

# Cultur'IA

*Pour une intelligence de confiance au service de la sécurité*

n°19

## IA et JO

Mars - Avril 2024



# Edito

Alors que les athlètes se préparent à l'échéance à venir des Jeux Olympiques, il en est de même pour l'intelligence artificielle qui sera expérimentée pour améliorer la sécurité via la vidéo protection. Cultur'IA détaille les divers cas d'usage de l'IA aux JO et les garanties mises en oeuvre pour assurer la protection des libertés individuelles. Au delà de 2024, nous explorons avec Philippe Blanchard, le futur du sport, notamment par son alliance avec la technologie: une découverte surprenante ! Nous sommes également heureux d'accueillir au sein de ce numéro, la sécurité civile, qui nous présente une approche prédictive pour la détection des incendies. Et, nous n'oublions pas nos réservistes citoyens qui nous livrent leur vision sur un sujet d'IA. Mais, tout de suite laissons la place à deux acteurs de l'actualité récente pour répondre aux questions de Cultur'IA: Mistral AI et Chat GPT !

Général Patrick Perrot  
Coordonnateur pour l'intelligence artificielle  
Conseiller IA auprès du ComCyber-MI  
Gendarmerie nationale

**Deux invités exceptionnels répondent aux mêmes questions de Cultur'IA : Mistral AI et Chat-GPT 3.5:**



vs



## Comment l'IA peut-elle être utilisée aux jeux olympiques ?

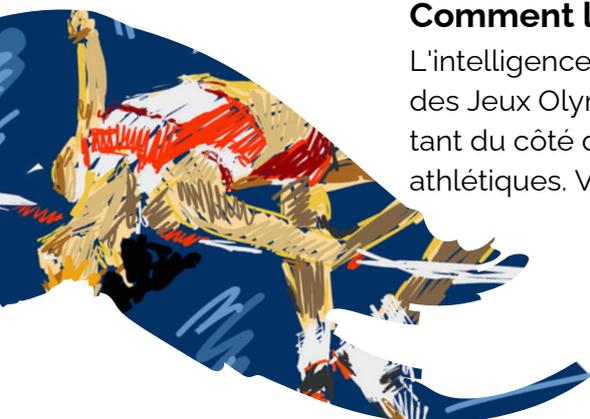
L'IA peut être utilisée de diverses manières aux Jeux olympiques, notamment :

1. Amélioration de la performance des athlètes : L'IA peut aider les athlètes à optimiser leur entraînement en fournissant des analyses détaillées de leur performance, en identifiant les faiblesses et en proposant des exercices personnalisés pour améliorer leur technique.
2. Prédiction des résultats : Les algorithmes d'IA peuvent être utilisés pour prédire les résultats des épreuves sportives en fonction de données historiques et de facteurs tels que la météo, l'état de santé des athlètes et leur performance passée.
3. Détection de fraude : L'IA peut être utilisée pour détecter les fraudes et les comportements suspects, tels que le dopage ou la manipulation de résultats.
4. Sécurité : L'IA peut aider à renforcer la sécurité des Jeux olympiques en détectant les menaces potentielles, en surveillant les foules et en identifiant les comportements suspects.
5. Diffusion et couverture médiatique : L'IA peut aider à améliorer la diffusion et la couverture médiatique des Jeux olympiques en proposant des angles de caméra optimaux, en identifiant les moments forts des épreuves et en fournissant des analyses en temps réel.

En somme, l'IA peut aider à améliorer l'expérience globale des Jeux olympiques pour les athlètes, les spectateurs et les organisateurs en fournissant des informations précises et en temps réel, en améliorant la sécurité et en optimisant la performance des athlètes.

## Comment l'IA peut-elle être utilisée aux jeux olympiques ?

L'intelligence artificielle (IA) peut être utilisée de plusieurs façons lors des Jeux Olympiques pour améliorer divers aspects de l'événement, tant du côté de l'organisation que du côté des performances athlétiques. Voici quelques exemples :



1. Analyse des performances athlétiques : Les données biométriques et les performances des athlètes peuvent être analysées en temps réel à l'aide de capteurs et d'algorithmes d'IA. Cela peut aider les entraîneurs à comprendre les forces et les faiblesses des athlètes, à identifier les domaines à améliorer et à adapter les stratégies d'entraînement en conséquence.
2. Prédiction des résultats : Les modèles d'apprentissage automatique peuvent être utilisés pour analyser les données historiques des athlètes, les performances précédentes et d'autres variables pour prédire les résultats des compétitions. Cela peut être utilisé à des fins de paris sportifs, mais aussi pour aider les entraîneurs à prendre des décisions stratégiques.
3. Optimisation des équipements sportifs : Les fabricants d'équipements sportifs peuvent utiliser des techniques d'IA pour concevoir et optimiser des équipements tels que les chaussures, les vêtements et les équipements de protection. Cela peut aider les athlètes à améliorer leurs performances et à réduire les risques de blessures.
4. Gestion de la logistique et de la sécurité : L'IA peut être utilisée pour optimiser la logistique des Jeux Olympiques, y compris la gestion du trafic, la sécurité des installations et la planification des itinéraires pour les athlètes, les officiels et les spectateurs.
5. Analyse des médias sociaux : Les organisations des Jeux Olympiques peuvent utiliser l'IA pour surveiller et analyser les discussions sur les médias sociaux afin de comprendre les opinions du public, d'anticiper les tendances et de répondre rapidement aux problèmes ou aux préoccupations.
6. Traduction et interprétation : L'IA peut être utilisée pour faciliter la communication entre les participants et les spectateurs internationaux en fournissant des services de traduction et d'interprétation en temps réel.

En utilisant l'IA de manière judicieuse, les Jeux Olympiques peuvent bénéficier de meilleures performances, d'une organisation plus efficace et d'une expérience plus enrichissante pour les participants et les spectateurs.

## **Comment l'IA peut-elle participer à la sécurité des jeux olympiques en France ?**

L'Intelligence Artificielle (IA) peut jouer un rôle significatif dans la sécurité des Jeux Olympiques en France de plusieurs façons :

1. Détection des menaces : L'IA peut être utilisée pour analyser les flux de données provenant des caméras de surveillance, des réseaux sociaux et d'autres sources pour détecter des comportements suspects ou des menaces potentielles. Elle peut identifier des schémas qui pourraient être difficiles à repérer pour les humains.
2. Gestion des foules : L'IA peut aider à gérer les foules en prévoyant les flux de spectateurs et en identifiant les zones de congestion potentielles. Cela peut aider à prévenir les écrasements et à faciliter les évacuations en cas d'urgence.
3. Sécurité des infrastructures : L'IA peut être utilisée pour surveiller l'état des infrastructures, comme les stades et les villages olympiques, et détecter d'éventuels problèmes ou risques.
4. Cybersécurité : Les Jeux Olympiques sont une cible majeure pour les cyberattaques. L'IA peut aider à détecter et à prévenir ces attaques en identifiant les activités suspectes sur les réseaux et les systèmes informatiques.
5. Santé et sécurité des athlètes : L'IA peut être utilisée pour surveiller la santé des athlètes, détecter les blessures potentielles et aider à prévenir le dopage.
6. Prévision et gestion des incidents : L'IA peut aider à prévoir les incidents potentiels, comme les perturbations météorologiques ou les problèmes de transport, et à élaborer des plans pour y faire face.
7. Assistance aux forces de l'ordre : L'IA peut aider les forces de l'ordre en fournissant des informations en temps réel, en identifiant les suspects et en prévoyant les incidents potentiels.

Dans tous ces domaines, il est important de noter que l'IA devrait être utilisée comme un outil pour aider les humains, et non pour les remplacer. De plus, l'utilisation de l'IA doit respecter les lois et les réglementations en matière de vie privée et de protection des données.

