Pourquoi l'intelligence artificielle est indispensable aux technologies modernes d'identité et de sécurité

CONTRÔLE D'ACCÈS
IDENTITÉ
VOYAGE
JUSTICE ET SÉCURITÉ PUBLIQUE

POSTÉ LE 27.04.23

L'utilisation de l'intelligence artificielle (IA) a un réel impact sur la société d'aujourd'hui. Nous commençons tout juste à en récolter les bénéfices et à aborder les défis qui y sont associés. Les cas d'usage des technologies d'IA deviennent de plus en plus répandus à mesure que les algorithmes d'apprentissage profond nous aident à résoudre des problèmes de plus en plus complexes. Appliquées aux domaines de l'identité et de la sécurité ces technologies ont permis des avancées considérables au cours de la dernière décennie, des avancées qui n'auraient pas été possibles sans une supervision humaine.

Ce qu'est l'IA, et ce qu'elle n'est pas

Briser le mythe des technologies d'IA

Soyons clairs sur une distinction importante : l'IA permet à une machine d'*apprendre* par elle-même, mais elle ne peut pas former une machine à *penser* par elle-même. **Alors, que désigne-t-on exactement par intelligence ?** Si l'on remonte à la racine latine du mot, il s'agit de la capacité à *comprendre*, une capacité propre à l'humain et indissociable de sa capacité à *penser*. Aussi troublantes que puisse être les prouesses de certaines applications récentes de l'IA désormais à la portée du grand public, il faut donc bien se garder de faire trop vite l'amalgame entre intelligence humaine et intelligence artificielle.

Le terme « intelligence artificielle » remonte aux années 1950, lorsque les experts étaient enthousiasmés par les progrès rapides des ordinateurs. Pendant des décennies, ce qui passait pour des « machines intelligentes » était en fait une programmation très élaborée qui permettait aux ordinateurs d'effectuer des tâches pré-formatées, comme jouer aux échecs, par exemple. Bien que constituant une véritable révolution à l'époque, ces ordinateurs étaient encore loin d'être de véritables sources d'intelligence (ou de compréhension).

Aujourd'hui, les technologies d'IA apprennent en passant au crible des tas de données et en **tirant des conclusions sur la base de modèles récurrents**. Elles apportent ainsi des clés de compréhension aux humains, mais elles ne sont toujours pas dotées de la capacité de *penser* et donc de *comprendre* par elles-mêmes leurs propres conclusions.

Pour apprendre et tirer des conclusions, les IAs utilisent des algorithmes (des guides étape par étape) pour accomplir des tâches dans un cadre prédéfini et pour répondre à des besoins spécifiques. Pour être une réelle source de compréhension (et donc d'intelligence), **cet apprentissage ne peut être réalisé qu'en partenariat avec des humains, jamais par la machine seule.**

In fine, la véritable source de l'intelligence reste humaine. C'est l'intelligence humaine qui, en amont, comprend le problème à résoudre et en défini le cadre. C'est elle également qui, en aval, est capable de tirer les enseignements de l'apprentissage et des conclusions apportées par la machine. En fait, l'intelligence artificielle est plus **un prolongement de l'intelligence humaine**, qu'une intelligence en soi.

En somme, les technologies d'IA sont un formidable outil au service de l'intelligence humaine. Elles ouvrent la voie à l'automatisation et à une prise de décision plus rapide, mais une supervision humaine est, et restera toujours, indispensable.

La technologie derrière le concept

L'apprentissage automatique (ou *machine learning* en anglais) est la technologie de base de l'IA. Elle consiste à apprendre aux ordinateurs à trouver de manière autonome des informations dans des ensembles de données. Une fois qu'une machine a reçu un exemple, elle peut passer les données au crible, trouver des modèles et des corrélations sur la base de ce qu'elle a appris. Lorsqu'une machine commence à tirer les bonnes conclusions, elle peut alors appliquer ces apprentissages à de nouveaux ensembles de données. L'algorithme s'adapte et s'améliore au fur et à mesure qu'il traite davantage de données.

