



TRIP DE PRINTEMPS 2024

28 et 29 mai

Table ronde 5
L'IA dans (presque) tous ses états

L'IA DANS (PRESQUE) TOUS SES ETATS

Animateur :

■ Patrick CHAIZE
Président de l'Avicca

Intervenants :

- **Manu REYNAUD**
Adjoint au Maire de Montpellier, délégué à la ville apaisée, respirable et numérique Montpellier Méditerranée Métropole
- **Philippe AJUELOS**
AMDAC, ministère de l'éducation nationale
- **Jean CATTAN**
Secrétaire général du Conseil National du Numérique (CNN)
- **Alix DURAND**
Chargée de mission Affaires politiques et transverses · ANSSI - Agence nationale de la sécurité des systèmes d'information
- **Laura LÉTOURNEAU**
Chargée de mission "transformations numérique et écologique" · Services du Premier ministre

Patrick CHAIZE

L'intelligence artificielle, je la vois vraiment comme étant un appui, un outil. Je ne la vois pas comme une menace. Elle a une certaine puissance et reste à contrôler. En quelques heures d'initiation, de belles choses sont possibles.

Alors il y a six mois, lors du trip d'automne, nous avons réuni les quatre lauréats de l'appel à projet Territoires intelligents et durables dans son volet démonstrateur d'IA frugal au service de la transition écologique dans les territoires. Pour mémoire, cet appel à projet s'inscrivait dans la stratégie d'accélération sur l'IA de France 2030 suite au rapport de Cédric VILLANI. Depuis, les annonces, les rapports sur l'IA en France, mais aussi dans le monde, se multiplient. Nous avons pu le constater à Vivatech la semaine dernière.

Nous avons donc souhaité rassembler des acteurs publics parmi ceux qui ne font pas simplement que réfléchir, mais parmi ceux qui agissent. Avant d'entrer dans la présentation de vos projets, nous allons faire un rapide tour de table des quatre organisations publiques où vous travaillez, et demander à chacun(e), quelle est sa définition de l'IA dans leur contexte éducatif, territorial, d'accompagnement, du changement et de cybersécurité. Alors tout d'abord, Philippe AJUELOS, vous êtes administrateur ministériel des données, des algorithmes et des codes sources au ministère de l'éducation nationale. Quel est le rôle d'un AMDAC ? Quelle est votre définition de l'IA dans cette fonction ?

Philippe AJUELOS

Donc, un AMDAC, c'est une personne qui identifie la politique de la donnée et qui permet non seulement de la matérialiser, mais de la mettre en œuvre avec l'ensemble de l'écosystème du ministère, notamment les collectivités. Dans ce cadre-là, et pour faire le lien avec l'objet de notre table ronde, il y a eu un travail de fond en matière d'intelligence artificielle qui ne date pas d'hier, qui ne date pas de la naissance ou de l'ouverture des IA génératifs au grand public. Nous on y travaille depuis 2016 et nous avons mis en place des outils pour l'accompagnement

pédagogique. Dans cette démarche, l'AMDAC il est là pour répondre à l'ensemble des questions qui peuvent se poser, des questions sur le partage de la donnée, sur la valorisation de cette donnée et sur le travail que nous pouvons faire avec les collectivités.

Ma définition de l'IA se présente en deux temps. C'est évidemment tout système d'information machine qui va simuler l'intelligence humaine. Et puis je voudrais simplement faire une incise et rappeler qu'il y a un texte qui est maintenant quasi d'application, c'est le règlement intérieur du parlement européen sur l'intelligence artificielle qui parle de système. Un système d'IA qui en plus de cette définition-là parle d'adaptation de cet outil pendant sa mise en œuvre sur des domaines d'apprentissage. C'est utiliser les outils basés sur l'IA et notamment l'IA générative et de le faire de façon éthique et coordonnée, partagée et en toute sécurité. La définition de l'éthique est un vaste sujet.

Patrick CHAIZE

Manu REYNAUD, vous êtes adjoint au maire de Montpellier, délégué à la ville et à la métropole numérique et intelligente de la métropole. Ce territoire est pionnier pour les usages numériques. Pouvez-vous rapidement nous présenter votre collectivité au travers d'une initiative dans le domaine des technologies de l'information et de la communication et nous indiquer également quelle est votre définition de l'IA avec cette vision locale ?

Manu REYNAUD

Montpellier est une petite ville de 300.000 habitants du sud de la France dans une métropole de 500 000 habitants. Nous avons fait une convention citoyenne sur la question de l'IA pour savoir comment appréhendons-nous cela ? Car la question qui se pose est l'acculturation. Comme le disait Cédric VILLANI : il n'y a pas de définition de l'intelligence artificielle, ce qui est certain c'est que l'intelligence artificielle ce n'est pas de l'intelligence. Ma définition est que ce sont des dispositifs, des concepts informatiques qui d'une certaine façon singent l'esprit humain. D'ailleurs le

biomimétisme est important. Je rajouterai qu'au vu de cette convention citoyenne, il nécessite qu'elle soit conçue, contrôlée et supervisée par des humains. Nous avons parlé d'informatique, du numérique, aujourd'hui nous parlons d'IA. Mais dans l'acception commune, ce sont des mots génériques qui se remplacent en fonction des époques. D'ailleurs aujourd'hui, vous l'aurez remarqué, il n'y a pas un dispositif numérique sur lequel nous n'avons pas collé une étiquette IA, c'est beaucoup plus vendeur. Après allez savoir ce qu'il y a dedans ?

Patrick CHAIZE

Nous allons passer la parole à Jean CATTAN, secrétaire général du Conseil national du numérique. Depuis 2011, cette instance consultative indépendante est chargée de conduire une réflexion ouverte sur la relation des citoyens au numérique auprès de la secrétaire d'état en charge du sujet. Pouvez-vous nous expliquer ce qu'est le CNUM, mais aussi quelle est votre définition de l'IA.

Jean CATTAN

Nous vivons un moment charnière. Comme vous l'avez exposé, cela fait douze ans que le Conseil accompagne la réflexion collective sur notre relation au numérique. Il l'a d'abord fait d'un point de vue économique, puis d'un point de vue réglementaire et ces derniers temps beaucoup plus d'un point de vue sociétal.

C'est justement dans cette prise en considération du fait numérique en tant que fait social total que nous avons abordé beaucoup de structures, beaucoup de personnes présentes sur l'ensemble du territoire dans la perspective de contribuer, de visibiliser, de rendre compte aussi de toutes les démarches de dialogue et de mise en concertation qui existaient déjà, qui étaient déjà portées. De toutes ces démarches d'éducation populaire au numérique, de familiarisation et d'expression, la ville de Montpellier en est un des exemples les plus probants aujourd'hui. Car si l'intelligence artificielle interroge, c'est bien l'intelligence collective qui apportera des réponses.

Patrick CHAIZE

Enfin, Alix DURAND, chef d'état-major adjointe chargée de mission de la sous-direction stratégie à l'Agence nationale de sécurité des systèmes d'information (ANSSI) et l'Autorité nationale en matière de cybersécurité et de cyberdéfense. Pouvez-vous présenter l'organisation de cette agence, nous donner quelques éléments très factuels et nous dire votre définition.

Alix DURAND

L'ANSSI, l'Agence Nationale de Sécurité des Systèmes d'Information, est l'autorité nationale en matière de cybersécurité et de cyberdéfense. L'ANSSI est organisée autour d'une direction générale, et de quatre sous-directions, dont fait partie la sous-direction stratégie à laquelle j'appartiens. L'ANSSI compte aujourd'hui près de 650 agents.

Nous sommes un service du Premier ministre rattaché au secrétariat général de la défense et de la sécurité nationale. L'ANSSI a une mission défensive, son rôle est de protéger la nation face aux cyberattaques. L'agence s'intéresse à l'intelligence artificielle de longue date, notamment initialement au travers de ses travaux de recherche orientés principalement sur des applications d'automatisation de la détection d'intrusion. Le terme IA recouvre des réalités et technologies très diverses. L'intelligence artificielle, en tant que méthodes statistiques d'apprentissage inscrutables, c'est cela qui nous pose des vrais enjeux nouveaux en matière de cybersécurité.

Statistique, parce que ce sont des algorithmes qui donnent des résultats qui ne sont pas certains, mais le résultat le plus probable compte tenu des données sur lesquelles l'algorithme a été entraîné. Cela pose problème en matière cyber pour l'évaluation des systèmes d'IA visant à s'assurer que le système fait ce qu'il doit faire, de manière certaine.

Apprentissage, puisque ce sont des algorithmes qui se paramètrent au travers d'une phase d'apprentissage et des données qui lui ont été données pour pouvoir se paramétrer. Cela pose un enjeu cyber, les données pouvant être manipulées (empoisonnement, etc.) afin de contraindre le fonctionnement du système d'IA d'y introduire des vulnérabilités.

Inscrutable, c'est le fameux fonctionnement en black box qui nous permet d'avoir un résultat sans autant pouvoir expliquer comment est-ce que nous sommes arrivés à ce résultat. C'est donc l'ensemble de ces caractéristiques des méthodes statistiques d'apprentissage inscrutable qui nous posent des défis nouveaux en matière de cybersécurité.