## Comment l'IA peut-elle participer à la sécurité des jeux olympiques en France ?



L'intégration de l'intelligence artificielle (IA) dans la sécurité des Jeux Olympiques en France pourrait se faire de plusieurs manières:

1. **Surveillance et Analyse des Données:** Les systèmes d'IA peuvent surveiller en temps réel les flux de données provenant de diverses sources telles que les caméras de surveillance, les réseaux sociaux, les capteurs IoT, etc. pour détecter les menaces potentielles, les activités suspectes ou les mouvements de foule anormaux.
2. **Reconnaissance Faciale:** Les technologies de reconnaissance faciale peuvent être utilisées pour identifier les individus à haut risque ou recherchés dans les zones sensibles, comme les stades ou les zones de rassemblement.
3. **Analyse des Risques:** Les algorithmes d'IA peuvent être utilisés pour évaluer et prédire les risques potentiels en analysant des facteurs tels que les conditions météorologiques, les données de sécurité antérieures, les activités terroristes présumées, etc.
4. **Détection d'Objets et d'Explosifs:** Les systèmes d'IA peuvent être formés pour détecter automatiquement les objets suspects ou les explosifs dans les bagages, les véhicules et les zones de passage.
5. **Surveillance des Réseaux:** L'IA peut être utilisée pour surveiller les réseaux de communication afin de détecter toute activité suspecte, comme des cyberattaques visant à perturber les infrastructures critiques.
6. **Prévention des foules et Gestion du Trafic:** Les algorithmes d'IA peuvent aider à optimiser la circulation des personnes et des véhicules pour éviter les encombrements et assurer une évacuation rapide en cas d'urgence.
7. **Analyse des Menaces sur les Réseaux Sociaux:** L'IA peut surveiller les médias sociaux pour détecter les menaces potentielles ou les intentions malveillantes et permettre une réponse rapide des autorités.
8. **Simulation de Scénarios:** Les modèles d'IA peuvent être utilisés pour simuler différents scénarios de sécurité et évaluer l'efficacité des stratégies de réponse.
9. **Identification des Points Faibles:** L'IA peut analyser les plans de sécurité existants et identifier les points faibles potentiels pour permettre une meilleure allocation des ressources de sécurité.

En combinant ces différentes applications de l'IA, les autorités françaises pourraient renforcer considérablement la sécurité des Jeux Olympiques en anticipant les menaces potentielles, en déployant efficacement les ressources de sécurité et en assurant une réponse rapide en cas d'incident. Toutefois, il est important de souligner que l'utilisation de l'IA dans la sécurité des Jeux Olympiques doit être réalisée de manière éthique et respectueuse de la vie privée des individus.





# Peut-on concilier la technologie (dont l'Intelligence Artificielle) et l'éthique du sport ?

**Philippe BLANCHARD**

La cérémonie de clôture des Phygital Games à Kazan (Russie), qui a réuni du 21 février au 3 mars 2024 près de deux mille participants venus de tous horizons, témoigne des interrogations pour ces nouvelles formes de compétition où le sport se marie à la technologie.

Si la mise en œuvre est actuellement russe, son origine est, elle, française et son développement international.

## **Futurous, le futur du sport**

Dès 2017, inspirés par une vision, celle du sport miroir de nos sociétés, nous nous étions donné un nom : Futurous, la combinaison des mots Futur & us - nous en anglais, et une mission, revisiter le sport sous le signe de la curiosité. Non pas celle du « vilain défaut » mais bien la disposition qui nous pousse à chercher l'intelligibilité du monde, l'appétit intellectuel qui nous fait « prendre soin », la cura des latinistes.

Le sport est effet un microcosme privilégié, qui s'articule dans deux domaines : le sport que l'on pratique et le sport que l'on regarde. Dans tout cet écosystème, une caractéristique permanente : la liaison harmonieuse entre les Lois de la nature (génétique, force de gravité ou de friction, agilité, endurance...) et les Lois de l'homme (cadre réglementaire, règles du jeu, espace public).

Forts de nos précédentes responsabilités au sein du Comité international Olympique, de la FIFA et de Fédérations internationales, nous identifions les évolutions du sport et son devenir : innovations ou évolutions technologiques, sociologiques mais aussi éthiques et réglementaires.

En utilisant la puissance du sport et de la compétition, nous mobilisons les 4 technologies qui structurent notre développement et les mettons en scène dans des compétitions sportives de 5 types (nos 5 « galaxies ») :

1. Technologies de l'information (intelligence artificielle, internet des objets.):
  - Minecraft;
  - Compétitions de esport (e-football, e-basketball, combat games) ;
  - Strategy games (MOBA)
2. Technologies de la mobilité: compétition de mobilité durable, mobilité autonome
  - Green prix : compétition de véhicule ancien rétro-fitted avec des moteurs électriques ;
  - Compétitions de drones : course interactive de drones, combat de drones,
  - Course de skateboard tirés par un drone
  - Course de Unicycle électrique
3. Robotique : haptique, exosquelette, interface cerveau-ordinateur...
  - Concours de robots
  - Combat de robots : poids mouche (1,5 kg), poids plume (13,6 kg), poids lourds (110 kg)
  - Danse Humain et robot
  - Course d'exosquelette
  - Exopentathlon: une équipe concourt dans 5 disciplines (course, agilité, saut, lancer, soulever des poids);
  - Concours de guidage par interface cerveau-ordinateur
4. Environnements virtuels et réalité augmentée : ce que les Russes ont appelé les Phygital Games (Physique et numérique)
  - Interactif Parkour
  - Combinaison sport et esport : basketball ; futsal ; hockey sur glace ; Mixed martial art
5. Nouveaux sports.
  - Surfing sur vague artificielle
  - Self-Propelled Watersports
  - Futurous Relay athletes and para-athletes: 4\*200
  - Danse de groupe dans soufflerie



Notre objectif est de créer de nouvelles activités sportives, initier et développer de nouvelles compétences et activités grâce à la recherche, la formation et des événements innovants.

### **Une collaboration public-privé**

Nos clients et partenaires sont souvent des organisations sportives ou des universités ou des agences publiques. A l'instar de Clémenceau qui considérait que « la guerre est une chose trop grave pour être confiée aux militaires », de plus en plus de territoires pensent en effet que le sport est trop important pour être laissé aux seules organisations sportives.

C'est une évidence. Que l'on observe la France et l'implication du Président de la République, ou de la Maire de Paris, pour les Jeux de Paris 2024 ; l'engagement du Prince héritier du Royaume d'Arabie Saoudite dans le développement du sport et de l'esport ; la rencontre du président du CIO avec le Président Ukrainien ou encore les représentations diplomatiques internationales lors des Phygital Games de Kazan.

Pour être franc, et même si le monde du sport s'en défend, le pouvoir politique a toujours perçu l'intérêt de la valorisation du sport, car il est « une manière d'encadrement idéologique des populations et d'une partie de la jeunesse » (Jean-Marie Brohm). Cette irruption du pouvoir politique interroge les institutions sportives, qui elles voient l'autonomie du sport comme le prérequis essentiel à leur survie.

Et on assiste donc à un paradoxe intéressant : d'un côté, l'institution sportive cherche officiellement un affranchissement du pouvoir politique. Et de l'autre, elle se rapproche des entreprises de technologie car si cette autonomie doit passer par la technologie, elle impliquera alors une négociation avec ses acteurs, la Big Tech.

### **Un engagement pour une Intelligence artificielle éthique**

Prenons l'exemple de l'intelligence artificielle/IA car elle représente aujourd'hui une rupture pour le développement du sport (et pour nos communautés).

- Pour l'athlète et l'entraîneur, elle améliore les conditions d'entraînement (santé et prévention des blessures, analyse et amélioration des performances du compétiteur ou de l'équipe).
- Pour le journaliste, l'IA donne des analyses du jeu ou permet de retrouver des images et des clips (informations non-textuelles) ou encore de générer des sélections de meilleurs moments d'une compétition (« highlights » et « best of »). Ces services enrichissent par ailleurs l'expérience des spectateurs et des fans.
- Pour le comité d'organisation, l'IA, avec sa capacité à analyser d'énormes quantités de données en temps réel, offre des opportunités sans précédent pour comprendre, suivre puis projeter les flux de circulation de la ville hôte.
- Pour les parieurs, elle permet d'affiner les statistiques de prévision des résultats...