L'apprentissage profond (ou *deep learning* en anglais), quant à lui, est un sous-domaine de l'apprentissage automatique. Il imite l'architecture des **réseaux de neurones** du cerveau humain. À la différence de l'apprentissage automatique qui s'appuie sur un exemple, les réseaux de neurones d'apprentissage profond s'appuient sur plusieurs couches de traitement (d'où le terme « profond ») pour identifier des modèles, classer des informations ou reconnaître des paroles, des images, etc. Les algorithmes d'apprentissage profond traitent des quantités incroyables de données brutes et c'est ainsi qu'ils apprennent et s'améliorent.

L'apprentissage profond : un changement de paradigme

Ces dernières années, les algorithmes d'apprentissage profond ont permis aux technologies d'IA de pénétrer d'innombrables marchés et industries. Aujourd'hui, il serait difficile de trouver un secteur (ou même une personne) qui ne s'appuie pas sur des solutions d'IA dans un domaine ou un autre de son activité ou de sa vie quotidienne. Mais d'où vient cet engouement ? C'est en grande partie nos propres habitudes de consommation qui ont poussé l'apprentissage profond au premier plan. Les appareils connectés, les villes intelligentes, l'IoT en général et nos habitudes en ligne : toutes ces avancées technologiques produisent une **abondance de données détaillées** et provenant d'un ensemble incroyablement diversifié de sources. Cette grande quantité de données, associée à une **augmentation notable de la puissance des ordinateurs** à partir des années 1980, à des algorithmes plus avancés et à une technologie devenue suffisamment mature au début des années 2010, a ouvert la voie à une manière plus efficace d'apprendre.

La capacité de trier des quantités massives de données, apportée par l'apprentissage profond, augmente les performances de manière exponentielle : **les problèmes peuvent désormais être modélisés avec des millions de paramètres**, ce qui approfondit le processus d'apprentissage et fournit des réponses à des problèmes plus complexes que jamais. L'exécution de tâches telles que la reconnaissance de formes ou la compréhension de la parole est devenue incroyablement efficace, ce qui a donné un coup d'accélérateur à des domaines entiers.

Pourquoi les algorithmes d'IA actuels sont-ils si efficaces ?

La puissance de la technologie d'apprentissage profond

L'être humain peut souvent être submergé par des volumes colossaux de données et, seul, il n'est capable d'en

exploiter qu'une partie limitée, ce qui laisse de grands volumes de données inutilisés. La technologie d'apprentissage profond, en revanche, est extrêmement extensible. De par sa conception, le réseau de neurones de l'apprentissage profond devient plus efficace avec l'ajout de nouveaux neurones. Cela signifie que les machines peuvent **absorber une quantité illimitée de nouvelles données**. Au lieu de provoquer une saturation, les vagues de données améliorent en fait les performances. À mesure que le réseau se développe, les performances augmentent et les modèles deviennent capables de traiter des problèmes de plus en plus complexes. L'apprentissage profond est également **un processus itératif**, ce qui signifie qu'il s'agit d'un système dynamique et qui s'adapte en permanence aux nouvelles données **pour trouver une meilleure réponse**. C'est encore une façon pour l'apprentissage profond d'imiter l'esprit humain : **comme nous, les algorithmes d'apprentissage profond s'améliorent avec l'expérience**. Mais la comparaison s'arrête là.

L'importance des données (et de leur précision)

La technologie d'apprentissage profond nécessite d'immenses quantités de données: **plus les données sont nombreuses, mieux c'est**. Mais pas n'importe quelles données. La collecte des données doit être **précise et exempte d'erreurs** pour que les résultats soient corrects et impartiaux. Elle doit également être **pertinente**. Autrement dit, les données doivent être obtenues sans perdre de vue le problème à résoudre et il est nécessaire de *comprendre* les applications envisagées afin de développer des outils technologiques en conséquence. L'importance des données est montée en flèche ces dernières années. Elles sont devenues un véritable avantage concurrentiel pour ceux qui les obtiennent et les utilisent correctement. Ce dernier point est essentiel : les données sont avant tout **une ressource précieuse qui doit être protégée**. Un cadre clair concernant l'éthique qui sous-tend la manière dont les données sont recueillies, stockées et utilisées est de la plus haute importance, surtout si l'on considère la manière dont l'utilisation des données a évolué et continuera d'évoluer au fil des ans.