Patrick CHAIZE

Autant d'approches différentes mais complémentaires. Pour ce deuxième tour de table, je vous propose de nous présenter des initiatives plus détaillées. Philippe AJUELOS, dans son plan d'action 2024-2027 pour une politique ambitieuse de la donnée au service de l'éducation nationale, de la jeunesse et des sports, l'intelligence artificielle est l'un des cinq thèmes clés avec l'IA. Le ministère ambitionne de renforcer son utilisation en soutenant le développement de projets innovants et éthiques. Qu'y a-t-il derrière le mot éthique ? Pouvez-vous nous présenter quelques-uns de ces projets ?

Philippe AJUELOS

Nous avons une démarche d'abord d'acculturation et de formation de l'ensemble des professeurs et des élèves. Parce que nous parlons beaucoup d'imaginaire, nous avons l'impression que l'IA, notamment l'IA générative, c'est magique. En fait, ce n'est pas magique. Ce sont soit des maths, soit de l'informatique. Depuis des années, nous nous sommes appuyés sur plusieurs rapports et travaux que nous avons menés d'ailleurs pour essayer d'amener tout un ensemble de professeurs et d'élèves à comprendre ce que cela peut être lié à le manipuler et dans ce cadre-là nous avons eu ces deux actions. D'abord travailler avec des laboratoires de recherche pour

expliquer, en matière d'intelligence artificielle. Nous parlons d'explicabilité. Cela n'existe pas en français mais pour l'IA cela existe. C'est même dans la définition de la CNIL. Donc il y a de la transparence et de l'explicabilité de l'intelligence artificielle. Nous sommes là pour déconstruire des imaginaires qui seraient faux, qui empêcheraient les générations, notamment futures, de manipuler des outils numériques.

Nous préparons les soignants de demain. Nous avons la culture. Nous simplifions. Mais aussi nous renforçons la complexité intellectuelle pour que ce soit des notions bien comprises. Nous ne ferons pas tous des ingénieurs et des ingénieuses, nous avons besoin de beaucoup de filles dans ces filières là, mais au moins que ce soient des citoyens éclairés. Nous avons donc produit énormément de documents pour les chercheurs, pour les professeurs. Nous avons créé des parcours de formation qui sont à disposition de tout le monde sur France Université Numérique. Il y a un parcours, qui s'appelle Artificial intelligence for teachers. En fait c'est un Erasmus+. Nous l'avons fait avec plusieurs pays et nous avons construit plusieurs outils. Parmi ces outils, il y en a un qui a fait l'objet de pas mal de communications, c'est MIA seconde. C'est la remédiation des élèves de seconde, qui est en test actuellement, et qui va être déployé en septembre. C'est tout ce que les élèves de seconde doivent avoir appris pour être au point pour le début de la seconde.

Je veux faire le point sur cinq solutions qui sont déployées depuis la rentrée de septembre 2022. Vous avez trois solutions en mathématiques, deux solutions en français qui permettent aux professeurs, aux assistants professeurs vis-à-vis des élèves, de personnaliser les parcours de formation en fonction du niveau de l'élève. Nous allons travailler sur ce que nous appelons la courbe d'apprentissage, c'est à dire la zone proximale de développement. Ce qui permet normalement à l'élève d'être confortable pour apprendre. La courbe de l'oubli, parce qu'évidemment c'est comme cela, quand nous avons un enfant qui apprend, nous oublions. Et puis la possibilité pour le professeur de constituer des groupes pour stimuler les élèves. Nous avons actuellement sur les 130.000 professeurs du cycle 2, donc CP, Science 2 qui pourraient utiliser cet outil, 45.000 qui l'utilisent.

Voilà au moins une des solutions. Nous sommes très satisfaits des premiers résultats. Nous faisons plusieurs choses. D'abord, avant de les mettre à disposition, nous évaluons les solutions. Et ensuite, il y a une deuxième évaluation par rapport aux traces d'usage et d'apprentissage.

Et nous utilisons l'intelligence artificielle pour valider certains algorithmes et savoir si ces algorithmes de recommandation sont efficaces et n'enferment pas les élèves. Mais je réponds à une de vos questions sur l'éthique. Une des premières démarches éthiques est de nous assurer que nous aidons les élèves, que nous ne les enfermons pas dans une difficulté ou dans une démarche où ils auront un parcours personnalisé mais qui ne fera jamais qu'ils croisent le parcours des autres, qu'ils soient avec les autres. C'est une démarche éthique, être sûr que les recommandations permettent réellement d'avoir une base commune. Ceux qui doivent s'améliorer encore plus, pourront le faire mais il faut qu'il y ait une base commune entre les élèves.

Vous avez un outil qui s'appelle Captain Kelly qui permet d'accompagner les élèves de primaire pour l'apprentissage tout à l'oral sans écran. La difficulté est que nous n'avons pas de données qui alimentent les algorithmes. Nous n'avons pas de données, de voix d'élèves français qui parlent en anglais. Donc nous avons dû constituer cette banque de données, cette dataset, qui permet à l'outil de bien parler anglais et de s'assurer que l'élève parle bien anglais avec un bon accent. C'est la difficulté de beaucoup de professeurs. Cet outil est plébiscité par les professeurs et par les élèves, parce qu'en plus de s'assurer de l'apprentissage de la langue, il y a aussi tout l'aspect, « anglo-saxon » de la motivation.

En matière d'IA générative, nous avons développé certains outils. Ce n'est pas des outils au sens technique, mais ce sont des outils pour accompagner les professeurs dans l'usage de certaines IAs génératives. Nous faisons donc la promotion d'IAs génératives qui soient transparentes. Ce sont des logiciels libres, dont les données sont en France, donc cela élimine pas mal de diagenératifs que vous connaissez par

ailleurs, mais qui marchent aussi. Nous travaillons avec l'équipe Albert de la DINUM, c'est un écosystème qui se parle et qui travaille bien. Pour nous, l'idée est de permettre d'avoir un assistant qui va aider le professeur dans la constitution de ses parcours de formation et qui va l'aider à pouvoir répondre à des questions facilement ou d'accompagner certaines étapes pédagogiques, parcours pédagogiques pour certains élèves.

Et puis, petite incise éthique, nous allons faire travailler l'esprit critique. Nous allons poser des questions à l'IA générative, nous allons attendre la réponse et nous allons faire travailler les élèves sur est-ce que la réponse est bonne ? Quelle serait la meilleure réponse pour que ce soit bon et pourquoi ? Donc nous développons les valeurs citoyennes en expliquant comment fonctionne une IA, notamment un algorithme de recommandation. Ce n'est pas une calculatrice de la pensée, c'est la solution, la réponse la plus probable par rapport à certaines données.

Encore faut-il savoir comment sont constituées les données ? D'où viennent-elles ? Qui a réalisé cet algorithme ? Et donc nous développons aussi les valeurs citoyennes de l'élève. Dans le plan d'action 2024-2027, nous avons plusieurs actions. Derrière chaque action, il y a des projets, des vrais projets avec des vraies personnes dotées de vrais moyens. Des projets sont accessibles sur Internet, tel Partenaires d'innovation. Ce sont des vrais morceaux d'IA. Il y a des projets en cours. Nous travaillons avec des partenaires en région académique et pour les opérateurs de l'État, CNED, Réseau Canopée, nos établissements, nos grands établissements. Actuellement, nous avons deux projets.

Un projet de chatbot RH qui permet à nos ressources humaines et nos gestionnaires RH de disposer de réponses sur des bases documentaires que nous maîtrisons, que nous alimentons avec un Small Language Model (SLM). Ce n'est pas un gros modèle de langage qui consomme beaucoup d'électricité. Ce sont des outils qui pourraient être déployés sur ordinateur. C'est du logiciel libre, des communs numériques. Ce sont des algorithmes qui sont publiés et cela consomme beaucoup moins que des gros modèles de langage. C'est aussi notre démarche éthique. Nous développons

des outils qui permettent à des gestionnaires d'avoir des réponses et de qualifier la réponse donc d'améliorer aussi par renforcement, l'IA. Nous nous sommes aperçus que les réponses faites par le chatbot sont beaucoup plus sympathiques que les réponses qui sont réalisées par nos propres agents. Ce sont les agents qui se sont aperçus de cela. Quand nous gérons 860 000 professeurs, nous n'avons pas forcément le temps, donc nous pouvons oublier d'être aimables. L'IA renforce la relation humaine entre les gestionnaires et les professeurs.

Nous avons développé un autre outil qui est dans le cadre d'un commun numérique et qui permet de créer des chatbots tout simples pour les professeurs. C'est plutôt magique et c'est très simple. Et cela permet pour des professeurs de créer des petits chatbots, de faire travailler les élèves et de faire comprendre comment ça marche.

Patrick CHAIZE

Manu REYNAUD, le 2 avril dernier à Marseille, la métropole de Montpellier a reçu le label Territoire innovant des interconnectés pour sa convention sur l'intelligence artificielle. Ces travaux ont abouti à la rédaction de préconisations sur l'IA pour les habitants et le territoire. La session a été présentée le 24 avril. Pouvez-vous nous expliquer cette démarche, comment et quand a-t-elle été initiée et pourquoi vous l'avez menée ?