Cependant, cette même technologie soulève des défis éthiques considérables. Elle pourrait potentiellement menacer les fondements philosophiques du sport en réduisant les athlètes à de simples exécutants de recommandations algorithmiques, en altérant la compétition par la prévisibilité des résultats ou même en compromettant l'authenticité des performances à travers des manipulations numériques telles que les deepfakes.

Cette question de société déborde de facto du pur cadre sportif et c'est ce que montrent actuellement les analyses de Futurcus. Comme le sport est un laboratoire privilégié de la définition de notre futur, il peut être aussi un espace de réflexion politique, au sens de « polis », la Cité.



## Quelles perspectives pour Paris 2024 et pour la France

Oui, le mariage du sport et de l'intelligence artificielle représente un défi stimulant, une chance de renouveler notre rapport à la technologie.

Oui, avec l'IA, la mobilisation de la puissance publique est un maintenant nécessaire. Car elle est et une « general purpose technology » (transversale à tous les pans de nos sociétés) et une technologie duale (civile et militaire).

À l'approche des Jeux de Paris 2024, puissance publique, institutions sportives, entreprises technologiques et société civile peuvent (doivent ?) s'accorder crucialement sur cette réflexion prospective et philosophique. Pour la France, à la fois territoire-hôte, berceau de l'olympisme et de l'institutionnalisation du sport (création du CIO et de la FIFA), c'est la possibilité de définir un cadre éthique pour l'utilisation de l'intelligence artificielle dans toutes les dimensions du sport. Afin de préserver ses valeurs fondamentales et de contrer les dérives potentielles d'un développement biaisé par la technologie.

En embrassant ces nouvelles perspectives avec sagesse et discernement, nous pouvons revitaliser le sport en tant que catalyseur de progrès humain et de cohésion sociale, tout en préservant son essence et son intégrité et inculquer aux développements en IA les valeurs fondamentales du sport : le respect de l'individu, la prise en compte de ses particularités (biologiques, culturelles ...) et la préservation de notre humanité.

### Nota bene :

Le constat du sport en tant qu'instrument de contrôle social ne date pas d'hier : Juvenal adorait le sport dans sa dimension physique (on lui doit « Esprit sain dans un corps sain ») mais il abhorrait les Jeux du cirque, « Panem et circenses ».

Jugement partagé par Ciceron : « Le mal n'était pas dans le pain et les cirques, en soi, mais dans la volonté du peuple de vendre ses droits en tant qu'homme libre pour un ventre plein et une excitation qui servent à les distraire des autres faims humaines que ni pain et ni cirques ne pourront jamais apaiser ».

C'est la perspective du sport comme spectacle et aliénation, la société du spectacle décrite par des penseurs comme Guy Debord ou par Neil Postman et attaquée par Jean-Marie Brohm : « La saturation de l'espace public par le spectacle sportif atteint aujourd'hui des proportions démesurées. Contenu idéologique dominant, souvent exclusif même, des grands médias, des commentaires politiques, des ragots journalistiques, des conversations quotidiennes, le spectacle sportif apparaît comme une propagande ininterrompue pour la brutalité, l'abrutissement, la vulgarité, la régression intellectuelle et pour finir l'infantilisation » (Article de Jean-Marie Brohm, MediaPart avril 2013).



Philippe Blanchard a été Directeur au Comité international olympique, puis en charge du dossier technique de Dubai Expo 2020. Passionné par les méga-événements, les enjeux de société et la technologie, il dirige maintenant Futurcus, une société de conseil en sport et méga-événements.



## L'IA et les Jeux Olympiques

Après une vision générative et une approche prospective, nous nous intéressons à la réalité de l'exploitation de l'IA aux JO.

**26 Juillet 2024:** Ce jour là s'ouvriront les Jeux Olympiques à Paris. C'est une échéance à laquelle se préparent les athlètes depuis déjà plusieurs années. Ils ont passé diverses sélections avant de pouvoir prétendre à l'or olympique. Ils sont engagés sur une, deux, trois, voire quatre disciplines. Et, leurs performances seront garanties par des contrôles anti dopage afin de s'assurer de la légitimité des exploits.

**26 Juillet 2024:** Ce jour là s'ouvriront les Jeux Olympiques à Paris. C'est une échéance à laquelle se préparent des intelligences artificielles depuis déjà plusieurs mois. Elles ont passé diverses sélections avant de pouvoir prétendre à un usage opérationnel. Elles ont choisi huit épreuves ni plus, ni moins. Les performances des IA seront garanties par un comité d'évaluation et un comité de pilotage afin d'assurer la légalité des moyens de protection de la population.

C'est donc une grande première initiée par la France qui déploiera dans un cadre expérimental stricte des systèmes d'intelligence artificielle (SIA) associés à la vidéo protection. Ce cadre est d'ailleurs proposé au sein de la réglementation européenne (AI Act) qui a ouvert cette possibilité en vue de tester la performance comme la pertinence des systèmes avant tout usage opérationnel. En d'autres termes, il s'agit d'ouvrir un régime juridique à la notion d'expérimentation.

Pour être en conformité avec la loi, chaque recours à la vidéo algorithmique devra faire l'objet d'un arrêté préfectoral, précisant la temporalité, la localisation et les motifs d'exploitation.

Les enjeux de l'exploitation de l'IA au sein de cette expérimentation sont multiples. Il s'agit tout d'abord d'un enjeu de protection de l'évènement afin de déterminer si l'IA s'avère utile dans la remontée d'alerte d'incident préalablement à l'engagement opérationnel d'une action humaine. L'ambition est d'accélérer l'intervention des pompiers ou des forces de police.



Cette expérimentation permettra ensuite d'évaluer l'acceptabilité sociétale. Une telle technologique doit être conforme au contrat social. Dès lors, il s'agira de mesurer la pertinence des SIA, leur proportionnalité et leur conformité aux finalités attendues. Il ne s'agit pas de surveiller la population mais bien de la protéger en transparence vis à vis du citoyen.

Enfin, cette expérimentation permettra de mesurer le niveau de performance de l'IA au regard d'une diversité de cas d'usage et dans un cadre à la fois opérationnel et complexe.



Comme il est précisé dans le délibération n° 2023-060 du 29 juin 2023, la CNIL a considéré que les garanties prévues permettent de limiter les risques d'atteinte aux données et à la vie privée des personnes et vont dans le sens des préconisations formulées dans sa prise de position sur les caméras « augmentées » publiée en juillet 2022.

Elle a également invité le ministère à mener, dès le début de l'expérimentation, une réflexion sur la mise en place d'un protocole d'évaluation permettant de mesurer de façon rigoureuse, contradictoire et pluridisciplinaire l'apport des technologies d'analyse automatisée des images.

Afin de prévenir tout risque, le ministère de l'intérieur a mis en place un comité d'évaluation et un comité de pilotage qui délivreront toutes leurs conclusions en mars 2025.



Le Décret n° 2023-828 du 28 août 2023 relatif aux modalités de mise en œuvre des traitements algorithmiques sur les images collectées au moyen de systèmes de vidéoprotection et de caméras installées sur des aéronefs, pris en application de l'article 10 de la loi n° 2023-380 du 19 mai 2023 relative aux jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions est accessible sous : <https://www.legifrance.gouv.fr/jorf/id/JORFTEXTO00048007135>

Ce décret fixe les conditions pratiques d'utilisation de l'IA en matière de vidéo protection et définit précisément les cas d'usage. Ils sont au nombre de huit:

- présence d'objets abandonnés ;
- présence ou utilisation d'armes, parmi celles mentionnées à l'article R. 311-2 du code de la sécurité intérieure ;
- non-respect par une personne ou un véhicule, du sens de circulation commun ;
- franchissement ou présence d'une personne ou d'un véhicule dans une zone interdite ou sensible ;
- présence d'une personne au sol à la suite d'une chute ;
- mouvement de foule ;
- densité trop importante de personnes ;
- départs de feux.