Comment les solutions d'IA aident les humains

L'IA, une alliée essentielle

Si le concept d'IA s'inspire de l'esprit humain, **les algorithmes d'apprentissage profond distinguent les modèles plus aisément que nous**, ce qui facilite le processus de prise de décision et permet une automatisation sans fatigue. L'IA est capable à la fois de mener à bien des tâches qui dépassent le champ d'action des ordinateurs traditionnels, tout en accomplissant des tâches fastidieuses et chronophages plus rapidement et de manière plus systématique que les humains. Concrètement, **les solutions d'IA permettent d'améliorer la prédiction, la détection et le tri dans tous les domaines** (par exemple pour la détection et la reconnaissance d'objets), **libérant ainsi un temps précieux pour des tâches à valeur ajoutée**, qui, elles, requièrent l'intelligence humaine.

Les avantages des technologies d'intelligence artificielle sont indéniables lorsqu'il s'agit d'analyser de grands volumes de données. Qu'il s'agisse d'analyser des itinéraires et d'identifier des modèles pour améliorer l'efficacité du service et l'expérience des utilisateurs dans le secteur des transports, de passer au crible les données d'appareils de santé portatifs pour améliorer les soins et les diagnostics dans le domaine médical ou de personnaliser le marketing et l'expérience d'achat dans le secteur de la vente au détail, les cas d'usage innovants de l'IA se multiplient dans tous les secteurs et toutes les industries. Les institutions financières et les organismes gouvernementaux s'appuient également sur les solutions d'IA pour détecter les fraudes et protéger les citoyens et les entreprises. **Grâce aux renseignements fournis par l'IA, les décideurs sont mieux informés pour prendre les bonnes décisions.**

Comment les algorithmes d'IA aident à éliminer les discriminations

Les biais dans la biométrie font l'objet de nombreuses discussions. En effet, dans la communauté scientifique, il existe un domaine de recherche entier consacré à « l'équité dans les systèmes d'apprentissage automatique » visant à mesurer, comprendre et atténuer les biais. Mais en réalité, **les biais sont bien plus répandus dans la nature humaine et dans la société en général que dans des algorithmes équilibrés et précis**. En fait, les algorithmes d'aujourd'hui représentent une solution viable à ce problème du monde réel. Cela étant dit, il est essentiel de se rappeler que les solutions d'IA doivent toujours être **combinées à l'analyse et à la décision humaine**. Dans le cas des autorités chargées de l'application de la loi, de la justice ou des frontières qui utilisent des technologies d'IA, la décision finale revient toujours aux personnes assermentées et autorisées par la loi à prendre la décision. **Les technologies d'IA ne sont qu'un soutien à l'humain pour accomplir une tâche, l'accélérer, tout en réduisant le risque d'erreur.**

L'industrie de l'identité et de la sécurité a fait des progrès considérables pour réduire les biais dans la reconnaissance biométrique. Notamment, au cours des dernières années, les tests indépendants menés par le National Institute of Standards and Technology (NIST) ont montré que les différences de performance des algorithmes d'identification biométrique entre les groupes démographiques peuvent être réduites à un point tel qu'elles sont **pratiquement indétectables**. Les meilleures technologies de reconnaissance faciale par IA se distinguent dans ces tests en combinant équité et précision.

Il est important de souligner que pour atteindre cet équilibre, **ces algorithmes n'apprennent pas d'eux-mêmes une fois déployés** et que les humains gardent le contrôle sur leurs performances. Les développeurs mesurent les taux d'erreur des algorithmes sur différents groupes, appliquent des mesures correctives et veillent à ce que l'équité soit toujours un critère déterminant.

Grâce à la capacité d'identifier tous les sujets de la même manière, indépendamment de leur groupe démographique, les technologies d'IA développées de manière responsable et éthique peuvent en fait **aider les humains à réduire les risques de discrimination**.

Comment l'apprentissage profond renforce-t-il les technologies d'identité et de sécurité ?

