

Synthèse des interventions

Conférence Intelligence artificielle : nouvelles puissances

Journée du 10 avril 2019 : L'IA et ses territoires en Europe, en région Occitanie, grands projets, robotique, santé, mobilité, startups, innovations

CNAM, Paris
10/04/2019

Table des matières

Mot d'accueil	4
Olivier Faron – Administrateur général du CNAM, et organisateurs	4
Keynote introductive	4
Keynote de la Région Ile-de-France	4
Alexandra Dublanche – Vice-Présidente de la Région Ile-de-France	4
Table ronde 1 : L'intelligence artificielle, secteur prioritaire pour la région Ile-de-France	6
Benoit Georges - Chef du service Idées et débats, Les Echos	6
Alexandra Dublanche - Vice-Présidente de la Région Ile de France, au développement économique, agriculture, ruralité	6
Juliette Mattioli - Senior Experte en intelligence artificielle, Thales	6
Bertrand Braunschweig - Directeur de la mission Inria de coordination du programme national de recherche en intelligence artificielle	6
Isabelle Guyon - Professeur à l'Université Paris Sud, LRI, Machine Learning, SVM	6
L'intelligence Artificielle de confiance, le vrai défi	8
David Sadek - Vice-Président recherche, technologie et innovation, Thales	8
IA, vision artificielle au Facebook AI Research Paris	9
Armand Joulin - Facebook AI Research Paris	9
IA, robotique, interactions homme-machine, émotions	10
Laurence Devillers - Professeur d'informatique, Sorbonne, LIMSI, CNRS, CERN	10
Stratégie de la région Occitanie pour la data et l'intelligence artificielle	12
Bertrand Monthubert - Conseiller régional délégué à l'enseignement supérieur et à la recherche, Président d'Occitanie Data, Mathématicien	12
L'Institut 3IA de Toulouse, un exemple de l'excellence française des régions	12
Nicholas Asher - Directeur de l'Institut 3IA Toulouse et Directeur de recherche	12
Table ronde 2 : La région Occitanie : son écosystème de l'IA	13
Luc De Andrade - Président du Think Tank NXU	13
Bertrand Monthubert - Conseiller régional délégué à l'enseignement supérieur et à la recherche, Président d'Occitanie Data, Mathématicien	13
Nicolas Asher - Directeur de l'Institut 3IA Toulouse et Directeur de recherche	13
Daniel Benchimol - Co-Président du grand cluster numérique d'Occitanie	13
Jean-Louis Fraysse - Co-fondateur de BotDesig, Docteur en pharmacie industrielle,	13
Administrateur Digital 113, Président de la Commission Biotech, Médecine et Santé NXU	13
Jérôme Maurel - Ad'occ, Responsable Unité Numérique et Systèmes Intelligents - Direction de l'Innovation	13
Patrick Seguela - Dirigeant Synapse Développement	13
Table ronde 3 : IA et santé, création du Health Data Hub	17
Sacha Alanoca - AI Policu Researcher and Program Manager, The Future Society	17

David Gruson - Membre du comité de direction de la chaire Santé de Sciences Po, fondateur de l'initiative Ethik IA.....	17
Christophe Richard - Directeur médical SANTEOS, ATOS.....	17
Raphael Canyasse - CTO ANAMNESE	17
Table ronde 4 : IA et mobilité transports – Hub France IA	19
Antoine Couret - CEO Geo4Cast, Président du Hub Francela.....	19
David de Almeida - Directeur Département Modélisation & Expérience Voyageurs, Direction Innovation & Recherche, SNCF.....	19
Luc de Andreade - Président du Think Tank NXU.....	19
Olivier Pages - CEO, FFLY4U.....	19
Table ronde 5 : Chatbots, assistants conversationnels, reconnaissance vocale, IoT et domotique	21
Jean Rohmer - Vice-président Institut Fredrik . Bull. Head of Research and partnership Pôle Universitaire Léonard de Vinci	21
Luc Truntzel – CEO IBENTA France	21
Yann Lechelle – COO, SNIPS	21
Enrico Valtolina – Direction Innovation & Systèmes, Software architect, Groupe LEGRAND	21
Jean-Luc Dormoy – Vesta-System	21
Table ronde 6 : Traitement de la donnée, qualité et création de valeur	23
Jean-Paul Pinte – Docteur en information scientifique et technique, maitre de conférence à l’Université catholique de Lille (FLSH), expert en veille et intelligence compétitive	23
Alice Froidevaux – Quantcube Technology	23
Frédéric Cuppens – Professeur à Telecom Bretagne, responsable de l’équipe SERES, Institut Mines Telecom.	23
Grégoire Siguel – CTO et cofondateur de GEOTREND.....	23
Stéphane Cordova – Vice-Président, technologies embarquées KALRAY.....	23
Keynote : Intelligence artificielle symbolique, calcul formel, apprentissage statistique : les synergies	24
Jean Rohmer - Vice-président Institut Fredrik . Bull. Head of Research and partnership Pôle Universitaire Léonard de Vinci	24
Clôture de la première journée	25
Olivier Kempf – Directeur La Vigie, Chercheur associé à la FRS, Président d’EchoRadar, Membre de la Chaire Cybersécurité et Cyberdéfense Saint-Cyr, Sogeti, Thales	25

Au cours de ces deux journées de conférences, de nombreuses thématiques ont été abordées, parmi lesquelles :

- La politique globale de la France en matière d'IA.
- La dimension européenne et internationale de l'IA.
- L'IA en régions et dans les territoires.
- IA et santé.
- IA, transports et mobilité.
- IA et cybersécurité.
- IA, confiance et éthique.
- L'IA confrontée à la formation et à la recherche.
- L'IA face à la justice.

Matinée

Mot d'accueil

Olivier Faron – Administrateur général du CNAM, et organisateurs

60 ans après la conférence fondatrice de Dartmouth, l'IA est devenue pour nos sociétés, économies et systèmes politiques, un sujet incontournable. Tous les secteurs d'expertise et d'activités sont impactés par la montée en puissance de l'IA, comme tous les pays. Il est donc essentiel pour la France et l'Europe de s'emparer dans cette compétition mondiale.

L'IA est une question centrale, liée à la recherche et au développement économique. Mais c'est aussi une question qui doit être pensée pour les territoires et dans les territoires.

Keynote introductive

Antoine Petit – Président Directeur Général, CNRS

Comment être plus efficaces en matières d'IA ? Un an après le rapport Villani, les progrès n'ont pas été au rendez-vous. Il y a autour de l'IA un certain renouveau, mais celle qui marche aujourd'hui c'est l'IA connexionniste et non pas la symbolique. La présence des industriels français dans le domaine est également un sujet de préoccupation. Il y a une compétition internationale féroce pour attirer les cerveaux, et les garder, de laquelle les français semblent être absents. On peut en effet noter à l'étranger certaines conditions réunies pour favoriser un certain dynamisme de l'IA (à savoir, des conditions attractives pour les chercheurs, mais aussi un lien fort entre les secteurs académiques et socio-économiques). Et pour l'instant, en France, elles ne sont pas réunies.

Est-on capables de faire de vrais choix, y compris de territoires ? Sommes-nous capables également de faire des efforts (surtout concernant les problèmes d'organisation) ?

Le besoin de rechercher dans le domaine de l'IA est encore très important. Beaucoup de choses restent à faire, d'autant plus dans un pays comme la France avec un si gros potentiel. Mais il faut exploiter ce potentiel en lien avec le secteur académique et le secteur socio-économique. Et s'il est bien de parler d'éthique, il ne faudrait pas que nous soyons le continent de l'éthique, en laissant les chinois ou les russes être le continent du business.

Certes, nous avons besoin de recherche en sciences dures : il faut être capable de traiter toutes les données incertaines, floues, qui vont voir le jour ; de comprendre comment désapprendre. Il y a un besoin extrêmement fort concernant toutes les questions de validation, vérification, de spécification. Ainsi, si l'on veut avoir une IA explicable, comprise et acceptée par la population, on va avoir besoin de techniques mathématiques pour prouver les algorithmes, mais on va aussi besoin de relations avec les sciences humaines et sociales. Ce qui semble clé, ce sont toutes ces questions relatives à l'explicabilité, à la prise en compte du biais.

Par conséquent, il est important collectivement de parler d'IA, certes, mais aussi d'en faire.

Keynote de la Région Ile-de-France

Alexandra Dublanche – Vice-Présidente de la Région Ile-de-France

La stratégie de l'Ile-de-France (IDF) en matière d'IA est toute arrêtée et se met peu à peu en place. En effet, le rôle de la région est essentiellement d'aider à faire croître cet écosystème, de permettre aux

acteurs de se rencontrer, et de donner à toutes les entreprises les clés et les ressources pour accéder à tous les atouts de la recherche en IA. Les régions sont, par ailleurs, la bonne échelle pour mener des politiques publiques agiles de développement de pôles d'excellence et d'écosystèmes innovants en IA. Nous sommes actuellement en train de vivre l'entrée dans la phase d'industrialisation de l'IA et l'Île-de-France y a une carte importante à jouer dans la mesure où c'est l'endroit où se joue l'avenir de l'IA en Europe (en tant que première région d'Europe en termes de recherche et de développement). Les GAFAs ont compris la dynamique à l'œuvre en IDF car depuis quelques temps, on observe une dynamique d'implantation de leurs centres de recherche en IA sur le territoire de la région. Mais les entreprises françaises ne sont pas en reste et se saisissent également des opportunités offertes par les technologies d'IA : la région IDF est alors présente pour les accompagner dans le processus.

