les lois physiques, et l'ordre de la « Raison », Raison régie, dans son usage pratique, par la loi morale. « Suivre la Nature dans ses actions », c'est agir en ne recherchant que les plaisirs (i.e. agir selon ce que Kant appelle des « déterminations sensibles ») : ce type d'existence est, pour le philosophe, une vie « animale ». En revanche « suivre la Raison dans ses actions », c'est suivre les impératifs de la loi morale (impératifs que Kant énumère dans son oeuvre, et dont l'un deux est de « traiter tout autre être doué de raison comme une fin en soi et jamais comme un moyen en vue d'une autre fin »). Or, plus on se conforme à la loi morale, plus on devient libre, et, par conséquent, plus on mène une existence proprement humaine.

Ajoutons que la réflexion éthique est presque toujours indissociablement liée à une réflexion politique. En effet, après s'être posé la question : « Où l'homme doit-il chercher un sens à son existence ? », le questionnement qui suit est : « Comment et dans quelles conditions l'homme peut-il réaliser et vivre ce qui donne sens à son existence ? ». Or, cette interrogation amène à se pencher sur le problème du régime politique et du cadre de vie dans lequel l'homme doit évoluer pour pouvoir réaliser, actualiser sa nature d'homme, et donc devenir heureux et/ou libre (selon le contenu qu'il donne à ce qu'il considère être la fin dernière de son existence).

« Bonheur » et « Liberté » : deux notions que l'on retrouve dans les deux grandes chartes éthiques desquelles se réclament les régimes démocratiques s'inscrivant dans la tradition des Lumières, à savoir : la « Déclaration des Droits de l'Homme et du Citoyen » de 1793¹³⁰ et la « Déclaration universelle des droits de l'homme et du citoyen » adoptée par l'ONU en 1948¹³¹. C'est donc en vue de permettre aux citoyens d'atteindre ces deux idéaux que les régimes européens se sont, à partir de l'époque des Lumières, organisés, donnant naissance à deux grands types de régimes : la République et la Monarchie Constitutionnelle. Est-il envisageable de voir émerger un modèle politique issu de la Révolution Digitale, et mettant au centre de son organisation les grandes valeurs éthiques au fondement des valeurs de l'Europe ?

Bref descriptif de la société qui émergera probablement de la « révolution digitale » :

Même s'il est difficile de décrire avec précision le modèle de civilisation qui émergera une fois que le monde et l'Europe auront achevé leur transition digitale, il est possible de s'en faire une idée en étudiant les descriptions que font certains experts d'une société que l'on pourrait qualifier « de type Troisième Révolution Industrielle ». Parmi eux, figure Jérémy Rifkin, dont les idées ont influencé l'Union Européenne à double titre : d'une part, parce que ses idées ont été inscrites dans une Charte adoptée par la Commission Européenne, mais aussi parce que la « Troisième Révolution Industrielle » est une notion qui est depuis quelques années mise en application dans la région des Hauts-de-France, sous le nom de projet « Rev'3 »¹³².

Selon l'analyse de Jérémy Rifkin, un changement de civilisation s'enclenche à partir du moment où une révolution apparaît dans trois secteurs : la communication, l'énergie et le transport. Quelles sont donc les innovations majeures marquant le passage du « monde de la Deuxième Révolution Industrielle » à une société « de type Troisième Révolution Industrielle »¹³³ ? Dans le domaine de la *communication*, c'est l'invention d'Internet (qui se substitue au système filaire ayant permis le

¹³⁰ Préambule : « Le peuple français, convaincu que l'oubli et le mépris des droits naturels de l'homme sont les seules causes des malheurs du monde, a résolu d'exposer, dans une déclaration solennelle, ces droits sacrés et inaliénables, afin que tous les citoyens, pouvant comparer sans cesse les actes du gouvernement avec le but de toute institution sociale, ne se laissent jamais opprimer, avilir par la tyrannie; afin que le peuple ait toujours devant les yeux les bases de sa liberté et de son bonheur; le magistrat la règle de ses devoirs; le législateur l'objet de sa mission. En conséquence, il proclame, en présence de l'Être suprême, la Déclaration suivante des droits de l'homme et du citoyen ». Article 1er : « Le but de la société est le bonheur commun ».

¹³¹ Préambule : « Considérant que la reconnaissance de la dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables constitue le fondement de la liberté, de la justice et de la paix dans le monde. ». Article 1er : « Tous les êtres humains naissent libres et égaux en dignité et en droits ».

¹³² <http://rev3.fr/>

¹³³ Les cinq piliers de la « Troisième Révolution Industrielle » sont ainsi décrits dans l'ouvrage éponyme de Jérémy Rifkin : « Voici les cinq piliers de la troisième révolution industrielle: (1) le passage aux énergies renouvelables; (2) La transformation du parc immobilier de tous les continents en ensemble de microcentrales énergétiques qui collectent sur site des énergies renouvelables; (3) le déploiement de la technologie de l'hydrogène et d'autres techniques de stockage dans chaque immeuble et dans l'ensemble de l'infrastructure, pour stocker les énergies intermittentes; (4) l'utilisation de la technologie d'Internet pour transformer le réseau électrique de tous les continents en inter-réseau de partage de l'énergie fonctionnant exactement comme Internet (quand des millions d'immeubles produisent localement, sur site, une petite quantité d'énergie, ils peuvent vendre leurs excédents au réseau et partager de l'électricité avec leurs voisins continentaux); et (5) le changement de moyens de transport par passage aux véhicules électriques branchables ou à pile à combustible, capables et de vendre de l'électricité sur un réseau électrique continental intelligent ».

déploiement du télégraphe, puis du téléphone) qui marque l'entrée dans cette nouvelle ère. En ce qui concerne l'énergie, le changement d'époque doit être marqué par le passage d'un système basé sur les énergies fossiles (pétrole et gaz) à un « Internet de l'énergie », où chaque bâtiment (bureau et/ou lieu d'habitation) va être amené à se transformer en « microcentrale de production énergétique basée sur les énergies renouvelables » : ces bâtiments pourront, du fait de leur connexion au nouveau réseau, à la fois produire et consommer de l'énergie, de la même façon qu'aujourd'hui une personne connectée à Internet, peut produire ou consommer de l'information. Enfin, les penseurs de la « Troisième Révolution Industrielle » comme Ryfkin envisagent, dans le domaine du transport, la création d'un « Internet du transport », qui relierait en réseau à la fois les centres logistiques chargés du transport de marchandises, et les infrastructures en charge du déplacement des personnes (aéroports, gares, ports, réseaux routiers...) : il serait alors possible, dans ce nouveau système (qui intégrera très vraisemblablement, à terme, les véhicules autonomes), de rationaliser le transport des individus comme des marchandises en proposant, pour un même trajet, des modes de déplacement multimodaux (« routier-ferré-aérien », par exemple, ou bien « naval-routier-ferré »). Le point commun de ces trois Internet (celui de la communication, celui de l'énergie et celui du transport) est qu'ils génèrent d'énormes flux de données (les fameux « Big Data »), qui ne pourront être gérés qu'automatiquement *via* l'intelligence artificielle.

Quelle pourrait être la place de l'homme dans cette nouvelle société ?

Face à ce changement de paradigme et de société, comment l'homme peut-il être amené à évoluer ? Même s'il est évidemment très difficile de faire des projections dans un avenir qui est par définition incertain, et qui l'est d'autant plus que nous sommes confrontés à une période inédite de l'histoire de l'humanité, l'éthique peut nous apporter quelques éléments de réflexion qui nous permettront d'avoir une vision des grandes directions qui s'offrent à nous dans la voie de notre évolution.