Biométrie

Les progrès de l'IA ont révolutionné le domaine de la biométrie. La capacité à modéliser des problèmes plus complexes et à traiter plus de données beaucoup plus rapidement a considérablement relevé la barre en termes de performances et de précision. Pour commencer, la simple quantité de données disponibles combinée aux capacités de calcul apportées par l'apprentissage profond rendent les algorithmes biométriques plus précis que jamais. Si les avancées dans le domaine de la **reconnaissance faciale** offrent sans doute le meilleur exemple de l'impact de l'IA sur la biométrie, l'apprentissage profond a également permis de faire progresser la **reconnaissance des empreintes** digitales et ne fait encore qu'effleurer le **domaine de l'iris**.

Au début, les algorithmes de reconnaissance faciale n'étaient en mesure d'identifier un visage que lorsque celui-ci était placé directement devant un terminal biométrique. Les progrès dans ce domaine, principalement dus à l'efficacité accrue de l'IA, ont permis d'**améliorer l'expérience des utilisateurs**.

La technologie actuelle de reconnaissance faciale par l'IA exige très peu de l'utilisateur pendant que son identité est vérifiée. Le procédé est **plus rapide, plus efficace et complètement fluide**. Par exemple, le visage d'un utilisateur peut être analysé avec précision, qu'il soit en mouvement ou statique, qu'il porte des lunettes ou qu'il sourit, qu'il soit face au terminal biométrique ou qu'il regarde dans une autre direction. Les algorithmes d'IA peuvent même vérifier la présence réelle du visage sans demander au sujet de prendre une pose ou de faire un mouvement spécifique.
La détection du vivant, c'est-à-dire la capacité de confirmer que le visage ou l'empreinte digitale analysés sont, en fait, réellement présentés, en personne, par leur véritable propriétaire (par opposition à une photo, un masque en silicone ou une fausse empreinte digitale), **améliore considérablement les systèmes de lutte contre la fraude**.

En ce qui concerne la reconnaissance des empreintes digitales, la technologie d'apprentissage profond permet de **lire plus efficacement les empreintes, même celles qui sont endommagées**. Elle permet également de vérifier avec

précision une identité avec un **système de contrôle d'accès entièrement sans contact**.

Contrôle d'accès fluidifié

Les systèmes de contrôle d'accès actuels peuvent également s'appuyer sur les données biométriques faciales pour **identifier à distance les visiteurs et les employés** lorsqu'ils entrent dans un bâtiment. Des algorithmes avancés peuvent créer une expérience d'identification biométrique véritablement transparente en permettant **la reconnaissance en mouvement** tout en garantissant la plus grande précision. La force de cette technologie réside dans la capacité des algorithmes d'IA à analyser l'ensemble de la situation autour des points d'accès, permettant à la fois de gérer des groupes et de détecter des comportements suspects.

Tout comme le monde en général s'oriente de plus en plus vers les méthodes sans contact, il en va de même pour le domaine du contrôle d'accès. Concrètement, l'utilisation d'un système de reconnaissance faciale par IA signifie qu' **aucun contact direct n'est nécessaire** avec un équipement de contrôle d'accès, une alternative bien plus hygiénique dans un climat post-pandémique.

Authentification des documents

Un autre exemple concret de la technologie d'apprentissage profond à l'œuvre est la vérification d'un large éventail de documents, comme des passeports, des permis de conduire, des visas, des documents d'immigration, des documents fiscaux, des cartes d'électeur, etc. Les algorithmes d'apprentissage profond peuvent détecter des documents placés sur un scanner ou devant la caméra d'un téléphone, identifier le type de document, lire le texte et les images, et s'assurer de leur authenticité, en vérifiant qu'il ne s'agit pas d'un faux document ou d'une photocopie, par exemple.
Cela signifie analyser les polices de caractères, les éléments de sécurité tels que les hologrammes, les filigranes et les codes à barres, et être capable d'identifier les manipulations d'images, les altérations de pixels, les altérations numériques et d'autres types de falsifications. L'IA est ici une ressource inestimable : elle vérifie simultanément tous les éléments de sécurité d'un document de manière plus efficace, plus rapide et plus sûre que jamais auparavant.
L'IA est capable de réaliser tout cela sur une multitude de documents, même à distance : une tâche sur laquelle même l'esprit humain le plus entraîné ne peut rivaliser.