Ainsi, aucune méthode biométrique ne sera utilisée, il n'y aura pas non plus de recoupement de fichiers afin de prévenir tout risque d'atteintes aux libertés individuelles. L'expérimentation mis en oeuvre a vocation à évaluer la pertinence de l'exploitation de l'IA dans le cadre de cas d'usage opérationnels de grande envergure,

# COMCYBER-MI

## Hacking vs hacking éthique

Le démantèlement récent du groupe de hackers le plus nuisible au monde, Lockbit, grâce à une vaste opération internationale dont ont fait partie les cyber enquêteurs de la Gendarmerie nationale est l'occasion de revenir sur le *hacking*, sa définition et ses formes. Le piratage informatique a pour objectif d'identifier et d'exploiter les failles d'un système d'information pour obtenir un accès non autorisé à des données.

Le piratage, dans sa forme illégale, est particulièrement développé en matière de cyber criminalité. À tel point, d'ailleurs, qu'il n'est plus utile d'être un habile informaticien pour réussir son coup. En dépit des moyens de lutte mis en oeuvre, les préjudices sont nombreux:

- atteinte à la réputation;
- vol de codes bancaires;
- vol d'identité numérique;
- dérober des informations confidentielles;
- transférer des fonds;
- détruire des informations sensibles;
- exercer du chantage sur des données personnelles;
- ...

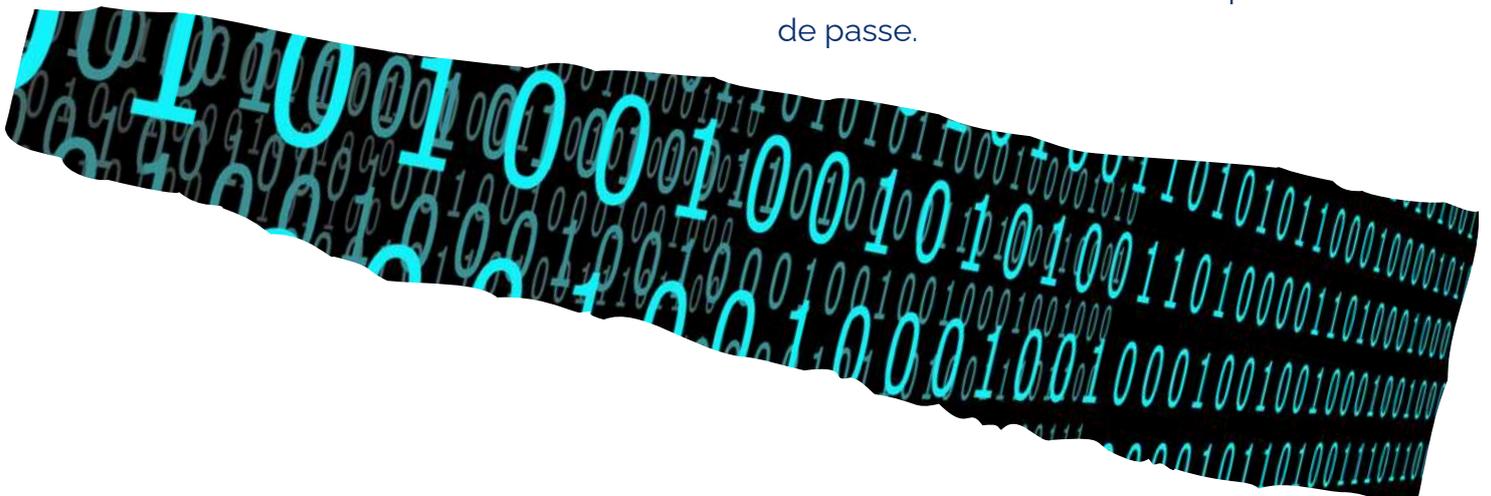


Les formes les plus classiques de piratage informatique sont les suivantes :

- **Le piratage (craquage) des mots de passe**

Les mots de passe sont d'une facilité déconcertante à identifier. Parmi les méthodes connues, il y a celles des **jeux d'essai/erreur** ou d'attaque par force brute. L'objectif est de déterminer la combinaison à craquer en testant un à un les différents codes possibles. Cette méthode est simple à concevoir d'autant que les pirates s'aident d'algorithmes d'IA pour accélérer la découverte des mots de passe.

Pour identifier un mot de passe, il existe aussi la méthode de **l'attaque par dictionnaire** qui consiste à exploiter un algorithme qui insère des mots courants dans le champ des mots de passe. Cette technique repose sur l'absence d'imagination dont nous faisons tous preuve dans l'élaboration de nos trop nombreux mots de passe.



# COMCYBER-MI

- **L'ingénierie sociale**

La méthode d'ingénierie sociale est connue pour son impact dans l'arnaque dite au Président ou encore qualifiée de FOVI (faux ordre de virement). L'objectif est l'obtention d'informations personnelles par des astuces parfois assez basiques de la part des pirates. Ils vont inciter leur interlocuteur à divulguer des informations sensibles (personnelles, financières ...) en prenant une fausse identité ou en usant de méthodes psychologiques. Ils peuvent par exemple faire usage de techniques d'hameçonnage, d'utilisation de courriels ou de messages instantanés voire à de faux sites web.

- **L'espionnage des courriels**

Par la création d'un code, il est possible aux pirates informatiques d'accéder à des messageries et donc d'intercepter et de lire les courriels. Fort heureusement, la plupart des messageries électroniques utilisent aujourd'hui des méthodes de crypto pour parer ce type d'attaques.

- **L'enregistrement des frappes au clavier**

Nous avons tous une façon différente de frapper au clavier au point d'en faire une signature à défaut d'une empreinte. Certains algorithmes sont capables de capter nos frappes au clavier via l'intégration d'un code malveillant inséré au sein de nos ordinateurs ou smartphones. Ce code enregistre chaque frappe permettant au pirate de connaître tout ce qui est tapé dont les mots de passe et ainsi d'infiltrer aisément un système.

- **L'infection par logiciels malveillants**

S'infiltrer dans un ordinateur ou un système d'information pour y installer un logiciel malveillant dépend du niveau de protection. L'une des méthodes les plus simples est d'adresser un e-mail pour proposer le téléchargement d'une application, d'un livre blanc ou d'une vidéo. Une fois le logiciel installé, l'attaque peut être dormante et se déclencher lorsque le pirate le souhaitera.

- **L'accès par une porte dérobée**

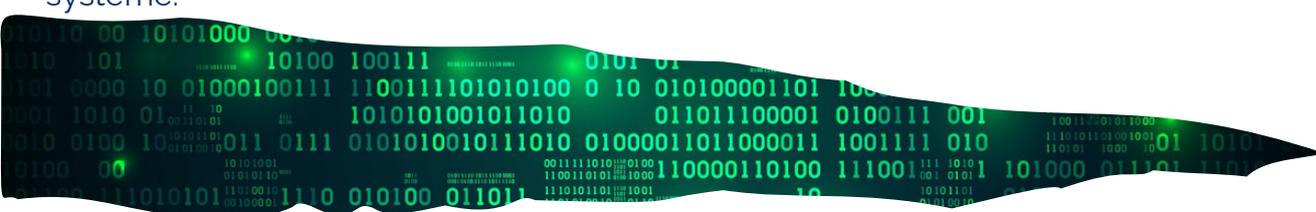
Une approche plus sophistiquée est la recherche de voies d'accès non protégées aux systèmes et ordinateurs d'un réseau. Le pirate introduit un programme par un cheval de Troie pour capturer ensuite des données sensibles en toute impunité.

- **L'exploitation des réseaux sans fil non sécurisés**

La multiplication des réseaux sans fil ouvre de belles opportunités aux cybercriminels car ces réseaux sont bien souvent peu protégés voire totalement ouverts. Une fois connecté au réseau, le pirate peut aisément accéder aux divers appareils connectés.