Manu REYNAUD

C'est une démarche un peu innovante qui va s'inscrire dans des propositions que fait le Président de la République ou plutôt des commandes politiques. Pourquoi en sommes-nous venus là ? Je vais prendre les choses de façon très macro et vraiment très d'en haut. Je voudrais rappeler que si nous avons inventé les machines, c'est pour qu'elles fassent les choses à notre place, plus vite et mieux. Deuxièmement, il y a un petit problème, c'est que l'être humain, un homme, une femme, peu importe, a toujours un petit souci à se faire challenger sur l'intelligence, c'est un peu ce qui fait notre spécificité. Alors certes, il y a l'intelligence des plantes, l'intelligence des animaux, mais on a du mal à se faire challenger.

Et pour la première fois, nous avons des machines, là nous allons parler d'IA générative. Pour se rassurer, nous disons c'est une machine, elle ne réfléchit pas, elle n'a pas de conscience. Mais en réalité, quand vous discutez avec la dernière version orale de chatgpt c'est redoutable. Il n'y a quasiment pas de temps de latence dans la réponse. Vous pouvez vraiment avoir une discussion avec la machine. Et en fait, toute la question est de savoir sous quel angle nous prenons le problème. L'angle géopolitique, l'angle économique, l'angle sociétal, l'angle d'éducation ? J'ai participé à plein de débats. Je suis allé voir des jeunes notamment en informatique parce que cela apprend des choses sur la génération du code. J'ai été frappé par un verbatim d'un élève qui devait avoir environ 22 ans. Il nous a dit « moi c'est formidable j'ai enfin mon chargé de TD à moi. Il me fait mon code, je peux discuter avec lui et je peux apprendre ».

Sciences Po, la métropole et la ville de Montpellier ont interdit Chatgpt. Mais en fait, nous n'interdisons pas, mais il faut se poser la question, comment apprenons-nous ? Et cela refond des modèles dans chaque profession. J'ai donc testé auprès de plein de professions quel va être l'impact de l'IA générative. Car l'impact de l'IA sur les métiers, ce n'est pas palpable. J'aurais aimé vous parler de notre plateforme d'IoT avec 10 000 capteurs, de la gratuité du tramway avec tous les capteurs que nous avons. Ce n'est pas palpable par tout un chacun. Par contre, l'IA générative, c'est de suite plus percutant. Et c'est vrai que quand nous posons la question à un professionnel, de quelque profession qu'il soit, nous obtenons la réponse immédiate « mon métier ne sera pas touché parce que dans mon métier c'est l'humain d'abord ». Je prends en exemple les médecins, les avocats et les enseignants, ils considèrent qu'ils ne seront jamais touchés. Il ne s'agit pas de dire c'est la fin de la démocratie, c'est la fin des métiers, mais il faut prendre conscience que cela va transformer des profils. Nous disons cela va rendre plus expert les experts, cela va supprimer potentiellement des stagiaires, des juniors. Mais alors du coup, comment allons-nous faire pour devenir senior ?

Comment va se faire l'expérience ? Il y a plein d'études très intéressantes, qui disent que beaucoup d'employés utilisent chatgpt sans le dire à leur supérieur hiérarchique. Certaines fois parce que c'est interdit, c'est le cas de 82% des grandes entreprises pour des questions de confidentialité, de droits de propriété, mais c'est aussi vrai pour plein d'autres raisons. Mais ils l'utilisent quand même parce que ça permet d'avoir certaines choses. Du coup, nous allons nous décadrer dans le cadre des relations humaines et de la gestion des RH sur des profils de postes qui ne correspondront pas à l'usage. Il y a plein d'effets induits qui vont transformer les choses. C'est pour cela qu'à la ville de Montpellier, nous avons décidé d'interdire chatgpt pour l'usage de nos agents et de tous les collaborateurs de toutes les sociétés avec lesquelles nous travaillons. Pourquoi ? Pas pour dire que nous étions contre la technologie, mais pour dire qu'à un moment donné, il faut faire les choses dans l'ordre. L'IA générative, c'est très addictif et c'est en partie illégal au niveau de l'utilisation des données, et cela procure des hallucinations. Et c'est illégal aussi parce qu'effectivement, vous avez la question des droits de propriété, la propriété intellectuelle.

Samsung s'est fait piquer lui-même ses codes sources. C'est quand même assez extraordinaire qu'une multinationale de ce type-là arrive à ce que des ingénieurs aillent filer leurs codes sources sur chatgpt. C'est assez unique, donc vous avez l'illégalité, vous avez la question de la confidentialité des données. Cela part où ? Comment c'est fait ? Comment c'est encadré ? Et puis vous avez les hallucinations, c'est le terme technique que les data scientists ou autres professionnels appellent pour dire que cela dit n'importe quoi. Nous allons faire les choses dans l'ordre. Si ce truc-là a tous ses inconvénients, nous allons d'abord instruire, voir le cadre juridique même si c'est en vente libre. Dans une société libérale, le législateur arrive en bout de course. Il voit la réalité et essaie de la codifier et l'appréhension est un peu différente. Depuis ces interdictions massives, nous expérimentons parce que ce sont des cas d'usage intéressants. Je précise, ne mettez pas de données confidentielles, mais par contre testez. Ce n'est pas un moteur de recherches, même si c'est l'utilisation première qui en est faite. Mais il faut dialoguer, prompter. Il faut savoir poser des questions, commenter une invite, un cahier des charges. J'ai vu Copilot qui est l'IA générative de Microsoft. Elle va être disponible à un coût relativement

élevé. Là, cela ne va plus être comme Chatgpt ou comme les solutions génériques des big tech. Cela va attaquer vos données d'entreprise. L'utilité c'est d'aller prendre vos données d'entreprise parce que derrière vous avez toute la question de l'expérience, du savoir-faire de la boîte. Est-ce le turnover dans les métiers ? Comment accède-t-on au savoir ? Donc nous décidons de faire une convention citoyenne. Nous faisons appel à des gens du Conseil national numérique pour participer, à un panel constitué avec une entreprise de panelistes. Alors évidemment, ce sont des habitants de la ville de Montpellier. C'est une photographie à l'instant T de ce qu'est l'état de la société avec ses défiances. Derrière nous allons le traduire en termes opérationnels c'est-à-dire que derrière il va y avoir une stratégie data IA, une comitologie avec des comités d'éthique. Là, nous rentrons dans les intentions. La première chose qu'ils nous ont dite : il nous faut une IA utile. Cela veut dire également qu'il y a aussi des IA qui ne servent à rien. Il faut se poser cette question-là. Ensuite, ils nous disent qu'il y a des impacts environnementaux. Alors là, nous avons dû parler d'appels à projets sur la question de la sobriété qui est essentielle. Ils nous posent beaucoup de questions. Ils sont aussi d'une exigence en termes d'intention et de contrôle dont le caractère opérationnel est à trouver par la suite. Il va falloir arriver à trouver et confronter à la réalité parce que jusqu'à maintenant quand nous faisons notre stratégie IA et data, nous compilons un état de fait de la situation des différents services. Ce n'est pas la même chose de la police pour les pouvoirs de police du maire qu'avec la question de la gestion de l'eau ou la gestion de la relation usagers. Il faut savoir qu'aujourd'hui dans les solutions commerciales qui sont proposées à toutes les collectivités en fonction des thématiques, vous avez beaucoup d'espoir dans les promesses qui sont faites. Dans la relation usagers, il y a plein de choses à inventer, de standards automatisés. Il y a des choses qui sont en train de changer, il y a une appréhension qui est en train de changer. Ce que nous avons fait en dehors de la convention citoyenne, c'est surinvestir sur ces sujets. Nous avons réuni autour de Mickaël DELAFOSSE, président de la métropole, des chercheurs et des chercheuses, des chefs d'entreprise. Et nous leur avons dit, quelles sont vos précautions ? Comment avance-t-on ? Et nous avons avancé avec cette convention citoyenne qu'ils nous ont proposées. Et derrière nous avons avancé avec des partenariats avec l'université, le rectorat, les lycées, les collèges pour dire nous allons faire de l'acculturation parce qu'il y a besoin d'acculturation, d'esprit critique.

Nous avons avancé en disant nous allons mettre un programme e Halle de l'IA qui est un système de programmation autour de tout ce qui pouvait se discuter là-dessus. Demain à Montpellier, nous avons les Legal Tech avec des juristes qui vont discuter et appréhender avec des outils, avec des exemples, avec des solutions commerciales ou pas pour mieux appréhender la chose. Le droit va être particulièrement touché. La logique a été de prendre sur le maximum d'angles que nous pouvions prendre à notre niveau, en espérant pouvoir susciter, pas forcément des vocations, mais au moins de se dire que la grosse difficulté de l'exercice pour les politiques, ce sont les angles. Il faut prendre un petit angle. Quand nous avons interdit le chatgpt, c'était de dire que faisons-nous quand nous pensons que c'est du ressort de l'écriture et de l'imprimerie et quand on est élu local pour susciter le débat. Nous l'avons interdit pour mieux aller de l'avant et être moteur dans la question de l'IA et pour la mettre au cœur du débat public.