La première voie qui s'offre à l'espèce humaine pour poursuivre son évolution dans cette nouvelle société est de rompre avec la pensée traditionnelle de l'éthique, et d'explorer un chemin inconnu où l'homme serait appelé à se « re-crée » : c'est la voie que propose notamment le transhumanisme.

Pour le transhumanisme, la frontière entre l'homme, amené à interagir de plus en plus dans son quotidien avec les robots et l'intelligence artificielle, et la machine, devrait s'amincir de plus en plus au fil du temps : l'intégration de composantes électroniques en l'homme (visant à développer, *via* la technologie, ses facultés naturelles) donnerait naissance à un « homme augmenté », prélude à la « post-humanité ». Dans la perspective transhumaniste, et contrairement au postulat qui a nourri la réflexion éthique classique dans la pensée européenne, l'être humain n'a ni « nature », ni (pour reprendre une terminologie plus philosophique) « essence » : cela signifie donc qu'il est impossible d'enfermer l'homme dans une définition, de déterminer *a priori* la direction vers laquelle il doit s'acheminer

dans son évolution pour vivre « une vie d'homme », et de fixer des normes (transcendantes et/ou immanentes) intangibles qu'il ne pourrait transgresser sans en avoir à subir les conséquences néfastes. Selon ce courant de pensée, la seule limite que l'homme peut rencontrer est celle de la faisabilité : dès lors que, grâce aux innovations technologiques, quelque chose d'impossible par le passé devient réalisable (choisir en conscience le génome de sa progéniture, obtenir une vue d'aigle en se faisant greffer une puce derrière la rétine, etc.), l'être humain est, sinon encouragé, du moins légitimé à en faire l'expérience.

Il n'y a donc pas, dans cette perspective, de modèle universel auquel l'Homme doit aspirer ; bien au contraire, l'être humain devient son propre projet, sa propre matière sur laquelle travailler pour s'inventer, sinon se (re)créer tel qu'il le souhaite.

Augmenter de façon exponentielle nos facultés perceptives et motrices, éviter ou soigner toute maladie, repousser les limites de la longévité, vaincre la mort... en un mot, trouver, grâce à l'hybridation homme/machine, des solutions aux problèmes existentiels qui engendrent de la souffrance : voici les objectifs désirables recensés par le courant transhumaniste qui, s'ils étaient atteints, verraient naître une espèce humaine bien différente de celle que l'on connaît aujourd'hui. C'est pourquoi la « révolution transhumaniste » débouche vers le « post-humanisme », c'est-à-dire le dépassement de l'humanité telle qu'on la connaît aujourd'hui, et donc, *in fine*, vers l'apparition d'une nouvelle espèce.

« La deuxième voie qui pourrait s'offrir à nous concernant le sens de notre évolution serait de s'inscrire dans la continuité de la pensée éthique issue de la Tradition, et donc de mettre l'ensemble des innovations technologiques au service du développement de l'Homme, tel qu'il a été défini et décrit par les penseurs aux origines de notre civilisation (dont Aristote figure au premier plan). »

Si notre société faisait le choix de suivre cette voie, les innovations technologiques promises par la Troisième Révolution Industrielle pourraient non seulement permettre de résoudre de grands problèmes sociaux et environnementaux (développement d'un système énergétique « propre », accès gratuit ou quasi-gratuit des populations à l'énergie, meilleure distribution des ressources en fonction des besoins, etc.) mais aussi donner la possibilité aux hommes de développer leur humanité, et de tendre vers un bonheur qui se trouve très certainement autour de valeurs que la société collaborative émergente met aujourd'hui en avant : empathie, bienveillance, solidarité, tissage de liens sociaux... autant de valeurs que Jeremy Ryfkin décrit dans son ouvrage *Une nouvelle conscience pour un monde en crise - Vers une société de l'empathie* Est-il utopique de penser que ces valeurs puissent aller de pair avec la « révolution digitale » ? Très certainement, si la société ne croit pas en ces notions, et surtout si personne - citoyens, professionnels, politiques - n'est prêt à fournir la quantité d'efforts nécessaires pour les mettre en pratique.

« Car, rappelons que, comme toute innovation technologique, le digital n'est qu'un outil, ni bon, ni mauvais en soi : ce n'est que l'esprit, l' « éthique » qui sous-tendra son utilisation qui pourra en faire un instrument au service de l'humain et de son développement. »

L'Europe, tête de gondole de l' « humanisme numérique » ?

Compte tenu de son histoire et de sa tradition, l'Europe pourrait tout naturellement ouvrir la voie à cet « humanisme numérique ». Il semblerait que c'est ce qu'elle ait déjà commencé à faire, en accueillant sur son territoire le projet « Rev'3 », initié par la région « Hauts-de-France » : ce projet oeuvre à la création d'une société de type « Troisième Révolution Industrielle », et intègre les aspects non seulement techniques, mais aussi éthiques impliqués par le passage à ce nouveau modèle de civilisation.

Ce qui est certain, concernant l'éthique, c'est que les programmes d'enseignement (à destination des étudiants) et de formation (à destination des professionnels) doivent intégrer des modules donnant aux apprenants les connaissances et les outils conceptuels leur permettant de mener une réflexion sur le *sens* à donner à la société qui est en train de se construire. Car, si le XXIème siècle est celui de l'économie collaborative, c'est par l'intelligence collective que les solutions aux grands problèmes éthiques pourront très vraisemblablement émerger : aussi doit-on donner les moyens aux artisans de la révolution numérique (*Data Scientists, Data Analysts, etc.*) et à leurs managers (*Chief Data Officers, Chief Data Scientists, etc.*) de contribuer au débat philosophique sur la place de l'homme dans la nouvelle société de type Troisième Révolution Industrielle.

Intégrer l'éthique au coeur de la formation professionnelle : c'est le choix qu'a fait l'École Polytechnique d'Assurances en créant, en juin 2015, un *Executive MBA « Manager Data Scientist des Métiers de l'Assurance »* incluant un pilier « Ethique », puis, en juin 2017, un Certificat « Enjeux stratégiques et éthiques du *Big Data* dans l'assurance ».

4 / LA SOCIALISATION ALGORITHMIQUE



de Jean-Sébastien Vaure

Post-doctorant - Télécom Ecole de Management / LITEM
(EA 7363)

Les réflexions sur l'éthique informatique ne sont pas nouvelles. Elles ont commencé avec l'avènement de la cybernétique¹³⁴ : Norbert Wiener¹³⁵ s'est dès le départ soucié des usages pernicious qu'il est possible de faire de cette science. Son positionnement politique est clair : il s'agit de protester vivement contre l'utilisation que certains groupes d'individus¹³⁶ peuvent faire de cette discipline comme instrument de contrôle. Nous retrouvons cette même préoccupation chez d'autres fondateurs des sciences de l'informatique et de l'intelligence artificielle comme Abbe Mowshowitz¹³⁷ et Joseph Weizenbaum¹³⁸. Bien que l'intérêt que ces deux auteurs portent à l'éthique informatique se manifeste différemment, ils s'accordent pour dire que : d'une part, les systèmes informatiques peuvent servir deux fonctions sociales fondamentales, c'est-à-dire la coordination de la diversité et le contrôle du désordre ; et d'autre part, que les hommes doivent s'organiser collectivement afin d'éviter toute dérive vers la fonction « contrôle ». Maryse Salles¹³⁹ rappelle alors que, dès les années quatre-vingt, l'éthique informatique devient un champ disciplinaire à part entière : elle est pluridisciplinaire et accueille différents chercheurs en philosophie comme James H. Moor¹⁴⁰, ou encore, Deborah G. Johnson¹⁴¹.