Quelles sont les applications de l'IA en matière d'identité et de sécurité ?

Que vous en soyez conscient ou non, l'IA est à l'œuvre dans divers aspects du quotidien, que ce soit pour les entreprises, les organismes publics ou les utilisateurs finaux. En faisant progresser la biométrie, l'analyse d'images et les systèmes de lutte contre la fraude, les solutions d'IA contribuent à protéger les identités, à simplifier leur vérification et à rendre le monde un peu plus fluide.

Vérification des identités et détection des fraudes dans tous les environnements

L'IA est présente dans toutes les situations où un niveau avancé de vérification d'identité et de détection de la fraude est nécessaire, que ce soit en personne ou en ligne :

- **Respect des règles de connaissance du client en ligne** pour les opérateurs mobiles, les institutions financières, les secteurs réglementés, etc.
- **Accès sécurisé aux services gouvernementaux en ligne**, à la santé, à l'éducation, etc.
- **Contrôle d'accès** pour les logements privés, les immeubles de bureaux et les sites industriels sensibles.
- **Amélioration de l'expérience utilisateur, du flux de passagers et du contrôle des frontières** dans tous les environnements de voyage, que ce soit par voie aérienne, terrestre ou maritime.

Prenons un exemple spécifique d'apprentissage profond à l'œuvre dans un processus de prise de décision : la

facilitation du flux de passagers. Ici, **toute une chaîne d'algorithmes d'IA est nécessaire à chaque étape d'un processus de vérification d'identité automatisé**. La première étape est la **détection et le suivi**. Par exemple, il s'agit de comprendre tous les éléments du flux vidéo provenant d'un portail automatique ou de localiser l'iris sur le visage d'une personne. Vient ensuite l'**évaluation de la qualité**, qui consiste à trouver les meilleures images à utiliser à des fins biométriques. Ensuite, la constitution d'un template (ou modèle) biométrique, c'est-à-dire l'**extraction des informations pertinentes** de l'image. Enfin, la **reconnaissance**, c'est-à-dire la mise en correspondance de données similaires. Dans cet exemple, les algorithmes d'apprentissage profond confirment l'identité d'un passager lorsqu'il scanne son passeport lors de l'enregistrement et lorsqu'il se présente devant une caméra à une porte automatique pour un dernier contrôle biométrique avant l'embarquement.

En résumé, l'IA compare la photo d'un passeport (et vérifie que la photo n'a pas été falsifiée) avec l'image en direct pour déterminer que la personne est bien celle qu'elle prétend être, **le tout en quelques secondes**.

Analyse intelligente des données pour une sécurité renforcée

Si le cadre juridique concernant l'utilisation de l'IA pour assurer la sécurité publique soulève des questions éthiques légitimes dans le monde entier, et continuera à évoluer, les solutions d'IA ont été et continueront à être **incroyablement utiles dans des situations très précises**. Tout d'abord, pour identifier les victimes de crimes ; ensuite, pour rechercher des personnes condamnées ou soupçonnées de délits majeurs ; et enfin, en cas de menace grave ou immédiate pour la sécurité publique. Dans ces situations, l'IA peut être utilisée pour extraire automatiquement des visages, l'image de véhicules ou d'autres objets apparaissant sur des séquences vidéo afin de déclencher des alertes automatiques lorsqu'ils sont détectés. **Elle donne un sens à toutes les données disponibles, économise du temps, des ressources et de l'argent**, tout en réduisant les erreurs humaines.

