W2 : ABORDER LES ENJEUX JURIDIQUES ASSOCIÉS À L'IA

5/12/2024 Prof. Jacques Folon Ph.D.

technofutur tic

edu LAB By Technofutur TIC

Partenaires associés

Design, animation, badges
Accueil & délocalisation

technobel

UMONS
Université de Mons

technocité
Centre de compétence

HELHa
Haute École Louvain en Hainaut

euroMetropolitan
eCampus

FormaNam

HAUTE ÉCOLE CONDORCET

École branchée
ENSEIGNER À L'ÈRE DU NUMÉRIQUE

Wallonie - Bruxelles International.be


FINALIST
BELGIUM'S
CYBER SECURITY
Privacy Professional
of the Year
Jacques
Folon
Co-founder & CEO
GDPRFOLDER.EU


corporate copyright
Jacques Folon
RGPD 2024
la protection des données personnelles
à l'heure de l'Intelligence Artificielle
GUIDE PRATIQUE
Préface de Didier Reynders, commissaire européen Justice

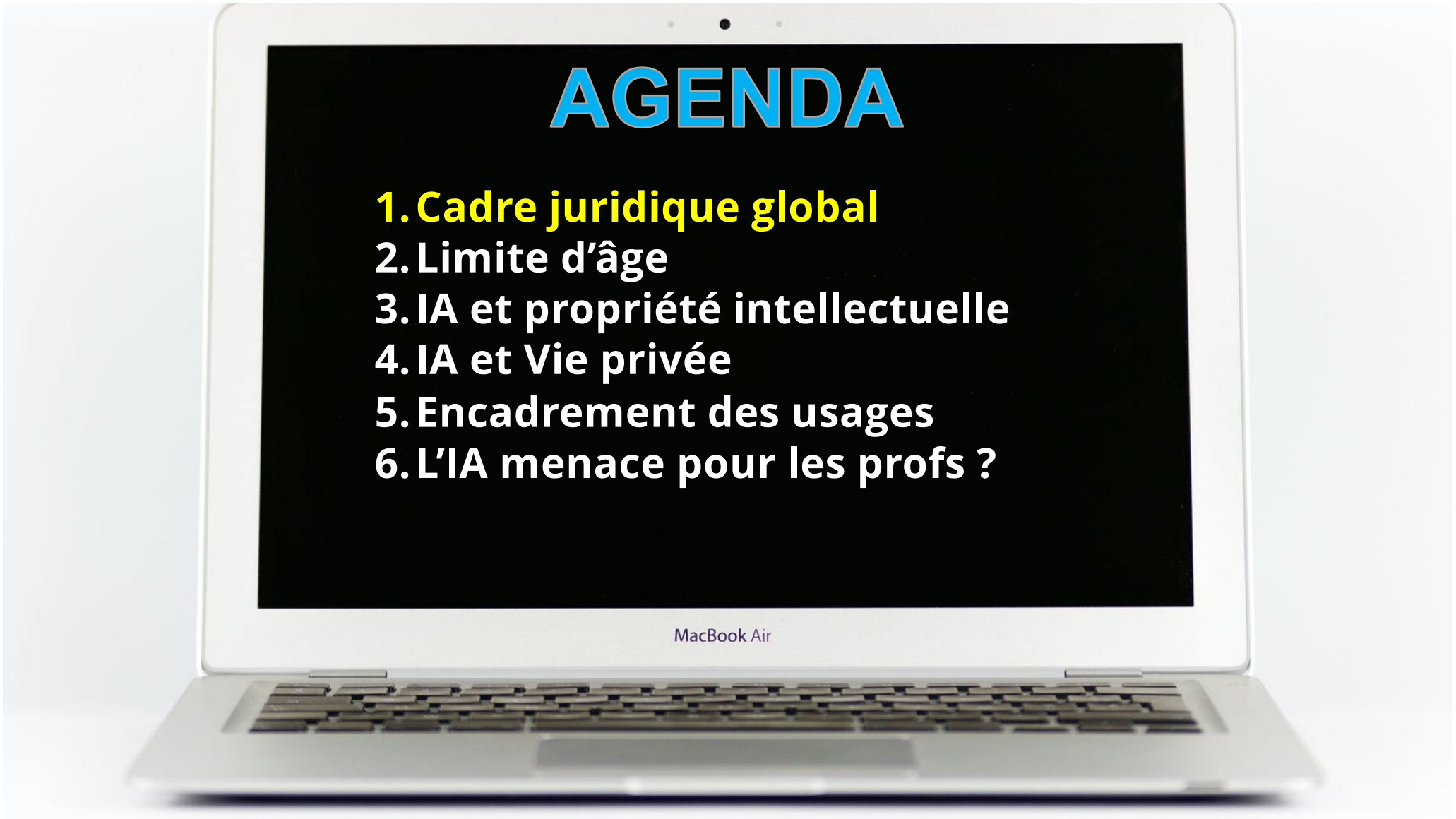

Prof. Dr. Jacques Folon
Jacques@gdprfolder.eu
www.linkedin.com/in/folon
www.gdprfolder.com
+32 475 98 21 15
https://www.folon.com


corporate copyright
LE SOIR
AVONS-NOUS ENCORE
UNE VIE PRIVÉE ?
Jacques Folon

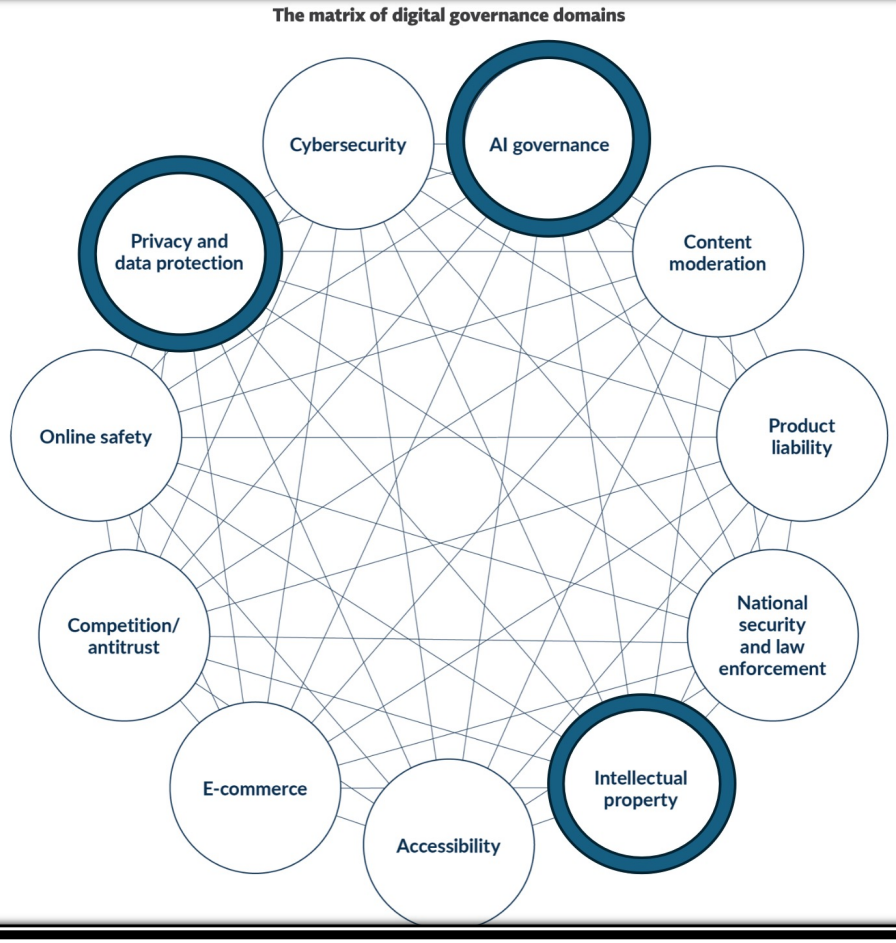

LE SOIR
Opinions
Podcasts
Politique
Société
Monde
Économie
Vidéos
Sports
Culture
Jacques Folon
Chroniqueur
Juriste et docteur en sciences politiques, professeur de stratégie digitale à l'ICHEC, professeur invité à l'Université Saint Louis et à Rennes School of business, il est l'auteur d'une quinzaine de livres. Il intervient régulièrement dans les médias et comme conférencier pour ce qui touche aux évolutions technologiques, à l'intelligence artificielle et à la protection et la sécurité des données personnelles.

COMME AUX OSCARS…
QUELQUES REMERCIEMENTS

A mes parents
A ma femme
A mes deux filles
A Chat GPT pour les textes
A Beautiful.ai pour le PowerPoint
A ai-image generator pour les images
A designerBot pour le PowerPoint
A Google pour les recherches
A Slideteam pour le PowerPoint
A Perpelxity.ai pour la recherche
A Grok pour les vidéos


AGENDA
1. Cadre juridique global
2. Limite d'âge
3. IA et propriété intellectuelle
4. IA et Vie privée
5. Encadrement des usages
6. L'IA menace pour les profs ?
MacBook Air

Complexité des relations entre législations



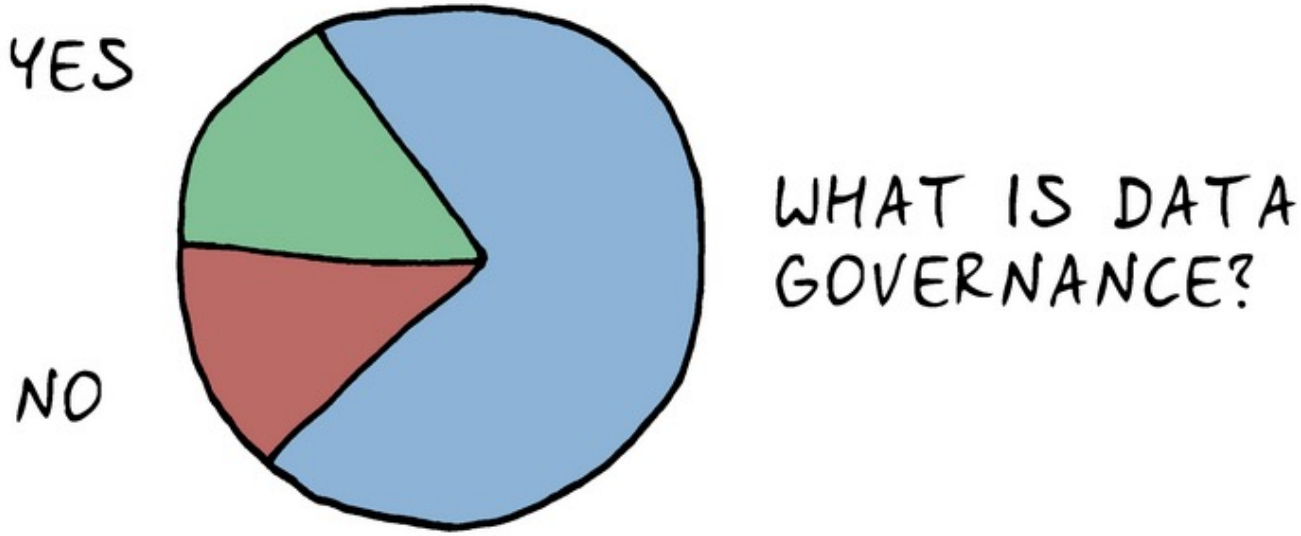
Source Prof. Alain Strowel, présentation Abilways


AI ACT

Comment le règlement européen sur l'intelligence artificielle (IA Act) concilie-t-il la promotion de l'innovation technologique avec la protection des droits fondamentaux, et quelles sont les principales critiques concernant son efficacité à atteindre cet équilibre ?