C'est dans le prolongement de ces travaux que nous proposons d'esquisser quelques éléments de réflexion sur la manière dont, non plus la philosophie, mais la sociologie peut contribuer à alimenter les débats sur l'éthique informatique à l'ère du *Big Data* et de la « nouvelle intelligence artificielle »¹⁴². Un peu à la manière dont la psychologie cognitive a joué un rôle fondamental dans l'histoire

de l'intelligence artificielle, nous pensons que la sociologie est, à l'heure actuelle, une des sciences les mieux à même de comprendre et critiquer, au sens constructif du terme, la conception et les usages des machines intelligentes.

De la gouvernamentalité algorithmique ...

Afin de saisir comment la sociologie peut réaliser un tel projet, il nous faut revenir sur la notion de « *gouvernamentalité algorithmique* »¹⁴³. Antoinette Rouvroy et Thomas Berns¹⁴⁴ ont élaboré ce concept afin de pointer les enjeux sociopolitiques associés à la diffusion des technologies *Big Data* au sein de la société. Plus exactement, la notion de gouvernamentalité algorithmique est une façon d'étendre le concept de « gouvernamentalité » de Michel Foucault¹⁴⁵ en le transposant au domaine de l'étude de ces nouvelles formes de pouvoir que cristallisent les dispositifs d'apprentissage artificiel (i.e., *Machine Learning*). La gouvernamentalité algorithmique désigne ainsi cette rationalité computationnelle que les machines produisent pour traiter les *Big Data* et en inférer des connaissances dont la fonction est d'automatiser une partie des décisions et des actions des acteurs socioéconomiques.

« Le développement concomitant des technologies d'intelligence artificielle et des mégadonnées participent à l'institution d'une gouvernamentalité algorithmique qui pose des problèmes éthiques importants. »

La pensée d'Antoinette Rouvroy et Thomas Berns¹⁴⁶ est dense : il est impossible d'en rendre compte en quelques lignes. Pour autant, à travers leur notion de gouvernamentalité algorithmique, ces auteurs s'intéressent, de manière générale, à la façon dont les technologies d'intelligence artificielle participent à produire des inégalités qui ne sont pas un bien pour la communauté. Un des exemples souvent mobilisés pour illustrer cet aspect est celui des algorithmes de reconnaissance des images qui apprennent les stéréotypes de genre ou de race¹⁴⁷ ; un phénomène qui peut avoir des conséquences sociales terribles lorsque de tels systèmes sont appliqués à la gestion des ressources humaines ou à celle de la sécurité publique. Pour faire face à ces problèmes, plusieurs spécialistes de l'apprentissage artificiel ont élaboré des technologies permettant de réduire ces biais (Cf. www.fatml.org). De notre point de vue, si ces initiatives sont nécessaires, elles n'en restent pas moins insuffisantes dans la mesure où elles n'embrassent pas la question éthique de la gouvernamentalité algorithmique dans toute sa dimension sociale et technique.

¹³⁴ Salles, M. (2015). *Décision et système d'information*. Londres : ISTE-Éditions.

¹³⁵ Wiener, N. (1950). *The human use of human beings. Cybernetics and society*. Boston : Houghton Mifflin.

¹³⁶ Les fascistes comme les acteurs économiques et politiques les plus puissants.

¹³⁷ Mowshowitz, A. (1976). *The conquest of will : information processing in human affairs*. Boston : Addison-Wesley.

¹³⁸ Weizenbaum, J. (1976). *Computer power and human reason : from judgment to calculation*. San Francisco : W.H. Freeman.

¹³⁹ Salles, M. (2015). *Décision et système d'information*. Londres : ISTE-Éditions.

¹⁴⁰ Moor, J. (1985). What is computer ethics? *Metaphilosophy*, 16 (4), 266-275.

¹⁴¹ Johnson, D. (1985). *Computer ethics*. Englewood Cliffs : Prentice-Hall.

¹⁴² Cardon, D. (2015). *À quoi rêvent les algorithmes. Nos vies à l'heure des big data*. Paris : Seuil-La République des idées.

¹⁴³ Rouvroy, A., & Berns, T. (2013). Gouvernamentalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? *Réseaux*, 1 (177), 163-196.

¹⁴⁴ Rouvroy, A., & Berns, T. (2013). Gouvernamentalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? *Réseaux*, 1 (177), 163-196.

¹⁴⁵ Foucault, M. (2004). *Sécurité, territoire, population*. Paris : Seuil.

¹⁴⁶ Rouvroy, A., & Berns, T. (2013). Gouvernamentalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ? *Réseaux*, 1 (177), 163-196.

¹⁴⁷ cf. <http://www.internetactu.net/a-lire-ailleurs/144849747113/>. Précisons qu'il existe bien d'autres exemples qui dépassent le cas des algorithmes de reconnaissance des images. Par exemple, les applications qui développent *International Business Machine (IBM) de Watson* dans le domaine de la santé feraient également l'objet de différents biais : certains journalistes affirment que les connaissances que produisent ces applications reflètent des spécificités qui sont propres à la population américaine et aux méthodes de traitement qui sont déployées aux États-Unis (cf. <https://www.statnews.com/2017/09/05/watson-ibm-cancer/>).

... à la socialisation algorithmique :

C'est précisément ici que se trouve, d'après nous, toute l'utilité du concept de socialisation algorithmique : ce dernier permet de combler le manque que nous venons de pointer. Mais qu'entendons-nous, au juste, par socialisation algorithmique ? Du point de vue du sociologue, cette notion peut être définie comme le processus de socialisation non-humain à travers lequel une machine apprend à adapter ses comportements à son environnement. Plus exactement, la sociologie propose plusieurs définitions de ce qu'est la socialisation et qui renvoient à des représentations du social qui sont différentes. Une des plus populaires est probablement celle qu'a développée Pierre Bourdieu ¹⁴⁸ (1994). Pour cet auteur, la socialisation est ce qui permet à un être humain d'intérioriser des dispositions, c'est-à-dire de développer les « structures mentales » qui orientent ses manières d'être, d'agir, de penser et qui ne peuvent être comprises que dans « un rapport de complicité ontologique [avec] les structures objectives de l'espace social » ¹⁴⁹ :

« [L]es dispositions communes et la doxa partagée qu'elles fondent sont le produit d'une socialisation identique ou semblable conduisant à l'incorporation généralisée des structures du marché des biens symboliques [i.e., les normes, les règles et les valeurs que véhiculent la société] sous la forme de structures cognitives accordées avec les structures objectives du marché » ¹⁵⁰.

