France Payments Forum – Plénière du 25 juin 2024
Table ronde « L'IA dans les paiements »

Jennifer Serfati (modératrice)

Bonjour à tous. Avant d'introduire la table ronde et le sujet, je propose que chacun d'entre vous présente sa structure en tant que nouveau membre.

Brice Perdrix (AdvanThink)

AdvanThink a été créée en 1990 par mon père, jeune chercheur en IA, dans le cadre des programmes ESPRIT. Les programmes ESPRIT étaient les premiers projets européens dont l'objectif était d'avoir une stratégie européenne pour faire émerger des acteurs de l'IA et avoir une puissance européenne dans l'IA. 35 ans plus tard, AdvanThink est une société toujours 100% française, 100% autonome, qui reste leader sur son marché et a réussi à être rentable. Le fait d'avoir des technologies d'IA qui fonctionnent à l'état de l'art tout en ayant réussi à rester complètement français, est quelque chose dont je suis assez fier.

Venant du monde de la recherche et de l'innovation, notre idée est d'apporter à l'échelle industrielle de nouvelles approches dans l'IA et la data (au sens large) qui vont permettre aux industries de passer à l'échelle et de les adopter dans leurs organisations. Notre approche est assez globale sur tous les secteurs d'activité, puisqu'aujourd'hui nous sommes bien sûr dans la lutte contre la fraude mais aussi dans du marketing, du recyclage des déchets nucléaires ou de la connaissance client. Au total, AdvanThink c'est plus de 1 000 projets en production d'IA, principalement pour les grands groupes.

Depuis les années 2000, nous avons spécialisé nos technologies dans la détection des fraudes au paiement en temps réel. Aujourd'hui, AdvanThink c'est 70 milliards d'euros protégés chaque jour en temps réel. La quasi-totalité des banques françaises nous font confiance. Notre part de marché est de 95% sur les paiements par carte et de 70% sur les virements, les

prélèvements et les paiements instantanés. Nous aidons aussi sur les relations des banques ou des Fintechs avec leurs clients, via la personnalisation de l'expérience client.

Luis Junes (Feedzai)

Feedzai est une société européenne basée à Lisbonne, qui propose une solution de lutte contre la criminalité financière. Nous travaillons principalement avec les banques, au niveau européen et mondial. Nous démarrons en France. Notre spécialité est de fournir une plateforme permettant aux banques de créer aisément des modèles de *machine learning* afin de couvrir de multiples cas d'usage comme la détection de la fraude en temps réel, et de définir leur propre stratégie de lutte contre la fraude.

Les co-fondateurs de Feedzai, qui sont toujours avec nous, ont commencé à l'Agence Spatiale européenne. À l'époque, ils avaient développé une solution pour corriger la trajectoire des fusées, et ils se sont dit « cette technologie peut être utilisée également pour d'autres cas d'usage, par exemple la fraude dans laquelle on a des millions de transactions par jour ». Ils ont développé ce qu'on appelle un *Streaming engine*, qui permet d'aller encore plus loin dans l'analyse fine de plusieurs données et sources de données en temps réel.

Yann Chassy (Datategy)

Datategy est une entreprise que j'ai rejointe il y a huit mois. Nous sommes éditeurs d'une solution appelée PapAI, qui est un logiciel de conception et de pilotage de l'ensemble des intelligences artificielles, qu'elles soient explicatives, prédictives ou génératives.

L'entreprise a été créée en 2016 par trois personnes, sur trois contrats dont un avec INFOGRESSE. L'idée était, pour les juges des tribunaux de commerce, de définir des plans de sauvegarde d'emploi, de ne pas se limiter à un simple score pour résumer la santé financière. Nous sommes donc partis de l'explicabilité pour arriver au score.

Nous avions également signé à l'époque avec la RATP, la SNCF, l'aéroport de Dubaï, pour travailler sur du *Computer vision*, c'est-à-dire l'analyse de vidéos ou de photos en temps réel, soit pour repérer des comportements à risque, soit pour faire de l'analyse de matériaux dangereux dans les pièces de train en vue de sécuriser la maintenance des appareils.