La grande majorité des entreprises qui représentent plus de 75% des emplois et 70% de la valeur ajoutée au niveau national est tenue à l'écart de cette quatrième révolution industrielle, alors même qu'elles se disent conscientes des enjeux que représente l'IA en France. Plusieurs barrières rendent le passage à l'acte plus difficile :

- Le foisonnement de l'offre dans la région peut avoir un effet contre-productif car il représente un obstacle à la lisibilité et cause des difficultés à s'orienter dans ce maquis francilien de l'innovation et de la recherche.
- Les interrogations sur la pertinence des solutions existantes.
- Un problème de compétences internes pour intégrer et maintenir les solutions acquises, les profils partant vers des grands groupes.

Pour répondre à ces problématiques, un plan IA 2021 a été lancé pour permettre à tout ce tissu francilien d'accéder à ces technologies et innovations, pour se moderniser, prospérer, créer de la croissance et de l'emploi. La démarche s'est d'abord matérialisée par un premier plan « *Smart industry* » pour aider les industries à se moderniser et se digitaliser. Puis, pour faciliter l'appropriation des technologies d'IA par les PME (Petites et moyennes entreprises) et les ETI (Entreprises de taille intermédiaires), la région a apporté son soutien à l'innovation Inria Techn, plateforme facilitant l'accès aux technologies de pointe des laboratoires franciliens d'Inria. La région a également conscience que favoriser l'accès à l'IA passe par l'accès à des données de volume suffisant et de bonne qualité. C'est pourquoi une plateforme spécialement dédiée à la mutualisation de données industrielles a été mise en place avec des partenaires tels qu'ATOS ou la SNCF. Le manque de talents bien formés peut être une barrière conséquente à l'entrée en IA des PME et ETI, qui n'ont pas besoin d'experts en IA mais plutôt de collaborateurs capables de suivre la mise en œuvre des solutions au sein de leur entreprise. Pour pallier ce défi, l'accent a été mis sur le développement de profils IA avec pour objectif la formation de 200 profils par an, et un premier lycée d'IA va être lancé dans le 12^e arrondissement (200 étudiants par promotion). Un nouveau programme de bourses doctorales a été mis en place, avec un budget total de 4 millions d'euros, pour faciliter le recrutement de thésards en entreprise afin de renforcer également le rôle de « carrefour de l'IA » que veut jouer la région. En parallèle, la région opère une accélération des coopérations internationales (Canada, Allemagne, Corée du Sud) et lance des challenges avec des partenaires privés et de la recherche.

L'ambition de la région est de positionner l'IDF et la France en général sur le devant de la scène en ce qui concerne ces technologies d'avenir. L'objectif est donc double :

- Développer l'écosystème d'innovation et de l'IA en soutenant les projets à fort potentiel et en attirant les pépites du secteur sur le territoire.
- Permettre que cette excellence scientifique et technologique reconnue dans le monde entier soit accessible à l'ensemble du tissu des entreprises de l'IDF afin qu'elles se modernisent, continuent à se développer et à exister.

Pour la région, le futur de l'IA se joue en France et plus particulièrement en Ile-de-France, qui compte sur l'ensemble des chercheurs et industriels pour continuer à se hisser à la pointe de l'innovation.

Table ronde 1 : L'intelligence artificielle, secteur prioritaire pour la région Ile-de-France

Benoit Georges - Chef du service Idées et débats, Les Echos

Alexandra Dublanche - Vice-Présidente de la Région Ile de France, au développement économique, agriculture, ruralité

Juliette Mattioli - Senior Experte en intelligence artificielle, Thales

Bertrand Braunschweig - Directeur de la mission Inria de coordination du programme national de recherche en intelligence artificielle

Isabelle Guyon - Professeur à l'Université Paris Sud, LRI, Machine Learning, SVM

❖ **Où en est la France concernant l'IA ?**

Dans l'ambition du plan national de recherche en IA, l'objectif est d'être dans les 5 premiers pays au monde, et d'être première en Europe. Par conséquent, dans cette course, nous sommes en compétition mais aussi en collaboration avec d'autres acteurs déjà largement avancés en la matière, ce qui explique la nécessité de se développer rapidement. La mise en place des instituts 3IA a pris un peu de temps mais il s'agit d'un projet ayant vocation à être mis en œuvre très rapidement.

2019 était le premier anniversaire de la remise du rapport Villani au Président de la République. Il s'est passé beaucoup de choses depuis, notamment autour des trois composantes du plan national :

- Le volet *Talents*, consacrée à la recherche et la formation.
- Le volet *IA dans l'économie et la société*, avec des actions menées telles que l'appel à manifestation d'intérêt sur la mutualisation de données, qui va conduire à des appels à propositions assez rapidement, la mise en place du *Health data Hub*, ou encore des projets relatifs à la mobilité.
- Le volet *Dimension sociale et éthique*, consistant d'une part à faire évoluer le comité consultatif national d'éthique, qui s'occupe principalement de bio pour traiter les sujets du numérique, et d'autre part la volonté de créer une instance internationale, le *International Panel on AI*.

Sur le volet recherche, la mesure la plus visible est certainement les Instituts 3IA. La publication d'appels sur des chaires en dehors des instituts 3IA et de thèses vont être lancés, ainsi que des appels à supercalculs.

L'institut de convergence Data IA est maintenant le lieu où se développent les enjeux d'IA sur le pôle de Paris Saclay, et même si l'Institut de Petry sera finalement le seul institut interdisciplinaire d'IDF, dans la mesure où la candidature de Saclay n'a pas été retenue, la région s'impliquera dans l'accompagnement de l'Institut. Il y a un contact permanent entre la région et l'Institut, pour avancer ensemble dans la même direction.

Les challenges visant à apporter des solutions aux verrous technologiques sur les filières essentielles, à savoir l'industrie, la santé et l'emploi, sont centraux dans le plan de la région en matière d'IA. Chaque challenge met en compétition des partenaires industriels avec un prix à la clé (par exemple, sur le thème de la réindustrialisation du territoire et le *transfer learning*).

❖ **Codalab**

Il s'agit d'un projet né il y a 6 ans et qui a grossi en tant que projet *open source*. L'Université Paris-Saclay en a maintenant la responsabilité pour coordonner l'effort de recherche et de développement autour de cette plateforme. La plateforme a mis un point d'honneur à être la plus transparente possible, ce

qui a favorisé son utilisation dans de nombreux challenges, par des acteurs du monde entier. Elle a également été choisie par la communauté européenne pour le projet d'envergure H2020. L'aspect innovant de la région IDF actuellement consiste donc à mettre en lien des industriels avec des données de pointe et d'intérêt national, et des petites entreprises qui n'auraient pas accès à ces données autrement, la plateforme étant le point de rencontre de ces acteurs (données accessibles uniquement sur la plateforme grâce à un code unique fourni aux PME, chacun des acteurs gardant la propriété intellectuelle de ses données, la plateforme devenant alors un outil d'évaluation transparente et juste). La plateforme permet donc, à l'issue des travaux, d'avoir des résultats quantitatifs sur des projets nationaux.

❖ **L'engagement de Thales en IA**

Depuis les 3 dernières années, il y a eu une accélération de l'engagement de Thales en IA avec une stratégie un peu plus construite, notamment pour la réponse aux projets. La collaboration avec des académiques ou l'écosystème startup, PME, TPE se fait dans des laboratoires communs. L'ambition est d'aller au-delà des quelques laboratoires existants et des travaux menés actuellement, par le biais de thèses par exemple.

L'IA chez Thales s'organise en deux pôles, le plus gros en IDF et le deuxième lancé fin 2017 au Canada. Environ 200 chercheurs s'intéressent à l'IA dans le global Thales, dont les trois quarts en IDF, en particulier sur le plateau de Saclay. Toutefois, les approches de l'IA sont différentes en France et au Canada, dans la mesure où l'approche française est plus traditionaliste, dans la rigueur, tandis que la canadienne est beaucoup plus pragmatique. L'enjeu est maintenant de voir comment les résultats de l'un, l'autre ou des deux, s'intégreront dans les produits Thales. L'objectif en tant qu'IA est de parvenir à bâtir une IA qualifiée, certifiée, expliquée et responsable, avec une grosse notion de l'ingénierie algorithmique.

Thales fait partie des groupes qui recrutent beaucoup dans le domaine de l'IA, mais il y a aujourd'hui un manque de talent dans l'IA au sens général du terme, et pas uniquement dans la data science. Il y a un véritable besoin de connectivité entre IA connexionniste et IA symbolique, car résoudre un problème complexe dans un système critique nécessite de combiner ces deux approches.

❖ **Sensibiliser à l'IA**

Les discussions relatives à la sensibilisation des étudiants à l'IA portent sur le projet de lycée dédié à l'IA, dans le 12^e arrondissement de Paris. La volonté de la région et des porteurs du projet est de faire de ce lycée un *living-lab*, un site expérimental de ce que peut apporter ce projet dans tous ses aspects, si bien des technologies venues de l'IA pour mieux s'en sortir, que des enseignements spécifiques sur l'IA (en restant au niveau lycée, évidemment). La contrainte apparaissant est qu'il s'agit d'un site expérimental où il n'y a pas de place pour l'erreur étant donné le caractère déterminant de cette expérience pour les jeunes qui y étudieront en termes de poursuite d'étude ou de perspectives de carrière. Il faudra un certain temps pour mettre tout ce chantier en place, la date d'ouverture restant pour le moment inconnue.

Parmi les mesures prises par la région IDF figurait également celle de rendre la région visible au niveau mondial, sur ce qui est fait par l'IDF et en IDF dans l'IA : l'ambition est donc maintenant d'accueillir une grande conférence mondiale sur le modèle du NeurIPS (sur les réseaux neuronaux) au Canada.