« La définition et la résolution de ces problèmes doivent être fondées sur une compréhension rigoureuse de la socialisation algorithmique. »

Il est alors intéressant de noter que cette définition de la socialisation humaine fait en elle-même écho à ce que nous nommons la socialisation algorithmique dans la mesure où, comme le souligne Gérald Bronner ¹⁵¹, elle est parfaitement compatible avec la perspective connexionniste que partagent les neurologues et les spécialistes de l'apprentissage profond (i.e., *Deep Learning*). Les travaux qu'a réalisés Jean-Pierre Changeux ¹⁵² sur « les bases neurales de l'habitus » en constituent un exemple parfait. Afin de mieux comprendre cette idée, il suffit de réfléchir à la question qui suit : que font les réseaux de neurones profonds que conçoivent des chercheurs comme Yann Lecun ou Yoshua Bengio ? Sur le plan purement informatique, ils font beaucoup de choses que nous ne pouvons pas détailler ici. Cependant, sur un plan sociocognitif, ils ne font rien d'autre qu'adapter leurs connexions neuronales aux structures corrélationnelles que recouvrent les masses de données qui autorisent leur apprentissage. Aussi, ces données traduisant, *a minima* dans certains cas, ce que Pierre Bourdieu ¹⁵³ nomme les « structures objectives de l'espace social », les architectures cognitives de ces réseaux de neurones peuvent, à l'instar de celles des humains, être comprises

« dans un rapport de complicité ontologique » avec les structures sociales. Et c'est précisément pourquoi ces technologies d'apprentissage artificiel (comme la plupart des autres) peuvent participer à reproduire les inégalités sociales dont nous avons précédemment parlé.

En conclusion, à la manière dont la sociologie nous a appris que, pour saisir les problèmes éthiques que recouvre la « gouvernementalité » ¹⁵⁴, il est nécessaire de comprendre la socialisation des hommes qui la font exister, nous pensons que cette discipline peut également nous aider à mieux poser et traiter la question de l'éthique de la gouvernementalité algorithmique en nous aidant à mieux comprendre comment est produite la socialisation algorithmique. Nous proposons ainsi de conclure en soulignant que, de façon analogue à celle des humains, la socialisation algorithmique n'a rien de naturel. Elle fait l'objet d'un cadrage sociocognitif qui peut être décomposé en trois dimensions.

- L'environnement d'apprentissage qui désigne l'ensemble des dispositifs de recueil et de structuration des données qui permettent à la machine de se construire une représentation du monde. C'est par exemple cet environnement qui est en jeu lorsque certains spécialistes pointent la nécessité de contrôler les bases de données qui nourrissent les algorithmes de reconnaissance des images.
- L'environnement de traitement qui désigne l'ensemble des dispositifs qui permettent à la machine de réaliser des inférences sur le monde à partir des données d'apprentissage dont elles disposent. C'est par exemple cet environnement qui est en jeu lorsque certains spécialistes pointent la nécessité de comprendre le fonctionnement des boîtes noires que constituent, par exemple, les réseaux de neurones profonds.
- L'environnement politique qui désigne l'ensemble des dispositifs d'évaluation qui permettent à la machine d'autoréguler ses apprentissages. C'est par exemple cet environnement qui est en jeu lorsque certains spécialistes pointent la nécessité de « déséconomiser » le travail inférentiel qu'effectuent les applications marchandes des technologies d'intelligence artificielle.

« La compréhension de la socialisation algorithmique doit être réalisée par l'étude sociologique de la conception de son cadrage sociocognitif et des usages qui en sont fait. »

En référence aux travaux issus de l'anthropologie et de la sociologie des sciences et des techniques, la combinaison de ces trois environnements cristallise des formes relationnelles particulières entre les trois grands types d'acteurs que sont : le concepteur, l'implémenteur et l'utilisateur. Autrement dit, c'est par le biais du cadrage sociocognitif dont nous venons de parler que la socialisation algorithmique contribue à la structuration des relations qu'entretiennent ces trois types d'acteurs. Il nous semble en ce sens que chercher à mieux comprendre

¹⁴⁸ Bourdieu, P. (1994). *Raisons pratiques. Sur la théorie de l'action*. Paris : Seuil.

¹⁴⁹ Bourdieu, P. (1994). *Raisons pratiques. Sur la théorie de l'action*. Paris : Seuil. p.151.

¹⁵⁰ Bourdieu, P. (1994). *Raisons pratiques. Sur la théorie de l'action*. Paris : Seuil. p.212.

¹⁵¹ Bronner, G. (2010). Cerveau et socialisation. Quelques éléments de discussion. *Revue française de sociologie*, 51 (4), 645-666.

¹⁵² Changeux, J.-P. (2006). Les bases neurales de l'habitus. Dans G. Fussman, *Croyance, raison et déraison* (pp. 143-158). Paris : Odile Jacob.

¹⁵³ Bourdieu, P. (1994). *Raisons pratiques. Sur la théorie de l'action*. Paris : Seuil. p.151.

¹⁵⁴ Foucault, M. (2004). *Sécurité, territoire, population*. Paris : Seuil.

comment se produit la socialisation algorithmique¹⁵⁵ doit nous permettre de questionner en profondeur l' « éthique de la conviction » et l'« éthique de la responsabilité »¹⁵⁶ que les hommes adoptent vis-à-vis des machines intelligentes qu'ils conçoivent, implémentent et utilisent. Et c'est à cette seule condition qu'il deviendra réellement possible d'identifier à quel point l'intelligence des machines, à l'ère du *Big Data*, participe à coordonner la diversité ou à contrôler le désordre qui compose la société¹⁵⁷.

¹⁵⁵ Soit, comment est conçu et utilisé le cadrage sociocognitif que nous avons présenté.

¹⁵⁶ Rappelons que chez Max Weber ([1919] 1959), l'éthique de la conviction pose la question de la légitimité des valeurs qui ont motivé un acte, peu importe ses conséquences ; à l'inverse, l'éthique de la responsabilité pose la question des conséquences d'un acte, peu importe la légitimité des valeurs qui l'ont motivées.

Weber, M. ([1919] 1959). *Le savant et le politique*. Paris : Plon.

¹⁵⁷ Mowshowitz, A. (1976). *The conquest of will : information processing in human affairs*. Boston : Addison-Wesley. Et, Weizenbaum, J. (1976). *Computer power and human reason : from judgment to calculation*. San Francisco : W.H. Freeman.

5 / CIBLER L'ACTION DE PRÉVENTION : CONDITION SINE QUA NON DE SON EFFICACITÉ



de Quentin Bériot

Directeur des opérations et de l'innovation Santé Prévoyance - COVEA

L'accès aux données de santé, sujet controversé, permettrait aux Organismes Complémentaires¹⁵⁸ (OCAM) de jouer pleinement leur rôle dans la Prévention.

Lors de la présentation de la stratégie nationale e-santé pour 2020, Marisol Touraine avait posé des limites en déclarant que les « assureurs n'auraient pas accès aux données des patients ». Pourtant, dans la mesure où les OCAM jouent un rôle essentiel dans la Prévention, leur donner un accès – réglementé, bien entendu – aux données de santé apparaît pourtant impératif afin de ne pas les limiter à de l'information seule. En effet, actuellement, les OCAM remboursent sans pouvoir pleinement utiliser les informations sur la nature des dépenses qui ont été engagées. Il est aisé de comprendre qu'il y a là une sorte de non-sens ...

Comment imaginer que la Prévention puisse concrètement atteindre les destinataires qu'elle entend cibler, concevoir et organiser sur le terrain des actions efficaces et délivrer des messages audibles par la population concernée, sans lui confédérer la possibilité d'utiliser des données personnelles ?

Encore faut-il que droits et devoirs d'usage de ces données par les OCAM soient sans ambiguïté. Voilà pourquoi nous proposons dans le respect du Règlement Général sur la Protection des Données Personnelles (RGPD) et dans la lignée du L1111-8 du Code de Santé Publique et de la Loi du 26 janvier 2016 de créer un nouvel usage de données, non qualifiée en raison de leur origine ou de ce qu'elles représentent, mais pour la finalité exclusive de la prévention. Ces données utiles pour la prévention seraient hébergées sur *une plate-forme dédiée* et feraient l'objet de mesures de sécurité spécifiques. Ainsi délimitées, ces données et la plate-forme feraient l'objet d'une reconnaissance spécifique – par exemple, une sorte de *labellisation* – qui permettrait ainsi à des professionnels de la prévention de les utiliser.