Nous commercialisons notre plateforme depuis un an. Nous avons signé avec plusieurs clients sur de la maintenance prédictive de pannes informatiques, ou sur de l'IA générative couplée à du prédictif et de l'explicatif pour aller chercher l'origine des pannes.

L'IA Act est notre boussole. Nous contribuons à l'écriture de cette norme. Nous l'avons vraiment comme boussole, car nous pensons que face à l'arrivée des Bigtechs, le fait d'apporter une sécurité, une proximité avec les clients et une explicabilité constitue un avantage. Aujourd'hui, lorsqu'une banque refuse d'accorder un crédit, elle est supposée motiver sa réponse. C'est la philosophie de notre norme PapAI.

Hervé Sitruk

Nous connaissons bien Thomas Dognin, qui travaille chez IBM, qui a animé pendant deux ans le GT Sécurité et lutte contre la fraude et qui a participé aux travaux de l'OSMP sur le quantique.

Jennifer Serfati

Le sujet de notre table ronde est l'IA dans les paiements. L'idée aujourd'hui n'est pas de développer un plan stratégique pour les prochaines années, mais plutôt de poser le cadre, de voir où nous en sommes aujourd'hui, quelles sont les opportunités et les risques. Nous reprendrons le sujet au sein de notre GT afin de produire un position paper et d'organiser de nouvelles tables rondes. N'hésitez pas à nous rejoindre, car l'expertise de chacun est nécessaire pour rendre ce sujet une opportunité dans les paiements.

L'IA est aujourd'hui un univers fascinant, avec des algorithmes très sophistiqués et une capacité à comprendre les données et à les travailler. Dans un monde de paiement instantané, on nous promet d'accélérer un parcours client sans friction, avec une détection de la fraude presque parfaite et tout aussi instantanée que les paiements.

Mais l'IA ne va pas sans risques. Il existe une opacité des décisions algorithmiques, imposé par un système qu'on ne comprend pas forcément, une sorte de boîte noire. Cela devient alors un sujet de préoccupation pour le superviseur, notamment un enjeu de protection avec l'IA Act.

L'intelligence artificielle est donc bien plus qu'un simple outil : elle va propulser notre économie numérique vers de nouveaux horizons, et l'objectif aujourd'hui c'est d'en comprendre les grandes lignes.

Je vais passer la parole en premier à Thomas : peux-tu nous expliquer ce que l'IA promet d'apporter dans le monde des paiements et à quels besoins des entreprises répond l'IA, pour quel cadre réglementaire ?

Thomas Dognin (IBM)

Avec les paiements, il y a une masse de données qui permet de percevoir, de comprendre, de segmenter, d'analyser les choses selon différents prismes. Un des prismes est le domaine de la fraude : quelles sont les méthodes potentielles pour détecter la fraude ?

Le premier élément est l'être humain, qui va permettre de prendre à un moment donné une décision. Le premier motif de l'IA est donc de savoir quelle est la place de la décision dans la chaîne de valeur de l'IA.

Le deuxième élément est les méthodologies mathématiques. L'IA existe depuis très longtemps. Vous vous souvenez peut-être qu'IBM avait fait en 1989 la preuve de battre un joueur d'échec. C'était la première fois que la machine battait effectivement un cerveau

absolu sur un domaine-clé qui est le jeu. Et puis en 2019, ce furent les débatteurs, trois ans avant l'IA générative (en fait, l'IA générative existait déjà, mais vous ne le saviez pas).

La clé est donc la recherche, des algorithmes qui avancent, qui prennent les situations et les affinent pour comprendre précisément ce qui se passe.