❖ **Comment faire en sorte que le tissu de PME, d'ETI, et de startup soient intégré dans le système local ?**

Chez Thales, il y a une véritable philosophie d'*open innovation*, où des agents sont chargés de faire de la veille dans les petites structures et sur différentes technologies du numérique suivies. Il a aussi de

nombreuses collaborations développées en matière de *proof-of-concept* et des challenges internes avec des PME pour permettre de les rencontrer, les connaître et développer des collaborations. Mais on observe également une réponse régionale, où les pôles et surtout le pôle systématique a cette fonction d'animer l'écosystème en IA, sans omettre les feuilles de route nationales. Les challenges organisés par Codalab sont également l'opportunité de tisser du lien, et ils se popularisent de plus en plus, ce qui permettra de servir de tremplin à l'IA en France si l'on stimule les chercheurs à emprunter cette voie.

L'intelligence Artificielle de confiance, le vrai défi

David Sadek - Vice-Président recherche, technologie et innovation, Thales

L'IA est aujourd'hui un des quatre piliers de transformation numérique dans laquelle Thales est engagé (avec la connectivité/IOT, le big data et la cybersécurité). L'IA apparaît dans l'ensemble des marchés de Thales, qui se distingue comme un acteur multisectoriel (de l'avionique jusqu'à la défense, en passant par le spatial et le transport terrestre par exemple).

En terme de volume d'activité chez Thales, on estime les effectifs à 200 experts en IA, avec pour objectif de doubler ce chiffre pour l'année à venir, étant donné le caractère structurant de l'IA au sein du groupe.

❖ *Etat des lieux de l'IA aujourd'hui*

Les technologies d'IA faisant parler d'elles actuellement sont principalement les technologies de reconnaissance de formes ou des technologies très dédiées à des applications spécifiques (domaine du jeu par exemple). Lorsque l'on pense à des aptitudes plus cognitives qui peuvent être la projection de ce qu'on peut avoir à l'esprit lorsque l'on pense à des systèmes intelligents, on est en droit de se demander s'il y a un continuum entre ce que l'on sait faire aujourd'hui et ces aptitudes, ou s'il existe en réalité un plafond de verre ? La réponse est relativement nuancée, même s'il faudrait considérer d'autres technologies en IA, notamment des technologies de représentation explicite des invariants du comportement intelligent.

Les technologies de reconnaissance de formes présentent des performances remarquables. Cependant, il y a quand même un ensemble de vulnérabilités à traiter :

- Le syndrome « boîte noire » qui fait que les technologies de *deep learning* en particulier ne présentent pas nécessairement de processus de prise de décision (entres autres) explicables.
- L'apprenabilité : les machines apprennent réellement ce que l'on veut qu'elles apprennent (différences entre les attentes et les résultats). La question de ce qui est réellement appris reste une véritable question scientifique et technique : quels sont les critères qu'un système d'IA utilise pour apprendre ?
- La possibilité de leurre de ces systèmes : comment, en maquillant un pixel de façon perceptible ou non, peut-on faire complètement basculer un système d'une catégorie à une autre ? La puissance des systèmes d'apprentissage est la capacité à mener des objets dans les systèmes à très grande dimension, et plus on augmente cette dimension (à un tel point que cela devient non intelligible pour un humain), plus on peut basculer d'une classe à l'autre relativement facilement.

Cela n'enlève en rien à la performance de ces systèmes, il faut simplement être conscient de ces écueils, d'autant plus lorsqu'ils sont utilisés pour des applications dites critiques (pas de possibilité d'appliquer du *test and learn*).

❖ **Qu'attend-t-on d'un système d'IA ?**

Le ratio est à calculer entre l'effet « Wow » (où l'on est impressionné par les capacités d'un système) et l'effet « What the hell (WTH) » (quel enfer). La confiance entre les systèmes d'IA est sensible : elle se gagne par gouttes et se perd par seaux. Il existe donc des conditions nécessaires à l'adoption des systèmes critiques :

- L'**explicabilité** : on a tendance à se concentrer sur l'explicabilité des systèmes statistiques ou des systèmes d'apprentissage. Mais même des systèmes symboliques peuvent être difficiles à expliquer. Chez Thales, l'ambition est de pouvoir expliquer le fonctionnement des systèmes au moins a posteriori, mais surtout en temps réel, pour que l'utilisateur puisse être en mesure de poser des questions de type « pourquoi ? ». Tout repose sur la différence entre le fait de retracer un calcul et expliquer un raisonnement avec des mots et des concepts intelligibles par l'humain.
- La **validité**, à savoir montrer ou démontrer que le système fait tout ce qu'il est censé faire, et rien que cela. Les spécifications sont importantes et doivent être claires, pour pouvoir vérifier que le système fait bien ce que l'on attend de lui. Une question va peu à peu devenir un véritable objet de recherche : celle des systèmes qui apprennent en continu, avec l'enjeu de la préservation des propriétés au fil de l'apprentissage.
- La **responsabilité**, ou la conformité des systèmes à des principes éthiques, légaux, ... Un des défis est l'équilibrage des corpus de données : comment faire en sorte qu'un système n'ait qu'un minimum de biais ? Synthétiser apparaît comme une solution pour tenter de minimiser ces biais. L'approche de Thales est de travailler sur la conformité dès la construction des systèmes, afin que les algorithmes puissent se conformer à certaines lois, principes ou dispositifs légaux, spécifiés par l'utilisateur ou l'application.

Un défi sous-jacent à la question des systèmes critiques est la question de l'embarquabilité des systèmes, à savoir le fait de concevoir des technologies qui peuvent être placées dans des dispositifs contraints et ceci quel que soit le type de contraintes (contraintes SWAP, soit Size, Weight, and Power). Une différence est à noter entre le monde de l'IT (ressources infinies) et le monde des *operational technologies* (de l'informatique industriel), qu'il faut toutefois parvenir à faire converger.

L'humain reste d'une manière ou d'une autre dans la chaîne de responsabilité et dans le processus de décision. L'IA nous permet aujourd'hui de nous questionner sur nos propres fonctionnements et comportements, et en cela elle est également un apport pour nos sociétés.

IA, vision artificielle au Facebook AI Research Paris

Armand Joulin - Facebook AI Research Paris

Le *machine learning* est une nouvelle forme d'informatique dans laquelle, au lieu de spécifier des programmes par des lignes de commandes, on les spécifie par des couples d'entrée-sortie, en particulier dans le milieu supervisé.

Le plus gros succès industriel date des années 2000 (Yann Le Cun, Turing Award 2018) : il s'agit de la reconnaissance de chiffres sur les chèques. Depuis 2015, on a commencé à devenir de plus en plus forts en matière de détection d'objet et d'identification. On est maintenant capables de faire de la détection de pose d'humains même quand les images sont en mouvement.

Cependant, le gros problème avec ces avancées est qu'elles dépendent de l'intervention initiale de l'Homme. En effet, si l'on veut avoir un système de *machine learning* qui identifie les objets, il faudra au préalable qu'un humain renseigne manuellement la qualification des objets à identifier, ce qui prend un certain temps. Le même problème se pose si l'on veut situer l'objet sur une image, ou dans le cas de la détection. Et à ces difficultés s'en ajoutent d'autres :

- Dans des images où il y a de nombreuses fois le même objet, il y a un risque de mauvaise identification, de négligence d'une partie des objets, ou de cadres de mauvaise qualité.
- On souffre de la qualité des annotations choisies dès le début. Si on a été trop peu précis initialement, il sera impossible d'affiner la qualification par la suite.

Pour résoudre ces problèmes, un gros effort suivi depuis plusieurs années a été d'essayer de travailler directement sur les données utilisées plus tard en application, pour retirer cette étape d'annotation qui biaise l'humain dans ses perceptions en faussant les applications a priori.

La quantité d'informations et d'images accessibles par Facebook (post publics des utilisateurs) a permis de passer d'une identification difficile des objets représentés sur les clichés (annotations peu adéquates ou impossibles) à la construction de data set automatiques avec une information beaucoup plus fine sur les images et une couverture exacte des données que l'on aura en application. Il y a même eu des indications qui relevaient d'une connaissance experte du domaine (grâce à des passionnés qui fournissent des informations très riches et précises). Cependant, énormément d'images restent dures à décrire, notamment du fait de leur richesse : c'est un véritable problème car même en utilisant des données méta comme les hashtags, on ne couvre pas tout le dataset, pas toute l'information contenue dans une image. Pour le résoudre, on revient aux données, en rapprochant ou éloignant des images présentant des champs sémantiques, des couleurs et représentations visuelles similaires ou opposés. L'intérêt de ce genre d'approches est qu'elles vont permettre de former des classes, auxquelles on va pouvoir ajouter des hashtags. Les méthodes non-supervisées vont par conséquent offrir la possibilité de s'adapter assez rapidement et facilement lorsque nous sommes confrontés au phénomène de nouveauté (car les images n'ont pas la même distribution d'une année sur l'autre).

Cette approche n'est pas la seule piste explorée pour tenter de résoudre la vision et d'améliorer les compréhensions visuelles sans apport d'information extérieure. Une autre approche est de se dire qu'une seule image peut également être très riche dans la mesure où elle peut être composée de plusieurs autres images. On peut donc également essayer d'apprendre de bonnes représentations visuelles en essayant de deviner ce que contient une image. On peut donc faire du *masking* : masquer des zones d'une image pour prédire ce qu'il y a derrière. On peut donc apprendre des choses assez fines à partir d'une seule et même image, et cela permet à Facebook d'enrichir ses représentations visuelles sans avoir à annoter quoi que ce soit (gain de temps considérable).

IA, robotique, interactions homme-machine, émotions

Laurence Devillers - Professeur d'informatique, Sorbonne, LIMSI, CNRS, CERNA

Il y a trois parties essentielles pour faire du *machine learning*, discipline dans laquelle les chercheurs ont une forte responsabilité :

- Des données bien choisies et non-discriminantes
- Des algorithmes bien testés
- Les paramètres utilisés dans ces différentes machines : si les chercheurs ne peuvent pas refaire les mêmes expérimentations en utilisant en *open-source* les paramètres (non-fournis par les grands groupes, qui pourtant mettent à disposition leurs algorithmes), les implications sont non-négligeables et influencent ce que la machine fera par la suite. Il ne suffit donc pas de demander quelles sont les données utilisées mais il faut aussi accéder aux paramètres afin de mener à bien les expérimentations.