Patrick CHAIZE

Interdire pour mieux s'en servir. Jean CATTAN, le CNUM, a participé à cette convention montpelliéraine. Vous l'avez rappelé, le Conseil du numérique a également contribué au rapport qui a été remis en mars au président de la République, l'IA, notre ambition pour la France. Mais surtout, vous accompagnez les travaux de réflexion avec des actions dans les territoires, dans des itinéraires numériques et désormais au travers des cafés IA. Est-ce que vous pouvez nous relater l'expérience en la matière ?

Jean CATTAN

Quand le Conseil national du numérique a été composé il y a trois ans, il l'a été pour aborder le fait numérique en tant que fait social total, d'où une composition très orientée vers les sciences humaines et qui répondait à une question du moment. Il faut s'en souvenir, et nous sommes beaucoup à avoir connu cette période-là, c'était à l'époque de la 5G, StopCovid, de la bascule vers le télétravail, etc. Le numérique était souvent au centre d'un choc très puissant à l'échelle sociétale, charriant de

nombreuses questions à mettre sur la table et avec le plus grand nombre. C'est pourquoi, et notamment à travers la publication en accès libre de nombreux ouvrages et entretiens, nous avons fait le choix non pas de nous positionner en tant que prescripteur mais en tant que soutien au débat à l'échelle du pays. Ce qu'évidemment beaucoup font déjà depuis de très nombreuses années sur l'ensemble du territoire national et qu'il revenait au fond de valoriser le plus.

Cette démarche a été cristallisée dans le cadre d'itinéraires numériques portée par le Conseil depuis deux ans. Sur la dizaine de personnes qui composent le secrétariat général, deux sont à temps plein en lien permanent avec toutes ces initiatives partout en France et surtout se déplacent chaque semaine dans une ou plusieurs localités pour recueillir, nourrir, partager et valoriser ce qui se fait. Finalement ce cycle d'échanges a débouché sur la production d'un ouvrage mais aussi sur la perspective, que nous avons formulée à la manière d'un oxymore, de constituer un service public de l'éducation populaire au numérique. A travers cette orientation, il s'agit de combiner deux choses : d'une part une approche faite d'initiatives spontanées et circonstanciées propre à l'éducation populaire et l'idée que le service public avait quelque chose à apporter au moins pour assurer la pérennité des dispositifs existants ainsi que leur possible extension. Notre hypothèse est qu'en rassemblant l'ensemble des acteurs concernés dans une action collective, coordonnée et mutualisée nous pourrions générer non pas des coûts mais des gains. Derrière cette proposition, il s'agit aussi de promouvoir une vision, déjà bien existantes en bien des endroits, où l'administration se met au service des activités citoyennes.

Après coup, cette proposition a rejoint une initiative portée de longue date par Gilles BABINET, de créer CaféIA. L'intelligence artificielle exige d'offrir des lieux d'échanges et de partage de clés de compréhension avec le plus grand nombre. D'où cette expression de CaféIA qui vise à dire que c'est avant tout dans nos lieux du quotidien que cela va se passer, dans nos environnements proches. Cette perspective répond notamment à des enseignements du baromètre du numérique qui montre bien combien l'apprentissage du numérique se fait beaucoup de proche en proche. Il ne se fait pas tellement par l'accès à un point de formation centralisé. Il se fait au jour le

jour par le contact avec d'autres personnes. Cela correspond à une vision en réseau complètement décentralisée en fait à un réseau de partage de connaissances, d'apprentissage. C'est un modèle assez intéressant à promouvoir et à nourrir pour peut-être voir émerger une nouvelle dynamique d'apprentissage collectif. Il ne s'agit pas du tout de renier ce qui se fait ici ou là. Il s'agit au contraire de valoriser et de rendre accessible au plus grand nombre ce qui se fait partout en France pour parfois des millions de personnes.

L'idée de faire Café IA s'est retrouvée en proposition numéro 1 du rapport de la commission IA remis au président de la République en mars dernier. Et ce 21 mai le président de la République, devant ce parterre de 200 spécialistes de l'IA, a chargé le Conseil national du numérique de structurer Café IA, en tant que démarche de débat généralisé et de partage de ressources pédagogiques sur l'intelligence artificielle. Ce qui induit l'idée de construire une démarche pérenne, avec de nombreux temps, et donc de manière un peu différente qu'un débat institutionnalisé, inscrit dans un temps donné ou convoqué. Aussi, et c'est fondamental, le Président a bien insisté sur la nécessité de prendre appui sur les réseaux déconcentrés ainsi que sur les élus. Ce qui est fondamental car cette démarche ne peut pas se penser de manière centralisée. Nous devons toujours être ramenés à cela. C'est-à-dire que la méthode doit servir l'exercice.

Ainsi, la méthode de construction doit être autant démocratique que la vocation de l'exercice. Dans cette idée, nous avons par exemple lancé des cafés ouverts. Toutes les semaines, de 13h30 à 15h, nous échangeons avec un peu moins d'une vingtaine de personnes, pour que tout le monde ait son mot à dire à chaque fois et tout le monde peut nous écrire à cafeia@cnnnumerique.fr. Notre lettre d'information hebdomadaire permet le partage de toutes les informations et notre calendrier est ouvert. Parce que je pense que nous avons devant nous l'opportunité de créer un dispositif d'expression citoyenne, celui-ci doit être construit de la façon la plus démocratique qui soit. Ce qui ressort de ces échanges est que ce sont les personnes qui sont au sein de leur communauté, de leurs collectifs, de leurs structures, qui savent le mieux comment parler à celles et ceux qui les entourent et avec quel niveau de langage. Ce sont aussi ces personnes qui savent le mieux mobiliser

d'autres personnes. Autant de dynamiques qui nous orientent clairement vers la création d'un maillage de pair-à-pair bien plus que vers la constitution d'un dispositif centralisé Je vous fais part des défis que nous avons devant nous. L'enjeu est alors de savoir comment concilier des dimensions qui peuvent parfois paraître contraires : dispositif de portée nationale et adaptation ultra-locale, savoirs techniques et accessibilité, temps d'échange et mise en action, etc. Une chose est certaine est que c'est en nous y mettant avec le plus grand nombre que nous y parviendrons.

Patrick CHAIZE

Donc l'humain est au centre de la diffusion de l'IA Et des clés de compréhension sur notre relation à la technologie. Notre société se numérise toujours un peu plus. L'humain a un peu des réticences, des craintes par rapport à tout cela. Parce que globalement, c'est aussi offrir des nouvelles portes à la cybercriminalité, aux escrocs et pas seulement aux virtuels, qui menacent notre souveraineté et déstabilisent souvent nos collectivités ou notre fonctionnement démocratique. Alors si cette technologie offre de nouvelles perspectives, il convient d'adopter une posture de prudence lors de son intégration dans un système d'information notamment. L'ANSSI a publié fin avril un guide de 35 recommandations pour la sécurisation d'une architecture de système d'IA générative. Pouvez-vous nous parler des principales recommandations ? Et comment vous avez travaillé sur le sujet au sein de l'agence ?

Alix DURAND

Je vais commencer par la deuxième partie de votre question. A l'ANSSI, nous avons travaillé sur l'IA. Nous avons lancé des travaux transverses il y a à peu près deux ans. Nous articulons nos travaux autour de trois axes différents. La cybersécurité de l'IA, par l'IA et face à l'IA.

La cybersécurité de l'IA concerne tous les enjeux de sécurisation de l'IA et de ses déploiements. Comme n'importe quel système d'information, les systèmes d'intelligence artificielle présentent des vulnérabilités et donc nous devons les

sécuriser et mettre en œuvre des mesures cyber adéquates. Donc la plupart des règles classiques de cybersécurité s'appliquent. Mais la nature singulière des systèmes d'intelligence artificielle nécessite aussi d'avoir une approche renouvelée du risque cyber. La donnée, par exemple, devient un vecteur potentiellement d'attaque de ces systèmes-là. Nous pouvons introduire des formes de biais dans les données d'entraînement qui pourraient biaiser les résultats du système, créer des portes dérobées au sein du système ou créer un canal d'intrusion dans le système privilégié. Donc autant d'enjeux nouveaux en matière de cybersécurité que nous devons prendre en compte et intégrer aussi dans notre doctrine et nos travaux. C'est l'axe principal de travail de l'agence aujourd'hui, c'est notre priorité. Parce qu'aujourd'hui nous avons une diffusion considérable de ces technologies dans la société, les entreprises et dans les administrations. Et cette diffusion des usages ne pourra se faire dans de bonnes conditions que si ces usages sont cybersécurisés bien évidemment.

Le deuxième axe qui est la cybersécurité par l'IA, cela concerne l'utilisation de l'intelligence artificielle pour la cybersécurité : automatiser, par exemple, la détection d'intrusions, la détection de codes malveillants dans des lignes de commande. Aujourd'hui à l'ANSSI nous avons notamment des travaux de recherche là-dessus. La recherche d'ailleurs est très prometteuse dans ce sens et des applications de cybersécurité exploitant des logiciels d'intelligence artificielle commencent peu à peu à s'industrialiser. C'est extrêmement intéressant, d'autant plus à l'heure où la menace cyber ne cesse d'évoluer extrêmement rapidement. Donc l'intelligence artificielle permet aussi d'offrir de nouveaux moyens de s'en prémunir, d'être toujours plus adaptable et détecter des signatures malveillantes sans qu'on ait pour autant une base de données exhaustive de tous les types de signatures malveillantes qui existent.