Avec les paiements, vous avez cette complexité comportementale qui fait que dans la banque, vous avez une connaissance de vos clients (KYC) et vous avez un référentiel de données de paiement qui, dans une certaine mesure, pourraient même être anonymisées. Vous pourriez vous en affranchir, comprendre des comportements au-delà des données personnelles, et ensuite l'appliquer sur des domaines. Quels domaines ?

Premier domaine : la vente car, comme l'expliquait M. Montebourg tout à l'heure, avant de bloquer quelque chose il faut déjà faire rentrer du revenu, car s'il n'y a pas de perspective commerciale il n'y a pas de perspective de blocage de risque. Le premier domaine est donc la connaissance du client, avec un niveau de finesse tel que vous pourriez tirer des « micro-segmentations » (le bon adressage du bon client). Or les algorithmes aujourd'hui sont de plus en plus performants.

On a tendance à oublier que l'intelligence artificielle, c'est d'abord des règles métiers, et ce n'est pas parce qu'il y a des algorithmes plus performants que les règles métiers ne sont pas intéressantes. Derrière, vous avez le *machine learning*, l'apprentissage supervisé, c'est-à-dire que vous connaissez la cible, et vous en déduisez les corrélations.

Deuxième domaine : les apprentissages non supervisés : vous ne connaissez pas la cible, vous segmentez, et vous voyez les écarts par rapport à un segment.

Troisième domaine : élément, le *deep learning*, qu'on a vu notamment avec Google, qui a fait combattre la machine contre la machine pour apprendre le jeu de Go. Le jeu de Go implique un tel niveau de connaissance que la machine a eu du mal à battre l'humain. La compréhension du langage s'appuie sur du *deep learning :* quand je parle et que la machine me capte, il y a des algorithmes de *deep learning* derrière, et vous avez beaucoup d'applications dans le domaine du commerce, du marketing, mais aussi des risques.

Jennifer Serfati

Merci Thomas, nous poursuivrons cette discussion dans le cadre du GT. Peux-tu, en quelques mots, nous expliquer ce qu'est un modèle LLM, à quel *use case* cela répond-il, et quels sont les risques aujourd'hui dans l'utilisation de ces modèles ?

Thomas Dognin

Avant le LLM, les banques qui voulaient faire du *machine learning* créaient les modèles qui avaient beaucoup de données en entrée et permettaient de déduire un score et de cibler une fraude, une association, une segmentation, etc. Un modèle avait un usage.

Aujourd'hui, l'idée est d'avoir une telle modélisation avec un niveau d'attributs en entrée et de chaînage d'attributs tels qu'on puisse avoir autant de possibilités que souhaité. Cet objet LLM est produit aujourd'hui par des éditeurs avec des capacités-machine énormes.

Imaginez ces modèles comme des ballons de football avec beaucoup de données à l'intérieur et avec des relations neuronales qui permettent à n'importe quelle demande d'identifier un chemin de réponse.

Je ne sais pas si vous en avez déjà fait l'expérience, mais quand vous posez deux fois la même question à ce LLM, vous avez deux réponses différentes. Donc les chemins ne sont pas uniques, ce qui veut dire que ces réponses sont des réponses purement statistiques, qui ne reflètent pas la vérité. Et là, on arrive sur ce qu'on appelle les biais cognitifs humains : dans la prise de décision, il doit y avoir un esprit critique.

Ce LLM permet de prendre en compte du langage naturel en entrée et en sortie, avec un niveau de précision qui est en général bon. Mais il y a beaucoup de réponses possibles, et ces réponses peuvent être fausses. Comment bloquer ou cadrer ces réponses fausses ? C'est le travail qui est en train d'être fait. Mais d'ici là, on est dans un monde de probabilité statistique, et on a donc besoin d'avoir des observateurs du risque qui permettent de déduire le niveau de risque potentiel de telle ou telle exécution d'un service.

Jennifer Serfati

Merci Thomas.

Yann, en tant qu'éditeur de solutions basées sur l'IA, comment vois-tu l'évolution des cas d'usage de ces modèles LLM et les problématiques de sécurité qui en découlent ?