L'IA joue un rôle de catalyseur dans toutes ces opérations et facilite dès lors le travail des pirates. Il est une technique intéressante pour prévenir et lutter contre ce hacking malveillant, c'est le **hacking éthique** que vous retrouverez dans le prochain numéro.

**À SUIVRE**





# La page du réserviste citoyen

## Les attaques malveillantes autour des IA génératives. Comment peut-on attaquer par exemple un Chat-GPT ou autre par du déni de service via l'envoi massif de prompts ...

L'intelligence artificielle générative est une branche de l'intelligence artificielle qui s'intéresse à la création de nouvelles données, telles que du texte, des images, de la musique ou des vidéos. Elle utilise des algorithmes d'apprentissage automatique (AA) pour apprendre à générer des données qui ressemblent à celles créées par des êtres humains.

L'IA générative est donc une technologie émergente avec un potentiel considérable de transformation de différents secteurs d'activité. Elle est encore en développement, mais elle a déjà un impact significatif sur notre vie quotidienne.

L'IA générative dès lors considérée comme l'une des approches les plus prometteuses pour parvenir à l'intelligence générale. Cela signifie qu'elle peut apprendre et s'adapter à de nouvelles situations, et qu'elle peut générer des solutions créatives à des problèmes complexes.

### Quels sont les usages nouveaux, par exemple, dans certains secteurs ?

La science et la recherche : L'IA générative est utilisée pour générer des hypothèses scientifiques, découvrir de nouvelles données et créer des modèles de systèmes complexes. Elle est également utilisée pour simuler des expériences et tester de nouvelles théories.

L'industrie et la production : L'IA générative est utilisée pour concevoir de nouveaux produits et processus, améliorer l'efficacité des chaînes de production et automatiser des tâches répétitives. Elle est également utilisée pour créer des simulations de produits et des prototypes virtuels.

L'art et le divertissement : L'IA générative est utilisée pour créer des œuvres d'art originales et uniques, telles que des peintures, des sculptures et des compositions musicales. Elle est également utilisée pour créer des effets spéciaux dans les films et les jeux vidéo.

Le commerce et le marketing : L'IA générative est utilisée pour créer des publicités personnalisées, des contenus marketing et des expériences d'achat immersives. Elle est également utilisée pour générer des prévisions de vente et des modèles de comportement des consommateurs.

### Quels sont les problèmes potentiels ?

Dans cette technologie nous pouvons identifier et analyser trois catégories principales de problématiques : les enjeux technique, éthique et sociétaux.

#### Les problèmes techniques

- Par une attaque DDoS. Cette dernière est une attaque informatique qui vise à rendre un serveur ou un réseau indisponible en l'inondant de trafic. Cette attaque peut être utilisée pour empêcher les utilisateurs légitimes d'accéder à un site Web, à un service ou à une ressource. Dans le cas d'un modèle de langage comme GPT, BARD (ou d'outils utilisant ces systèmes), une attaque DDoS pourrait avoir pour effet de ralentir ou de rendre impossible l'accès à ces services. Cela pourrait être utilisé pour empêcher les gens d'obtenir des informations, de communiquer ou de réaliser des tâches.



# La page du réserviste citoyen

- L'IA générative est une technologie complexe qui peut être sujette à des erreurs ou des biais. Ces problèmes peuvent entraîner des conséquences négatives, telles que la diffusion de fausses informations ou la discrimination. En effet, l'IA générative peut être utilisée pour créer des images, des vidéos ou du texte qui sont difficiles à distinguer des informations réelles. Cela pourrait être utilisé pour diffuser de la propagande ou pour manipuler l'opinion publique. ou offensant.

Les problèmes éthiques : l'IA générative peut être utilisée à des fins malveillantes, telles que la création de deepfakes ou la diffusion de propagande. Ces problèmes posent des questions importantes sur l'utilisation et la régulation de cette technologie.

Les problèmes sociétaux : l'IA générative pourrait avoir des conséquences significatives sur la société, telles que la perte d'emplois ou la montée de l'inégalité. Ces problèmes sont encore mal compris, mais ils méritent d'être pris en compte.

Ainsi, l'IA générative peut être attaquée et manipulée. Elle est un modèle de langage et est formé sur un ensemble de données de texte et de code. Cela signifie qu'elle peut être utilisée pour générer du texte, traduire des langues, écrire différents types de contenu créatif et répondre à des questions de manière informative. Cependant, elle peut aussi être utilisée pour générer du texte qui est faux, trompeur ou offensant.

## Quels sont les parades possibles ?

L'utilisation d'un réseau de diffusion de contenu (CDN) : un CDN est un réseau de serveurs répartis dans le monde entier qui distribue le contenu d'un site Web.

Cela peut aider à atténuer l'impact d'une attaque DDoS en répartissant le trafic sur plusieurs serveurs.

L'utilisation d'un pare-feu : un pare-feu est un dispositif de sécurité qui filtre le trafic entrant et sortant d'un réseau. Cela peut aider à bloquer les attaques DDoS en empêchant les paquets de trafic malveillant d'atteindre le serveur cible.

L'utilisation d'un système de détection d'intrusion (IDS) : un IDS est un dispositif de sécurité qui surveille le trafic réseau à la recherche d'activités suspectes. Cela peut aider à identifier les attaques DDoS en cours afin qu'elles puissent être traitées rapidement.

Cependant, il est important de noter qu'il n'existe aucune protection absolue contre les attaques DDoS. Même les mesures de sécurité les plus sophistiquées peuvent être contournées par des attaquants déterminés. Concernant les problématiques de deepfakes ou de diffusion d'information de propagande. Les réponses appartiennent aux sciences de l'information et de la communication.



# INTELLIGENCE ARTIFICIELLE ET FORMATION

Focus sur un Master de Droit IA  
créé en 2021 en France!

L'arrivée de l'AI ACT appelle les jeunes étudiants au métier du droit afin d'accompagner les entreprises & institutions vers une juste et responsable appropriation de l'IA.

## 1. Pourquoi un master de droit de l'IA et quels enseignements peut-on y trouver ?

**DGL:** Le Master en droit de l'intelligence artificielle de l'Institut catholique de Paris (ICP) est le premier de la sorte. Il se démarque des autres Masters en droit du numérique par le grand nombre d'enseignements résolument centrés sur les enjeux juridiques de l'IA. Avant même la proposition de règlement sur l'IA de la Commission européenne en avril 2021, avant même la déferlante ChatGPT à partir de novembre 2022 – le Master a ouvert en septembre 2021 –, il répond à la croissance des usages de l'IA qui crée de nouveaux risques juridiques, ce qui justifiait de former la nouvelle génération de juristes à ces enjeux.

Outre des enseignements relativement classiques de droit du numérique (droit des données personnelles, droit de la propriété intellectuelle, contrats du numérique, etc.), les étudiants se familiarisent avec les différents textes régulant l'IA, étudient les chartes éthiques de plusieurs entreprises du secteur, réfléchissent aux enjeux de responsabilité en cas de dommages causés par des systèmes d'IA (véhicules autonomes ou autres), à l'utilisation par l'Etat des algorithmes, aux impacts de l'IA dans une entreprise, aux questions d'extraterritorialité de la réglementation et de souveraineté, ... Ils abordent également les régulations sectorielles de l'IA – dans le domaine de la police et de la justice, ou encore de la santé – et des technologies connexes – smart contracts, blockchain, cryptomonnaies, etc.

En outre, le Master droit de l'IA de l'ICP, qui est une université pluridisciplinaire, offre des enseignements non seulement en droit, mais également en philosophie et en éthique. Il ne s'agit pas seulement de faire des étudiants de bons techniciens du droit, mais des acteurs éclairés du monde de demain. Enfin, parce qu'on ne saurait prétendre raisonner ou réguler sans connaître son objet d'étude, des ingénieurs initient les étudiants aux aspects proprement techniques de l'IA.