Et enfin, la cybersécurité face à l'IA. Ce troisième axe, concerne l'utilisation potentiellement malveillante de l'intelligence artificielle à des fins de cybercriminalité ou de cyberattaque au sens plus large. Aujourd'hui ce que nous constatons c'est que l'intelligence artificielle peut permettre de générer du code malveillant, peut permettre de démultiplier les capacités des acteurs malveillants en

leur donnant des nouveaux outils à leur disposition. Donc c'est plutôt une croissance en volume des cyberattaques plutôt qu'une vraie refonte des modes opératoires d'attaque qui serait de nature à remettre en question toutes les mesures de cybersécurité classiques qui existent. Je ne serais trop vous encourager à continuer à utiliser des bonnes mesures de cybersécurité pour vous en prémunir. Et pour autant, cela va donner à l'avenir des opportunités considérables aux cyberattaquants. C'est un outil qui permet de pouvoir automatiser des attaques à grande échelle, multi-canaux, multi-langages. C'est aussi un enjeu qui nous intéresse particulièrement.

Et fort de tous ces enjeux-là en matière de cybersécurité, l'agence a effectivement publié, il y a de cela deux semaines, un guide sur la sécurisation de l'IA générative. Ce guide est en libre accès [sur notre site internet](#). Les mesures principales sont les suivantes. Premièrement, c'est qu'aujourd'hui nous constatons que les technologies d'intelligence artificielle font l'objet de beaucoup de mises à jour, cf. les différentes versions de GPT. Mais les mises à jour cherchent toujours à gagner en termes de performance mais pas en termes de conditions de sécurité. Donc nous trouvons tous les jours des vulnérabilités dans tous les systèmes d'IA générative qui sont déployés. Il faut se rappeler que ces systèmes-là ne sont pas immuns aux cyberattaques. Il convient de les utiliser avec prudence et de les intégrer dans des projets de déploiement qui soient sécurisés. Les enjeux liés à la sécurisation des déploiements dans des infrastructures nuagiques s'appliquent en particulier sur ces systèmes-là. Par ailleurs, ce que nous recommandons également dans le cadre de ce guide, concerne l'aspect statistique des résultats produits par les intelligences artificielles. Il faut toujours bien avoir à l'esprit de garder sa capacité de discernement par rapport aux résultats qui sont donnés par le système. Un de mes collègues ici présent parlait des phénomènes d'hallucination, c'est le fait que l'intelligence artificielle puisse parfois donner des résultats fantaisistes. Il ne faut pas que l'intelligence artificielle aujourd'hui se substitue à la capacité d'entendement de chacune et de chacun, ni aux expertises métiers que nous pourrions consulter. Quand nous ne sommes pas capables de challenger le résultat fourni par une IA, cela peut être embêtant.

Enfin, un autre point, c'est le cloisonnement, l'interconnexion d'applications d'intelligence artificielle avec d'autres applications de bureautique, étant donné qu'une application d'intelligence artificielle peut être un canal d'entrée pour une cyberattaque. Afin d'éviter les risques de latéralisation, il faut toujours bien cloisonner les systèmes, les héberger dans des infrastructures bien distinctes. Tout cela s'applique toujours avec autant de vivacité. Il ne faut pas oublier qu'aujourd'hui à partir des résultats d'une intelligence artificielle, nous pouvons retourner aux données, retrouver les données qui ont servi à leur entraînement. Donc chaque donnée que vous allez donner à un système d'intelligence artificielle, c'est une donnée que vous perdez et que vous donnez à ce système-là. Donc si le système n'est pas installé en local et qu'il est utilisé en libre-service sur une plateforme Internet, y fournir des données, c'est les donner à la plateforme Internet. Si ce sont des données sensibles ou autres, il faut plutôt éviter et les installer sur des infras en local.

Patrick CHAIZE

Nous voyons bien qu'il y a effectivement les deux facettes de l'IA qui se confrontent et qui nous interpellent aussi dans notre réflexion. Selon vous, face à l'IA ou plus exactement face aux IA, puisque nous voyons qu'il reste quelque chose d'assez multiples, quelles limites, et pas seulement les limites techniques, devons-nous fixer à titre individuel, mais surtout aussi de façon collective ?

Philippe AJUELOS

J'ai deux niveaux de réponse. Je n'ai pas envie qu'il y ait de limites parce que j'ai envie de travailler sur les concepts et en même temps dans ce que je vous ai présenté, nous sommes passés du conceptuel, de l'abstraction à des choses réelles, tangibles, des outils qui ont été co-construits. Je ne l'ai pas dit, avec les professeurs, parce la meilleure transparence d'un algorithme c'est de construire avec les professeurs directement, avec les parents et avec les élèves. Cela c'est la meilleure transparence que nous pouvons offrir au-delà de publier les algorithmes. Plus particulièrement sur la partie éducation, il faut exposer toutes les capacités, toutes les possibilités de ce que peut apporter le numérique et l'IA en particulier.

C'est notre devoir de tout montrer en termes d'explication et d'explicabilité. Nous parlions de Skynet, je ne sais pas si tout le monde a la référence, moi j'aurais parlé aussi de Big Brother et de 1984 qui se rapprochent autant de la réalité et de la difficulté et des risques d'intrusion dans la vie privée et professionnelle, dans la vie du citoyen et donc dans la liberté. La limite va être d'assurer que nous ayons une technologie du numérique et une IA française, européenne qui respecte la transparence, les communs numériques et aussi la capacité à proposer des outils qui soient réellement utilisés par tous et pas que par certains.

Ce sont nos limites ou nos pré-requis.

La deuxième chose, c'est de préparer les futures générations à être des citoyens complets et des citoyens numériques et ne pas préparer les exclus de demain. Nous devons préparer ceux qui vont réfléchir avec cela, qui vont travailler avec cela et nous voulons absolument que ce soit dans un cadre sécurisé et éthique. Par exemple, un élément d'éthique, un des projets, c'est l'orientation des élèves. Comment accompagner l'orientation des élèves de manière éthique ? Avec les mêmes données à l'entrée, une démarche non éthique va consister à dire : « par rapport à ces résultats, voilà ce que tu vas être ». Cela, enferme et c'est exactement ce que nous ne voulons pas. La souveraineté commence par la tête. C'est la liberté et la capacité aux élèves d'être des citoyens pleins et entiers. Mais la démarche éthique, c'est de dire, voilà tes résultats, dis-moi ce que tu veux faire et les outils d'orientation avec un conseiller d'orientation vont expliquer les efforts que tu dois faire.

Manu REYNAUD

Je souscris intégralement à ce qui vient d'être dit parce que je pense que c'est la philosophie générale. Moi j'allais dire pour conclure, il nous faut des lois fondamentales type les lois de la robotique. À un moment donné il faut que les choses soient simples. Historiquement les recherches et les travaux ont plus de 50 ans. Mais la réalité c'est que nous sommes au début de l'usage massif avec toutes les perspectives que cela peut avoir de sociétal, géopolitique, économique.

Il nous faut des lois fondamentales de la place du numérique et de l'IA en particulier et de l'humain, ainsi que des lois fondamentales qui soient copartagées à une échelle européenne. Il faut quand même le dire, c'est la déception totale sur l'IA Act. En réalité, ce sont des systèmes d'autorégulation consentis. Nous sommes très loin d'avoir une approche.

Aujourd'hui, nous n'avons pas les moyens d'aller auditer le code de TikTok ou des réseaux sociaux qui aujourd'hui influencent la politique et nos démocraties. Ce sont des sommes colossales. La réglementation européenne impose effectivement aux big tech, au-delà d'un certain nombre de millions d'utilisateurs, certaines obligations. Nous pouvons aussi inverser la charge de la preuve, dire que c'est à eux de prouver un certain nombre de choses et pas à ceux qui voudraient leur demander des comptes. Concernant l'IA générative, je suis toujours en tête pour essayer de voir les choses macro parce qu'il faut voir qu'aujourd'hui l'IA générative codifie l'existant. C'est à dire qu'elle amplifie les discriminations, les inégalités. Donc nous allons pénaliser encore plus ceux qui sont déjà pénalisés. Et la même chose avec les prestations sociales. Il y a eu un gros scandale aux Pays-Bas. Il y a eu des choses pas très nettes au niveau de la CAF aussi, on l'a appris il y a quelques temps sur la question du code source. Nous discriminons de plus en plus ceux qui sont déjà discriminés. Donc toutes ces questions-là elles interrogent réellement. Et je vous le dis en conclusion quand on pense que tout cela c'est du ressort de l'écriture et de l'imprimerie. Au début il y avait une certaine inégalité. Les lettrés, les copistes et tout cela a évolué de plus en plus. Si nous sommes dans cette perspective-là, il faut toujours se référer à notre donnée matérielle parce que tout cela c'est de la gestion humaine. Dans les relations humaines, nous avons quelques centaines d'années voire plus, d'expérience dans la cohésion. Il faut retranscrire des modèles. Ce n'est pas modéliser l'existant parce que c'est aussi un autre monde mais ce n'est pas non plus Second Life ou le métavers. Mais pensez toujours à si c'est du ressort de l'écriture et de l'imprimerie, il faut prendre les choses à leur mesure.