Une solution serait d'aller vers des systèmes d'IA répondant de l'éthique appliquée, qui est un équilibre entre bénéfices et risques respectant un certain nombre de valeurs éthiques importantes : déontologie et responsabilité des concepteurs, émancipation et responsabilité des utilisateurs, évaluation,

transparence, explicabilité, loyauté, non-discrimination des machines, et coévolution homme-machine (pas de vérification des intentions de la machine).

Par ailleurs, un autre problème se pose : la représentation des femmes en IA. On parle de 50% d'interactions avec des machines en 2020, à la voix, qui a un fort pouvoir. Or, ce seront des voix féminisées étant donnée la large présence des figures féminines en IA. Elles sont assistantes, soumises, corvéables et robots-sexuels... 80% des robots décodeurs sont des hommes, et 80% des chatbots sont des présences féminines : n'y a-t-il pas un rapport à vérifier ?

❖ *L'affective computing*

L'affective computing est composé de trois catégories de capacités :

- Détecter les émotions dans le comportement des humains
- L'intégrer dans un système de dialogue
- Générer des réponses

On va donc détecter ces émotions et comportements dans des signaux, audios, sur des visages, grâce aux gestes, mais sans se préoccuper des aspects culturels. Tous ces éléments ne sont pas encore entièrement pris en compte et les systèmes qui arrivent sur le marché sont encore assez simples en termes de facteurs pris en compte. Mais grâce au *deep learning*, on peut montrer que l'on arrivera à la même capacité et même plus : perceptivement, les robots auront une acuité visuelle et acoustique meilleure que la nôtre.

Le profil émotionnel et interactionnel de la personne est construit dans l'interaction avec elle, pour ensuite modifier la stratégie du robot. On a ainsi recours au nudge, une méthode destinée à orienter les comportements sans jamais contraindre ni culpabiliser les individus mais en se servant des biais cognitifs et émotionnels. Les chatbots vont amplifier cela, en utilisant les biais existants. Les travaux sont fondés sur la réflexion d'Antonio Damasio « Nous ne sommes pas rationnels sans être émotionnels », même s'il faut garder à l'esprit qu'il n'y a pas d'émotion, pas de désir, pas d'intention ou d'intuition dans la machine. Deux courants de pensée s'opposent alors : ceux pour qui il y aurait une émergence de la conscience dans les machines, et ceux qui contestent cette opinion. Par contre, soyons alertés sur le fait que nous sommes attentifs et percevons selon nos émotions, ce qui donnent naissance à deux biais majeurs :

- Le biais d'attention, c'est-à-dire les perceptions influencées par nos intérêts
- L'ancrage mental, ou l'influence laissée par la première impression.

Nous anthropomorphisons les machines, projetant ainsi des comportements humains sur les robots, notamment si le robot se présente comme émotionnel, amusant, fragile, vulnérable, ect. Le « sexe » du robot peut donc également avoir une réelle influence. Le robot ayant une acuité plus forte qu'un humain, des dérives possibles apparaissent en filigrane (récupération de données privées et sensibles, influence psychologique et commerciale, ...). Des expériences de nudge sont donc réalisées dans la vie réelle pour comparer différentes méthodes lorsque l'on tente d'orienter des personnes vulnérables vers certains comportements et trouver les facteurs les plus efficaces (jouer sur l'affectif en parlant à la première personne ou riant, les répétitions, ou autres exploitations) dans cette entreprise. Il y a beaucoup de challenges autour de ces aspects, d'où l'importance de les prendre en compte.

Stratégie de la région Occitanie pour la data et l'intelligence artificielle

Bertrand Monthubert - Conseiller régional délégué à l'enseignement supérieur et à la recherche, Président d'Occitanie Data, Mathématicien

La région Occitanie est actuellement en train de développer une stratégie numérique régionale. Dans le cadre de cette stratégie et en rencontre avec d'autres éléments des stratégies mises en place au niveau régional, l'une des ambitions maitresses est d'attirer les femmes vers les carrières du numérique, point extrêmement important pour ne plus trouver la présence féminine uniquement dans les représentations mais également parmi les acteurs.

Plusieurs secteurs s'interpénètrent et sont présents en Occitanie (IA, Data science, cybersécurité, IoT, robotique, ...).

Une stratégie IA a donc été mise en place à l'échelle de la région Occitanie, en s'appuyant sur plusieurs piliers :

- Soutenir l'institut 3IA (engagement à hauteur de 6 millions par an)
- Accompagner les entreprises à travers l'agence de développement économique AdOcc, les clusters Digital 113, AeroSpace Valley, et avec la création d'Occitanie Data, car la data est le moteur du développement de l'IA. La mise en place de cette structure est apparue en réponse au constat qu'il y avait dans la région des atouts et certains gros producteurs de données, mais que leur exploitation était souvent handicapée par le fait que les données se trouvent dans des silos alors mêmes qu'elles ne peuvent prendre leur pleine valeur que lorsqu'elles sont croisées avec celles d'autres acteurs (difficulté à le faire aujourd'hui en l'absence de cadre commun, de modèle de partage et de modèle économique, aggravé par les questions de protection des données sensibles).

L'ambition d'Occitanie Data, créée en janvier 2019, est donc de favoriser la création d'un guichet unique de services data. Plusieurs travaux ont déjà été lancés :

- La définition d'un modèle économique et d'un cadre éthique
- La veille, le montage et la gestion de projets
- La recherche de financements
- L'animation de réseaux

Cette association rassemble si bien des acteurs publics (acteurs académiques, institutions publiques nationales, collectivités territoriales) et que privés, et inclue également des acteurs non implantés en Occitanie, en respectant un esprit de respect d'une souveraineté européenne.

L'Institut 3IA de Toulouse, un exemple de l'excellence française des régions

Nicholas Asher - Directeur de l'Institut 3IA Toulouse et Directeur de recherche

En avril 2018, le Président de la République a formulé l'ambition de développer des centres de recherche à forte visibilité mondiale, d'éducation et de développement économique en IA.

❖ **Pourquoi faire de l'IA à Toulouse ?**

Il s'agit d'un très grand centre de recherche en IA, avec une communauté importante de chercheurs et une communauté d'étudiants exceptionnelle également. L'écosystème économique est par ailleurs très favorable (leader mondial de l'aéronautique et acteurs centraux dans les domaines de l'espace et la météorologie).

❖ **L'Institut 3IA**

Les trois ambitions soutenues par l'Institut 3IA sont la recherche, la formation et le développement économique. Ils travaillent sur l'IA hybride, avec des projets tels que l'application de la robotique en industrie ou encore des recherches sur le climat et la santé. Avec des méthodes formelles, il est difficile d'avoir des systèmes adaptatifs et des données dans de hautes dimensions. L'objectif est donc l'acceptation par les grands acteurs et le public d'assistants IA au sein des structures (acteurs industriels ou autres), il faut pouvoir leur garantir des propriétés techniques telles que la robustesse, la fiabilité, l'adaptabilité, et qu'ils soient embarquables.

Dans dix ans, l'Institut 3IA aimerait être un point de référence dans l'IA hybride, avec des applications certifiables et vérifiées d'IA adaptatif mais aussi sûres dans le transport, la santé et le monitoring de l'environnement. La formation étant le deuxième pilier de l'Institut 3IA, l'objectif est de doubler le nombre d'étudiants d'ici une dizaine d'années. Et afin de faire en sorte que ces derniers restent auprès des industriels français, des stages et des programmes en apprentissage seront mis en place. Enfin, l'Institut souhaite s'attaquer au problème d'acceptabilité de l'IA : le danger que l'IA soit vue comme un problème sociétal et non pas un bénéfice est réel. Or, les utilisations positives sont nombreuses, tout comme les bénéfices à en retirer.

Table ronde 2 : La région Occitanie : son écosystème de l'IA

Luc De Andrade - Président du Think Tank NXU

Bertrand Monthubert - Conseiller régional délégué à l'enseignement supérieur et à la recherche, Président d'Occitanie Data, Mathématicien

Nicolas Asher - Directeur de l'Institut 3IA Toulouse et Directeur de recherche

Daniel Benchimol - Co-Président du grand cluster numérique d'Occitanie

Jean-Louis Fraysse - Co-fondateur de BotDesig, Docteur en pharmacie industrielle, Administrateur Digital 113, Président de la Commission Biotech, Médecine et Santé NXU

Jérôme Maurel - Ad'occ, Responsable Unité Numérique et Systèmes Intelligents - Direction de l'Innovation

Patrick Seguela - Dirigeant Synapse Développement

Le think tank NXU a été créé pour analyser l'impact sociétal lié à la grande convergence NBIC (Nanotechnologies, biotechnologies, informatique et sciences cognitives), car cela aura sûrement un impact tant au niveau sociétal qu'économique, mais aussi sur nos démocraties. L'idée est de rendre ces sujets accessibles au-delà des aspects technologiques et des NBIC, en synthétisant et analysant les points de vue des leaders d'opinion et en analysant également l'information que l'on peut en retirer. Pour ce faire, le think tank réunit un réseau d'experts issus de la recherche et de l'enseignement mais aussi du privé, dans un grand métissage des métiers.

❖ **L'agence Ad'Occ**

L'agence Ad'Occ compte en 2018 3800 entreprises accompagnées, avec quasiment un évènement par jour organisé au niveau de l'agence. Il s'agit d'une agence très territoriale, présente sur tous les bassins d'emploi de l'Occitanie et même à l'international. Sa mission principale est de soutenir l'économie, en étant financée majoritairement par la région, mais aussi par l'Etat et l'Europe.