¹⁵⁸ Les OCAM – Organismes Complémentaires d'Assurance Maladie – contribuent au système de Protection Sociale en complément de la Sécurité Sociale. Ils couvrent les frais de maladie et la prévoyance (arrêts de travail, décès).

Ainsi les OCAM, parties prenantes de notre système de Protection Sociale, pourraient accompagner leurs assurés en toute sécurité, avec un niveau de sécurité aligné sur les règles les plus exigeantes.

Sans ciblage populationnel, pas de prévention efficace :

L'OMS en 2000 puis *The Lancet* en mai 2016 ont estimé que notre système de santé était l'un des plus performants au monde. Mais, paradoxe français, c'est aussi le lieu de fortes inégalités. Quelques chiffres permettent d'illustrer les facteurs favorisant l'émergence de ces inégalités.

Le *facteur social* est probablement le plus important. Par exemple, le bulletin épidémiologique de février 2017 de Santé Publique France souligne que sur 189 000 personnes atteintes d'un cancer entre 2006 et 2009, celles qui souffrent d'un cancer de l'estomac, du foie, des lèvres, de la bouche et du larynx sont issues des catégories sociales les plus défavorisées.

L'appartenance à certaines *catégories populationnelles* telles que des populations dites invisibles (réfugiées, prisonniers, transsexuels, etc.), en grande exclusion, les seniors ou les jeunes¹⁵⁹, peut aussi engendrer des inégalités spécifiques.

Le *cadre géographique* n'est pas non plus indifférent... Ainsi l'écart d'espérance de vie à la naissance entre un homme né dans la région Midi-Pyrénées et autre né dans le Nord-Pas-de-Calais est de cinq ans¹⁶⁰.

Enfin, il est irréfutable que certaines *professions* exposent à des pathologies spécifiques. L'asthme provoque 7 millions de journées d'arrêt de travail par an notamment chez les boulangers, les meuniers, les éleveurs d'oiseaux et les employés de cliniques vétérinaires. Autre exemple parmi d'autres, la leptospirose atteint 1 personne par jour et est particulièrement présente dans les activités d'assainissement et la pisciculture. Inutile de multiplier les exemples.

À ce que l'on pourrait appeler des déficits du capital chance individuel, s'ajoutent d'autres disparités liées à l'information ou à l'accès aux soins.

Ainsi ne suffit-il pas d'être malade pour être soigné. Il faut être *en situation de recevoir l'information*, voire être réceptif à ce type de message : déserts médicaux, inégalités géographiques et sociales peuvent constituer des barrières à l'information.

Bien que le nombre de médecins en activité en France n'ait jamais été aussi élevé¹⁶¹, *l'accès aux soins n'a jamais été aussi problématique*. Pour ne citer que la région Île-de-France les zones sous-médicalisées sont concentrées dans les zones rurales à faible densité avec une corrélation étroite entre la densité médicale et le revenu moyen. Et que dire de l'existence du *médecin de famille* ? Sa fin semble tout simplement programmée.

¹⁵⁹ En 2003, 14% des garçons boivent une boisson alcoolisée plus de 10 fois par mois (Santé, pour une politique de prévention durable- IGAS, Rapport annuel 2003).

¹⁶⁰ INSEE 21/12/2016.

¹⁶¹ En 1968, on décomptait 60 000 médecins, 107 000 en 1981, et 215 000 en activité en 2016. Le numerus clausus a plus que doublé : 8800 en 2017 (3600 en 1995).

Sans ciblage des messages, pas de prévention efficace :

L'éducation comportementale (dont les grandes priorités sont manger mieux, éviter la sédentarisation, pratiquer une activité physique) constitue l'essentiel de la prévention primaire. Et c'est dès le plus jeune âge qu'il convient de s'atteler à créer les bons réflexes pour la vie future. Les fameuses injonctions *Manger 5 fruits et légumes par jour* et *Manger, bouger !* vont dans ce sens. Cependant, la connaissance « intellectuelle »¹⁶² est d'une façon générale insuffisante, donc dans le domaine de la santé également. C'est pourquoi une stratégie de prévention efficace doit s'inscrire dans le long terme et *adapter ses messages à ses cibles*. Par exemple, inculquer à des adolescents que fumer tue en leur évoquant les maladies chroniques dont ils pourraient souffrir plus tard n'a que très peu impact. A contrario, « les faire réfléchir sur le fait que les multinationales du tabac profitent d'eux et n'en ont rien à faire de leur santé »¹⁶³ les intéressera, les révoltera et produira plus facilement l'effet recherché. Ainsi, le couple Message-Population ciblée est clé : il faut anticiper la façon dont ses messages sont accueillis et interprétés par le récepteur.

Par ailleurs, comme dans toute démarche de marketing et de communication, la stratégie média est déterminante. Quelques tendances nouvelles sont à prendre en compte, telles que surfer sur les effets de mode, utiliser des nouveaux médias, rendre « contagieux » certains comportements ou attitudes en utilisant des mangas ou des « *Serious Games* », et bien entendu *s'appuyer sur les réseaux sociaux*.

Enfin, si les outils tels que le *Nudge*¹⁶⁴, les sanctions ou les incitations (récompenses) sur les comportements de santé sont encore peu connus¹⁶⁵, ils constituent certainement des outils appropriés dont le bon dosage sera à définir en fonction des contextes et des populations.

Donner aux OCAM les moyens de leur action :

La diversité des populations nécessite en conséquence de cibler les actions et les messages de Prévention. La collecte et l'analyse de données sont donc indispensables pour mieux connaître les comportements et les pathologies. Les OCAM peuvent utiliser les données collectées à la souscription et durant la vie du contrat. Bien utilisées – on ne le répètera jamais assez – ces données permettraient de réduire les aléas, d'identifier des corrélations entre des métiers, des habitudes de vie et des pathologies. La connaissance de ces éléments renforce le positionnement de « préventeur » et « accompagnateur » au regard du simple rôle passif de « payeur ».

Ces orientations ne sont pas des vues de l'esprit, elles ne sont ni abstraites ni vagues. On peut au contraire, dès à présent les inscrire dans une réalité concrète.

L'accès aux données permettra à un OCAM d'affiner la connaissance du risque de leurs clients (grande entreprise, branches professionnelles) et de cibler plus finement les actions à conduire au regard des pathologies rencontrées. Il pourra identifier des professions exposées à de nouveaux risques (risques de pollution, iatrogénie grave) dont l'impact est méconnu ou mal connu. Il proposera individuellement des informations et des conseils pour accéder à des dispositifs sanitaires et sociaux ou encore à des données objectives sur la qualité des soins et des prestations. Il pourra faciliter l'accès aux soins et permettre une diminution du renoncement à se faire soigner. Il incitera l'assuré à une bonne observance de son traitement, au respect du calendrier thérapeutique. Ces avantages pour les deux parties – OCAM et assurés – sont si parlants qu'il semble superflu de dresser ici une liste exhaustive.

Dernier avantage, et de taille, le ciblage des actions permettrait de diminuer drastiquement les coûts de dépistage et de diagnostic.