Yann Chassy

Ma réponse vient surtout du fait que nous avons participé à beaucoup de salons, que nous travaillons sur beaucoup de marchés. Nous avons fait VivaTech, Santé Expo (où nous travaillons sur la maintenance prédictive de machines, la recherche sur le cancer), les Bank Tech Days où on a parlé de LLM, et je viens de faire Eurosatory dans le domaine de l'armement.

Les cas d'usage en fonction des métiers vont être très variables en demande de sécurité et de fiabilité. Ces scores sont statistiques : ils calculent juste la probabilité de mettre un mot après l'autre, un pixel après l'autre, et c'est « gavé » de phénomènes hallucinatoires et de fuites de sécurité.

Il n'y a donc pas de « bonne IA » ou de « mauvaise IA », cela dépend du cas d'usage, que l'on peut classer en **trois catégories**.

- **Les cas d'usage qui demandent de la création**. C'est ce que nous utilisons tous avec ChatGPT pour faire un résumé conversationnel ou pour commencer à chercher des points

de différence avec nos concurrents. C'est super créatif, mais la réponse correspond-elle à la réalité ou est-elle complètement hallucinante ? Quand je fais une requête, en commençant par indiquer que je suis Yann Chassy, directeur commercial de Datategy, tout ce qui suit devient de l'information sur Datategy **s**ur le web. Si je l'utilise pour préparer un discours pour Arnaud Montebourg, ça me dépanne, mais je dois mettre des faux noms, des fausses choses du genre « aidez-moi à rédiger quelque chose en langage ministériel… ».

- **Les cas d'usage qui demandent un cadre.** C'est ce qu'on commence à voir au Crédit Mutuel Arkea (qui est très en avance) ou au Crédit Agricole. Il s'agit de fabriquer des *chatbots* ciblés sur des bases de connaissances que vous avez sécurisées sur vos serveurs et organisées pour vous-mêmes et également adossées à des modèles de RAG qui vont réduire un peu les hallucinations.

- **Les cas d'usage qui demandent de la recherche et de la complexité.** C'est ce qu'on voit beaucoup aujourd'hui dans la santé ou dans le domaine militaire, où l'erreur est beaucoup moins permise. Ce sont des modèles complexes qui vont croiser l'IA explicative, l'IA prédictive et l'IA générative pour commencer à converser avec vos systèmes de fraude.

  Vous avez plusieurs systèmes de fraude aujourd'hui. Faites-les parler avec le reste de vos systèmes pour rechercher l'origine des pannes qui souvent, va être une simple intervention humaine. Vous verrez qu'en surveillant des signaux faibles, vous trouverez des solutions très simples de formations à mener dans vos entreprises.

Jennifer Serfati

Merci Yann. On parle de modèles systématiques dans la prise de décision. Nous sommes orientés « paiements » et nous nous inquiétons un peu : demain dans le parcours client, ce modèle systématique un peu opaque ne va-t-il pas apporter une solution systématique ?

Yann Chassy

Quand on parle de modèles mathématiques systématiques, on parle de modèles mathématiques très ciblés sur un domaine : les paiements, le juridique, la prédiction des défaillances d'entreprise…

Il s'agit de modèles micro, qui présentent l'avantage qu'étant très ciblés, ils sont extrêmement réactifs et vous permettent de répondre vite à la menace qui se présente devant vous. L'inconvénient est que ces modèles ne sont pas assez macro et empêchent d'avoir une vision hégémonique sur vos systèmes. Avec les plateformes de dernière génération (qui sont forcément européennes parce que développées dans le cadre de l'IA Act, avec un principe d'explicabilité et de transparence), on va réunir les IA dans une seule interface et vous permettre de piloter ce qu'on appelle le *drift* des modèles.