## 2. Quels sont les profils & vers quels métiers se tournent-ils ?

**DGL:** Les étudiants sont pour la plupart titulaires d'une Licence en droit mais peuvent aussi venir d'autres horizons. La diversité des bagages intellectuels des étudiants fait aussi la richesse des réflexions au sein d'une promotion. Des étudiants issus d'un autre cursus, dès lors qu'ils ont fait un peu de droit et ont un intérêt marqué pour les enjeux de régulation de l'IA, sont ainsi les bienvenus. Naturellement, les doubles cursus en droit associé à une autre discipline (philosophie, science politique, mathématique ou autre) ont également toute leur place dans le Master.



# INTELLIGENCE ARTIFICIELLE ET FORMATION



Contrairement à ce que l'on pourrait instinctivement penser, les débouchés sont extrêmement larges. D'abord parce que le numérique et l'IA envahissent tous les secteurs de la société – santé, éducation, monde des affaires, justice, etc. Ensuite, parce que l'éventail des métiers possibles à l'issue de ce Master est également très large : avocat, juriste d'entreprise, délégué à la protection données, compliance officer, start-uppeur... sans compter que ces juristes spécialisés peuvent aussi bien trouver à s'employer en think tank, pour un lobby, dans une association, ou au sein d'institutions publiques, nationales, européennes ou internationales. Sans oublier, enfin, la recherche ! En droit de l'IA, il y a encore beaucoup de prospective, c'est un terrain magnifique pour la recherche en droit. Là encore, dans le processus de recrutement de mes étudiants, je veille autant que faire se peut à privilégier la diversité dans leurs aspirations professionnelles.

## Comment concilier IA & responsabilité ?

**DGL:** la confrontation des avancées scientifiques – médicales ou technologiques – avec le monde du droit est souvent problématique : faut-il réguler en amont (mais le droit n'est-il pas voué à avoir toujours un train de retard ?) ? convient-il plutôt de prévoir une réponse juridique en aval, sous forme d'obligation de réparer les dommages injustement causés ?

C'est précisément l'objet du droit de la responsabilité civile.

Dans cette optique, l'avènement de l'IA introduit de nouveaux risques de dommages (accidents mortels impliquant des véhicules autonomes, résultats d'un moteur de recherche attentatoires à la réputation, violation du droit à l'image par la création de deepfakes, propos insultant d'un chatbot, ...). L'enjeu juridique est de déterminer si ces dommages sont réparables – aux conditions de droit commun ? à des conditions spécifiques ? – et qui doit être tenu à réparation. C'est passionnant car cela permet de confronter notre système juridique à des faits inédits. En cela, le juriste d'aujourd'hui est un peu dans la même situation que lors de la révolution industrielle, lorsque des nouveaux accidents sont intervenus, pour lesquels les règles du Code Napoléon n'avaient pas été pensées, et qu'il a fallu trouver des moyens pour indemniser les victimes.

## Et la place des femmes en IA ?

**DGL:** On lit souvent des chiffres alarmants sur la faible proportion de jeunes femmes dans les études scientifiques. Sans remettre en cause ce constat, je souhaiterais le nuancer un petit peu : dans le secteur de l'ingénierie en général ou de l'IA en particulier, il n'y a pas que des profils scientifiques ; des professionnels ou chercheurs en sciences sociales sont également impliqués. Or dans ces secteurs-ci, et en particulier en droit, le nombre de femmes n'est pas un problème – elles sont même bien plus nombreuses que les hommes.

**Diane Galbois-Lehalle**

**Directrice du Master droit de l'intelligence artificielle**

**Institut Catholique de Paris**



## IA et feux de forêt : La détection précoce en pleine évolution grâce à la vision assistée par ordinateur (computer vision)

Les récentes évolutions technologiques liées au traitement de la donnée, combinée à l'amélioration de captation d'images ont permis de faire évoluer les différents techniques de prévention et de lutte contre les feux de forêts et plus particulièrement lors de la phase de détection précoce.

### La détection précoce : une pratique ancienne en pleine transformation grâce à l'intelligence artificielle

Traditionnellement, dans les massifs forestiers, en période de risque, des « guetteurs » se positionnaient sur des points hauts afin de détecter les premiers signes d'un départ de feu (fumées). Cela permet une intervention rapide sur un sinistre naissant, bien plus facile à maîtriser qu'un sinistre pleinement développé ou des très nombreux moyens deviendront vite nécessaires pour tenter de le contenir, puis de l'éteindre. Sur l'arc méditerranéen le relief naturel permet de trouver des points d'observations alors que dans les landes de Gascogne, des vigies ont été installées pour surplomber la canopée. Ces missions de vigie étaient traditionnellement réalisées par des sapeurs-pompiers avec des jumelles.

De plus, il convient de préciser que dans l'arc méditerranéen, en période de risque élevé, des avions bombardiers d'eau chargés réalisent des vols « préventifs » afin de détecter et d'éventuellement traiter des feux naissants par largage, cela est appelé le guet aérien armé.

Nous nous concentrons dans cet article à de la détection précoce par l'intermédiaire d'images sur point fixe ou depuis des structures mobiles.

La détection précoce : une pratique ancienne en pleine transformation grâce à l'intelligence artificielle

### La détection précoce sur point fixe

Il y a une quinzaine d'années le SDIS des Landes a fait le choix d'installer dans les tours de vigies des caméras. Celles-ci pouvaient ainsi détecter des fumées s'échappant de la canopée. Une fois la levée de doute effectuée par un opérateur, des moyens opérationnels peuvent être alertés pour traiter le sinistre naissant. Ce premier système a été co-construit avec les sapeurs-pompiers des Landes et l'entreprise française Paratronic. Cette solution a été déployée dans plusieurs départements du sud de la France et même dans le grand ouest, dernièrement c'est la Sarthe qui a inauguré son système de détection précoce (2021).

Généralement, les caméras utilisées sont dans le domaine visible ou le domaine infrarouge. Les premières vont détecter un panache de fumée, et les secondes détectent des contrastes de température. La portée de la détection varie en fonction des caractéristiques des boîtiers optroniques utilisés. A titre d'exemple, les 18 tours de guet du département des Landes sont désormais équipées de 54 caméras de vidéosurveillance, pour une surface couverte d'environ 660 000 hectares.

Aujourd'hui plusieurs solutions sont disponibles sur le marché, avec des coûts et des qualités de détection variées, en fonction du nombre et de la qualité des boîtiers et de la qualité des algorithmes de détection. Il y a quelques années les bases de données de départs de feu étaient relativement rares et peu fournies. La multiplication des captations par caméras fixes a permis une augmentation de la quantité et de la qualité des bases de données d'image de détection de feux.



Cela contribue à une nette amélioration des performances algorithmiques. Même si les bases de données se sont étoffées, les quantités restent faibles comparées à d'autres bases de données utilisées dans d'autres usages du computer vision (analyse du trafic routier par exemple).

Il convient de préciser que dans des massifs plus escarpés, il est parfois difficile de couvrir d'importante surface avec des caméras sur infrastructure fixe. La détection précoce peut alors s'envisager sur des points hauts temporaires (ballon captif) ou des points haut mobiles (principalement drone ou avion)

### **La détection précoce sur point temporaire ou mobile**

- Détection précoce par ballon captif ou drone filaire

Permettre de créer un point haut ponctuel permet de limiter les coûts liés à la construction et au maintien opérationnel des infrastructures, tout en préservant le paysage. Des tests ont été réalisés par le Bataillon des Marins-Pompiers de Marseille pour positionner des capteurs optroniques sur un ballon d'observation captif (2021).



Celui-ci est mis en station lorsque les conditions sont à risque. Gonflé à l'hélium, le ballon loué à la société A-NSE, s'élève à plusieurs centaines de mètres d'altitude au-dessus de Marseille et ses deux caméras embarquées, une pour le jour, l'autre pour la nuit, peuvent détecter un départ de feu sur une dizaine de kilomètres de rayon autour du ballon. Il est en permanence rattaché à une base lui permettant de faire fonctionner ces caméras.