Droits des OCAM vis-à-vis des assurés :

Les OCAM agissent comme second étage de la Protection Sociale. Cela leur impose des devoirs clairs quant à l'utilisation des données personnelles et de santé de leurs assurés. Au-delà du strict respect du Règlement Général sur la Protection des Données Personnelles (RGPD), comme :

- Dans le domaine de la Protection Sociale, l'utilisation éthique respectera les principes de solidarité et naturellement exclura toute utilisation à des fins de discrimination, de sélection, ou de tarification différenciée ;
- Les OCAM doivent s'engager à ne pas divulguer ni vendre les données de santé ;
- Les OCAM doivent recueillir le consentement express de l'assuré quant à l'usage qu'il fera de ses données.

Aussi, sous réserve du consentement explicite de l'assuré, les OCAM pourraient utiliser les données dans le cadre des deux principaux « usages »¹⁶⁶.

Appelons le premier *usage de masse*, lorsqu'il s'agit – à l'échelle d'un portefeuille, d'une branche d'une grande entreprise – de réaliser des études sur un risque spécifique (épidémiologique, comportemental, etc.) ou sur le suivi des traitements.

Le second concerne un *usage au niveau de l'individu* : l'objectif serait d'adopter une démarche personnalisée pour mieux accompagner l'assuré. Ainsi, les OCAM

¹⁶² 100% des français connaissent la dangerosité du tabac, mais 32% se déclarent fumeurs, même parmi les plus éclairés. C'est bien connu : aucun médecin ne fume...

¹⁶³ Pr Gérard Dubois, médecin de santé publique

¹⁶⁴ Le Nudge consiste à mettre l'individu dans un contexte de choix qui l'incite à un comportement spécifique.

¹⁶⁵ Quelques chaires soutenues par des OCAM, dont Prevent'Horizon à Lyon, investissent le sujet des mécanismes d'adhésion aux messages collectifs de prévention et sur l'efficacité des interventions individuelles.

¹⁶⁶ Cela est conforme au cadre de la Loi du 26 janvier 2016, article 193 sur les deux finalités interdites : « V.-Les données du système national des données de santé ne peuvent être traitées pour l'une des finalités suivantes :

- 1° La promotion des produits mentionnés au II de l'article L. 5311-1 en direction des professionnels de santé ou d'établissements de santé ;

- 2° L'exclusion de garanties des contrats d'assurance et la modification de cotisations ou de primes d'assurance d'un individu ou d'un groupe d'individus présentant un même risque ».

pourraient s'appuyer sur les nouvelles technologies (*Big Data*, objets connectés, etc.) pour étendre leur champ d'action en termes d'éducation sanitaire et sociale, d'éducation thérapeutique, et de services d'accompagnement au plus près de l'assuré.

Profiter des promesses du coaching santé personnalisé ... Tout en restant vigilant sur les risques de dérives :

Depuis deux ans, fleurissent bon nombre d'applications santé, associées ou non à des objets connectés. Or à ce jour, ces dispositifs de prévention ont un effet très limité.

Les premières conclusions indiquent que le nombre d'applications santé dépasse les 150 000, et que seule une infime partie d'entre elles est transparente quant à l'usage qui est ensuite pratiqué des données collectées. Comment sécurisent-elles les données que nous leur confions, comment les commercialisent-elles ? Le nombre des objets connectés est en forte croissance, mais bien peu de ces objets peuvent, à juste titre, être qualifiés de fiables.

Une autre tendance mérite encore d'être signalée : les programmes de coaching qui se multiplient en proposant diverses récompenses (baisse de tarification en Italie et aux US, bons d'achat en France ou aux Pays-Bas). Sous couvert de prévention, ces programmes sont utilisés comme des outils de conquête marketing et favorisent une sélection déguisée du risque. En effet, ils peuvent avoir des effets pervers d'exclusion de certaines catégories de population. Par exemple, afficher des *critères conditionnels* qui, une fois atteints, permettent une baisse de tarifs ou des bons de réduction revient – par construction – à favoriser ceux qui sont déjà en mesure de les atteindre. L'exemple le plus commun, ce sont les fameux *10 000 pas par jour*... Or qui aujourd'hui parcourt 8 km à pied tous les jours ? Qui est physiquement capable de marcher 8 km tous les jours ? Instaurer un tel critère, c'est s'adresser aux personnes en bonne santé, plutôt les jeunes ou les couples sans charge de famille. Autrement dit, cela revient à viser d'emblée les meilleurs risques et, dans certains cas, à renforcer des mécanismes d'exclusion¹⁶⁷. Aussi, nous pensons qu'il faut être extrêmement vigilant autour des offres « assurantielles comportementales¹⁶⁸ » que certains organismes d'assurance mettent sur le marché.

Nous proposons une plate-forme dédiée aux traitements et données à finalité de prévention :

Une plate-forme technique dédiée à la prévention sur laquelle les données déposées seraient exclusivement dédiées à des travaux relatifs à la prévention. Quelles pourraient être ces « données » ?

Elles peuvent être issues de données personnelles, de santé, etc. collectées à partir 1) des informations client, de leurs comportements, des objets connectés,

des réseaux sociaux, 2) des données métiers telles que les primes et prestations payées, les garanties souscrites et 3) des données que l'on aura croisées (risques communs à une profession ou une population).

Nous proposons par conséquent de créer un nouvel usage de ces données, non qualifiée en raison de leur origine ou de ce qu'elles représentent, mais pour la finalité exclusive de prévention.

Ces données utiles pour la prévention seraient hébergées sur une *plate-forme dédiée* et feraient l'objet de mesures de sécurité, de traçabilité, de stockage, de mise à jour, de traitement et de droits d'accès spécifiques, dans la droite ligne de celles qui sont appliquées pour le SNDS –et notamment le SNIRAM.

Ainsi délimitées, ces données et traitements à finalité de prévention et la plate-forme feraient l'objet d'une reconnaissance spécifique – par exemple, une sorte de *labellisation renforcée* – qui permettrait ainsi à des *professionnels* de la prévention de les utiliser.

C'est à ces conditions que les organismes complémentaires pourront pleinement jouer le rôle qui leur revient, avec efficacité et au bénéfice de leurs assurés. En outre, cela devrait pouvoir constituer ainsi une barrière distinctive vis à vis de nouveaux entrants qui n'ont pas les mêmes réflexions éthiques morales quant à l'utilisation des données personnelles.

Sous réserve du consentement de l'assuré, nous proposons que les OCAM puissent mettre en place une plate-forme technique sécurisée, dédiée aux données et traitements à finalité exclusive de prévention.

¹⁶⁷ Par exemple, dans un contrat collectif, promettre que 10 000 pas quotidiens feront gagner des bons cadeaux, 1) c'est écarter une partie des 6% d'handicapés qui ne sont pas en situation d'atteindre cet objectif et 2) leur faire supporter le coût du programme. Par conséquent, de tels programmes renforcent les mécanismes d'exclusion.

¹⁶⁸ « L'assurance comportementale » a pour objet de lier la nature des garanties, des services ou des tarifs au comportement de l'assuré.