Prenons un cas d'usage très simple : dans l'armée, j'ai un véhicule blindé dont les pneus crèvent souvent. Il ne faut pas que le pneu crève pendant que je suis au combat, etc. J'ai déjà des algorithmes systématiques qui permettent de dire que le pneu est crevé, qu'il est en train de se dégonfler ou qu'il est fortement usé. Réunir vos IA dans une seule interface et les croiser entre elles va vous permettre de vous dire que les pneus crèvent parce que (a) le conducteur conduit « comme un bœuf » sur des routes pleines de trous et (b) à l'atelier, ils ne mettent pas assez de graisse dans l'amortisseur. Si, avec un peu de formation consistant à mettre plus de graisse et à ralentir la conduite, j'aurai moins souvent besoin de changer mes pneus.

C'est là où les plateformes hégémoniques et globales comme PapAI vont vous permettre d'aller dialoguer avec la machine, avec des capteurs, avec vos serveurs, avec votre réseau, avec vos systèmes de fraude, pour rechercher l'origine de la panne.

Pour se prémunir de cela, il y a deux solutions : (a) surveiller le *drift* dans une interface pour vérifier que l'algorithme correspond à l'évolution de votre menace (la fraude, pour ce qui vous concerne) et (b) s'aligner avec l'IA Act et construire des systèmes intelligents dans lesquels c'est vous qui pilotez vos algorithmes. C'est à vous de définir vos objectifs et la manière dont vous voulez les atteindre, qui correspondent à vos valeurs et à vos politiques.

Jennifer Serfati

Merci Yann.

Quand nous parlons d'IA dans les paiements, le premier cas d'usage qui ressort est la fraude. Nous sommes dans un contexte d'instantanéité et la réglementation impose à toutes les banques de proposer et d'accepter l'Instant Payment. On a donc un paiement qui va de plus en plus vite, dans un contexte de fraude de plus en plus complexe, où les fraudeurs ne sont plus des fraudeurs « petit bras » mais jouent à armes égales avec nous et d'autant plus sur l'IA (tout le monde a accès à ChatGPT).

Luis, derrière cette réglementation qui pousse à l'instantanéité, vous avez développé des outils qui permettent de détecter la fraude de plus en plus vite. Comment faites-vous ? Quelles sont les perspectives ? Où on en est aujourd'hui ?

Luis Junes

Je vais redescendre un peu sur le concret et sur les techniques qui marchent bien pour la détection de la fraude en temps réel.

Dans le *machine learning*, il y a plusieurs méthodes qui ont été déjà évoquées : l'apprentissage supervisé et non supervisé, mais aussi le choix de l'algorithme, qui est un élément-clé. Pour permettre la détection en temps réel, il faut choisir un algorithme à la fois explicable (conformément à la réglementation européenne) et performant.

Un deuxième élément encore plus important dans un contexte de temps réel est l'infrastructure sur laquelle les modèles vont tourner. Un composant-clé est ce qu'on appelle le *streaming engine*. Les modèles ont besoin des paramètres. Si on parle de fraude, un modèle reçoit des paramètres et des analyses qu'il faut être capable d'expliquer. C'est à l'algorithme de choisir et après, on va définir s'il y a fraude ou pas. La capacité à envoyer des paramètres en temps réel, qui sont à jour et encapsulent le comportement des consommateurs en temps réel, avec des fenêtres de temps qui peuvent aller jusqu'à une année, est fondamentale, surtout dans un contexte de paiements instantanés.

Jennifer Serfati

Merci Luis.

Brice, Advanthink est reconnu sur la Place depuis des années pour la détection de la fraude. Comment, avec l'IA, peut-on améliorer encore des modèles qui fonctionnent déjà très bien aujourd'hui ?

Brice Perdrix

L'IA est un formidable outil pour les différents métiers dans les organisations, avec un premier cas d'usage très connu qui est la détection des fraudes. Aujourd'hui utiliser l'IA est indispensable pour être à l'état de l'art quand on est responsable de la fraude aux paiements dans une institution financière.