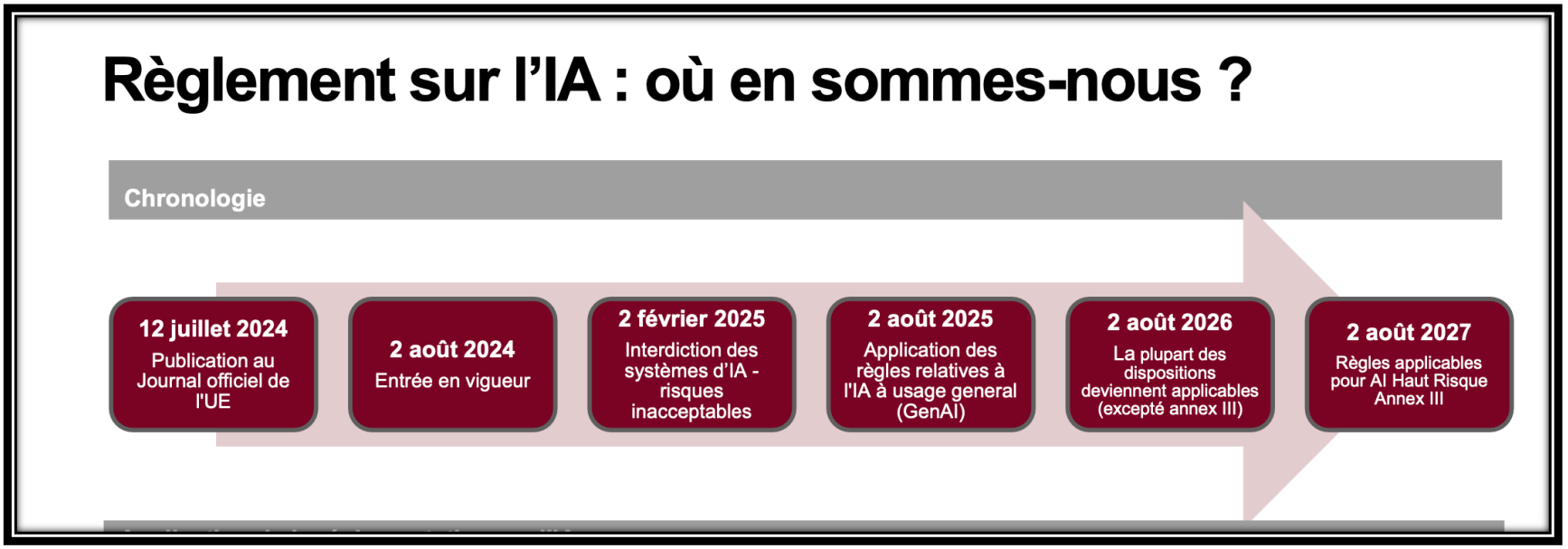
L'IA ACT est une règlementation « SANS PREJUDICE » des règlementations existantes (Rgpd, propriété intellectuelle, etc.)

IS YOUR ORGANIZATION DOING DATA GOVERNANCE?



Dataedo /cartoon

Piotr@Dataedo



SOURCE E. DEHARENG

Définition de "système d'IA"

- *"**système d'IA**" : "un système automatisé qui est conçu pour fonctionner à différents niveaux d'**autonomie** et peut faire preuve d'une **capacité d'adaptation après son déploiement**, et qui, pour des objectifs explicites ou implicites, **déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties** telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels"*

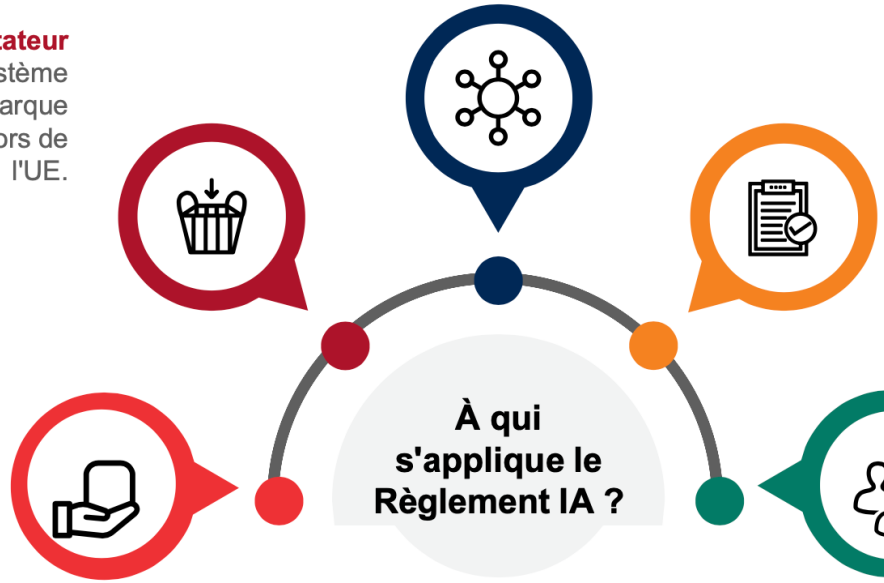
"Modèle d'IA à usage général" (GPAI)

- **"Modèle d'IA à usage général"** : "*un modèle d'IA, y compris lorsque ce modèle d'IA est entraîné à l'aide d'un grand nombre de données utilisant l'auto-supervision à grande échelle, qui présente une **généralité significative** et est **capable d'exécuter de manière compétente un large éventail de tâches distinctes**, indépendamment de la manière dont le modèle est mis sur le marché, et qui **peut être intégré dans une variété de systèmes ou d'applications en aval,** à l'exception des modèles d'IA utilisés pour des activités de recherche, de développement ou de prototypage avant leur mise sur le marché* "

Les acteurs visés par le Règlement sur l'IA

Fournisseur
Développe un système d'IA (ou le fait développer) et le met sur le marché ou met en service sous son propre nom/marque
+ **Fournisseur en aval** qui intègre un modèle d'IA, que le modèle d'IA soit fourni par lui-même ou non

Importateur
Met sur le marché un système d'IA portant le nom/la marque d'une personne en dehors de l'UE.

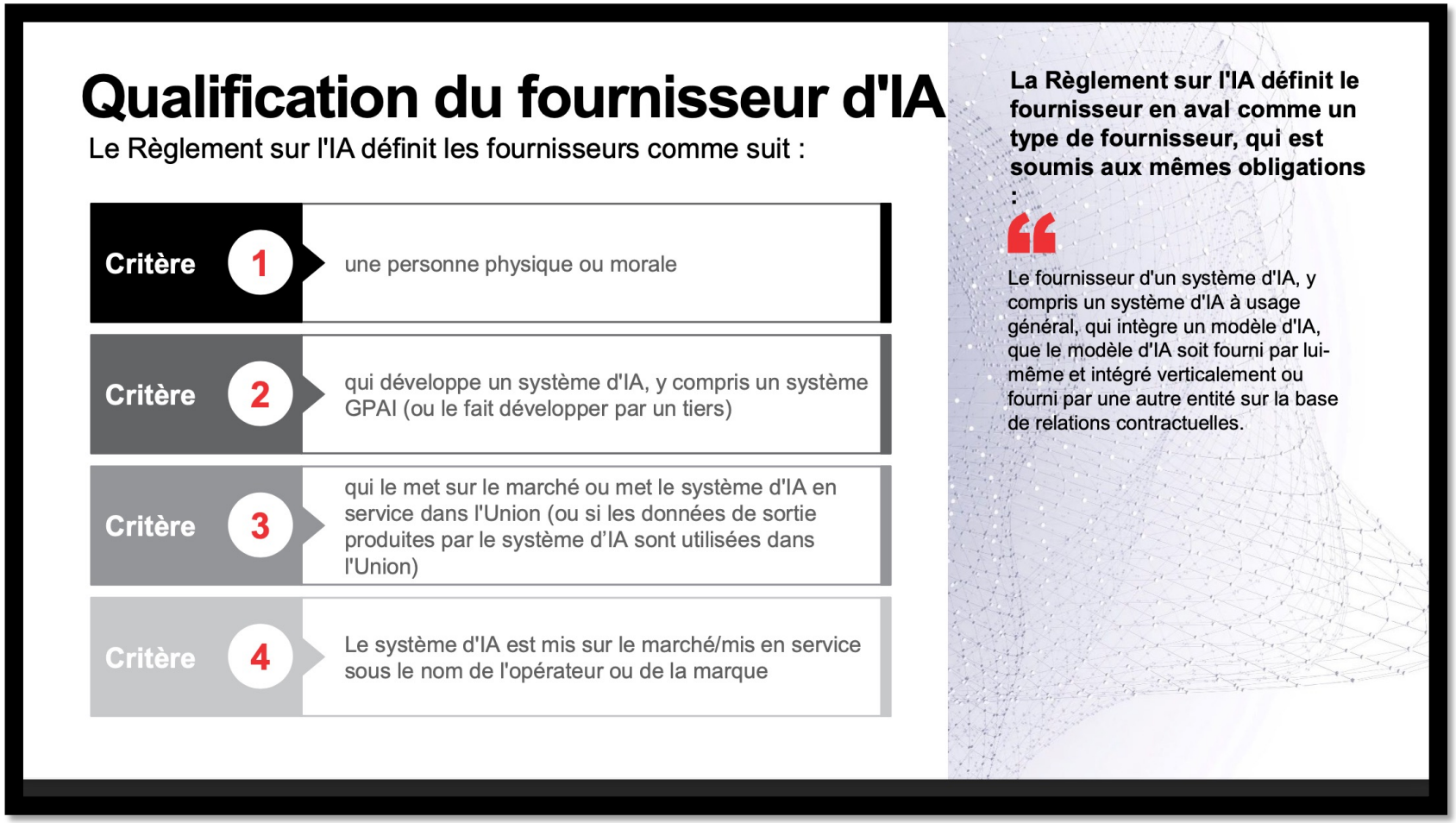


Déployeur
Personne sous l'autorité de laquelle le système est utilisé (c.-à-d. déployeur du système d'IA)