L'Occitanie est une région qui produit énormément de data, donc la stratégie de l'innovation « 3S » (volonté de spécialiser les territoires) a été refondue suite au rapprochement des deux territoires

(Pyrénées et Languedoc-Roussillon), pour produire encore davantage de data. Ce projet s'est donc structuré autour d'une stratégie régionale, les actions reposant sur trois piliers fondamentaux :

- La recherche
- La cybersécurité et la sûreté de l'information (que ce soit dans les échanges d'un écosystème très IOT et embarqué, l'enjeu est de faire progresser les PME dans des démarches de sûreté, de sécurité et de protection de l'information, d'où la création d'un centre technique à préciser lors d'une rencontre à venir). Derrière cela apparaît également un élément plus prospectif, le quantique, qui est plutôt orienté sur le calcul.
- La formation, ou la volonté de créer des double-profilés dans cette région qui crée le plus d'emplois industriels en France, et avec un énorme potentiel technique (15 pôles de compétitivité dont un mondial).

❖ **L'accompagnement de la filière IA par Digital 113**

Rassemblant 400 entreprises, Digital 113 est un cluster numérique. En 2011, il fallait montrer à l'écosystème régional mais aussi au national qu'il y avait une vie à Toulouse à côté des grands industriels du spatial et d'Airbus, qui favorisaient effectivement les technologies et les *deep tech*. Cela a permis de montrer que les entreprises du numérique étaient une véritable industrie en Occitanie, et qu'il y avait une véritable richesse dans ces entreprises qui créent de l'emploi et sont au service des industries locales, mais pas uniquement.

Mais, à quoi sert un cluster ? Cela sert à potentialiser les entreprises, surtout les petites, pour les aider à faire le lien avec la recherche. C'est également utile pour réfléchir au financement de ces économies et entreprises. En définitive, un cluster, c'est mettre en commun de l'intelligence collective. Digital 113 s'autofinance à hauteur de 60%, les 40% restant étant financés par des fonds publics et de la région.

Digital 113 a été un organe de consultation lorsqu'il a fallu répondre au projet soumis par les laboratoires de recherche. En effet, une enquête a été menée auprès des TPE et PME pour savoir si elles étaient intéressées par l'IA, qui a finalement révélé qu'un tiers de ces dernières avait un lien de près ou de loin avec l'IA. Ils ont ensuite ouvert une *open factory* sur l'IA qui va évangéliser dans les lycées sur ce qu'est l'IA pour donner envie à des lycéens de s'y intéresser, mais également auprès des PME, et créer des événements pour la communauté technique et du cluster. Enfin, cela permet de faire des rapprochements avec des clusters internationaux, pour dresser des ponts entre des écosystèmes technologiques en terme d'IA.

❖ **La région pourra-t-elle recueillir suffisamment de données pour ses projets ?**

Le point de vue de la région Occitanie est qu'il est possible de développer, par rapport aux GAFAs et aux BATX qui ont une puissance colossale, des activités qu'eux n'ont pas du tout (par exemple, dans le secteur de la santé, la France, grâce à son système très national avec des acteurs qui possèdent 80% des données, possède un avantage considérable sur ces leaders du marché). La quantité de données que l'on pourra recueillir dépendra de notre capacité collective à nous demander ce qui nous donne un intérêt à agir en commun plutôt qu'individuellement, à l'inverse de ce qui se fait aujourd'hui dans une optique de développement individuel des entreprises. Si la région parvient à trouver ce cadre dans lequel les intérêts des individus sont respectés d'une part, et d'autre part, le travail d'acquisition et l'actif stratégique est respecté en le sens qu'il pourra avoir des retombées collectives, alors la région Occitanie aura suffisamment de données pour mener à bien ses projets.

❖ **L'IA dans le médical**

L'IA et la santé sont aujourd'hui des exemples assez classiques (les robots moins invasifs lors des interventions médicales, les traitements individualisés du cancer après analyse du protéome, les outils numériques et robots conversationnels utilisés dans le pré diagnostic de l'autisme). Le gros

bouleversement de l'IA dans la médecine est l'autorisation donnée à un robot par la FDA aux USA en juin 2018 de faire le diagnostic de la rétinopathie diabétique (alors qu'en France seulement un certain nombre de professionnels de santé peut faire du diagnostic).

Aujourd'hui, la médecine représente beaucoup plus de patients mais dans un contexte de réduction considérable des moyens, alors que l'IA vient bouleverser toutes les règles qui s'appliquent à la médecine. Une question revient sans cesse : l'IA remplacera-t-elle, à terme, le médecin ? Il semble actuellement que les robots n'ont pas de corps, alors que la médecine est basée sur l'expérience humaine, que par définition les robots n'ont pas. Ils ne remplaceront pas les regards compatissants, les gestes rassurants, ou encore la négociation relative à l'observance d'un traitement.

De plus, le numérique ne doit pas créer d'inégalités supplémentaires, et il s'agit d'une question d'éthique fondamentale. Il faut aussi faire en sorte que les professionnels de santé soient aussi performants que les machines, alors que la formation en médecine n'évolue pas depuis quelques années, contrairement à l'IA qui progresse toujours plus rapidement. Il faut donc conjuguer plusieurs éléments : la confiance (en ce que font les algorithmes mais aussi en la gestion des data), l'acceptabilité (si les robots ne sont pas acceptés par le patient, le numérique devient inutile), et l'interopérabilité (si les gens n'ont pas la capacité de mettre l'IA en œuvre, cela devient tout autant inutile).

Enfin, l'arrivée de la block chain, moins rapide qu'ailleurs du fait des rares applications, bouleverse le milieu de la santé. Une voie alternative prônée en collaboration avec des associations de patients est de créer des block chain de consortium où l'on pourra mettre des données qui finiront par être vendues. Seulement, le fruit de la recherche ne bénéficiera pas à la personne qui a vendu les données, mais sera plutôt mis à disposition de structures communes pour faire de la recherche et de la médecine : le croisement des données est donc extrêmement important. Il y a des croisements de données gigantesques à faire entre la médecine, la mobilité, et le climat ; mais également un modèle économique à trouver, d'autant plus lorsque l'on observe la taxation des données en France.

Après-midi

Keynote : L'initiative JEDI (Joint European Disruptive Initiative)

André Loeseckrug-Pietri – Fondateur, Porte-parole JEDI

Depuis quelques mois, il y a eu une accélération phénoménale en matière d'IA (déclaration des USA annonçant qu'ils reviendraient sur la Lune à partir de 2025, copie génétique d'un bébé par un scientifique chinois, destruction d'un satellite en orbite basse par des indiens).

La stratégie Européenne en IA repose sur une contribution de la Finlande, Italie, Suède, Allemagne, Suisse, France, et du Royaume-Uni pour établir un cadre commun de perspectives. Mais d'ici quelques années, nous aurons à nouveau un marché européen fragmenté. Il y a 2, 3 ans, nous avons passé un cap singulier. En effet, le flux d'information nous arrive désormais à tout moment via les diverses applications et plateformes de communication et il dépasse notre capacité à comprendre le monde qui nous entoure. L'ennemi réel, dans tous les domaines, est maintenant la pensée linéaire, par opposition à la pensée disruptive, que l'humain perd à partir de ses 5ans.

JEDI est l'équivalent de la DARPA américaine, créée en 1957, date à laquelle les américains ont réalisé à quel point la technologie pouvait renverser les rapports de force. La DARPA a donc adopté pour devise « pas de surprise technologique », et elle a toujours eu un coup d'avance (création du réseau centralisé résistant aux attaques nommé Internet, le GPS, la furtivité, le premier challenge de véhicule autonome, ...). L'objectif de JEDI est donc de se baser sur ce modèle pour créer un outil à mi-chemin entre la recherche fondamentale et l'utilisation pratique dans le marché et les forces. Par ailleurs, l'ambition de JEDI serait de financer tout ce qui est aujourd'hui trop risqué ou sur un trop long terme pour que le secteur privé s'engage à le faire. L'enjeu est central car la croissance, la prospérité, la force de nos économies et de nos sociétés dépendra en grande partie de nos technologies. Les enjeux sont grands, car les technologies sont devenues les vecteurs de nos valeurs, d'autant plus que si on ne se fait plus confiance, c'est la base de nos démocraties qui s'écroule. Dans la même optique, le leadership technologique est important, d'autant plus que nous nous trouvons dorénavant dans un monde où il n'y a plus de place pour les numéros deux.

L'idée de JEDI est de profiter du rebattage des cartes pour inventer la nouvelle frontière, et cela ne viendra pas d'une administration. Le projet est donc de réunir la totalité de l'écosystème de la *deep tech* dans tous les pays européens pour en tirer de l'innovation. Le problème n'est pas un manque d'argent : l'Europe a investi 220 milliards d'euros dans sa recherche depuis 35 ans. Cela signifie par conséquent qu'il y a un problème de méthode, et qu'il va falloir en changer, pour aller vite dans les décisions, savoir arrêter les projets qui ne fonctionnent pas, et faire le grand pont entre recherche fondamentale et prototypes.

Enfin, le problème majeur auquel nous nous trouvons désormais confrontés est que nous ne savons plus « attribuer », c'est-à-dire savoir qui nous attaque. Et sans savoir qui est notre ennemi, c'est la base de notre souveraineté qui disparaît.