La pertinence de l'apport de l'IA dans la détection de fraude est centrée sur la capacité de l'organisation à adopter les derniers outils et avoir confiance dans leur utilisation, à les déployer et à les faire évoluer en conditions opérationnelles.

Un exemple : Dans la détection de fraude, on est aujourd'hui face à des organisations de fraudeurs qui utilisent massivement des LLM sur des *deepfakes*, etc. Lorsqu'on met en place une contre-mesure basée sur l'IA, le lendemain, l'équipe d'en face est déjà en train d'adapter sa stratégie pour vous attaquer. Il faut donc avoir des responsables fraudes qui ont confiance dans ce qui va être déployé, et qui ont la capacité à anticiper. En IA on parle alors de *drift :* C'est aussi un enjeu de porter ces concepts mathématiques liés à l'IA dans des métiers pour que ceux-ci puissent les adapter au quotidien.

Mon deuxième point est que l'IA est aujourd'hui un secteur de recherche extrêmement dynamique en termes de nouveaux algorithmes mais surtout, en termes de disponibilité des données et de puissance de calcul. Aujourd'hui, la plupart des institutions financières ont adopté ces stratégies et arrivent à les utiliser en temps réel : on parle d'un scoring en 1 à 2 millisecondes sur 100% des paiements français.

Enfin, il faut comprendre que le passage à l'échelle industrielle de nouvelles techniques d'IA ne réside pas que dans la partie recherche. On peut avoir le meilleur algorithme du monde, mais pour que celui-ci passe en production dans une banque, il y a beaucoup d'autres choses

à anticiper qui relèvent de la confiance, de la conformité, de la mise en place d'une organisation de gestion du risque dont l'IA devient l'un de ses outils de base.

Jennifer Serfati

Merci Brice.

Si on considère le parcours client, aujourd'hui le maillon faible dans la chaîne du paiement, c'est souvent l'humain. Et on ne va pas remplacer un humain qui va acheter un produit sur un site de e-commerce par une machine. Luis, comment faire (grâce aux technologies) pour contrer ce maillon faible qu'est l'humain au moment de l'achat ?

Luis Junes

Les modèles ont besoin de données pour apprendre, pour modéliser le comportement d'un consommateur. Dans un contexte d'e-commerce, il y a plusieurs moments où on peut effectuer les contrôles de fraudes : au niveau du marchand, on peut déjà faire une analyse de la transaction ; au niveau de l'acquéreur ou du processeur, on peut faire un deuxième contrôle, spécialement au niveau de l'autorisation de la transaction.

Il y a plusieurs types d'arnaques au faux conseiller. L'arnaqueur appelle la victime et lui dit « Nous avons a constaté que votre compte a été victime d'une fraude. Nous vous conseillons de faire des virements vers un compte sécurisé ». Les fraudeurs sont assez malins : connaissant les seuils, ils disent « Faites plusieurs virements de 2 000 euros ou un peu moins de 2 000 euros ».

Comment contrer cela ? Au moment où la victime va effectuer les virements depuis son application mobile, on va détecter la première transaction (par exemple 2 000 euros) et détecter que la durée de la connexion est plus longue que la normale. Habituellement, quand cette personne se connecte, elle effectue sa transaction en 50 ou 60 secondes, mais ici, la connexion dure nettement plus longtemps. On va aussi détecter des signaux, comment la personne interagit avec l'appareil : il y a beaucoup de mouvements inhabituels. On peut éventuellement détecter un appel actif, c'est-à-dire détecter que c'est le fraudeur qui est en train d'appeler la victime.

En même temps, quand la transaction est initiée, on va aussi mélanger ces données-là avec l'historique transactionnel de la personne : la victime, a fait déjà un virement de 2 000 euros, mais c'était il y a 6 mois, et en outre le bénéficiaire vient d'être ajouté 2 ou 3 minutes avant. Donc, on construit une « histoire » autour de la transaction. Il n'y a pas de certitude qu'il s'agit d'une arnaque, mais cela donne des indices pour avertir la personne qu'elle est peut-être victime d'une arnaque.