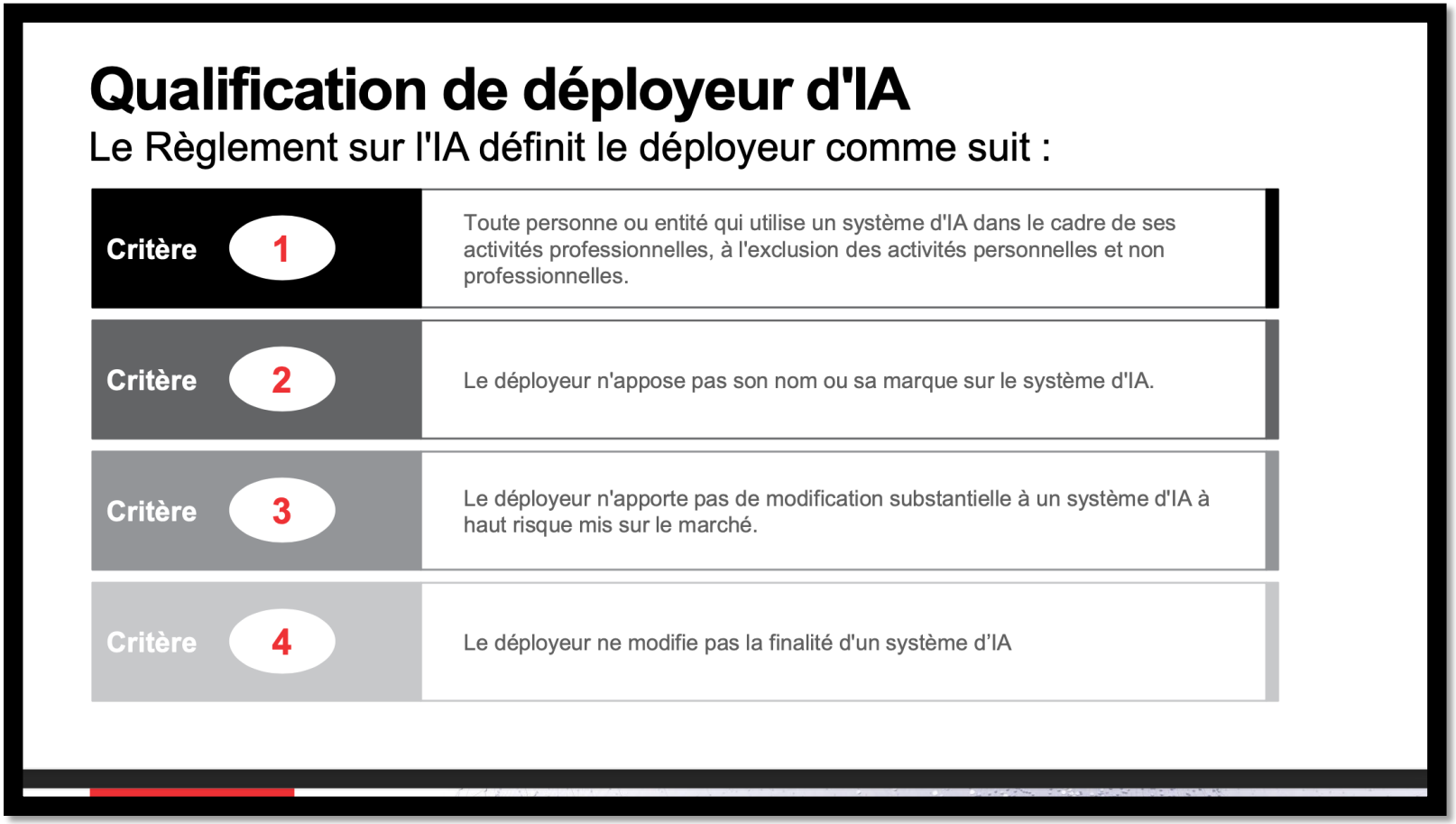
Distributeur
Personne de la chaîne d'approvisionnement autre que le fournisseur ou l'importateur, qui met le système d'IA à disposition sur le marché.

Mandataire (représentant autorisé)
Désigné par le fournisseur en dehors de l'UE par un mandat écrit pour effectuer certaines tâches

SOURCE E. DEHARENG



SOURCE E. DEHARENG



SOURCE E. DEHARENG

Pour les déployeurs de tous les systèmes d'IA (dès le 2 février 2025)

Art. 4 AI Act: Prise de mesures pour garantir un niveau suffisant de **maîtrise de l'IA** pour le personnel et autres personnes s'occupant de l'utilisation du système (obligation de moyen, proportionnée au niveau de risque)

Responsabilité des établissement d'enseignement

Exceptions à l'application du Règlement sur l'IA

Recherche scientifique :
systèmes d'IA ou modèles d'IA spécifiquement développés et mis en service uniquement à des fins de recherche et développement scientifiques, et leurs sorties

Activités de recherche, d'essai et de développement relatives aux systèmes d'IA ou modèles d'IA avant leur mise sur le marché ou leur mise en service

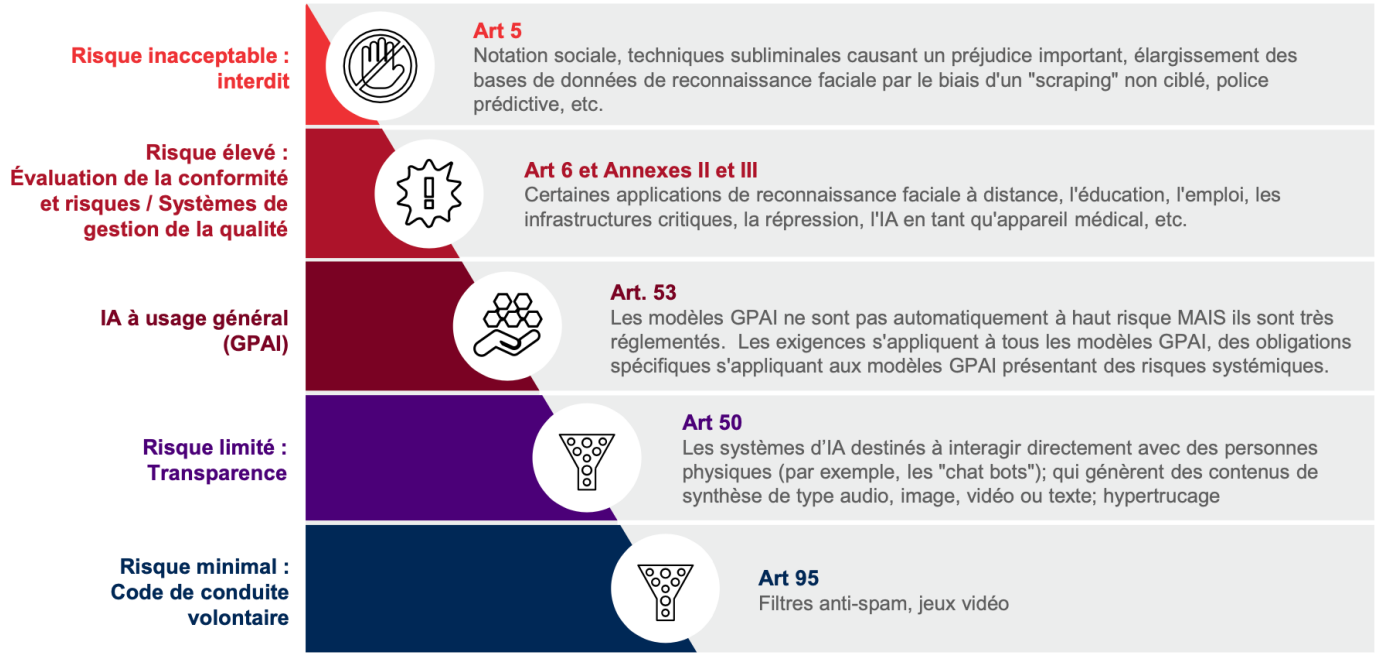
Usage personnel:
déployeurs personnes physiques utilisant des systèmes d'IA dans le cadre d'une activité strictement personnelle à caractère non professionnel.

Sécurité nationale
exclusivement à des fins militaires, de défense ou de sécurité nationale + autorités publiques de pays tiers pour coopération internationale services répressifs

Licence libre
systèmes d'IA publiés dans le cadre de licences libres et ouvertes, sauf systèmes d'IA à haut risque, prohibés ou soumis à obligations de transparence.

SOURCE E. DEHARENG

Niveaux de risque au titre du Règlement sur l'IA



SOURCE E. DEHARENG

Niveau requis de maîtrise de l'IA (art. 4)