Jean CATTAN

Je partage le constat sur les actes et je tendrai pour ma part vers une forme de régulation de l'interconnexion entre les fournisseurs de contenus et les agents conversationnels pour ne parler que d'eux. Laisser à des relations bilatérales comme nous le voyons aujourd'hui les liens d'alimentation de certains agents conversationnels pose énormément de questions auxquelles nous savons répondre grâce aux outils que beaucoup dans la salle connaissent, notamment dans la mise en œuvre du droit des télécoms.

Ensuite il y a d'autres limites qui sont à prendre en compte, qui sont d'ordre environnemental. Et là aussi je crois, grâce au président CHAIZE, que nous sommes à la pointe mondiale. Grâce aux lois REEN et REEN2, nous avons une capacité de collecte de données environnementales auprès des acteurs du numérique. En tirant le trait, un jour que j'espère très proche, nous enverrons juste un mail à OpenAI et ses concurrents avec le même questionnaire que celui qui a été envoyé au titre de la loi REEN à Apple, à Google, etc. au titre du droit des télécoms. Et ce, afin que nous ayons toutes les informations nécessaires pour alimenter le débat public. Dans notre mission d'animation du débat public, nous allons en avoir besoin.

Car c'est en partie cette connaissance, et le fait de mettre l'ADEME et l'Arcep autour de la table dans un observatoire dédié qui a beaucoup stabilisé et éclairci le débat sur l'impact environnemental du numérique. Cela ne signifie pas que la tendance s'améliore mais nous avons le dispositif qui permet d'établir un dispositif de régulation proportionné.

Alix DURAND

Pour conclure, je rejoins mes collègues ici présents. Je pense qu'aujourd'hui, l'intelligence artificielle n'est pas l'alpha et l'oméga de tout. Nous pouvons faire de l'automatisation sans forcément utiliser de l'apprentissage automatique, de l'apprentissage profond, etc. Etant donné les risques que l'intelligence artificielle peut comporter, il convient d'avoir une bonne capacité de jugement. Cela permet

d'avoir un bon discernement entre la nécessité de déployer une IA alors qu'un autre algorithme peut-être moins gourmand en données, en énergie, pourrait être utilisé pour la même finalité. Si l'IA apporte d'énormes opportunités, elle comporte également des risques. Il ne faut pas non plus que son usage se substitue à la consultation d'expertise humaine et donc il ne faut pas non plus remplacer tout humain par une IA. L'IA doit rester un outil d'aide, d'accompagnement, de démultiplication des compétences, oui, mais pas de substitution.

Ariel TURPIN

Quelles sont les données d'entrée sur les élèves qui alimentent les algorithmes ? Les développements qui ont été réalisés, Tchadbot RH, Tchadbot MD, sont-ils mis à disposition en source libre ?

Philippe AJUELOS

Nous avons dû créer des données d'entrée parce qu'elles n'existaient pas. Nous avons beaucoup parlé des algorithmes, mais pas de la qualité de la donnée qui fait que les résultats sont bons. Nous avons récupéré, collecté des données d'entrée de vrais apprenants que nous avons tout de suite anonymisées et nous avons fait ce que nous appelons des profils d'apprenants. Nous avons bâti des profils d'apprenants pour être sûrs que nous ne recoupons pas d'informations. De ces profils d'apprenants, nous avons créé des parcours personnalisés et ensuite nous avons développé le nombre de profils d'apprenants et le nombre de parcours pour que ce soit toujours adressé à la bonne personne sans savoir qui c'est. Et en plus nous avons un système qui s'appelle le gestionnaire d'accès aux ressources qui permet qu'il n'y ait pas d'identification entre l'outil que nous utilisons et l'élève qui utilise. Donc, nous sommes toujours dans des systèmes où nous ne pouvons pas faire le lien entre le petit Benjamin ou le petit Nicolas et en fin de compte la personne qui va suivre le parcours. Il n'est pas possible de remonter à la source de l'information parce que nous sommes à la source de l'information et donc nous anonymisons et il n'y a pas de possibilité de faire le lien. C'est validé par la CNIL, tout cela est vérifié. Nous sommes audités et c'est notre assurance. Nous appliquons ce que nous appelons une analyse d'impact pour la protection des données et tout cela est

vérifié. Nous avons dû d'ailleurs pendant la réalisation de ces outils, modifier notre système d'anonymisation parce que l'exigence de la CNIL avait changé. Donc nous avons tout repris, nous avons perdu 6 mois pour être sûrs d'être conforme avec la CNIL.

Sur ChatMD, c'est déjà en commun numérique, donc presque tout le monde peut y accéder. Il faut juste être professeur, cela concerne 860 000 personnes. Nous allons sûrement élargir l'accès à chatMD. Ce sont des problèmes de droits d'accès, mais tout est en logiciel libre. Et pour la partie concernant Cassandra, c'est le nom du projet, c'est développé en open source aussi et nous allons publier dès que ce sera un peu après le POC, après la preuve de concept, les algorithmes pour justement que nous déversions à la communauté. Cela sera accessible et nous essaierons de faire une version avec l'ADNUM, qui soit accessible aux autres administrations.

Ariel TURPIN

Il y a besoin de données de qualité pour avoir des bonnes réponses. Ces données qualitatives ne sont pas infinies. Le niveau des IA va-t-il baisser ?

Jean CATTAN

Je peux juste faire référence à une initiative qui a été prise pour contrer les défauts de Midjourney et qui a été prise par l'entreprise de VTCHetch, afin de nourrir une de ses campagnes publicitaires. Ce qu'a révélé cette campagne est que quand vous tapez « un mariage en France » vous aviez un beau village et quand vous tapiez « un mariage dans une banlieue en France » vous aviez un théâtre de guerre. Ils ont fait une campagne « Greetingsfrom la banlieue » au titre de laquelle ils ont envoyé des cartes postales de la banlieue pour que les concepteurs de Midjourney puissent alimenter l'IA générative avec des données plus justes. Ce qui nous renvoie à la constitution des banques de données mais aussi au travail d'annotation des données et à la modération des réponses, le tout requérant un travail humain colossal, et finalement un ensemble de décisions bien humaines.

Ariel TURPIN

Une question pour l'ANSSI, qui gagne la course entre IA malveillante et IA anti-IA malveillante ?

Alix DURAND

La question se pose sur beaucoup d'autres sujets en cybersécurité. Aujourd'hui, pour pouvoir entraîner des IA, nous avons besoin de données et en matière de cybersécurité, les données ne sont pas facilement accessibles, en particulier en volume suffisant pour entraîner des IA. Pour entraîner des applications d'intelligence artificielle, que ce soit à des fins malveillantes ou à des fins bienveillantes, le manque de bases de données partageables et exploitables freinent les développements d'applications cyber de l'IA, tant bienveillantes que malveillantes. Plusieurs défis persistent. Tout d'abord, les données sur lesquelles repose la détection d'intrusion sont complexes, et ne se réduisent pas facilement aux types de données ayant concentré l'essentiel de la recherche en IA jusqu'ici (images, texte, données tabulaires, etc.). De plus, la constitution de jeux de données annotés suffisamment représentatifs est un défi important, tant du fait de la diversité des SI à protéger que de la rareté relative de certains comportements malveillants. J'aurais tendance à dire, mais peut-être que je prêche pour ma paroisse, que l'IA pour la cybersécurité a un temps d'avance parce que nous disposons de données sur les cyberattaques pour pouvoir développer des applications pour faire face à de nombreux types de cyberattaques existantes de longue date.]

Ariel TURPIN

Combien de centres de calculs nécessaires en France et en Europe pour faire face aux usages croissants de l'IA ?

Jean CATTAN

C'est là qu'il nous faut faire des choix. Voulons-nous que le pays se transforme en data center ou pas ? Voulons-nous que notre grille électrique soit orientée vers ce genre d'activité au détriment de très nombreuses autres ? Comment évaluer les

gains ? Je ne sais pas dire aujourd'hui si l'équation est bénéfique ou pas. Y a-t-il des modèles plus vertueux que d'autres ? La course au gigantisme sert-elle l'ouverture ou la dépendance à quelques entreprises ? Toutes ces questions doivent trouver des réponses qui doivent elles-mêmes soutenir un choix démocratique.