Après, la personne peut toujours contrôler la transaction. En cas d'arnaque au sentiment, si la personne est vraiment convaincue qu'elle va envoyer de l'argent à son chéri, on ne peut rien faire.

Jennifer Serfati

Merci Luis.

Ces dernières années, on a vu une explosion du e-commerce mais aussi de l'omnicanalité. Brice, comment l'IA peut-elle aider l'entreprise à gérer l'omnicanalité (Par exemple, un achat en e-commerce et un remboursement en boutique) ?

Brice Perdrix

Ce n'est pas forcément l'IA, c'est plutôt comment, dans une organisation, voir la fraude comme un outil de pilotage de l'expérience-client. Aujourd'hui, avec les approches massivement omnicanal, il est important de mettre en place d'un hub fraude de gestion de l'expérience client via les différents canaux d'interaction avec le client.

Être *customer-centric* dans la gestion de la fraude, c'est avoir la capacité non seulement d'arrêter des fraudeurs, mais surtout de piloter une expérience client omnicanal, donc d'être capable de croiser facilement, par exemple, une souscription de compte avec un enrôlement de nouveaux *devices*, un enregistrement de bénéficiaire puis l'émission d'un paiement carte.

Aujourd'hui, dans l'omnicanalité, l'ouverture ou non de nouveaux services, la complexification d'un parcours sur une application, ça va être aussi des scorings d'IA qui vont avoir vocation à activer ou non une vérification supplémentaire de l'identité de la personne. Ceci se traduira par un coût pour la banque et une complexification de l'expérience client à optimiser.

Jennifer Serfati

Merci Brice.

Nous approchons de la conclusion de notre table ronde.

Yann, j'imagine que tous tes prospects veulent mettre de l'IA « du sol au plafond ». Quels sont les cas d'usage pour ceux qui signent et quels sont les freins pour ceux qui ne signent pas encore ?

Yann Chassy

Sur les marchés militaires ou santé, ça signe et ça passe à l'échelle beaucoup plus vite. Sur les banques ou sur le retail, c'est beaucoup plus lent.

Aujourd'hui, les IA explicatives et prédictives présentent un ROI très fort face aux IA génératives. Il y a un effet « pschitt » sur le génératif du fait du constat de tous ceux qui ont signé ces dernières années ou derniers mois, constatant des phénomènes d'hallucinations, de fuite de données. Et surtout, on ne comprend pas ce qu'il y a sous le capot.

Les projets qui commencent à passer en production et qui marchent sur vos data, avec des RAG, des moteurs de contraintes, avec PapAI, nous allons baliser toutes les data qu'on va enregistrer dans votre LLM. C'est nécessaire pour des militaires en opération : je ne peux pas leur dire de passer à droite alors qu'il y a des missiles qui arrivent, mais plutôt leur donner des éléments de contexte pour que l'humain garde la décision sur l'IA.

Jennifer Serfati

Merci Yann.

Thomas : IA, opportunité ou menace ?

Thomas Dognin

Opportunité avec menace, donc il n'y a pas d'IA sans gouvernance. Cela me fait penser à cette banque qui, en 2021, a mis en place un système de gouvernance sur la plateforme IBM Watsonx, car Watsonx avait été fournisseur de services d'IA, supervisés et non supervisés, et ils se sont dit « il y a risque ». Donc, quand j'implémente l'innovation, j'implémente forcément la gouvernance dans une dynamique de confiance et de responsabilité.

Quelle gouvernance ? Pas la gouvernance de l'IA, mais la gouvernance du risque lié à l'IA. Cela induit des mécanismes bien connus dans les banques, de supervision des risques opérationnels liés aux modèles et liés aux impacts de ces modèles. Donc, il n'y a pas d'IA possible sans gouvernance, et de toute façon, l'IA Act vous l'imposera.

Jennifer Serfati

Merci Thomas.

Brice : IA, opportunité ou menace ?