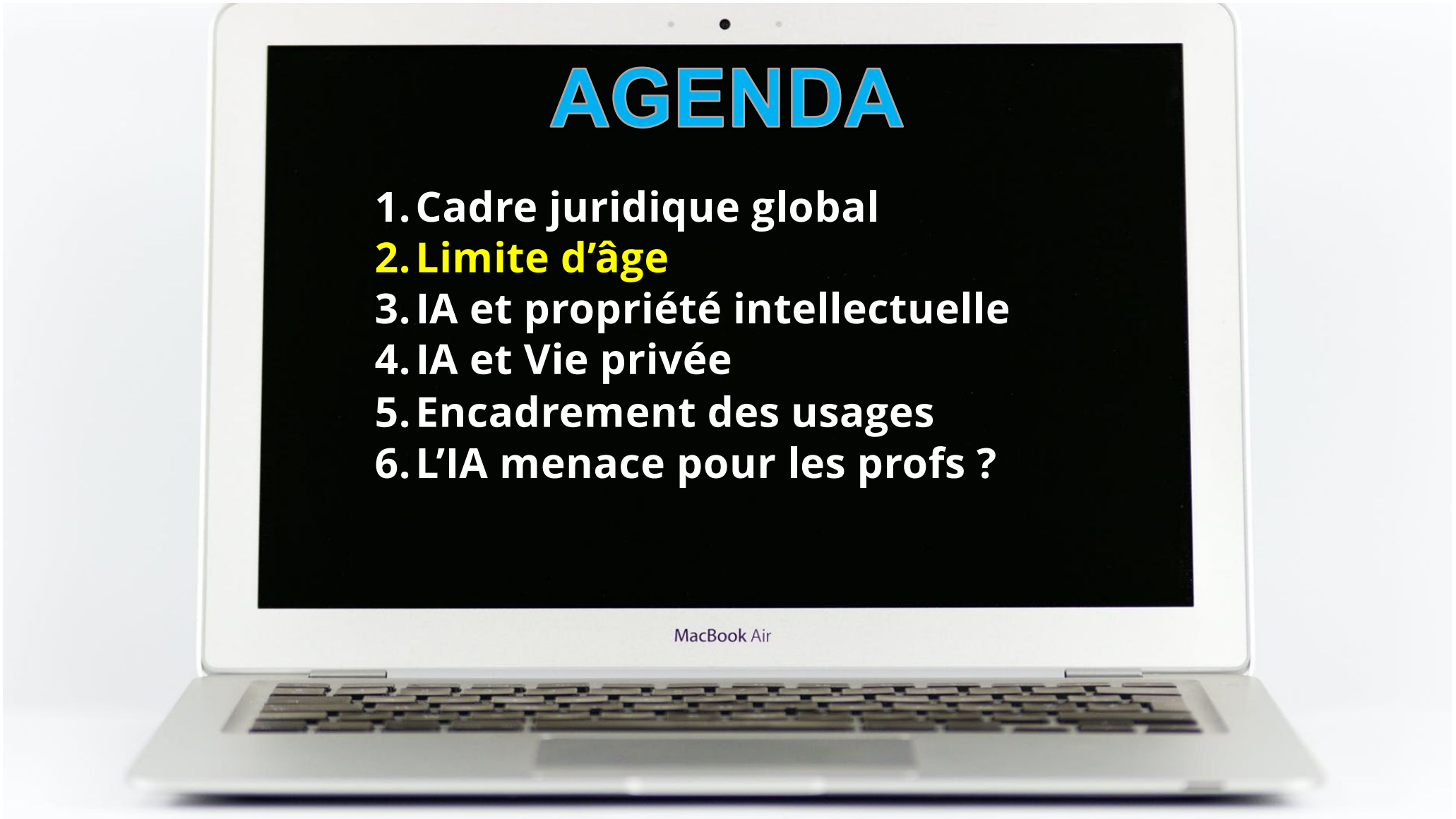
- Par "**maîtrise de l'IA**", on entend les compétences, les connaissances et la compréhension qui permettent aux fournisseurs, aux déployeurs et aux personnes concernées, compte tenu de leurs droits et obligations respectifs dans le contexte du Règlement sur l'IA, de déployer des systèmes d'IA en toute connaissance de cause, ainsi que de prendre conscience des possibilités et des risques de l'IA et des préjudices potentiels qu'elle peut causer - article 3, § 56, de la loi sur l'IA.
- Les fournisseurs et déployeurs sont tenus de prendre des mesures pour **garantir un niveau suffisant de maîtrise de l'IA** pour leur **personnel** et autres personnes s'occupant du fonctionnement et de l'utilisation des systèmes d'IA pour leur compte, en tenant compte de leur expérience et formation et du contexte.
- Responsabilité permanente
- La conformité doit être démontrée

SOURCE E. DEHARENG

Conformité à l'AI Act : les 10 étapes

1. Dressez un inventaire de vos systèmes/modèles d'IA et déterminez s'ils entrent dans le champ d'application de l'AI Act
2. Classez vos systèmes/modèles d'IA
3. Identifiez votre rôle pour chaque système/modèle d'IA
4. Définissez vos obligations pour chaque système/modèle d'IA
5. Identifiez les éventuels chevauchements réglementaires
6. Dressez un inventaire de la documentation & processus existants et procéder à une analyse des lacunes
7. Identifiez vos ressources internes et besoins de ressources complémentaires
8. Préparez une feuille de route et répartissez les responsabilités
9. Suivez l'évolution de la réglementation
10. Impliquez-vous dans les "bacs à sable réglementaires" et les consultations publiques

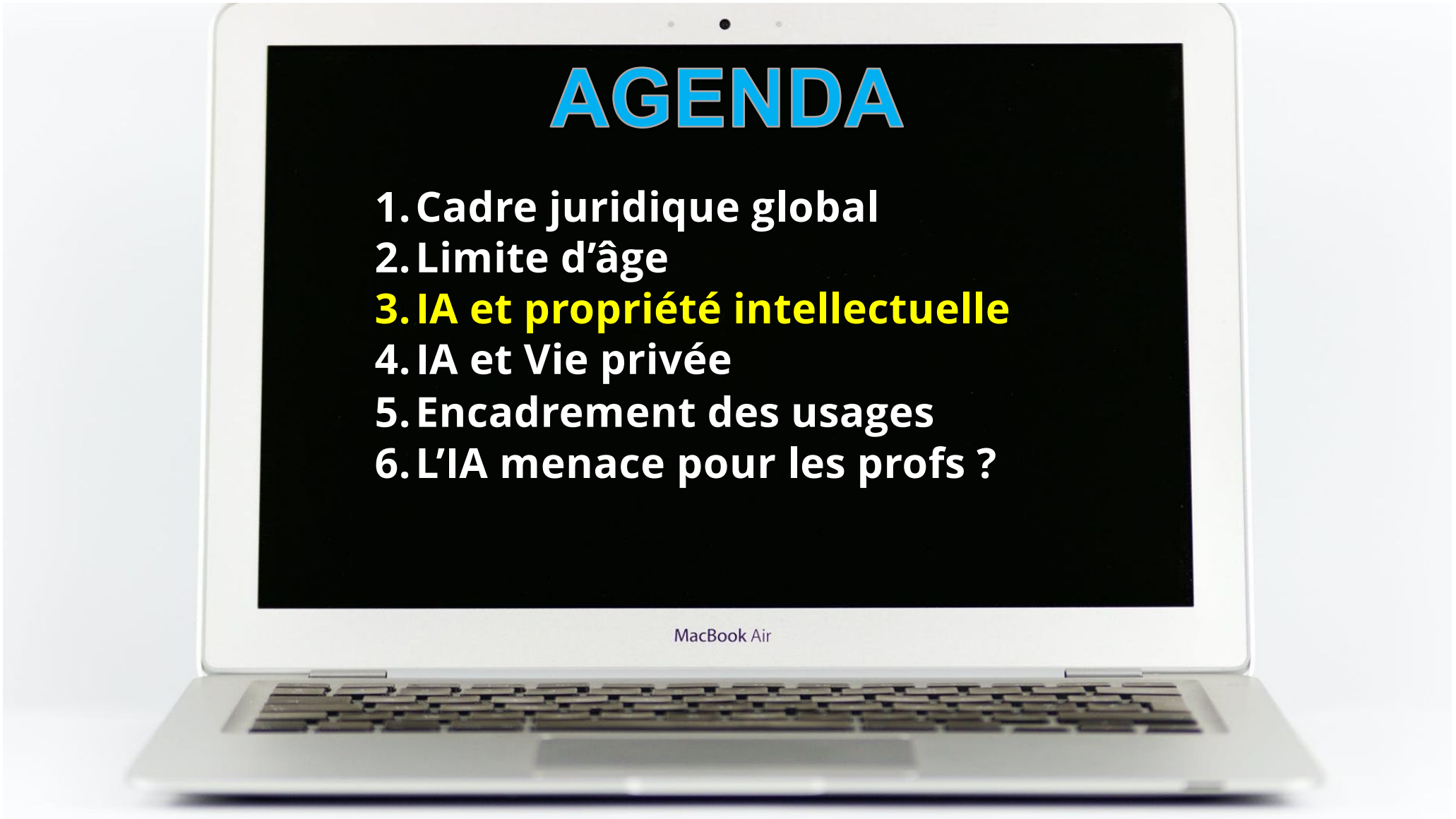
SOURCE AG HAIE, STEPTOE


AGENDA
1. Cadre juridique global
2. Limite d'âge
3. IA et propriété intellectuelle
4. IA et Vie privée
5. Encadrement des usages
6. L'IA menace pour les profs ?
MacBook Air

unesco

Une limite d’âge de 13 ans

Le Guide de l'UNESCO présente ensuite sept étapes clés que les gouvernements doivent suivre pour réglementer l'IA générative et établir des cadres politiques pour son utilisation éthique dans l'éducation et la recherche. Il recommande par exemple l'adoption de normes mondiales, régionales ou nationales en matière de protection des données et de vie privée. Il fixe également une limite d'âge de 13 ans pour l'utilisation des outils d'IA dans les salles de classe, et appelle à former les enseignants spécifiquement sur ce sujet.

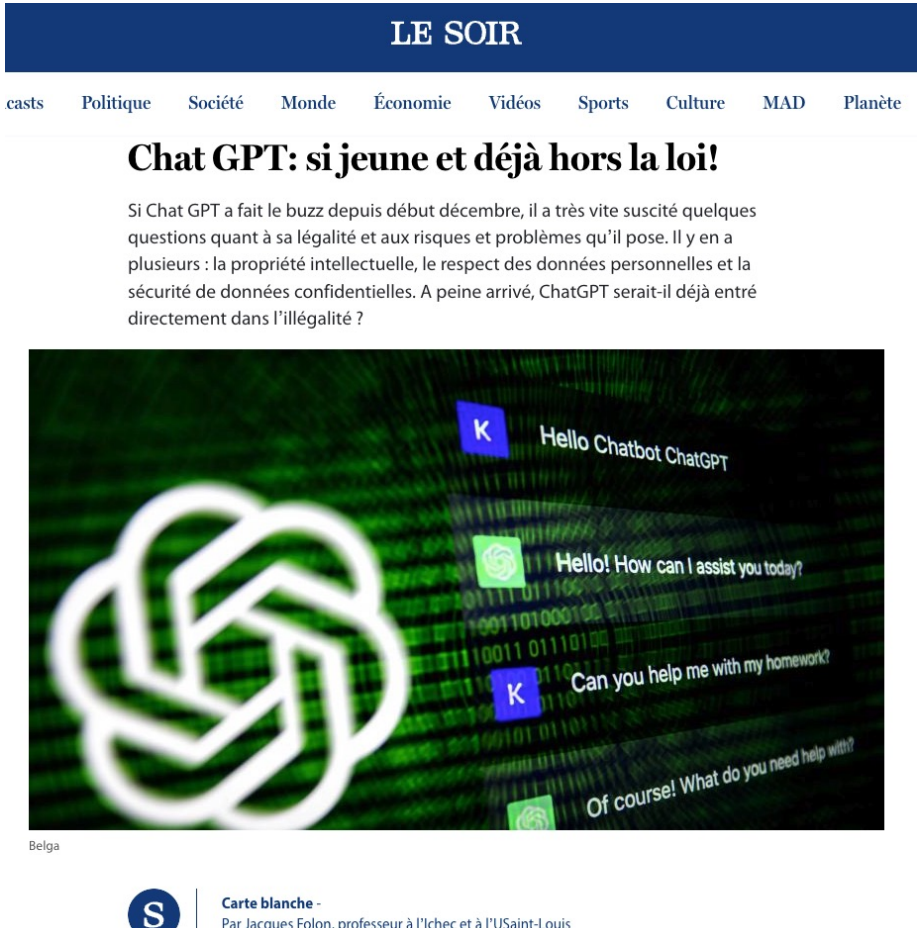

AGENDA
1. Cadre juridique global
2. Limite d'âge
3. IA et propriété intellectuelle
4. IA et Vie privée
5. Encadrement des usages
6. L'IA menace pour les profs ?
MacBook Air


COPYRIGHT CLAIM
TAB

Le copyright peut stopper l'essor de l'IA, selon Yann LeCun, l'un des pères de cette technologie

« Si l'on déclare que c'est une violation copyright, je vous le dis tout de suite, l'industrie de l'IA s'arrête. Ça ne peut pas marcher sans ». « Il va falloir trouver un moyen de ménager la chèvre et le chou » peut-être avec des plates-formes qui mettraient en rapport ceux qui produisent des contenus et ceux qui entraînent les modèles, avec « des droits » d'un côté et « des revenus » en face.