En quoi l'éthique et la responsabilité sociale sont inextricablement liées aux technologies d'IA

La technologie est formidable, mais tout l'enjeu est dans la façon de l'utiliser

La technologie n'est pas bonne ou mauvaise en soi, tout dépend de la manière dont on la met en œuvre. Dans le secteur de l'identité et de la sécurité (où l'on utilise, par exemple, des machines pour vérifier des identités en s'appuyant sur des données biométriques), l'éthique est un facteur extrêmement important. Afin d'apaiser les inquiétudes légitimes du public et de créer la confiance, le secteur doit être vigilant et se tenir responsable de la mise en œuvre de ces technologies révolutionnaires. **Des règles strictes doivent être appliquées**. Par exemple, la supervision humaine est essentielle. Si les technologies d'IA ont permis à l'industrie de progresser à pas de géant, nous ne pouvons pas oublier qu'il existe une réelle différence entre une machine et un humain. Les gouvernements et des organismes tiers sont également intervenus en ce sens pour mettre en place **des cadres réglementaires** afin de garantir une utilisation responsable de la technologie.

Développer la confiance en contrôlant la machine

La mise en œuvre d'**un processus industriel avec des tests et des validations**, à chaque étape, est une partie importante du développement de technologies qui reposent sur des algorithmes d'apprentissage profond. Par exemple, la façon dont les machines apprennent doit toujours être supervisée par un être humain. Et si l'amélioration des performances est importante, **il est crucial d'identifier et de corriger les biais éventuels**. La tâche est très complexe, mais constitue néanmoins une part primordiale du travail.

La correction des biais est désormais un critère de qualité et de performance

Ces dernières années, la façon dont les performances sont mesurées a nettement évolué. Fait notable, le National Institute of Standards and Technology (NIST) inclut le contrôle de la correction des biais dans ses évaluations de référence en matière de biométrie faciale depuis 20191. Cela signifie que **la correction des biais est non seulement possible, mais qu'elle constitue également un critère qualitatif** lorsqu'il s'agit d'évaluer les performances d'un algorithme d'IA pour la reconnaissance faciale. En fin de compte, les données créent un avantage énorme, mais elles

ont leurs limites. Par exemple, si l'ensemble de données n'est pas assez représentatif, il peut entraîner des biais. Cela s'est produit aux débuts de l'apprentissage profond (certaines des premières expériences d'apprentissage profond sont ainsi tombées dans le piège des biais liés au genre ou à l'ethnie). Ces erreurs ont depuis été corrigées. Aujourd'hui, une base de données peut être analysée grâce aux statistiques, ce qui permet de **détecter un déséquilibre éventuel dans l'ensemble de données utilisé pour l'apprentissage**, puis de le contrebalancer.

Autre exemple d'intervention humaine: afin d'éviter les biais, les programmeurs et les ingénieurs ont réalisé l'importance absolue d'obtenir une **image de haute qualité de toutes les teintes de peau, dans toutes les conditions d'éclairage**. Avec l'aide de l'IA, ils ont créé une boucle de contrôle pour optimiser le gain et régler l'obturateur de la caméra afin de garantir la même qualité d'image quelle que soit la couleur de la peau. Une autre façon d'éliminer les biais est de **travailler directement sur le nombre d'images et d'identités par groupe** dans l'ensemble de données d'apprentissage.

Utiliser des données anonymes pour protéger la vie privée

Face aux préoccupations croissantes concernant la protection de la vie privée, il est important de noter que les acteurs responsables du secteur s'engagent à protéger la vie privée des utilisateurs finaux en utilisant uniquement **des bases de données anonymes** pour entraîner les algorithmes d'IA. D'un point de vue technologique, lors de l'entraînement d'un algorithme de reconnaissance des visages, il n'est pas nécessaire d'attribuer les données biométriques à une personne spécifique. L'algorithme n'a besoin que de photos du même visage sous différents angles, dans différentes conditions d'éclairage, avec différents accessoires ou coupes de cheveux, ou à différents âges. En d'autres termes, **les utilisateurs n'ont besoin que des réponses du système, et non des données** réelles utilisées par les algorithmes d'IA dans le processus de prise de décision.

Pour dissiper toute inquiétude persistante, des autorités et des réglementations en matière de protection de la vie privée, telles que le RGPD en Europe, ont été mises en place afin de définir **des lignes directrices claires pour la collecte et l'utilisation des données**, et de garantir la conformité.

L'IA de demain: que réserve l'avenir pour les technologies de l'identité et de la sécurité ?