- Détection précoce et suivi par drones et avions

L'avantage pour le drone comme pour l'aéronef, c'est qu'il est en capacité de se déplacer et donc de couvrir une zone beaucoup plus importante à des altitudes où un opérateur humain ne serait pas en capacité de détecter des départs. L'autre avantage est de pouvoir se concentrer sur une zone d'intérêt, pour suivre l'éclosion et la propagation du sinistre et ainsi pouvoir apporter des éléments précieux aux forces de secours présentes sur le terrain pour optimiser leurs réponses.

Pour le drone, les principales difficultés sont l'autonomie de vol liées à la charge d'export de la boule optronique. Une expérimentation va débuter avec la société française x-Sun (pour la partie drone) et la start-up française Midgard (pour la partie détection algorithmique et suivi de feu). Ce projet est soutenu par la Direction générale de la sécurité civile et de la gestion des crises et financé par un fonds achat innovant de la Direction des Achats de l'État. Cette expérimentation vise à déployer et à tester un système de drone de grande autonomie doté d'un système optronique de détection et de suivi.



Les images captées dans le domaine visible et infrarouge par le capteur optronique sont ensuite traitées par un algorithme d'IA pour permettre la détection, la localisation et le suivi d'un feu de forêt. L'avion lui peut avoir des possibilités d'emport plus importantes et peut donc prendre à bord des capteurs plus lourds. Il peut également, en fonction des modèles emporter une charge d'eau qu'il sera susceptible de larguer sur un feu naissant. Une jeune entreprise française (AriaFirefighting) propose une captation géo-référencée des sinistres en direct grâce à des capteurs positionnées sous les avions dans une boule optronique. Les capteurs couplés au traitement des données via des algorithmes permettent de détecter les départs mais aussi d'analyser les images captées dans les différentes longueurs d'ondes (visible et infrarouge (NIR et LWIR)) afin d'identifier les contours du sinistre, et les points chauds avec précision.

### **Les captations d'images en direct, une mine d'or pour l'avenir des modèles de prédiction**

Avec les dernières solutions évoquées, il sera possible de détecter mais également de mieux prédire. En effet, De plus en plus de données relatives à la météo (vent, hygrométrie, ...) à la forêt (type de végétation, taille de végétation, ...), mais aussi aux terrains (reliefs principalement) sont disponibles avec une grande précision. Ces trois grandes catégories de paramètres sont clés pour comprendre le comportement d'un feu de forêt.

Des modèles de propagation qui mêlent ces trois grandes typologies de données se développent et permettent de mieux appréhender leurs impacts sur la propagation des sinistres. La France s'illustre sur ce sujet.

Le CNRS de Corte a développé le simulateur de propagation Firecaster. Si les résultats de ces types de modèles sont intéressants, ils ne sont pas réactualisés pendant l'avancée du sinistre. Cela cantonne souvent l'utilisation de ces simulateurs à une analyse post-sinistre et non opérationnelle.

Demain, l'extraction automatisée par IA des données du feu de forêts géo-référencés, réalisées lors de survol pourrait permettre de créer une perméabilité à haute valeur ajoutée avec les modèles de prédiction décrit précédemment.

Ainsi les simulations pourraient s'actualiser en se basant sur le développement réel du sinistre. Cela permettrait aussi un apprentissage par renforcement en comparant les prédictions du modèle à la réalité « minutes après minutes ».

#### **Thibaut REFFAY**

**Chargé de mission stratégie achat sécurité civile et animation du réseau des SIS  
Direction de l'évaluation de la performance,  
de l'achat, des finances et de l'immobilier  
Service de l'achat, de l'innovation et de la  
logistique du ministère de l'Intérieur**

#### **Sources / Plus d'informations :**

<https://www.paratronic.com/realisation/adelie-sdis-40-les-landes>

<https://firecaster.universita.corsica/>

<https://www.linkedin.com/pulse/barbaggio-janvier-2024-autopsie-dun-feu-aria-fire-3kdte>

## La Gendarmerie et l'IA



### TOP Contributor European Tool Repository Prize

La Gendarmerie nationale a été récompensée par EUROPOL pour la mise à disposition d'outils d'IA directement opérationnels que ce soit dans le domaine de la police judiciaire, du renseignement ou de la cybercriminalité. L'ensemble des applications a été développé en interne par le Pole Judiciaire de la Gendarmerie nationale et le Commandement du ministère de l'intérieur dans le cyber espace.

Transcription automatique de parole, base de données synthétiques, outils de traduction automatique, géolocalisation d'images ou encore détection d'objets sont, entre autres, les outils mis à disposition.

Développer des outils d'IA en interne à partir d'*opensource* est une philosophie et s'inscrit dans une ambition plurielle : maîtriser les systèmes utilisés, mettre à disposition des outils directement opérationnels au profit des gendarmes, mieux assister le personnel dans des tâches d'enquête chronophage, faire de meilleurs choix industriels et refuser d'exploiter l'IA comme une boîte noire.

Développer ses outils c'est aussi garantir leur conformité au regard de notre charte éthique IA & des réglementations. Tout ceci s'inscrit dans la stratégie CapIA élaborée, il y a 4 ans et qui se décline progressivement autour de ses piliers : formation, recherche et développement , éthique & réglementation, partenariat et valorisation, service à l'utilisateur.

Proposer des outils d'IA directement exploitables c'est rendre l'IA accessible à hauteur d'homme par des applications opérationnelles et contribuer "à rendre le monde plus sûr" telle qu'énoncée par la devise d'EUROPOL.





## Et si j'expliquais l'IA à mon enfant

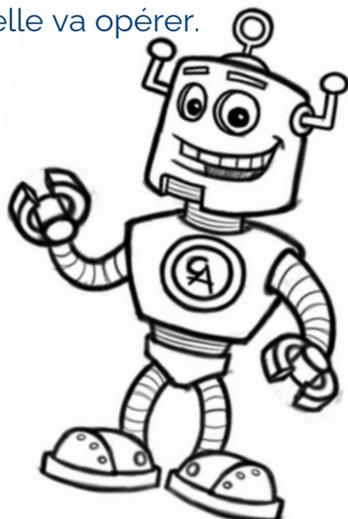
Définir l'intelligence artificielle est déjà particulièrement difficile à l'âge adulte, alors comment faire pour expliquer à un enfant une technologie qui fera partie de son quotidien?

D'abord, il est important que l'enfant se représente ce que cela est, avec des analogies faciles à saisir.

### Qu'est-ce que l'IA?

Chez l'être humain, c'est le cerveau qui commande tout. Cet organe guide nos décisions et nous permet d'agir, parfois avec nos bras et nos jambes. L'IA, c'est le cerveau que les humains mettent dans un ordinateur ou dans un robot. Grâce à cela, l'ordinateur va pouvoir mieux saisir ce que nous cherchons et voulons sur le net par exemple. Et pour le robot, cette intelligence va lui permettre de se déplacer dans un environnement déterminé.

Pour que cela soit possible, l'IA doit apprendre à saisir correctement la demande humaine et le contexte dans lequel elle va opérer.



### Comment l'artificiel devient intelligent ?



La machine apprend comme un enfant. Elle a néanmoins besoin de beaucoup plus d'exemples qu'on appelle les données. Par exemple, une IA verra des milliers d'images de chats pour pouvoir en reconnaître un alors qu'un enfant, il lui suffit d'en voir deux.

Une machine apprend de différentes façons:

- **apprendre par coeur / apprentissage supervisé:** cet apprentissage c'est comme pour les tables de multiplication par exemple ou la lecture. On montre une image de chien et on y associe le mot "chien" pour dire que c'est pareil. Et, une fois que la machine a appris on peut lui poser n'importe quelle question, elle saura répondre car elle connaît les similitudes. Si on lui dit que les images qu'on lui met dans sa mémoire sont des loups elle va le retenir à la condition qu'on lui en donne plusieurs. Et donc, dès qu'elle verra un loup elle saura que c'en est un.