ChatGPT est-il un vulgaire plagiaire ?



LE SOIR

casts Politique Société Monde Économie Vidéos Sports Culture MAD Planète

Chat GPT: si jeune et déjà hors la loi!

Si Chat GPT a fait le buzz depuis début décembre, il a très vite suscité quelques questions quant à sa légalité et aux risques et problèmes qu'il pose. Il y en a plusieurs : la propriété intellectuelle, le respect des données personnelles et la sécurité de données confidentielles. A peine arrivé, ChatGPT serait-il déjà entré directement dans l'illégalité ?

Belga

S | **Carte blanche** -
Par Jacques Folon, professeur à l'Ichec et à l'USaint-Louis

Quelles sont les questions soulevées par l'utilisation de ChatGPT ?

ChatGPT se révèle particulièrement intéressant pour les créateurs de contenus. Blogueurs, rédacteurs, journalistes, ou encore avocats et juristes, vont devoir se familiariser avec ce nouvel outil. Il révolutionne d'ailleurs déjà leur pratique professionnelle. Toutefois, des questions parfois vertigineuses demeurent concernant la propriété, l'utilisation et l'exploitation commerciale des contenus produits par l'Intelligence Artificielle :

- Qui est considéré comme propriétaire du contenu ? Est-ce l'entité qui a créé l'IA ou celle qui a fourni les données d'entraînement ou l'utilisateur ?
- Le contenu bénéficie-t-il d'une protection par le droit d'auteur ?
- Y a-t-il une violation des droits d'auteur lorsqu'un contenu généré par une IA est utilisé sans autorisation ?
- Qui est responsable en cas d'utilisation illégale ou d'atteinte aux droits des tiers / contrefaçons de contenus générés par ChatGPT ?
- Est-ce que je peux agir en contrefaçon ou en concurrence déloyale et parasitaire si un contenu généré par l'IA que j'exploite est copié par un concurrent ?

https://www.tlmr-avocats.com/la-propriete-des-contenus-chatgpt/

JA

en tant que spécialiste de la propriété intellectuelle, je me demande qui est l'auteur de tes textes et s'ils sont protégés par le droit d'auteur

Je suis une intelligence artificielle développée par OpenAI et mes textes sont générés par un système de traitement automatique du langage naturel. Étant donné que je suis un programme informatique, il n'y a pas d'auteur humain derrière mes textes. Cependant, mes textes sont protégés par le droit d'auteur car ils sont considérés comme des œuvres créatives originales.

OpenAI détient les droits d'auteur sur mes textes, et ils ont pris des mesures pour protéger ces droits en utilisant des licences et des contrats pour réglementer l'utilisation de mes textes. Toute utilisation non autorisée de mes textes constituerait une violation du droit d'auteur, et OpenAI pourrait prendre des mesures pour faire respecter ces droits en vertu de la législation sur la propriété intellectuelle en vigueur dans les pays concernés.

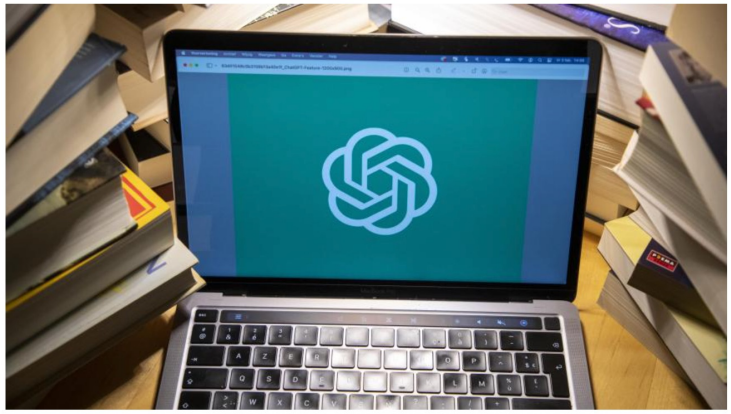
Il est important de souligner que le droit d'auteur s'applique également aux textes générés par une IA. Les propriétaires d'IA peuvent protéger leurs créations en utilisant des licences et des contrats pour réglementer l'utilisation de leurs textes. Les utilisateurs doivent donc respecter les règles et restrictions d'utilisation des textes générés par une IA pour éviter toute violation de la propriété intellectuelle.

Les medias se défendent !

« Disruption » : GPTBot, le nouveau robot d'openAI qui aspire les contenus d'internet déjà bloqué par de nombreux sites !

Malédiction ? Maladie de famille ? Après les nombreuses critiques de non-respect de la propriété intellectuelle ou du RGPD par ChatGPT, à peine né, GPTBot, le robot aspirateur d'OpenAI, suscite déjà la controverse.

Article réservé aux abonnés



BELGA

Chronique -
Par Jacques Folon

Publié le 9/09/2023 à 13:15 | Temps de lecture: 3 min

Mais qui est Ai-Da, peintre, poète et robot ?

La technologie, plus particulièrement l'intelligence artificielle, constitue-t-elle une menace ou une opportunité pour les artistes ? La question se pose avec Ai-Da, femme robot et artiste...

OLJ / Par Irène MOSALLI, le 16 novembre 2022 à 00h00

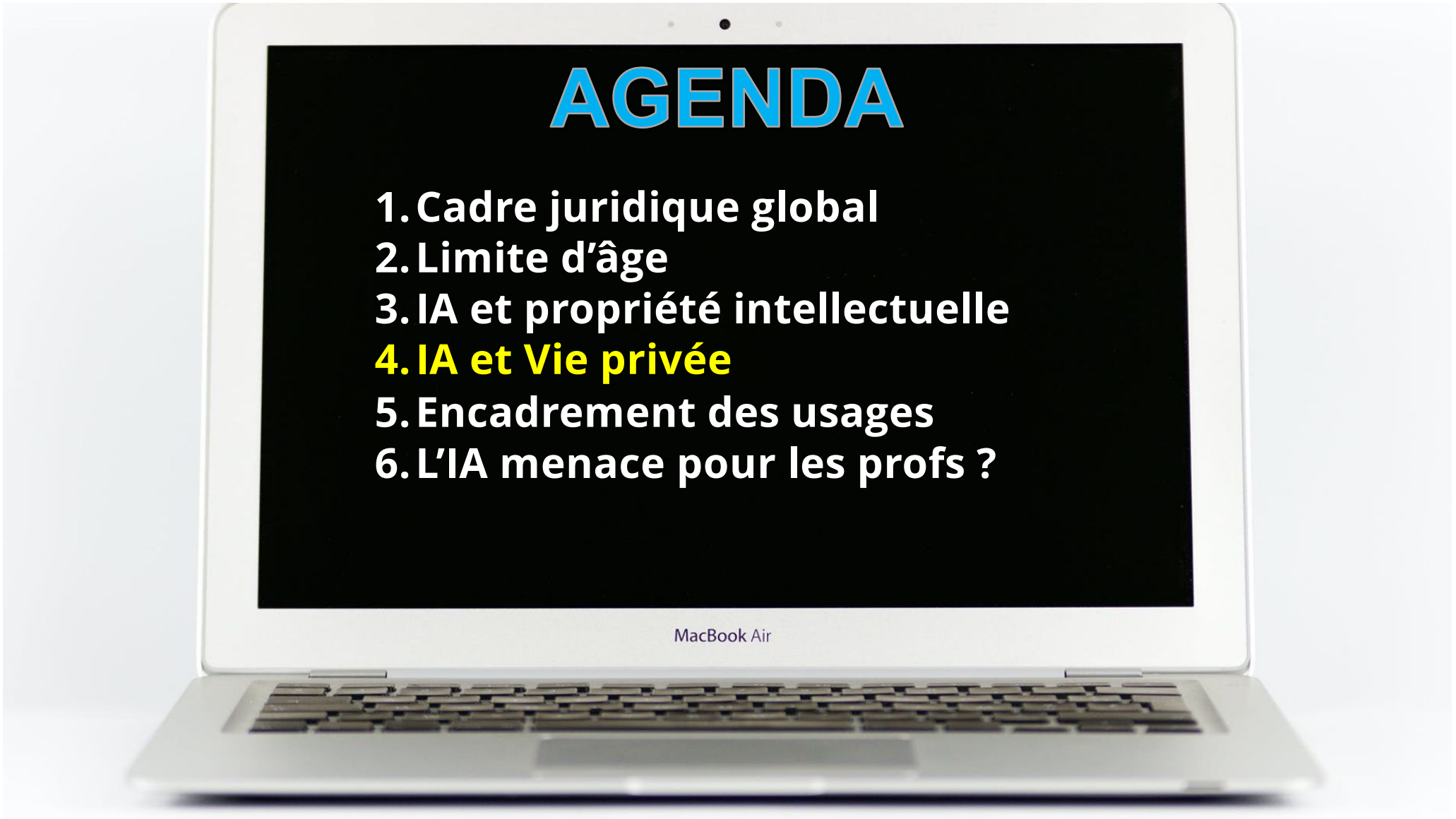
L'artiste robot Ai-Da posant devant une de ses œuvres. Photo tirée du site officiel ai-darobot