Les données du futur

La vague technologique ne cessant de déferler, on peut affirmer sans risque de se tromper que **les volumes de données ne vont cesser de croître** de manière exponentielle. Cela signifie qu'une quantité considérable de données non étiquetées est créée chaque seconde de chaque jour, des données qui ne sont pas encore utilisées à leur plein potentiel. Cette augmentation des volumes de données continuera très certainement à alimenter les modèles et les cas d'usage de l'IA à l'avenir.

Le changement qui se profile à l'horizon est le passage de l'apprentissage **supervisé** (utilisant uniquement des données étiquetées) à l'apprentissage **semi-supervisé** (utilisant des données étiquetées et des données non étiquetées), **faiblement supervisé** (utilisant des étiquettes indirectes) ou même **non supervisé** (utilisant uniquement des données non étiquetées). Ces techniques permettent d'augmenter l'utilisation des données même lorsque les étiquettes ne sont pas disponibles ou trop difficiles à produire. Mais pour couper court à toute ambiguité, que les données soient étiquetées ou non, le *processus d'apprentissage*, tout comme la mesure de ses performances, resteront sous supervision humaine.

Expliquer l'IA

Nous commençons à comprendre ce qui se passe à l'intérieur des réseaux de neurones ; un travail qui va continuer à progresser dans les années à venir. Aujourd'hui, les experts en IA **s'intéressent de plus près à la manière dont les algorithmes d'apprentissage profond parviennent aux conclusions qu'ils tirent**, notamment lorsqu'ils n'atteignent pas le résultat escompté. Cela dit, il est important de se rappeler que si un algorithme permet à une machine d'apprendre par elle-même, il est également soutenu par un processus industriel. Les humains ont toujours la tâche extrêmement

importante de valider, de tester, de mesurer les résultats et de faire tout ce qu'il faut pour garantir l'exactitude des algorithmes. **Nous, les humains, ne pouvons pas simplement développer la technologie et lui laisser libre cours.**

Les engagements d'IDEMIA concernant les technologies d'IA

Chez IDEMIA, l'IA n'est pas simplement un outil pour analyser les données commerciales ou optimiser la logistique comme dans beaucoup d'autres entreprises, elle est **au cœur des solutions que nous développons**. Plus précisément, nous l'utilisons pour permettre à nos systèmes de dégager des informations significatives à partir de données visuelles, et d'agir ou de faire des recommandations en conséquence.

Conformité et confidentialité des données

Avant tout, IDEMIA reconnaît la nature sensible de toutes les données personnelles. **Nous nous engageons à protéger les données, non seulement lors de la phase d'apprentissage des algorithmes d'IA et du développement des solutions, mais aussi lorsque nos solutions sont utilisées sur le terrain.** Nous considérons qu'il est absolument essentiel de s'assurer que nos solutions ne peuvent pas être détournées, altérées ou contournées. À cette fin, nous accordons une attention particulière à la manière dont les données sont traitées et aux réglementations applicables. En fait, bien avant que le RGPD n'existe, nous avions mis en place nos propres processus et infrastructures pour gérer les données personnelles en toute sécurité. Ces processus sont désormais également conformes aux réglementations sur la protection de la vie privée telles que le RGPD en Europe, les réglementations américaines sur la protection de la vie privée ou leurs équivalents dans d'autres régions.

Collecte et utilisation des données

Afin de créer les algorithmes les plus précis, nous devons constamment accéder à davantage de données, et ce, de manière responsable. Nous obtenons des **données de nos clients**, dans le respect des réglementations pertinentes en matière de protection de la vie privée, afin d'entraîner leurs algorithmes et de leur fournir des produits et solutions aux performances avancées. Nous nous appuyons également sur les **données partagées sur la base du volontariat par nos employés** pour alimenter notre base de données année après année. Enfin, nous créons des images synthétiques en utilisant un réseaux antagoniste génératif (RAG, ou GAN en anglais, pour Generative Adversarial Network). Cela nous permet de générer **des images faciales et des empreintes digitales synthétiques** qualitatives et totalement fictives. Ainsi, lorsqu'un client nous demande de partager des données pour tester l'efficacité de nos algorithmes, nous pouvons partager ces données synthétiques.