6 / LE PROJET ETERNESIA : VERS UN HUMANISME NUMÉRIQUE, UN PATRIMOINE COMMUN ET UNE MÉMOIRE DE L'HUMANITÉ



de Dominique Pon et de Serge Maîtrejean

Co-fondateurs – Association Eternesia



Nous avons passé le cap d'un nouveau millénaire, il y a maintenant plus de quinze ans, heureusement sans cataclysme apparent, sans fin du monde, sans extinction de l'être humain. On nous avait pourtant fait miroiter un inimaginable désastre sous forme d'un bogue universel et les millénaristes en salivaient, mais il s'avéra n'être, au fond, qu'une autre de ces vaines tentatives de frisson collectif et en guise de jugement informatique dernier nous n'eûmes rien d'autre que l'impression d'une imposture : il faut croire que l'on a les apocalypses que l'on mérite. Avec le recul nous avons appris à en sourire et cette pantalonnade internationale ne fut qu'un de ces nombreux faits qui contribuent à rendre notre époque peu lisible, confuse et parfois inquiétante. Vivons-nous une période de rupture, un de ces moments de l'histoire où les perspectives se brouillent et où les voies dans lesquelles engager l'avenir sont incertaines ? Sommes-nous submergés par les masses d'informations parfois contradictoires issues d'internet, au point de ne plus très bien savoir les synthétiser ? Sans doute un peu les deux.

À travers ce que nous avons coutume de nommer nouvelles technologies, nous avons la sensation de vivre, depuis une trentaine d'années, un bouleversement aussi ample que celui qui fut apporté par Gutenberg et l'imprimerie, mais alors que cette invention fut clairement à la base de l'essor de la renaissance, de l'humanisme puis plus tard des lumières, il n'est pas très simple de savoir quelles idées réellement nouvelles sont véhiculées par les révolutions que nous vivons. Ce que l'on nous présente comme des avancées majeures de la pensée n'est le plus souvent qu'une reformulation moderne d'idées très anciennes. Prenons le cas du mouvement transhumaniste par exemple. Nous sommes face à un groupe minoritaire, mais très influent, dont l'un des crédos est la modification en profondeur de l'être humain avec pour perspective l'allongement indéfini de la durée de vie par des moyens technologiques. Il y a sept ou huit siècles, cela s'appelait l'élixir de longue vie, les NBIC étaient alors la graine d'ellébore ou les sucs de crapauds, et les promoteurs de ce curieux rêve étaient nommés alchimistes. Il y a aussi en marge de cette mouvance des tenants d'une autre étrange idée qui consiste à imaginer qu'un jour, pas très lointain, la conscience humaine pourrait être « téléchargée » dans un ordinateur. Ceci présuppose qu'il

existerait une mystérieuse substance immatérielle (l'information ?) capable de s'affranchir de son support matériel (notre corps) pour gagner un milieu presque éthéré. On réinvente ainsi l'âme, une âme athée sans autre dieu qu'un ensemble de techniques, l'ordinateur et les réseaux jouant le rôle du paradis ou de l'enfer. Cette pensée moderne a donc douloureusement accouché d'une idée qui a plus de trois mille ans ! Notre époque ne peut-elle pas mieux faire ? Peut-être sommes-nous parvenus aux limites de ce que nous pouvions imaginer, qui sait ? Mais alors, quitte à s'appuyer sur des concepts anciens, pourquoi ne pas en choisir de plus récents et donc pourquoi ne pas continuer dans la tradition humaniste, ni *post*, ni *trans*, qui nous a permis de construire ce que nous avons aujourd'hui ?

« Pourquoi ne pas employer les avancées techniques dans des entreprises destinées à remettre l'humain au centre, à accepter ce qu'il est, même si cela échappe à une définition précise ? »

L'humanisme reste présent dans nos sociétés mais il semble notablement s'affaiblir et nous voyons resurgir des nationalismes extrêmes, des fanatismes, un racisme que nous ne pouvons plus qu'endiguer avec peine, sans compter certains dérapages du système économique qui le font oeuvrer parfois au détriment de la très grande majorité. De plus, la mise au premier plan de l'individualisme dans une formulation extrêmement primaire a contribué à atténuer la notion de destin commun et a réduit l'importance de ce que nous partageons. Nous peinons à recréer des projets d'ensemble en partie parce que l'ombre du collectivisme plane, de manière irrationnelle, sur l'image de tout ce qui est susceptible d'oeuvrer pour la communauté. La difficulté à mettre en place des politiques de développement durables en est une parfaite illustration. La raison les impose mais venant, sous certains aspects et temporairement, en opposition avec le confort individuel, elles sont suspectes d'être des réminiscences de pensées marxistes pour une frange non négligeable de la population. Pourtant la force du milieu associatif, les mouvements citoyens spontanés ou la prise de conscience globale des nuisances de certains pans de l'activité humaine, montrent qu'une part importante de la population cherche à s'inscrire dans des initiatives au service de tous, où l'on ne chercherait pas à transmuter l'espèce humaine mais au contraire à l'accepter pour préparer un futur viable : des projets par et pour l'humanité, en un mot des projets humanistes.

Il est aussi un autre point symptomatique de l'époque : l'érosion progressive de la valeur d'une vie. Depuis quelques dizaines d'années, et en particulier en ce début de XXIème siècle, nous assistons à la résurgence d'un phénomène rampant de hiérarchisation des existences où certaines deviennent le modèle à suivre tandis que d'autres sont considérées comme insignifiantes. Le succès sans démenti de la presse « people » est une illustration de ce classement. L'anonyme y regarde, comme à travers les grilles d'un zoo, des êtres inaccessibles et oublie la valeur de sa vie en rêvant à celles d'autres. On pourrait arguer que les quinze minutes warholienne ont la capacité de rebattre ces cartes, mais il y a tellement plus d'inconnus que de quarts d'heure ! Dans un registre bien plus dramatique, le

sans domicile fixe qui devient l'ombre de nos rues et qui n'a presque plus le statut d'être humain, tant tout ce qui le rendait digne a été effacé, est lui aussi une manifestation de la dépréciation de la valeur de certaines existences. On pourrait poursuivre cette sinistre énumération en mentionnant guerres larvées, migrants mourant sur des plages, terrorisme, mais l'objet de ces lignes n'est pas de faire un inventaire dépressif des maux de l'époque. Pourtant une vie étant initiée par une combinaison génétique ne s'étant jamais produite avant, suivie d'un enchaînement de vécus, de sentiments, de sensations tout aussi improbables est par nature unique. Nous sommes tous différents, c'est là une de nos plus grandes richesses, mais nos existences ont une égale valeur au titre de cette rareté, seul critère de jugement indépendant de tout relativisme subjectif.

« À ce stade, deux choix sont possibles : aucune vie n'a une quelconque valeur ou, au contraire, toutes les existences sont inestimables. Nous pensons qu'il faut faire ce second choix en proposant de sanctuariser la mémoire libre et volontaire de chaque être humain, de toute l'humanité passée, présente et à venir. »

Il n'est pas concevable qu'une poignée d'individus, GAFa ou BATX, puisse continuer à privatiser ce patrimoine commun qu'est la mémoire numérique de l'humanité. C'est pourquoi nous avons lancé ETERNESIA¹⁶⁹, un projet philanthropique, ouvert à tous, sans discrimination d'aucune sorte, dont le but est de permettre à tous ceux qui le désirent de constituer une mémoire numérique de leur vie et tout mettre en oeuvre pour que ces mémoires restent préservées et accessibles pour les temps à venir, sans limite de durée. Il a aussi pour objet d'étendre cette possibilité à ceux qui nous ont quittés, sous la supervision de leurs descendants ou de leurs héritiers. Ce que nous entendons ici par mémoire est bien plus général que la connotation biographique habituellement associée à cette notion.