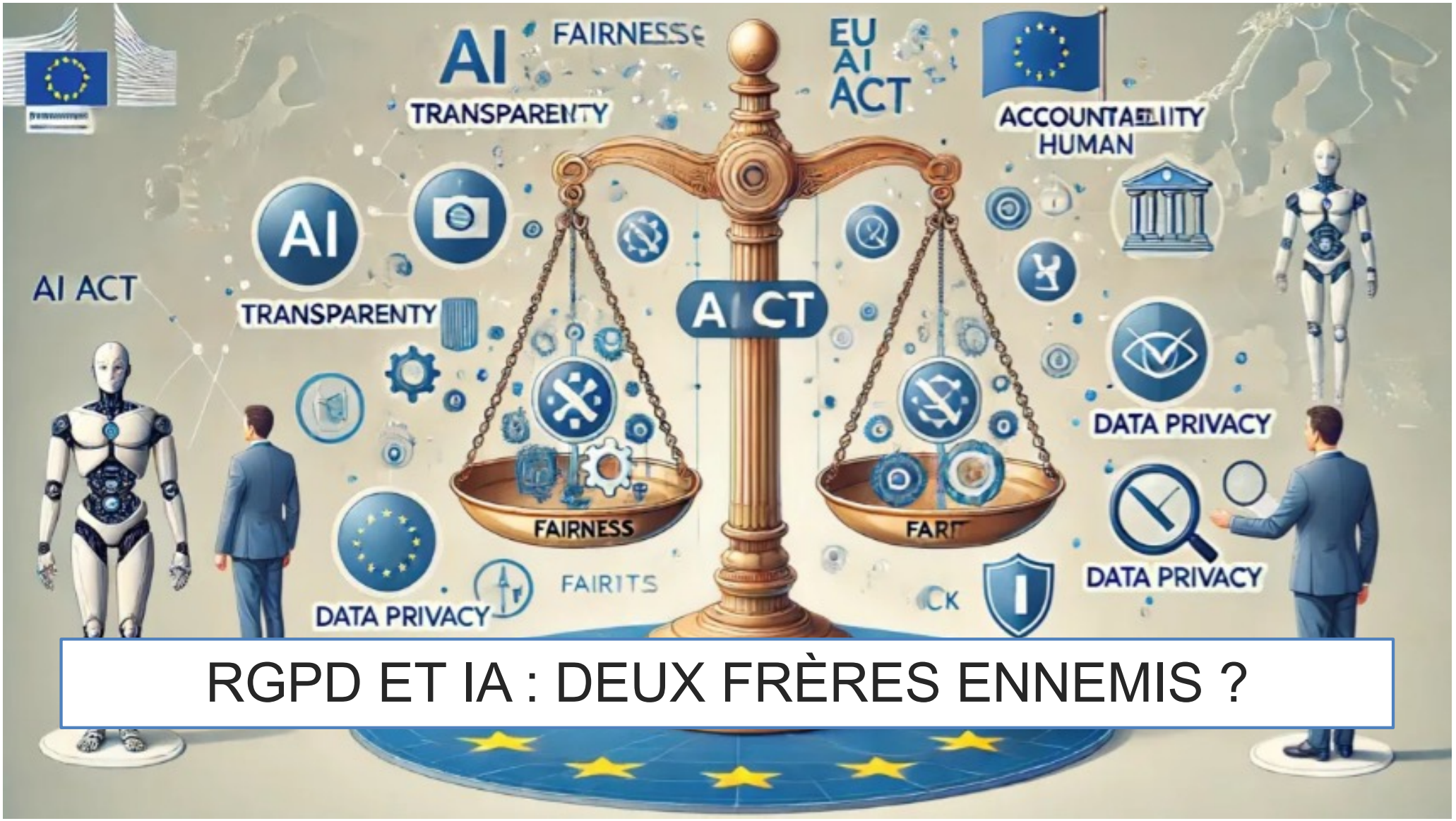
Il semblerait que l'IA ne soit pas un auteur d'où à partir de quand la production d'un étudiant est-elle sienne ?

Je lis dans les chartes qu'il ne faut pas citer l'utilisation de l'IA pour la reformulation, la correction grammaticale/orthographique et la recherche d'idées mais qu'il faut que l'enseignant soit en mesure d'évaluer l'étudiant.

Qu'en est-il selon vous ?

Merci.


AGENDA
1. Cadre juridique global
2. Limite d'âge
3. IA et propriété intellectuelle
4. IA et Vie privée
5. Encadrement des usages
6. L'IA menace pour les profs ?
MacBook Air



RGPD ET IA : DEUX FRÈRES ENNEMIS ?

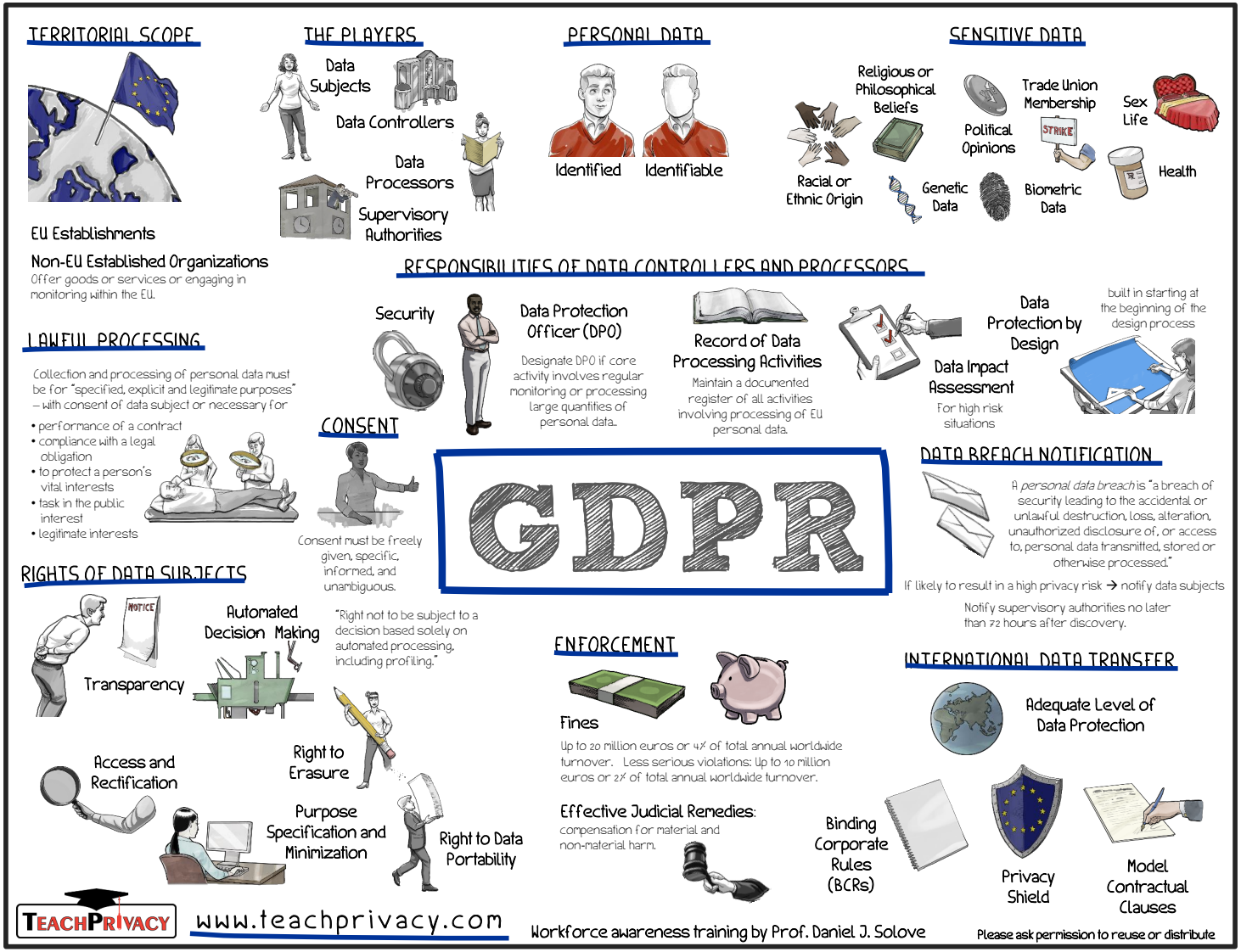
10:10 Les liens entre l'IA et le RGPD - points d'attention pour la protection des données à l'heure du développement de l'IA ?

- Comment veiller au respect des règles de confidentialité et de sécurité lors de l'utilisation de l'IA ?
- Comment permettre le respect de l'obligation de transparence lorsque des décisions sont fondées sur des systèmes d'IA pour lesquels les sources et l'explicabilité des algorithmes sont obscures ?
- Comment recueillir le consentement des individus pour collecter et traiter leurs données personnelles à des fins d'analyse ou de prédiction ?
- Quelles mesures de sécurité robustes mettre en place pour protéger les données traitées par les algorithmes d'IA ?
- À quoi faut-il penser pour permettre l'utilisation de l'IA au sein de votre organisation tout en étant en mesure de répondre aux demandes des personnes concernées (droit d'accès, de rectification et de suppression) ?
- Comment encadrer et accompagner les responsables de traitement quant à l'utilisation de nouvelles technologies afin de sécuriser les traitements de données à caractère personnel ?
- Comment analyser les propositions de la CNIL pour encadrer les projets IA ?

Jacques Folon
DPO
Founder, GDPRFolder.com
Expert, **EDPB**
Auteur du « *Guide de survie du DPO* »
Professeur **ICHEC – USAINT-LOUIS - RENNES SB**

AU RISQUE DE VOUS DÉCEVOIR…
IL Y A BEAUCOUP DE QUESTIONS QUI SE POSENT AU SUJET DES RELATIONS ENTRE IA ET RGPD
ET JE N'AI PAS LA RÉPONSE À TOUTES LES QUESTIONS