Brice Perdrix

Dans la spécificité de la fraude, on voit une généralisation de l'IA générative, des LLM. C'est aujourd'hui principalement une menace sur la lutte contre la fraude, parce que c'est un super outil qui est dans la besace des fraudeurs pour générer facilement une fausse vidéo de votre président qui vous appelle pour un virement de 200 000 euros en urgence, ou pour faire dans toutes les langues des mails quasiment parfaits de demande de connexions à votre plateforme étatique, alors qu'on a vu que pour faire de la détection de fraude en temps réel on a un enjeu de confiance énorme.

L'IA, c'est aussi une opportunité, car à côté de toute cette vague sur l'IA générative, il y a tout le reste qui représente 90% du marché de l'IA dans le monde, le scoring prédictif pour des cas d'usage business, où on voit effectivement des superbes innovations au quotidien, et surtout

une maturité qui est en train de monter dans les banques pour faire de l'IA un outil du quotidien.

C'est donc une superbe opportunité pour la banque pour transformer son expérience client et déployer des nouveaux services tout en respectant ces enjeux réglementaires et de rempart sécuritaire pour le citoyen. À travers l'IA, un formidable terrain de jeu est en train de se déployer dans les banques.

Jennifer Serfati

Merci Brice.

Luis : dans 5 ans, que sera l'IA dans notre quotidien ?

Luis Junes

Dans les 5 ans à venir, on verra un écosystème se développer, pas forcément des LLM mais des modèles multimodaux : de la vision, du langage, du son, qui seront connectés à des API pour permettre l'exécution des tâches au quotidien.

J'ajouterai qu'en réfléchissant à cette question, deux points importants m'ont frappé :

- La plupart des méthodes et techniques qu'on utilise aujourd'hui existent depuis plus de 60 ans. Il y a eu dans les années 1950-60 une époque qu'on appelait « l'hiver de l'IA ». Pourquoi peut-on parler d''IA aujourd'hui ? C'est grâce à l'avancée dans la partie hardware et dans le traitement des données : pour l'instant, l'innovation dans l'IA n'est pas encore là.
- Je n'ai pas besoin de montrer à mes enfants 10 milliards de photos pour qu'ils sachent reconnaître un chat d'un chien. Il y a encore du progrès à faire pour créer un modèle qui ait juste besoin de deux ou trois photos. Ceci montre tout ce qu'il reste à faire.

Jennifer Serfati

Merci beaucoup.

Hervé Sitruk

Au sein de France Payments Forum, nous avons un groupe de travail Sécurité et Lutte contre la fraude (SLF) qui aborde les moyens de contrer la fraude avec l'IA. Ce groupe va continuer à fonctionner car dans ce domaine de la lutte contre la fraude, nous voulons apporter des réponses concrètes et faire des propositions, y compris à l'OSMP. C'est notre rôle d'aiguillon, mais c'est aussi un moyen de soutenir le développement de ce marché.

À côté du GT SLF, nous allons créer une réflexion sur l'IA dans les paiements au sein du GT Perspectives Innovations et Relations Fintechs animé par Jennifer SERFATI et Benoît OUINAS,

pour que les réflexions sur les stratégies IA dans les paiements se développent et que vous-mêmes ayez tous une culture assez forte dans ce domaine, afin que nous puissions élaborer ensemble un certain nombre d'orientations, de propositions par rapport à l'IA dans les paiements.

Dans son intervention, le ministre Arnaud Montebourg a parlé de MiCA. MiCA est une réglementation qui a tué beaucoup d'activités en développement dans les crypto-payments en Europe : MiCA a tout verrouillé, et le marché n'a pas suivi.

Il faut donc que nous soyons force de propositions pour faire que les réglementations européennes apportent bien sûr une sécurité et un encadrement des pratiques, pour protéger tout un chacun contre des usages abusifs, mais permettent également le développement du marché. Ce qui est parfois oublié.

Merci à tous.

****