Table ronde 3 : IA et santé, création du Health Data Hub

Sacha Alanoca - AI Policu Researcher and Program Manager, The Future Society

David Gruson - Membre du comité de direction de la chaire Santé de Sciences Po, fondateur de l'initiative Ethik IA

Christophe Richard - Directeur médical SANTEOS, ATOS

Raphael Canyasse - CTO ANAMNESE

❖ **Qu'est-ce que le Health Data Hub (HDH) ?**

Le HDH est une initiative créée suite au rapport Villani, qui conseillait de faire de la santé un des quatre piliers forts de la stratégie de la France en IA. Le Health Data Hub se décline sous forme d'une plateforme gérée par l'Etat français qui permet d'accueillir et partager les données des citoyens avec des acteurs privés ou publics. Il doit permettre une exploitation massive et éthique de ces données pour des chercheurs, des startups et des grands groupes.

❖ **Espoirs, craintes et risques relatifs au Health Data Hub**

Comment faire lorsque l'on a besoin d'un jeu de données pour y accéder, dans la mesure où faire de l'argent sur des données de santé est généralement mal perçu et que très peu de structures ne s'attaquent par conséquent à cette tâche de généralisation de l'information ? Le Health Data Hub apparaît donc comme un guichet unique vers lequel se retourner en cas de besoin d'un jeu de données. Cela va aussi être un système d'appel à projets pour structurer ce jeu de données.

Le risque éthique principal est de ne pas s'ouvrir au pilotage par les données, ou au numérique, dans un contexte où notre système continue à porter trop de zones d'insuffisance liées au non-partage par les données. Avoir une plateforme nationale de partage de ces données est alors un élément de garantie éthique pour permettre un déploiement rapide de l'innovation en santé. Les pouvoirs publics tentent de le rendre opérationnel le plus rapidement possible, avant que cette innovation ne nous soit imposée par d'autres. En effet, si l'on se ferme trop en Europe, on prend le risque de laisser libre cours à l'utilisation de systèmes étrangers par des patients français et également un risque d'effet retour sur le régime de solidarité de la Sécurité Sociale car tous ne pourront pas accéder aux innovations si elles se développent à l'étranger et pas en France. Sans le RGPD et sa transposition dans le droit français, cette initiative ne se serait peut-être pas développée sous le concept de régulation positive (s'ouvrir en essayant de réguler les risques).

Par ailleurs, l'opportunité du HDH est colossale, grâce à des aspects clés :

- La confiance : ouvrir les données de santé pour les partager et les valoriser en termes de santé, tout en apportant une garantie des règles du jeu.
- Organisation voire régulation de l'écosystème : en amenant une gouvernance des données de santé, de leur utilisation et de leur usage.
- La mécanique doit aussi rendre les données accessibles, utilisables par les différents acteurs.
- La notion de modèle économique doit être abordée : le HDH doit permettre de faire émerger des domaines qui ne soient pas forcément basés sur la vente des données de santé, et peut-être sur leur sécurisation et leur mise à disposition.

En Europe, on essaye de se démarquer dans le champ de l'éthique et de la confiance, qui permettent de gérer des données sensibles.

Ce qui est appréciable dans le HDH, au-delà de l'outil, c'est le fait de reconnaître que la donnée de santé est majeure et que l'on ne peut rester dans des citadelles. La mission au démarrage est donc un

vrai partenariat public-privé (avec un risque et une grande tendance de mêler la gouvernance centrale dans cet outil).

Etant déjà loin derrière les acteurs majeurs du domaine (Chinois et américains), il ne faut pas abandonner mais il est nécessaire de la repérer sur des créneaux de compétitivité (la médecine d'excellence en France). Pour ces opérateurs, la difficulté est effectivement l'accès aux données sur leur champ spécifique.

Il y a un intérêt commun à mutualiser les données au niveau local, régional et national. La France a déjà les meilleures bases de données de santé au monde grâce à la CNAM (Caisse Nationale d'Assurance Maladie), qui a de magnifiques bases de données médico-économiques de remboursement très profondes, centralisées et organisées qui offrent des conditions techniques très favorables. Mais le problème concerne les données cliniques brutes (scan, IRM sur lesquels on va entraîner les algorithmes de reconnaissance d'images), car cette donnée se trouve chez les professionnels libéraux ou dans les établissements de santé. Le rôle du Hub, technologiquement, c'est de rendre plus facile le contact entre la donnée du SNIIRAM (Système national d'information inter-régimes de l'assurance maladie) et la donnée clinique brute.

Le HDH ne doit pas être un espace où l'on va agréger des données dont on ne va pas savoir quoi faire, mais plutôt un écosystème pour fluidifier les interactions entre les différents acteurs qui ont des projets, afin qu'ils puissent se trouver et réaliser leur projets en respectant les règles éthiques, la finalité du produit. Il faut mettre en place une réelle gouvernance.

Pour ce faire, face à la problématique de souveraineté des données, le bon échelon pour favoriser un échange des données est l'échelon européen. La diversité évitera également certains biais dans les traitements. Toutefois, il ne faut pas instaurer une compétition entre les différents acteurs mais plutôt stimuler l'écosystème pour que les projets émergent (sans avoir uniquement des projets publics).

Le fonctionnement du HDH repose sur un tiers de confiance, l'Etat. On présuppose donc que les citoyens ont assez confiance en l'Etat pour lui partager des données aussi sensibles que celles concernant la santé. Or aujourd'hui, on est dans un contexte global assez tendu, notamment avec la crise de Gilets jaunes : ne surestimons-nous pas le degré global de confiance des citoyens envers l'Etat ? Des autres gouvernances de données alternatives telles que les data trust placent ces données dans un tiers de confiance non-étatique (existe déjà pour la recherche contre le cancer). Cependant, ces systèmes de gouvernance peuvent-ils cohabiter avec le HDH ?

Il y a la nécessité de plateformes technologiques sécurisées, le hub y concourt, mais il faut créer un système de guidelines éthique permettant de former et d'accompagner, pour pouvoir jouir si bien de la protection des données personnelles et de la vie privée, que de la qualité du service médical rendu. Nous sommes dans un moment où nous avons besoin de tester des manières de faire de la politique. Il faudrait maintenant reprendre les initiatives et sans cesse les retoucher, pour ne pas tout normer., et avoir une vision plus prospective : l'IA va révolutionner la santé, mais il faudrait que ce soit le patient qui en bénéficie. Assurons-nous, dans ce cas, que le HDH sera un accélérateur sur ce sujet (et pas seulement en termes économiques).

Table ronde 4 : IA et mobilité transports – Hub France IA

Antoine Couret - CEO Geo4Cast, Président du Hub FranceIA

*David de Almeida - Directeur Département Modélisation & Expérience Voyageurs,
Direction Innovation & Recherche, SNCF*

Luc de Andreade - Président du Think Tank NXU

Olivier Pages - CEO, FFLY4U

La mobilité - transport est le deuxième grand sujet évoqué dans le rapport Villani, et représente quelques centaines de milliards d'euros en terme d'impact économique sur l'Europe.

On a l'impression que de nombreuses choses existent, mais n'a-t-on pas un déficit de connaissance sur ce qui se fait en France en IA et qui est déjà en partie opérationnel ou réalisé ?

Il existe beaucoup de technologies opérationnelles et l'IA dans le transport a une dynamique vertueuse dans le sens où elle permet de l'optimiser (grâce à l'interconnexion et les objets connectés, on perd moins de temps, on supprime les intermédiaires, diminue le nombre d'accidents, et réduit les émissions de gaz à effet de serre, aussi grâce aux nouvelles technologies). On a donc une mobilité intelligente dans les villes, avec une promotion de l'autonomie. Il y a eu, dans le champ de l'IA en transports, une accélération des progrès très importante, qui dépasse toutes les attentes.

La création de valeur se fait majoritairement à partir de données brutes (tels que le suivi température, la géolocalisation et les capteurs de mouvement, qui créent beaucoup de données et saturent les réseaux). Avec l'IA embarquée et les process de *machine learning*, on est parvenu à traiter la data à l'intérieur du *device* pour envoyer un résultat dans le cloud, mais on ne peut pas raisonner en énergie infinie. L'IA et le *machine learning* prendra de plus en plus d'ampleur en local, et ce sera d'autant plus vrai concernant le véhicule autonome, les systèmes devenant de plus en plus intelligents et moins en moins consommateurs d'énergie. La France est en avance sur ces logiques de consommation d'énergie finies et contraintes. De plus, les acteurs qui travaillent sur les technologies implantées dans des *devices* autonomes en énergie, et les professionnels capables d'arbitrer entre qualité des algorithmes et conservation de l'autonomie d'énergie sont rares. On a du mal à trouver des compétences dans ce domaine extrêmement nouveau. Pour ne pas perdre le savoir-faire que l'on a dans le domaine, il serait par conséquent intéressant d'intégrer la dimension énergétique aux projets de grande ampleur, qui a un véritable impact en matière de choix technologiques.

Par ailleurs, les opportunités de l'IA à la SNCF se déclinent à trois niveaux :

- Un niveau en lien avec les **enjeux industriels**. Certains projets existent déjà, notamment en lien avec la sécurisation des infrastructures. Un des enjeux majeurs dans ce domaine concerne d'ailleurs le train autonome. En ce qui concerne l'optimisation des capacités prédictives, beaucoup de choses sont d'ores et déjà à l'œuvre, notamment en ce qui concerne l'optimisation des capacités de prédictions de ressources, des techniques qui ont un pied dans l'IA et un pied en dehors (techniques d'optimisation, de recherche opérationnelle), et beaucoup de réalisations en ce qui concerne la prédiction de données (prédiction de flux, de retard, d'affluence, des défaillances systèmes, en s'approchant du domaine de la maintenance prédictive). Enfin, le dernier chapitre concerne l'aide à la décision pour la gestion des opérations en temps réel, mettant en avant les approches hybridantes et apprenantes (gestion des circulations, adaptation des plans de transport, supervision assistée de périmètre de production).