- **apprendre par récompense/sanction / apprentissage par renforcement:** à l'image de la maîtresse qui donne des bons points ou des punitions, l'informaticien envoie un signal à l'IA pour la récompenser ou la punir. C'est comme cela qu'on fabrique des voitures autonomes par exemple. Un signal négatif (sanction) est envoyé si une erreur se produit (cogner un trottoir par exemple) et un signal positif si elle agit correctement (un virage bien négocié par exemple).

- **apprendre par comparaison / apprentissage non supervisé:** quand on est petit et qu'on voit un chat passer, puis un autre, notre cerveau est capable de dire que ces deux animaux se ressemblent même si nous ne sommes pas capables de dire que ce sont des chats. Le schéma est le même pour la machine : l'informaticien ne lui envoie pas deux mais des milliers d'images de chats sans lui dire que c'est un chat et la machine saura que ce sont des images de même nature. L'objectif de cette forme d'apprentissage est de regrouper les choses qui se ressemblent même si elles ne sont pas nommées. C'est ce qui se passe lorsque vous regardez NETFLIX et qu'un film vous est conseillé. C'est une IA qui, derrière, fait le lien entre des goûts ciblés à partir des visionnages précédents sur cette plateforme et la bibliothèque des films à sa disposition.

### **Mais alors l'IA apprend comme nous?**

Il est vrai que les procédés d'apprentissage entre la machine et l'humain se ressemblent mais l'IA apprend en consommant beaucoup plus d'exemples que l'humain et surtout consomme beaucoup plus d'énergie, ce qui coûte à l'environnement. Un cerveau humain consomme 20W, l'ordinateur AlphaGo 20kW.

Et ce qui nous différencie de l'IA, c'est que nous, nous retenons plusieurs situations en même temps et en plus nous sommes capables de faire des liens avec des données inconnues et des sources très différentes. En deux mots, nous avons une meilleure capacité à généraliser nos apprentissages.

### **L'IA est-elle dangereuse et pourrait-elle nous remplacer?**

Non. L'IA n'est pas dangereuse car elle n'a aucune volonté et donc aucune ambition de détruire l'être humain ou de prendre sa place. Mais, il faut tout de même comprendre que le système d'IA peut être utilisé de la mauvaise manière ou avec de mauvaises intentions. Et donc ce n'est pas l'IA qu'il faut accuser. C'est aux êtres humains qui la créent de s'assurer de sa bonne conception et de sa bonne utilisation. Et, c'est à chacun de nous, d'utiliser cette IA avec prudence. On parle alors de responsabilité individuelle comme collective.

**Le 19 février 2024**

**la loi N°2024-120 visant à garantir le respect du droit à l'image des enfants a été publiée.**

**Il y est rappelé la responsabilité des parents face à leur obligation de protéger le droit à l'image de leur enfant mineur.**



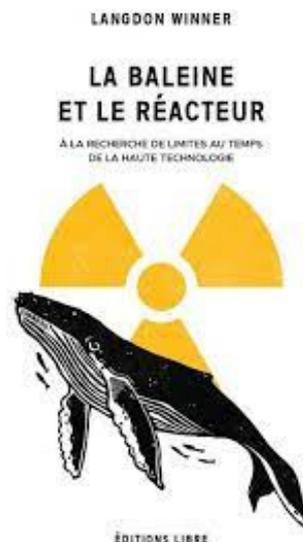


2.2.2024

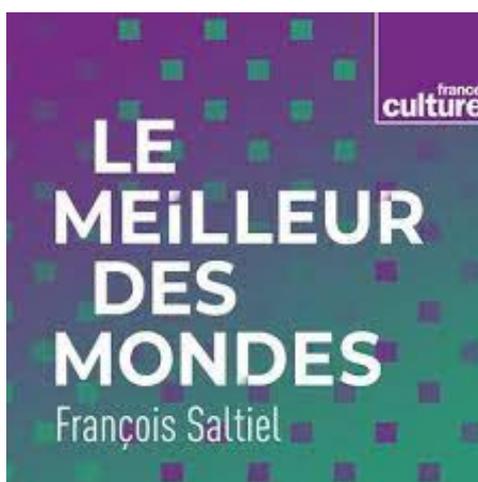
## PROVISIONAL AGREEMENT RESULTING FROM INTERINSTITUTIONAL NEGOTIATIONS

**Subject:** Proposal for a regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts 2021/0106(COD) (COM(2021)0206 – C9-0146(2021) – 2021/0106(COD))

Qui a dit que le droit était indigeste, surtout en anglais? La réglementation IA toute fraîchement votée tient sur 245 pages et va encadrer tous nos usages dans les mois à venir!  
À défaut de lire les 245 pages, les 80 premières sont importantes car elles signent la vision & le modèle technologique défendus par l'UE.



## PODCAST & LITTERATURE



Ce podcast est un pas de côté nécessaire pour comprendre l'ensemble du processus technologique dans lequel s'inscrit IA. Câbles sous-marins, l'IA & la musique, les communs numériques... Des thèmes variés pour combler nos appétits techno!

Et si apprendre à coder l'IA c'était avant tout apprendre à lire?

M. Desmurget rappelle à juste titre que notre cerveau est d'abord calibré pour la lecture, socle de la créativité & de l'esprit critique... déterminants ensuite pour saisir l'IA. Ses propos sont étayés d'études scientifiques et ont le mérite d'interroger les drogués digitaux que nous sommes !



# IA INFO

**CYBERSECURITE:** un « ver informatique » capable d'infester l'intelligence artificielle générative est apparu. Des chercheurs en cybersécurité de Cornell Tech ont créé le « ver MorrisII » capable de se propager automatiquement en brisant certaines des protections de sécurité de modèles comme Gemini Pro, ChatGPT 4.0, ou le LLM open source LLaVA

**BIGTECH :** avec un score de 81,2% sur le benchmark MMLU, Mistral Large se positionne fièrement en 2e place, juste derrière #GPT4 et ses 86,4%. Pourtant, le partenariat de Mistral AI avec Microsoft fait grincer des dents à Bruxelles. En dépit de son accord avec le géant américain, la start-up française assure vouloir rester indépendante et ne pas renoncer à publier des modèles en open source.



**AGENCE IA:** le gouvernement annonce une enveloppe de deux milliards d'euros pour l'intelligence artificielle de défense sur la période 2024-2030 et créé l'AMIAD (l'agence ministérielle pour l'IA de défense). Rassembler les compétences pour appréhender l'IA dans toutes ses dimensions avec l'objectif de penser, concevoir et fabriquer les systèmes d'armes de demain.

**PROPRIETE INTELLECTUELLE:** En Chine, un tribunal a condamné vient de une société d'IA générative pour violation du droit d'auteur du personnage de série japonaise Ultraman.



**LLM:** Anthropic, avec Claude 3 propose des LLM rivalisant avec ses principaux concurrents. La version Optus se révèle être la plus performante face à GPT d'OpenAI ou Gemini Pro de Google. Elle intègre aussi les images pour devenir multimodal.

**GEMINI:** la version améliorée du chatbot d'intelligence artificielle de Google a récemment fait polémique par sa génération d'images de soldats nazis noirs et de Vikings asiatiques, et son refus de faire la promotion de la viande... Ses détracteurs crient au parti pris anti-Blancs comme au wokisme. face à l'ampleur de l'évènement, Sundar Pichai, le PDG de Google a, enchaîné excuses et déclarations.

**FRANCE:** Le 13 mars a été remis au président de la République par la commission de l'intelligence artificielle, un rapport pour éclairer les décisions du gouvernement afin de faire de la France un pays à la pointe de cette nouvelle technologie. Des propositions concrètes pour déployer une stratégie nationale ont été formulées. Ce rapport dresse un état des lieux sur l'impact de l'IA notamment sur les emplois et les meilleures façons de s'en servir et de la déployer.

# Cultur'IA

## Au sommaire du prochain numéro

- Les réseaux de neurones récurrents
- Le hacking éthique
- La menace de l'IA en cyber
- L'IA au coeur des conflits
- La page du réserviste citoyen