« Le projet ETERNESIA se veut une matrice pour la transmission aux générations futures de tout ce que chacun considère comme les contributions de sa vie à l'ensemble. »

Cela peut être un savoir, une oeuvre, une phrase, un talent, une construction ou bien seulement ce que l'on a vécu car une existence est en elle-même une réalisation dont les traces sont dignes d'être transmises. Cette idée de trace, bien plus large que celle de mémoire, est la notion emblématique d'ETERNESIA. Sa portée est suffisamment large pour être même compatible avec la notion d'oubli car une empreinte peut rester à jamais anonyme.

ETERNESIA n'est surtout pas une nouvelle émanation des pensées *trans* ou *post humaniste*, comme l'arrière-plan informatique pourrait le suggérer. La technologie n'est dans ce projet qu'un élément pour parvenir à un but humaniste, rien d'autre.

¹⁶⁹ www.eternesia.org

S'il existait, comme dans la légende du roi Midas, des roseaux pour raconter l'histoire d'une vie sous l'effet de la brise, nous n'évoquerions ni serveurs, ni Internet : nous sèmerions. Pour que la conservation sans limite des mémoires devienne une réalité, ce projet a besoin de s'appuyer à la fois sur le secteur économique pour prendre en charge les aspects techniques et sur des institutions laïques et religieuses pour apporter la garantie d'une pérennité à travers les siècles. Ainsi, afin de garder la neutralité indispensable pour fédérer autour de son but organismes nationaux et internationaux, institutions, entreprises et tous les particuliers que le projet intéresse, ETERNESIA est une initiative associative à but non lucratif, par nature éthique, ouverte, indépendante et respectueuse de tout pouvoir ou de tout système de valeur. Les rôles respectifs de tous ces partenaires seront équilibrés pour que se constitue un écosystème participatif dédié. En parallèle, pour que la construction de ce réseau mémoriel se fasse sur une assise de principe solide, ETERNESIA se veut porteur d'un nouveau droit de l'homme, le droit à la mémoire et à la postérité pour tous, dont le droit à l'oubli fait aussi partie intégrante.

« Il est, à notre sens, une des meilleures manières de traduire l'idée que chaque existence est inestimable et peut donc être élevée au rang d'élément immatériel du patrimoine de l'humanité. »

La société humaine est notre plus magistrale construction, mais à la différence des pyramides ou de la grande muraille de Chine, chaque élément la constituant, donc chaque vie, a autant d'importance que l'ensemble et c'est aussi cela qu'ETERNESIA veut transcrire. L'histoire, sans les histoires de chacun est, par nature, incomplète et la possibilité offerte par ce projet est aussi une façon de l'enrichir, de restituer d'une autre façon la trame de notre époque et de celles à venir.

ETERNESIA ne changera pas le monde. Seul le monde, lui-même, le peut et seulement dans de rares cas. Mais ETERNESIA peut replacer l'humanisme au centre du débat en inscrivant à jamais une forme d'altruisme dans la mémoire que l'on offre à ceux qui nous succèdent, acceptant de fait notre finitude, exact contrefeu de cette espèce de quête vaine et narcissique d'immortalité promise par les transhumanistes. ETERNESIA ne peut être issu de la pensée d'une petite minorité qui déciderait unilatéralement de ses objets et de ses modalités. Il doit être porté par un vaste consensus qui embrasse au mieux toutes les sensibilités et toutes les visions de l'existence. C'est pourquoi la participation à son édification est ouverte à tous ceux en qui il éveille un écho, afin que chacun puisse y apporter une contribution (éthique, philosophique, juridique, économique, technologique, etc.) et que nous puissions collectivement redonner des couleurs aux valeurs humanistes qui nous sont chères.

CONCLUSION

D'une manière générale, l'évolution des technologies de l'information engendre des répercussions considérables à tous les niveaux : elle transforme la société dans son ensemble, mais également les organisations et les institutions. Cette révolution numérique modifie aussi toutes les interactions sociales et même les individus. De nouveaux défis, mais aussi des conflits, ont émergé. D'après le déterministe technologique, les NTIC et les *Big Data* ne sont pas neutres. Elles influencent ses utilisateurs, les conditionnent et modifient leur vision du monde (Cf. Chapitre I).

Les NTIC qui permettent d'exploiter les données numériques, notamment dans le secteur de la santé et de l'assurance, procèdent d'un changement radical du paradigme dans la relation entreprise-citoyen *via* le traitement des données à caractère personnel. La performance numérique concerne aussi bien le volume de données étudiées, la diversité des sources et la recherche d'une réponse en temps réel. Cette nouvelle approche fait naître de nouvelles stratégies d'analyse des données fondées sur les probabilités, la manipulation des distributions complètes. Dès lors, les « données massives » se sont fait une place croissante au sein des entreprises et des structures, marquant un tournant dans la stratégie et l'organisation de ces dernières (Cf. Chapitre II).

Toutefois, cette «datasphère» suscite certaines préoccupations éthiques de leurs usages et des déviances qui peuvent en découler. La gestion informatique de la donnée numérique à caractère personnel appelle à une vigilance accrue en particulier pour sa protection et ne pourra être envisagée que dans le respect de certaines conditions. Ceci nous amène à nous poser la question de la valorisation, de la protection et de la réglementation autour des données numériques (Cf. Chapitre III).

C'est pourquoi, la quête de sens qui marque ce virage numérique entraîne nécessairement un questionnement sur les valeurs qui orientent nos comportements et nos actes tant individuels que collectifs. Cette éthique centrée sur l'humain doit être située au cœur des systèmes algorithmiques et des *Big Data* qui les alimentent. Dans ces conditions, une prise de conscience de la valeur des données issues des NTIC devient essentielle, tout comme un meilleur encadrement de l'usage des algorithmes de traitement à l'égard des individus. En effet, si nous voulons vivre harmonieusement dans ce nouveau monde régi par la « gouvernance algorithmique », nous devons intensifier nos efforts sur l'utilisation des données qui permet NTIC d'apprendre, sur leur maîtrise par l'utilisateur et sur la transparence de leurs usages (Cf. Chapitre IV).

C'est à partir de ce constat qu'ADEL a accompagné et structuré la rédaction de ce *vade-mecum* sur les réflexions et les bonnes pratiques d'un traitement algorithmique des données numériques. L'objectif était de donner un espace de

parole et d'expression aux différents acteurs de la société civile afin qu'ils puissent nous donner leurs ressentis et leurs points de vue sur ce sujet. En définitive, la conception, la mise en place et l'usage du traitement des données numériques passent inéluctablement par une réflexion éthique sur des procédures de contrôle et d'encadrement de ces derniers afin de conserver une place prédominante au sens, à la transparence, à la sécurité, et donc à la confiance auprès des acteurs du numérique. Dès lors, l'anonymat *via* les *Big Data* est devenu algorithmiquement impossible. C'est pourquoi, une « éthique algorithmique » devient décisive afin que les professionnels des *Big Data* trouvent un juste équilibre entre le traitement rationnel et mesuré des données, dans le respect de la vie privée, et un surtraitement qui serait contre-productif notamment pour le citoyen.

REMERCIEMENTS

Toute l'équipe d'ADEL tient à remercier tous les interlocuteurs et les auteurs qui ont contribué via leurs réflexions à l'élaboration de ce livre blanc, et en particulier tous les membres de son Comité d'experts indépendants d'ADEL qui l'accompagne dans cette approche vers une éthique du traitement des données numériques.

Pour plus de renseignements au sujet du label éthique ADEL

info@ADEL-Health.com



www.adel-label.com



Tous droits réservés - ADEL



www.adel-label.com