Il y a aussi une question de souveraineté qu'il faut intégrer, mais je rejoins effectivement le propos de Jean CATTAN. C'est vraiment un sujet de fond que nous n'allons pas pouvoir traiter là. Je crois que nous avons beaucoup trop des datacenters et j'ai entendu des annonces du gouvernement qui allaient simplifier les procédures pour permettre d'en installer des nouveaux. Alors pour d'autres raisons, Microsoft a eu une augmentation de mémoire. Quand nous simplifions les procédures, cela se généralise. J'ai cru que Microsoft qui avait des objectifs notamment en matière de zéro carbone vient d'avancer l'inverse avec 25% d'avancée. Quand nous parlons de souveraineté, je pense que nous nous trompons de mot, pas dans cet auditoire, pas forcément au Parlement, le législateur, mais vis-à-vis du grand public. Il faut prendre le mot souveraineté dans un sens de maîtrise et de capacité à faire. Car, une fois de plus je pense que c'est un débat à avoir. Que le combat du cloud sur à quel endroit, s'est mise en place la question des législations américaines sur l'emprise. Il faut repenser la souveraineté en termes de maîtrise des données et des maîtrises de ce que nous faisons.

Je préfère avoir des centres, des supercalculateurs qui soient en France avec des clouds et qui protègent les données des enfants en France ou en Europe. Ce n'est pas dissonant. Mais la maîtrise c'est une chose, mais être sûr que nous ayons la main dessus c'est autre chose. Et encore une fois, le débat de design en France, fait en Chine, cela me pose problème, surtout quand ce sont les données des élèves, parce que juridiquement ce n'est pas des données sensibles, donc c'est compliqué

Ariel TURPIN

Nous allons conclure non pas par une question mais par une réflexion. Donner ses données, n'est-ce pas un peu comme faire un don pour le bien commun de l'humanité ?

Patrick CHAIZE

Je vous propose donc que nous répondions à la question dans un prochain colloque. Puisque je suis persuadé que ce sujet de l'IA va se réinviter dans nos programmes tant ce sujet prend beaucoup d'importance, accélère très vite et se transforme très vite avec des questions qui sont des questions de fond auxquelles nous n'avons pas répondu ou que nous n'avons pas abordées aujourd'hui. L'IA dépassera-t-elle demain l'intelligence humaine ? Je vous laisse réfléchir pour le colloque d'automne où nous pourrions réaborder le sujet.

Avant de conclure tout à fait, nous avons une vidéo à vous passer. Nous avons convié à ce débat Laura LETOURNEAU, chargée de mission Transformation numérique et écologique au service du Premier ministre. Nous voulions qu'elle vienne participer à cette table ronde et qu'elle nous présente son travail sur les infrastructures de données, qui étaient appelées auparavant les plateformes publiques. Ce travail, elle l'avait présenté avec un autre ingénieur des mines, comme elle, Clément BERTHOLLET, dans un livre qui était paru en 2017 et qui s'appelait « Ubérisons l'État avant que d'autres ne s'en chargent ». Elle a ensuite appliqué cette méthode pour les données télécom à l'Arcep, où elle a été quelques années, puis dans le secteur de la santé et finalement dans le domaine de l'écologie. C'est surtout de ce dernier rapport entre écologie et données dont elle nous parle à présent dans cette vidéo.

Laura LÉTOURNEAU

Je ne vais pas vous parler d'intelligence artificielle aujourd'hui ou un petit peu seulement, je vais vous parler des infrastructures de partage de données qui non seulement ont un lien avec l'IA, mais sont surtout très importantes en soi. Les infrastructures de partage de données, aujourd'hui, ce sont les grandes oubliées du numérique, et nous allons le voir, c'est extrêmement problématique. Il faut absolument que nous arrivions à les remédier ensemble.

Pour illustrer le propos, je vais essayer de partir d'un exemple en particulier, qui sont les infrastructures de partage de données pour la planification écologique, en vous présentant la feuille de route numérique et données pour la planification écologique, qui est en concertation publique jusqu'à fin mai. Le travail qui a été fait est un collectif réalisé avec 300 agents publics nationaux et territoriaux impliqués sur ces sujets. Il est titanesque, presque vertigineux. Ce sont 300 pages avec évidemment une synthèse. Mais ce sont huit thématiques, mieux se déplacer, mieux se loger, mieux préserver les ressources, la biodiversité, mieux consommer, mieux produire, mieux se nourrir, transversal. C'est très gros car l'écologie concerne tout.

Pour ne pas se noyer, ce travail est structuré en partant du pourquoi on travaille, pourquoi nous sommes là ? Quelle est la raison d'être de cette feuille de route ? En allant ensuite sur le quoi, qui présente la logique de plateforme publique et justement des infrastructures de partage de données sous-jacentes. Et ensuite, le plus important et le plus compliqué, en finissant par le comment.

Le pourquoi est évidemment essentiel, parce que le numérique, les données, l'IA, l'innovation et l'argent, ce ne sont pas des fins en soi. Ce sont des moyens malheureusement presque indispensables pour atteindre des objectifs de politique publique plus nobles. Donc il faut absolument définir ces objectifs de politique publique en l'occurrence dans la planification écologique. Ce que nous avons fait dans les deux premiers paragraphes du manifeste que nous avons écrit collectivement ici, c'est de dire, en réalité, rendons-nous compte que le numérique est essentiel tout simplement pour mettre en œuvre une transition écologique efficace et juste. Si nous voulons ne serait-ce que produire un rapport du GIEC, savoir où mettre au mieux des RER métropolitains, les éoliennes, gérer les pénuries sur l'eau, cibler les aides vers les ménages et les entreprises les plus précaires, suivre la qualité des sols, c'est de l'information, c'est-à-dire des données, c'est-à-dire des outils numériques pour les produire. Voilà, c'est beaucoup plus efficace que le papier. En revanche, ne soyons pas naïfs, soyons lucides. Le numérique, c'est le pire comme le meilleur. Comme nous disons, inaugurer le navire, c'est inaugurer le naufrage. Il y a plein de risques de naufrages associés au numérique qui sont franchement stressants. Il faut absolument développer un numérique qui soit éthique,

humaniste, citoyen et souverain et qui lutte proactivement contre tous les risques associés au numérique, que ce soit tous les risques associés à l'IA, tous les risques de fracture numérique, les risques de technosolutionnisme, les risques d'impact environnemental du numérique négatif, les risques d'atteinte à la vie privée, etc. Ce manifeste a deux jambes. Cela est le pourquoi, c'est la partie essentielle mais facile.

Ensuite, nous avançons sur le quoi pour arriver à notre sujet. Le quoi a lui aussi deux jambes. La première jambe détaille en fait ce manifeste qui est un peu une déclaration d'intention générique. Le détail part de terrains et de personas qui aujourd'hui ont des problèmes, ont des irritants dans leur vie quotidienne pour exercer leur métier, à cause de nous, experts des sujets numériques et données, qui n'avons pas suffisamment bien organisé le travail pour faire en sorte que ces gens puissent travailler tout court ou de façon efficace. Par exemple, nous avons plein de personas des territoires. Nous ne savons pas quelque chose sur mieux se déplacer, , nous avons Claire qui est chargée d'études dans un EPCI qui doit dimensionner les lignes de transport à la demande et évaluer l'impact sur la qualité de l'air. Nous avons Patrick qui travaille dans une AOM sur les plans de mobilité qui doit mettre en avant le covoiturage et le vélo. Nous avons Nadège qui est dans une sous-préfecture qui doit évaluer l'impact environnemental de projets et les accompagner. Nous avons Nadège qui est en agence d'urbanisme, qui travaille sur la biodiversité. Nous avons quelqu'un dans un conseil régional. Nous avons un maire, etc. Aujourd'hui, une partie de ces gens ont du mal à faire leur métier, parce qu'il y a des problèmes d'accès aux données, d'interopérabilité des outils numériques qui sont en silo, de méthodologies qui ne sont pas accessibles, etc. Et vous voyez, nous n'avons pas que les territoires qui rencontrent des difficultés. Nous avons aussi les agriculteurs, les entreprises, les citoyens qui veulent rénover leur logement, les bâtiments, les ONG, nous-mêmes, les agents publics au niveau national, quand nous voulons évaluer les politiques publiques, etc. Donc cela, c'est la partie un peu déprimante, mais qui permet de mettre à plat l'état des lieux. C'est la première jambe du quoi.