- Un niveau concernant **l'interaction humain-machine**, l'assistance aux agents et aux voyageurs. Le premier volet concerne toute l'information en temps réel personnalisée. Mais on exploite aussi l'IA pour apporter de l'assistance aux agents, notamment en ce qui concerne l'analyse documentaire pour aider les agents à mieux questionner les nombreuses couches de référentiel à la SNCF et avoir un diagnostic plus rapide et plus précis en exploitant les référentiels. On a donc du traitement automatique du langage à base de corpus descriptif, mais également des logiques d'apprentissage, pour tirer profit des retours d'expérience. Il y a également de la valeur à comprendre et anticiper les états cognitifs des agents (stress, charge mentale).
- Un niveau en lien avec la **cybersécurité**. Le système ferroviaire est caractérisé par le concept de *security by design*, avec des preuves de sécurité assez exigeantes. Dans un contexte de digitalisation croissante de l'exploitation ferroviaire, il y a des sujets à traiter en matière de *monitoring* des flux et au niveau de la sécurisation des couches télécoms (utilisation valorisée des algorithmes d'IA dans ce domaine).

Aujourd'hui, les réglementations concernant le transport sont relativement anciennes : il faudrait qu'elles se reglobalisent plutôt que d'avancer au coup par coup. Avec les algorithmes, on délègue des tâches à la machine, à des entités collectives ou à des concepteurs. L'enjeu est qu'on peut également donner à l'utilisateur l'opportunité de paramétrer lui-même ses choix éthiques (cas du véhicule autonome). On a donc une fiabilité de l'IA par rapport à l'intelligence humaine qui se met en place. En effet, lorsqu'une machine fait un choix éthique, il s'agit de l'application de la rationalisation, tandis que les choix humains reposent sur l'impulsivité : ces choix vont donc influencer l'éthique et par conséquent, potentiellement, la réglementation. La question cruciale est alors de savoir si l'intégration de l'éthique dans les algorithmes va diluer les responsabilités de l'Homme. La réponse conditionnera une révision de la réglementation en vigueur, ce qui aura également, par extension, un impact sur nos développements économiques. Le problème principal n'est donc pas la technologie mais la réglementation en l'état.

Plusieurs freins gênent encore les progrès que l'on pourrait faire en matière d'intégration des technologies d'IA :

- Les démarches actuelles de démonstration de preuves de sécurité et de démonstration. Ce n'est pas spécifique à l'IA mais c'est une preuve de contribution.
- La capacité, en cours de conception d'un système, à les expérimenter pour générer de la donnée et qualifier les approches technologiques.
- La capacité à passer à l'échelle, d'autant plus dans un contexte industriel.
- Le rapport à l'erreur, pour être en capacité de voir ce qui fonctionne ou non, ce qu'il faudrait améliorer.

Mais deux exigences sont à raccrocher à cela :

- Une exigence de transparence sur les algorithmes, et la nécessité de savoir ce qu'il se passe
- Une exigence éthique et de valeur de confiance.

❖ **Que va-t-il en être de la destruction créatrice ?**

Nous avons retrouvé ce phénomène de destruction créatrice à chaque nouvelle révolution industrielle, l'idée consistant à dire que les nouveaux marchés se mettent à côté des anciens et des concurrents, jusqu'à les étouffer et les anéantir, en créant plus d'emplois qu'ils n'en ont détruit. Le problème réside donc uniquement dans le laps de temps entre la destruction et la création d'emplois, vers la synthèse créatrice. Aujourd'hui, nous nous trouvons face à une accélération technologique forte, d'où

les nombreux débats. Selon les décisions qu'il prendra, le législateur aura donc le pouvoir soit d'accélérer soit de ralentir cette création d'emplois.

Table ronde 5 : Chatbots, assistants conversationnels, reconnaissance vocale, IoT et domotique

*Jean Rohmer - Vice-président Institut Fredrik . Bull. Head of Research and partnership
Pôle Universitaire Léonard de Vinci*

Luc Truntzel – CEO IBENTA France

Yann Lechelle – COO, SNIPS

*Enrico Valtolina – Direction Innovation & Systèmes, Software architect, Groupe
LEGRAND*

Jean-Luc Dormoy – Vesta-System

L'objectif concernant l'IA dans ce domaine consiste à présent à se démarquer de grandes ensembles de données (issues d'internet ou d'entreprises) pour ne plus avoir de grands systèmes d'IA mais plutôt des systèmes par millions, concernant chacun d'entre nous. Quatre grands groupes ont accepté de présenter leur utilisation de l'IA dans le cadre de leurs activités.

VESTA SYSTEM

Les systèmes intelligents sont des systèmes anticipatifs, prédictifs, qui apprennent comment fonctionnent les bâtiments (cas des tours énergétiques) mais aussi les utilisateurs, pourvu qu'ils consentent à fournir leurs données au système. Du point de vue de la vie privée, leur encadrement est très strict, le tout étant déterminé par des contrats, les données n'étant même pas transmises à l'utilisateur lui-même.

Les tours énergétiques posent de nouveaux enjeux, notamment avec l'utilisation de l'IA pour leur fonctionnement :

- Des factures négatives : l'énergie devient un revenu pour les habitants, et le niveau d'efficacité énergétique est atteint grâce à la technologie.
- Les niveaux d'échange monétaire engendrés pourraient changer le mode de paiement de l'énergie, car c'est en réalité un service que l'on achète, alors que l'on pourrait aussi vendre l'énergie à coût fixe.

IBENTA

Depuis 2005, l'entreprise s'attelle à la création de chatbots pour les entreprises (anciens « agents virtuels »), des robots présents sur les sites web qui répondent immédiatement aux questions posées en langage naturel, particulièrement présents dans le domaine de la banque ou des assurances. Une nouvelle expérimentation consiste à exporter ces bots dans la vraie vie, avec le même usage que l'on en aurait dans la vie quotidienne. Plusieurs dimensions sont mesurées : une dimension technologique (le robot n'a pas de tablette sur le torse, pour avoir une interaction similaire à celles que nous avons entre hommes et femmes, mêlant langage corporel et vocal, ce qui représente un grand défi technologique) mais aussi la dimension de l'acceptabilité ou non des robots auprès des visiteurs de l'agence.

Par ailleurs, pour pouvoir répondre aux questions posées, ces assistants vocaux compilent plusieurs « briques » :

- La reconnaissance vocale

- Le traitement automatique du langage (ou *Natural Language Processing*), qui consiste à essayer de comprendre le texte pour proposer une réponse correspondante. Deux sous-couches composent cette brique : le *Natural Language Understanding* (à la réception de la question, le bot recherche dans une base de réponses pré-écrites celle sera la plus adéquate) et le *Natural Language Generation* (capacité de créer des réponses à partir de données brutes et non structurées, qu'aucun bot ne possède à l'heure actuelle).
- La synthèse vocale, à savoir la capacité à vocaliser la réponse.

Il faut alors distinguer deux approches existantes pour concevoir ce NLU :

- L'approche symbolique, qui consiste à donner des règles à la machine afin qu'elle apprenne ce que l'on attend d'elle. Il s'agit d'une méthode robuste, mais qui présente certaines limites dans la mesure où on ne peut pas tout conceptualiser avec des règles.
- L'approche *machine learning*, qui elle n'est pas basée sur des règles mais une quantité bien plus importante de données. La machine apprend alors sa propre logique avec son système de réseau neuronal artificiel, logique intelligible pour l'homme mais qui permettra de conceptualiser des choses qui restaient inaccessibles pour l'IA traditionnelle.

Chez IBENTA, l'approche est historiquement plus symbolique. Il s'agit d'une approche déterministe qui dérive aujourd'hui vers une dimension plus hybride, grâce au recrutement de data scientists, reflétant ainsi le cheminement que nous humains avons également suivi (apprentissage de la langue maternelle sans règle au plus jeune âge, puis scolarité qui a apporté des règles pour structurer cette connaissance et apprendre d'autres notions telles que l'écriture, la lecture, ou d'autres langues).

Les enjeux concernant les questions réglementaires et la vie privée sont primordiaux chez IBENTA, qui ne signe d'ailleurs aucun contrat tant que les critères imposés par le RGPD ne sont pas remplis. Les peurs relatives à l'IA ne concernent pas les technologies et leurs innovations, mais plutôt leur usage. Le RGPD a pour cela été très bénéfique, car il a permis de réguler ces usages et de progresser vers l'acceptabilité. Beaucoup de chartes éthiques ont été développées, mais l'enjeu est de parvenir maintenant à un label. Les audits et les réglementations sont donc des nouveaux points de réflexion considérés, qui doivent être pensés sans pour autant qu'ils ne viennent bloquer l'innovation.

LEGRAND

La relation du groupe LEGRAND avec l'IA a commencé il y a plus de 15 ans, avec des moyens initialement très limités mais animé par la volonté de comprendre quand et dans quelle mesure la technologie pourrait apporter une valeur ajoutée à leur marché et leurs clients. Aujourd'hui, deux approches différentes sont principalement utilisées :

- *Artificial intelligence as services*, catégorie regroupant l'ensemble des situations dans lesquelles les produits LEGRAND peuvent tirer un bénéfice des algorithmes IA développés par quiconque, y compris leurs partenaires. Cette décision a été poussée par le marché, leurs clients leur demandant de proposer une nouvelle expérience-utilisateur, basée sur l'interaction vocale, pour manager l'entreprise.
- *Artificial intelligence by design*, correspondant au développement d'outils IA intégrés à leur offre de services.

Le groupe LEGRAND est très concerné par les enjeux de vie privée et les questions réglementaires. Des sommes d'argent considérables ont été investies pour protéger leurs données, ils ont défini des *policy procedures* à suivre pour les entreprises et ont repoussé les approches standards de cybersécurité, et des tests de pénétration sont poursuivis de manière régulière pour s'assurer de la robustesse de la protection en place.