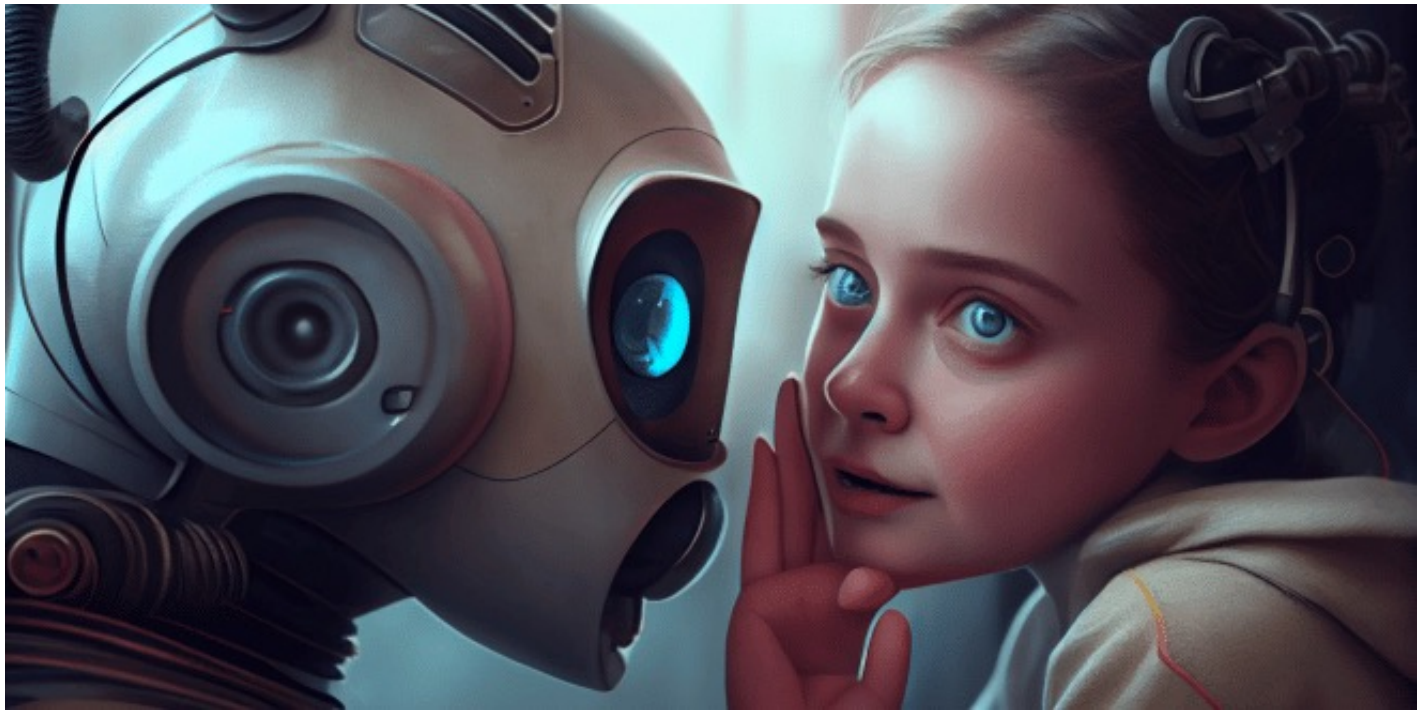
Conséquences pour les écoles



- QUI EST RESPONSABLE DE TRAITEMENT ?
- QUELLES DONNÉES PERSONNELLES ?
- QUELLE EST LA BASE LÉGALE ?
- QUELLE EST LA FINALITÉ ?
- PRIVACY BY DESIGN
- MINIMISATION ET MACHINE LEARNING
- ARCHIVAGE ET DURÉE DE CONSERVATION
- MESURES TECHNIQUES ET ORGANISATIONNELLES
- DROITS DES PERSONNES CONCERNÉES
- PRISES DE DÉCISIONS AUTOMATISÉES
- LES BIAIS DES ALGOS
- LES CRAINTES DES ENTREPRISES
- NÉCESSITÉ DE FORMATION AU RGPD MAIS PAS QUE..

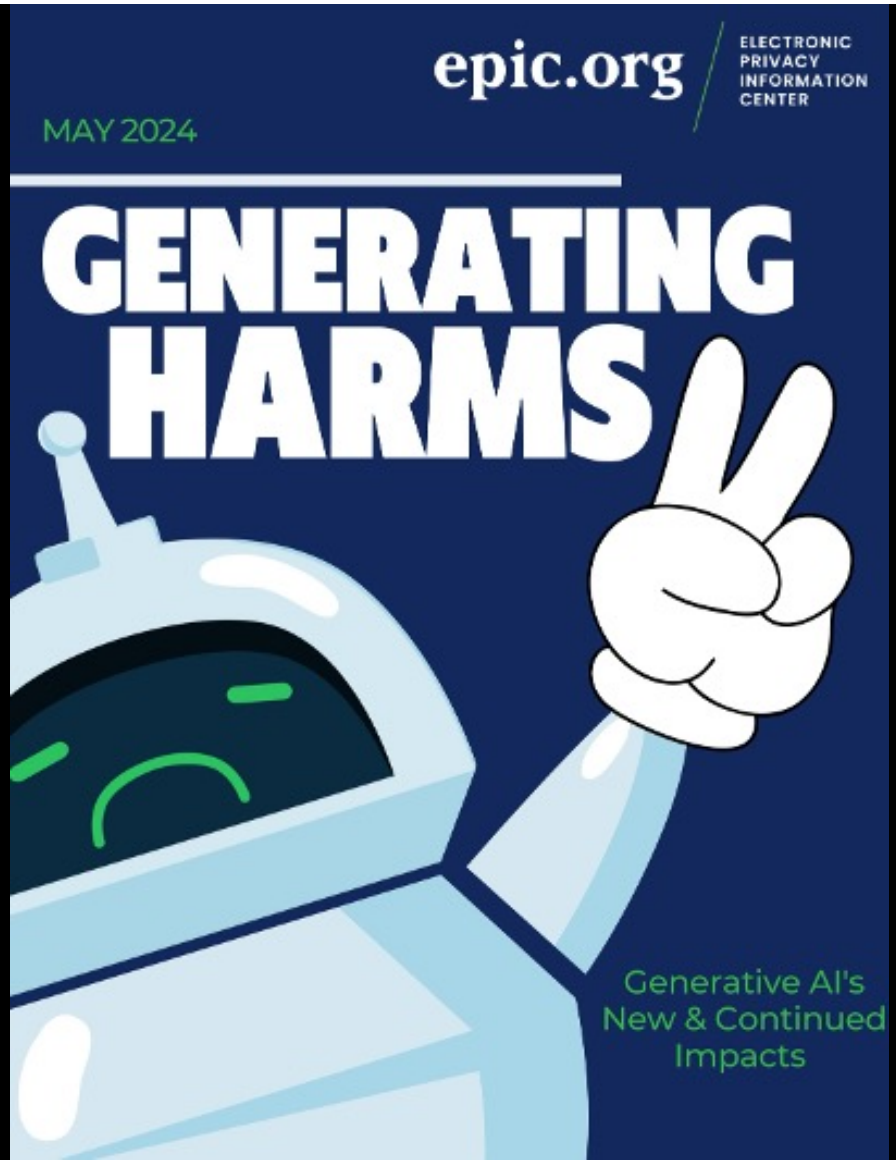
ARRIVÉE DE L'IA ET DES RISQUES EN MATIÈRE DE VIE PRIVÉE

Quels sont les risques au niveau du rgpd si une école introduit ses indicateurs du gouvernement ainsi que des objectifs spécifiques en vue de demander de l'aide à l'IA de lui trouver un plan d'actions cohérent dans le cadre du pilotage des écoles?



Quels sont les dangers d'utiliser dans un prompt à ChatGPT ou Copilot des données confidentielles, par exemple récoltées en stage (paramédical, entreprise ou autre) ?

Est-ce plus sûr, dans une optique de protection des données, d'utiliser les versions pro ou payantes ?



HARMS

- **Physical**: Generative AI systems may reveal data that could put a person at risk, whether real or perceived. For example, sensitive information, such as a person's email address or home address may be revealed to stalkers, abusers, or other bad actors.
- **Reputational/Relationship/Social Stigmatization**: Generative AI can reveal a person's sensitive information, which may result in damage to reputation or social stigmatization. A person's sexuality may be inferred where sexual images, information related to sexual behaviors, or location information were fed to an LLM.
- **Economic**: Businesses whose trade secrets have been incorporated into training sets or individuals whose economic information has been incorporated face potential economic injuries.
- **Psychological**: Individuals may suffer from anxiety or fear due to the lack of control over removing their personal data from training sets and may fear consequences from the ways in which the data is used. People may also be angry, frustrated, or feel exploited that their information has been used to feed a for-profit LLM, even where the data is anonymized.
- **Autonomy**: Individuals cannot control the collection and use of their personal information, including whether it is used to train datasets.
- **Discrimination**: Biased data can be scraped and fed into an LLM, which will likely then produce biased results built from historic discrimination.

A recent report[50] found that "an organization can expect around 660 daily prompts to ChatGPT for every 10,000 users, with source code being the most frequently exposed type of sensitive data, posted by 22 out of 10,000 enterprise users and generating, on average, 158 incidents monthly. This is ahead of regulated data (on average, 18 incidents), intellectual property (on average, four incidents), and posts containing passwords and keys (on average, four incidents) every month."[51]

OpenAI's chatbot ChatGPT falsely accused an American law professor by including him in a generated list of legal scholars who had sexually harassed someone, citing a non-existent *The Washington Post* report.

In an opinion piece published in USA Today, professor Jonathan Turley from George Washington University wrote that he was falsely accused by ChatGPT of assaulting students on a trip he "never took" while working at a school he "never taught at".

"It is only the latest cautionary tale on how artificial 'artificial intelligence' can be," he said on Monday, highlighting some of the accuracy and reliability issues with AI chatbots like ChatGPT.

Microsoft, a strong proponent of generative AI and the developer of one of the most popular generative AI systems, accidentally incorporated two employees' back up computers—including passwords, encryption keys, and Teams threads—into its training data.[53]

We should not underestimate the real threats coming from AI, mostly GenAI.

13/9/2023

Leonardo Cervera Navas

Director of the European Data Protection Supervisor.

EDPS

European Data Protection Supervisor

“Nous devrons avoir une interprétation souple du RGPD dans le cadre du développement de l’intelligence artificielle”

Journée d’étude DPOPRO du 25/8/2018 à la FEB

"*Les menaces associées à l’essor de cette technologie sont multiples : peur de voir disparaître certains emplois, crainte d’une utilisation à des fins malveillantes, atteintes à la propriété intellectuelle, exploitation illicite de données personnelles…*"
Pour *créer les conditions d'une utilisation éthique, responsable et respectueuse de nos valeurs*, il faut *comprendre, accompagner et contrôler. On ne peut bien réguler qu’un objet que l'on comprend*

Présidente de la Cnil Marie-Laure Denis
18/9/2023

QUELLES DONNÉES PERSONNELLES ?

- LES DONNÉES DÉJÀ SUR INTERNET
- LES DONNÉES INCLUSES DANS LES PROMPTS
- L'IA DISPOSE-T-ELLE DE L' AUTORISATION DE LES UTILISER ?
- LE BLOCAGE DU CRAWLER DE OPENAI

LA COLLECTE DES DONNÉES SANS AUTORISATION !

LE SOIR

ions Opinions Podcasts Politique Société Monde Économie Vidéos

ACCUEIL • OPINIONS • CHRONIQUES

« Disruption » : GPTBot, le nouveau robot d'openAI qui aspire les contenus d'internet déjà bloqué par de nombreux sites !

Malédiction ? Maladie de famille ? Après les nombreuses critiques de non-respect de la propriété intellectuelle ou du RGPD par ChatGPT, à peine né, GPTBot, le robot aspirateur d'OpenAI, suscite déjà la controverse.

Article réservé aux abonnés

Par Jacques Folon

Publié le 9/09/2023 à 13:15 | Temps de lecture: 3 min

La création de programmes malveillants

Sur les forums clandestins de hackers, les cybercriminels débutants expliquent comment ils se servent de ChatGPT pour créer de nouveaux chevaux de Troie, sans avoir aucune connaissance en programmation.