Notre expertise en cryptographie au service de la protection des données et des systèmes

En tant que leader dans notre domaine, nous nous engageons à créer des solutions qui protègent les données personnelles et garantissent qu'elles ne peuvent pas et ne seront pas utilisées à mauvais escient. Pour ce faire, nous appliquons notre expertise des techniques de cryptographie et des droits de gestion d'accès pour **concevoir des bases de données de telle sorte que les utilisateurs autorisés puissent rechercher une personne particulière dans une base de données sans pour autant leur donner accès à la liste des personnes contenues dans cette base**. Cela signifie que personne ne peut en extraire des données personnelles, ni IDEMIA, ni nos clients, ni les gouvernements, ni quiconque tenterait de s'y introduire. En outre, chaque fois que cela est possible, nous concevons **des solutions et des systèmes pour garantir que les données personnelles ne sont détenues que par leurs propriétaires individuels** (cryptées dans l'élément sécurisé d'un document, d'une carte ou d'un smartphone, par exemple).

Alors que la technologie et les techniques cryptographiques ne cessent de progresser, nous continuons à investir dans de nouveaux moyens pour protéger toujours plus efficacement les données personnelles et garantir un accès restreint à celles-ci.

Véritablement garantir l'inclusion

Aujourd'hui, nous pouvons affirmer avec fierté que **nos algorithmes d'apprentissage profond sont si efficaces que les biais en sont à peine mesurables**

, une affirmation tout aussi audacieuse que rare dans notre secteur. Mais ce n'est pas une mince affaire ! Nos équipes dédiées sont expertes dans le processus complexe qui consiste à préparer les données d'entraînement et à ajuster la façon dont un algorithme apprend sur un ensemble de données déterminé. Elles s'assurent également que nos bases de données contiennent une variété d'images d'un même élément dans diverses conditions d'acquisition afin de garantir une véritable inclusion.

Utilisation éthique des technologies de l'IA : une approche collective

Tous les acteurs de l'écosystème doivent faire leur part pour protéger les utilisateurs. Cela inclut les acteurs industriels comme IDEMIA, les groupes de travail et groupes de réflexion nationaux et internationaux, les universitaires, les régulateurs et les clients utilisant la technologie. Au fil des années, IDEMIA s'est positionné comme **un partenaire privilégié dans l'écosystème français de l'IA**. Nous travaillons en étroite collaboration avec la CNIL et l'Agence Nationale de la Recherche ; nous participons aux ateliers organisés par le *Facial Recognition Project* du *World Economic Forum* ; nous soutenons l'écosystème académique en travaillant avec plusieurs chaires de recherche de haut niveau, notamment sur l'IA. En outre, nous mettons un point d'honneur à **analyser soigneusement la manière dont nos clients pourraient utiliser nos solutions d'IA** et à ne nous associer qu'avec ceux qui respectent nos normes éthiques.

Dans un contexte international de plus en plus compétitif, **nous appelons à une réglementation stricte autour de la collecte de données à des fins de recherche** afin de respecter les normes éthiques, tout en soutenant la compétitivité de l'industrie. Pour l'avenir, nous envisageons de continuer à explorer d'autres pistes, comme la création d'un label pour les « fournisseurs de confiance » au niveau européen par exemple. Lorsque l'on sait que la reconnaissance faciale par l'IA peut être utilisée dans divers contextes gouvernementaux (contrôle des frontières, par exemple), **garantir l'origine de la technologie** n'est pas seulement un élément clé de **la souveraineté nationale**, mais cela soulève des questions sur la performance, la méthodologie, l'éthique, etc. Nous considérons qu'il est impératif de disposer d'une structure qui puisse aider les clients à choisir sereinement la solution technologique la plus adaptée à leurs besoins, sur la base de **critères techniques clairement définis et évalués**. L'objectif final est qu'un jour, les clients utilisant **l'IA « de confiance**, **»** ou plus précisément la technologie qui en résulte, puissent avoir l'assurance qu'elle respecte toutes les normes du secteur.

---

[1] https://www.nist.gov/publications/face-recognition-vendor-test-part-3-demographic-effects

---