Une fois que nous avons dit cela, comment faisons-nous mieux demain ? Eh bien, Nous commençons par regarder ce qui existe déjà. Cela ne se fait pas tout le temps, c'est important de se dire quels outils, quelles briques numériques, quels standards

sont déjà à notre disposition pour rendre les parcours de ces personas beaucoup plus fluides. Et une fois que nous les avons, il convient de les réorganiser pour en supprimer, parce que certains sont en doublon, parce que nous manquons d'organisation, pour en rajouter, parce qu'il manque tel standard, tel identifiant, pour les rendre plus interopérables, pour tout simplement s'organiser. Et pour s'organiser, nous avons cette doctrine, que nous avons essayé de détailler dans « Ubérisons l'État avant que d'autres ne s'en chargent » avec Clément BERTHOLLET, qui est la doctrine de plateforme publique qui propose de s'inspirer du mode de gouvernance d'une ville pour répartir les rôles sur qui fait quoi dans le numérique entre le public et le privé, et ensuite entre les différents échelons géographiques au sein du public. Nous nous disons que dans une ville les pouvoirs publics font deux choses. Ils font les règles, le code de la route, le code de l'urbanisme, etc. Ils font aussi les infrastructures de base physiques qui permettent l'échange et le partage, les routes, le réseau d'égouts, le réseau d'électricité, le réseau d'eau. En revanche, ils ne font pas toutes les maisons de la ville, les maisons sauf exception, sauf HLM. C'est le privé, ce sont les associations qui les font. Notre travail, pouvoir public au sens large, c'est de vérifier que ces maisons respectent le code de l'urbanisme, les règles, et qu'elles se raccordent aux infrastructures, qu'elles jettent leurs égouts dans le réseau d'égouts et pas dans le jardin du voisin d'à côté. Dans le numérique, que ce soit dans l'écologie, dans la santé, dans l'éducation, partout, c'est le même schéma. Les règles sont des règles d'éthique pour lutter contre tous les risques de vie en introduction, des règles de sécurité, des règles d'interopérabilité. Cela, c'est du papier, c'est du texte, c'était standard. Ensuite, nous avons des infrastructures qui ne sont pas des égouts ou des réseaux d'eau, qui sont des infrastructures numériques. C'est de cela dont je veux vous parler. Nous avons l'équivalent de l'eau ou des électrons du réseau d'électricité, c'est tout un tas de données métiers, le DPE, la qualité des sols, les données de l'eau, etc. Et des données d'identité qui sont toujours victimes de la tragédie des communs alors qu'elles sont essentielles. L'identité d'un patient dans la santé, l'identité d'un agriculteur, l'identité d'une parcelle agricole, l'identité d'un bâtiment, l'identité d'un animal, sont des éléments essentiels pour suivre l'évolution d'une politique publique dans le temps et arriver à croiser les bases de données. Et ces données doivent circuler dans des tuyaux, soit pour être publiées en open data, soit pour circuler dans un cercle restreint fermé d'acteurs. Tout un tas d'infrastructures qui sont nécessaires pour faire en sorte, par exemple, de mettre en

œuvre l'affichage environnemental sur du textile, sur un vêtement ou dans l'agriculture, sur tout un tas de produits alimentaires, l'agriculteur produit des données et dit combien il a utilisé de pesticides, d'eau, etc. pour produire son blé, qui doit transférer ces données au meunier qui fait la farine, qui doit transférer ces données à la coopérative agricole, qui doit transférer ces données à l'ASP pour toucher les aides de la PAC, qui doit transférer ces données au ministère de la Transition écologique pour passer ces données à la calculette et mettre sur place l'affichage environnemental, etc.

Ces fondations de la maison, c'est la plateforme publique, cela doit être public. Parfois c'est public du niveau national, par exemple France Connect. Parfois c'est public du niveau territorial, parce que dans certains cas cela se justifie que ce ne soit pas pareil en Nouvelle-Aquitaine ou en Guyane. Parfois c'est public du niveau européen, par exemple le RGPD, c'est un standard européen. Ce qui est important, c'est de préciser de quel échange géographique c'est, d'en débattre et de l'acter pour que le schéma d'urbanisation soit cohérent. C'est important, sinon nous construisons tout le reste sur du sable et après nous ne comprenons pas pourquoi cela dysfonctionne.

Tout le reste, c'est quoi ? C'est la partie émergée de l'iceberg, ce sont tous les services numériques qui ne sont pas publics, ce sont les maisons de la ville qui ne sont pas publics, qui sont construites par des acteurs privés, par des associations, par exemple tous les logiciels des médecins, des agriculteurs, des gens qui gèrent les déchets, etc. Évidemment, ce n'est pas le public, c'est du domaine concurrentiel. En revanche, le boulot des pouvoirs publics, pour que ce ne soit pas le bazar, c'est de faire en sorte que ces logiciels respectent les règles, qu'ils soient éthiques, sécurisés, interopérables, et qu'ils se raccordent aux infrastructures pour alimenter en données des infrastructures de partage de données. Pour que nous soyons sûrs que ce soit fait, il faut réguler, c'est-à-dire activer le bâton, rendre cela obligatoire, etc., c'est le nuage d'évaluation, et activer la carotte, c'est le nuage d'innovation et financement.

Les infrastructures de partage de données sont au cœur de cela. Nous n'en parlons quasiment jamais au détriment de sujet comme l'intelligence artificielle, par exemple, qui est dans le nuage de la maison, l'innovation en haut, qui évidemment peut aider à résoudre tout un tas de cas d'usage. Mais très sincèrement, 98% des cas d'usage et des problèmes réels identifiés dans la santé, dans l'éducation, dans l'agriculture, ne demandent pas d'intelligence artificielle, ou très peu. Je ne dis pas que c'est inutile et qu'il ne faut pas y aller. Mais il faut y aller dans un cadre responsable, éthique, etc.

C'est comme pendant le COVID, le système d'information COVID... ce n'est pas l'intelligence artificielle qui nous a aidé à sortir de la crise. C'est important, mais ce n'est pas le cœur du sujet. Et surtout, même pour faire de l'intelligence artificielle, nous avons besoin de données. Dans tous les cas, il faut ces infrastructures de partage de données pour alimenter les modèles de langage, d'intelligence artificielle. Voici le schéma d'ensemble.

Une fois que nous avons cette maison, cette cartographie, ce schéma d'urbanisation informatique, nous le mettons à plat sur chacune des politiques de la planification écologique. Vous voyez, nous avons fait une petite gare pour mieux se déplacer, une petite écomaison pour mieux se loger, une petite ferme pour mieux se nourrir, etc., qui sont reliées par des tuyaux, par des animaux, par des oiseaux, pour faire le lien entre toutes ces thématiques. Dans chacune de ces thématiques, dans l'agriculture, dans le logement et la rénovation des bâtiments, etc., sur la finance verte, l'industrie verte, etc., il y a toujours des infrastructures de partage de données qui sont insécurisées, sur lesquelles nous ne sommes collectivement pas au niveau aujourd'hui. Dans la santé, c'était pareil.

Nous avons énormément travaillé pendant trois ans sur les identifiants, sur le tristement fameux DMP que nous avons complètement mis à l'état de l'art technologique pour en faire un espace santé qui est un succès en train de décoller. Notre cas d'usage était de faire en sorte que l'ordonnance, le compte-rendu de biologie, les images de radiologie circulent avec le patient et avec les professionnels

de son équipe de soins, son médecin traitant, son hôpital, son biologiste. Pour cela, il fallait, comme d'habitude, un identifiant unique et des briques d'infrastructures de partage de données. Ce sont des chiffres absolument remarquables de l'alimentation de mon espace santé aujourd'hui. Nous avons 80 % des hôpitaux qui sont connectés, les deux tiers des libéraux et déjà 12 millions de français qui l'utilisent, alors que c'est un service qui n'est pas obligatoire, qui n'a que deux ans d'existence. C'était pareil pendant le COVID, c'était la maison de santé version COVID, CIDEP, que nous avons réussi à faire en trois semaines, c'était une infrastructure de partage de données, pour arriver à déclencher le contact tracing, faire le pass sanitaire, etc.

J'en arrive pour conclure sur le comment. Comment faisons-nous en sorte de mettre sur pied ces infrastructures sans lesquelles nous ne pouvons pas travailler. Nous ne pouvons pas efficacement mettre en place nos politiques de transition agroécologique, de gestion de la pandémie, de rénovation des bâtiments, etc. Il y a deux volets. Alors Il y a plein d'infrastructures qui existent à différents stades de maturité. Je vous ai parlé un peu de l'agriculture, dans l'éducation, dans la justice, dans la culture. C'est vraiment toujours victime de la tragédie des communs. Pour les mettre en place, il y a deux volets. Il y a un volet culture interne. Il faut absolument que nous changions ensemble la façon de travailler, nous, acteurs publics au niveau national, et aussi avec vous, au niveau territorial, en étant vraiment proches du terrain, en agissant avec détermination, en faisant bien plus preuve de solidarité, de coordination entre nous. Et deuxième volet, en travaillant de façon extrêmement efficace avec les acteurs externes. Donc là, les mots des territoires qui ont construit la feuille de route, qui s'en montrent très satisfaits et qui sont très preneurs à l'idée de continuer à mettre en œuvre la partie la plus compliquée ensemble. Et puis, les parties prenantes extérieures, que ce soit des ONG, des industriels, l'ONU, etc., qui s'en félicitent. C'est extrêmement important que nous y arrivions et si nous activons ces deux leviers de travailler ensemble mieux en interne et mieux en externe, nous allons y arriver. Et c'est absolument essentiel parce qu'aujourd'hui, nous sommes dans une forme de « bidonville numérique » où chacun tire ses lignes électriques, récupère son eau de pluie, la traite, etc. Et nous n'arriverons jamais à passer à l'échelle sur des enjeux de transition écologique notamment, si nous ne réindustrialisons pas le bidonville, si nous ne le réurbanisons pas pour avoir demain

un bidonville qui devienne une ville avec des maisons qui tiennent debout. Donc c'est absolument indispensable que nous travaillions ensemble sur ce sujet précis des infrastructures de passage de données et que nous nous donnions les moyens d'y arriver. Je suis absolument convaincue que c'est compliqué mais que c'est possible.

Donc Laura nous fait toucher du doigt un vrai sujet. C'est de pouvoir être sur des mêmes bases, travailler avec les mêmes référentiels pour pouvoir partager et faire en sorte que nous puissions construire le numérique de demain.