SNIPS

Le groupe SNIPS est concerné par la souveraineté des données personnelles appliquée au sujet d'interface vocale, notamment vis-à-vis des géants qui y opposent une barrière conséquente. Un nouveau paradigme est désormais considéré, permettant de se demander si le modèle « tout cloud » est un modèle souhaitable au quotidien. Cette vague de questions ne s'est pas encore posée en France et différentes logiques s'opposent selon les pays en ce qui concerne le système (en Chine, le système est parfaitement connecté mais aussi à 100% dans la traçabilité des individus ; tandis qu'aux USA le système est beaucoup plus libéral et exécute les tâches qu'on lui donne jusqu'à ce qu'on l'arrête ; et en Europe, le système est plutôt basé sur le discernement, plus complexe, avec un objectif d'être plus en phase avec l'individu que la machine centrale).

Table ronde 6 : Traitement de la donnée, qualité et création de valeur

Jean-Paul Pinte – Docteur en information scientifique et technique, maître de conférence à l'Université catholique de Lille (FLSH), expert en veille et intelligence compétitive

Alice Froidevaux – Quantcube Technology

Frédéric Cuppens – Professeur à Telecom Bretagne, responsable de l'équipe SERES, Institut Mines Telecom.

Grégoire Siguel – CTO et cofondateur de GEOTREND

Stéphane Cordova – Vice-Président, technologies embarquées KALRAY

❖ **La collecte de données**

Pour comprendre des processus, il faut pouvoir collecter, analyser, synthétiser des informations. Il s'agit d'opérations pratiques, mais très coûteuses en termes de temps. Il y a 20 ans, la complexité était de trouver la bonne source d'information. Aujourd'hui, c'est de trier parmi toutes celles que l'on a : le temps devient donc la ressource pour le traitement. Si la collecte peut être automatisée et l'analyse en partie, pour la synthèse, l'automatisation reste encore trop compliquée à réaliser. Toutefois, l'intelligence reste une solution pour faire des économies de temps, surtout dans ce contexte de menace de l'infobésité qui pèse sur nous.

La collecte de données permet de créer de nouveaux services à valeur ajoutée intéressants pour les individus, mais qui se révèlent très intrusifs pour la vie privée. Des solutions de protection de données et d'anonymisation sont génératrices de valeur pour la donnée.

On a parfois un problème de partage de la donnée, dans la mesure où, ce faisant, cela reviendrait à partager le « savoir-faire » de ceux qui les cèdent, ce qui pose problème. Ce dont on a besoin, c'est de faire des croisements de données, rendus impossibles pourtant par une anonymisation de la donnée (dans le sens « génération d'open data »). Mais dès lors que l'on connaît la finalité de la donnée il est possible de l'anonymiser (rendre possible le croisement en se préservant contre le risque de réidentification et d'inférence). Car dès que l'on connaît cette finalité – la finalité étant par ailleurs une exigence de la CNIL et du RGPD - on peut mettre en place des techniques d'anonymisation adaptées qui vont préserver la sécurité d'un côté et l'utilité des données. Le chiffrement homomorphe est une solution parmi d'autres et correspond à ce besoin en permettant de faire le traitement sur une donnée chiffrée sans avoir besoin de la déchiffrer, par exemple. Même si on a des problèmes de performance, en termes de besoin, des solutions existent.

❖ **L'IA de confiance**

L'IA de confiance est aujourd'hui la clé des systèmes embarqués, autonomes (en termes de sûreté de fonctionnement). Tout ce qui concerne la sécurité et la sûreté va devenir primordial (rôle majeur dans la création de valeur). Ce n'est pas une valeur financière mais elle va apporter une plus-value à la marque, donc plutôt une valeur marketing.

❖ **Quels livrables peut-on fournir aux clients ?**

Il est possible de proposer actuellement des graphiques de relations entre acteurs, avec des couleurs différentes en fonction des liens détectables et connus, pour visualiser rapidement la nature de la concurrence ou des relations partenariales. L'IA va aussi permettre aux entreprises de fournir des bases de confiance et des indices de pertinence de l'information à leurs clients, pour se concentrer sur leurs intérêts sans pour autant faire abstraction de certaines informations tierces. La cartographie s'est révélée utile pour les clients.

❖ **L'avenir de l'IA pour les systèmes d'anonymisation**

L'avenir de l'IA passe par la réponse au besoin de mutualisation des données, de pouvoir les croiser et d'agrèger ces données pour obtenir des résultats de plus en plus riches. Il faut donc que les données soient sécurisées. Dans un contexte industriel compétitif, il est peu probable qu'il y ait un accord entre industriels sans que les transactions ne se fassent de manière sécurisée.

❖ **Challenges environnementaux et marketing**

Le niveau de confiance que les clients placent en la sécurité va beaucoup jouer sur l'image de marque que l'IA véhicule. En ce qui concerne l'impact environnemental, l'enjeu est de parvenir à proposer des solutions à faible consommation d'énergie. Les économies d'énergies sont réellement au cœur des préoccupations des concepteurs aujourd'hui. Dans les systèmes embarqués, il est vital d'en limiter la consommation. L'IA consomme de plus en plus (énergie, électricité) et il faudra s'en soucier.

Keynote : **Intelligence artificielle symbolique, calcul formel, apprentissage statistique : les synergies**

*Jean Rohmer - Vice-président Institut Fredrik . Bull. Head of Research and partnership
Pôle Universitaire Léonard de Vinci*

Pour des raisons de simplification, le calcul formel est ici associé à l'IA symbolique.

❖ **Des ressemblances entre IA symbolique et IA connexionniste**

Un premier point commun entre ces deux disciplines est que dans chacune d'entre elles, la France se distingue particulièrement. L'IA symbolique fut inventée il y a 400 ans par René Descartes, dans la lettre à Mersenne de 1629, où il énonce totalement le programme de l'intelligence symbolique.

Par ailleurs, ce sont toutes deux des disciplines qui se méprisent cordialement, et portent des projets assez fous dans la mesure où l'IA symbolique prétend mettre au point des langages qui vont pouvoir faire le portrait et décrire parfaitement le monde. L'IA symbolique a une approche scientifique. A la base, c'est une notion de langage, qui n'existe pas en IA connexionniste (qui est data scientist: elle prétend qu'on va tout découvrir et que le langage n'est pas nécessaire pour ce faire).

❖ **Qui renvoient pourtant à des différences fondamentales**

Il existe trois types de données : les données primaires (ne dépendent pas de l'Homme et émanent de la nature), secondaires (créées par l'Homme, telles que l'industrie) et tertiaires (tout ce qui est humain). Il faudrait cependant une catégorisation plus forte de la nature des données que l'on traite. Les calculs faits par chacune des deux IA sont également très différents même s'ils se ressemblent de prime abord : l'IA connexionniste travaille sur des symboles fixes. L'IA symbolique déplace des valeurs sans les modifier, tandis que l'IA connexionniste modifie des valeurs sans les déplacer, et les conséquences de ces divergences sont impactantes.

❖ **La synergie**

Une synergie s'opère depuis 2013 du fait de la prédominance, à partir de cette année, de la traduction automatique à base de réseau de neurones sur les performances de la traduction automatique faite à base de systèmes symboliques.

Une hybridation est en effet en cours, d'abord car l'IA symbolique est plus ou moins dépassée, et deuxièmement car la connexionniste se sent obligée de lancer des produits de matrice. Mais il est possible que l'IA symbolique ne redémarre jamais car plus personne ne sait enseigner, et que la connexionniste doive sortir de ses coups d'éclat.

Clôture de la première journée

Olivier Kempf – Directeur La Vigie, Chercheur associé à la FRS, Président d'EchoRadar, Membre de la Chaire Cybersécurité et Cyberdéfense Saint-Cyr, Sogeti, Thales

Nous avons pu constater grâce à l'ensemble des thèmes précédemment évoqués qu'il existait une grande diversité des champs couverts par l'IA. Seulement, trois thèmes majeurs semblent se distinguer :

- Les **questions relatives à l'énergie**, et notamment de la consommation et de l'économie de l'énergie. Dans la mesure où l'IA connexionniste consomme désormais énormément de données, et requiert également beaucoup d'énergie, un champ de réflexion intéressant semble reposer sur ces enjeux
- La **confidentialité** soulève par ailleurs bon nombre de préoccupations. Puisque la donnée a de la valeur, sa protection est essentielle et peu compatible avec la connectivité, qui implique de partager. Comment partager si on veut garder une partie de la donnée pour soi-même ?
- Le **travail en local** : l'IA est énormément fondée sur le réseau, le nuage, le partage. Les conséquences de l'économie d'énergie et de la confidentialité font que l'on va se méfier de ce réseau. On se retrouve donc avec de l'IA *on the edge*.

Si l'IA est devenue l'expression à la mode, il y a encore une dizaine d'années, c'était le mot cyber qui était le plus fréquemment employé (à l'époque relatif au numérique, alors que maintenant il regroupe plutôt le domaine de la sécurité et de la défense). Dès lors que l'on associe cyber et IA, trois thèmes majeurs apparaissent :

- **La sécurité de l'IA** : l'IA est-elle robuste à des attaques cyber ? Mais est-elle fiable (robustesse interne et externe) ? On ne parle plus ici que de cybersécurité de l'IA mais aussi de sa sûreté, de sa sécurité, de sa fiabilité.
- **L'apport de l'IA aux perspectives de sécurité**, tout d'abord informatiques : comment l'IA va-t-elle contribuer à la cybersécurité ? Permettra-t-elle d'améliorer les capacités de défense (renseignement, robotique, entraînement) ? Ou encore de fournir de nouveaux mécanismes de sûreté industrielle (chimie, biologie, industrie lourde, transports...).

- **Le rôle de l'IA dans les questions de souveraineté numérique** : quels dispositifs de recherche, publics ou privés ? Quelles administrations et collectivités territoriales vont participer à l'établissement de cette souveraineté numérique ? Faut-il une régulation internationale ?