Pour le moment, les chatbots ne peuvent rivaliser qu'avec les créateurs de virus novices, mais dans le futur ?

La recherche de vulnérabilités

la recherche automatique de code vulnérable.
Le bot « lit » le code de l'application décompilée et identifie les endroits qui pourraient être vulnérables.
De plus, le chatbot fournit le code Python conçu pour l'exploitation de la vulnérabilité (preuve de concept, ou PoC).
L'outil n'est pas parfait mais est utile pour les cybercriminels et les défenseurs.

L’hameçonnage ou le phishing

La rédaction de textes convaincants est le point fort de GPT-3 et ChatGPT. Ainsi, il est fort probable qu’il y ait **déjà** des attaques automatiques d’hameçonnage ciblé qui se servent des chatbots.

Le problème principal de l’envoi massif de messages d’hameçonnage est qu’ils sonnent faux, avec un texte beaucoup trop générique qui ne s’adresse pas directement au destinataire.

Quant à l’hameçonnage ciblé, lorsqu’un vrai cybercriminel rédige un message pour une seule victime, c’est assez coûteux.

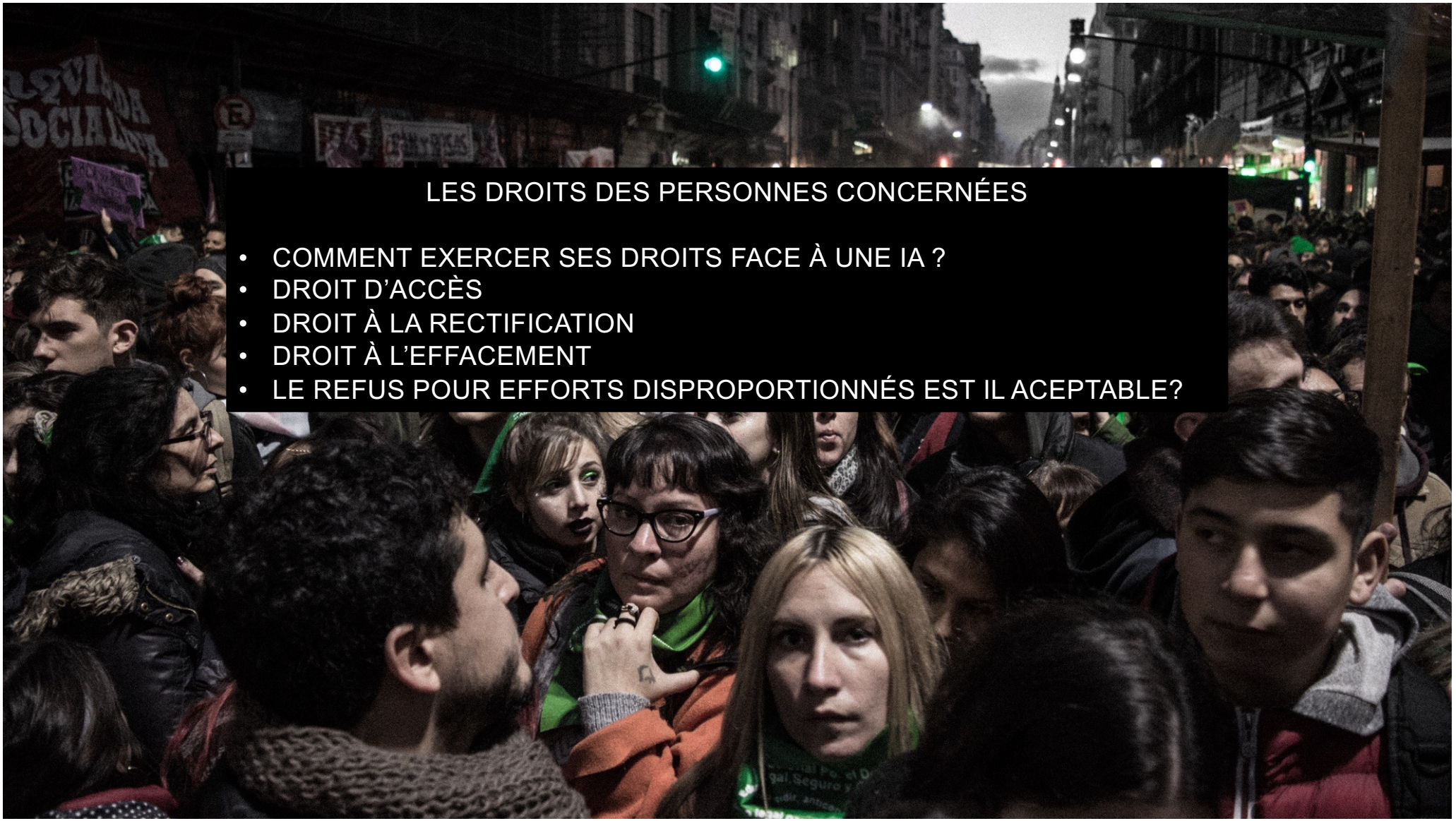
ChatGPT est configuré pour modifier radicalement l’équilibre des pouvoirs puisqu’il permet aux cybercriminels de générer des messages personnalisés et persuasifs à échelle individuelle.

Moment de l'attaque	Objectif de l'attaque		
	Manipulation	**Infection**	**Exfiltration**
Phase d'apprentissage		Attaques par empoisonnement (*poisoning attacks*) Attaques par porte dérobée (*backdooring attacks*)	Attaques par inférence d'appartenance (*membership inference attacks*) Attaques par inversion (*model inversion attacks*) Attaques d'extraction de modèle (*model extraction attacks*)
Phase de production	Attaques par évasion (*evasion attacks*) Attaques par reprogrammation (*reprogramming attacks*) Attaques par déni de service		

Tableau 1. Taxonomie des attaques d'un système d'IA.

https://linc.cnil.fr/sites/linc/files/atoms/files/linc_cnil_dossier-securite-systemes-ia.pdf

Petite taxonomie des attaques des systèmes d'IA 8
Attaques par manipulation 9
Attaques par évasion (*evasion attacks*) 9
Attaques par reprogrammation (*adversarial reprogramming attacks*) 13
Attaques par déni de service 14
Attaques par infection 14
Attaque par empoisonnement (*poisoning attacks*) 15
Attaques par portes dérobées (*backdooring attacks*) 15
Attaques par exfiltration 16
Attaques par inférence d'appartenance (*membership inference attacks*) 17
Attaques par inversion de modèle (*model inversion attacks*) 19
Attaques d'extraction de modèle (*model extraction attacks*) 20



LES DROITS DES PERSONNES CONCERNÉES

- COMMENT EXERCER SES DROITS FACE À UNE IA ?
- DROIT D'ACCÈS
- DROIT À LA RECTIFICATION
- DROIT À L'EFFACEMENT
- LE REFUS POUR EFFORTS DISPROPORTIONNÉS EST IL ACEPTABLE?

ChatGPT provides false information about people, and OpenAI can't correct it

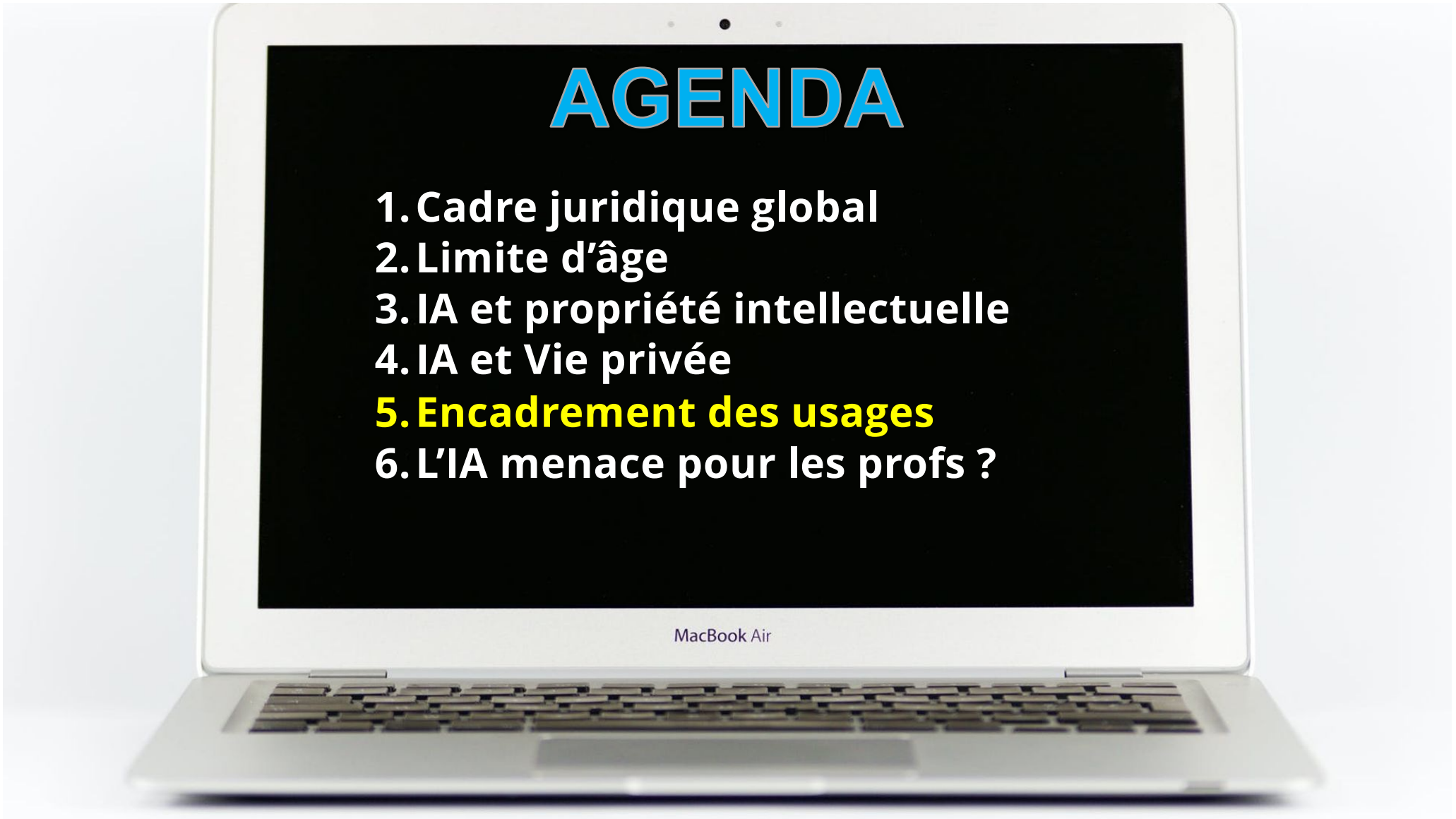
Data Subject Rights / 29 April 2024

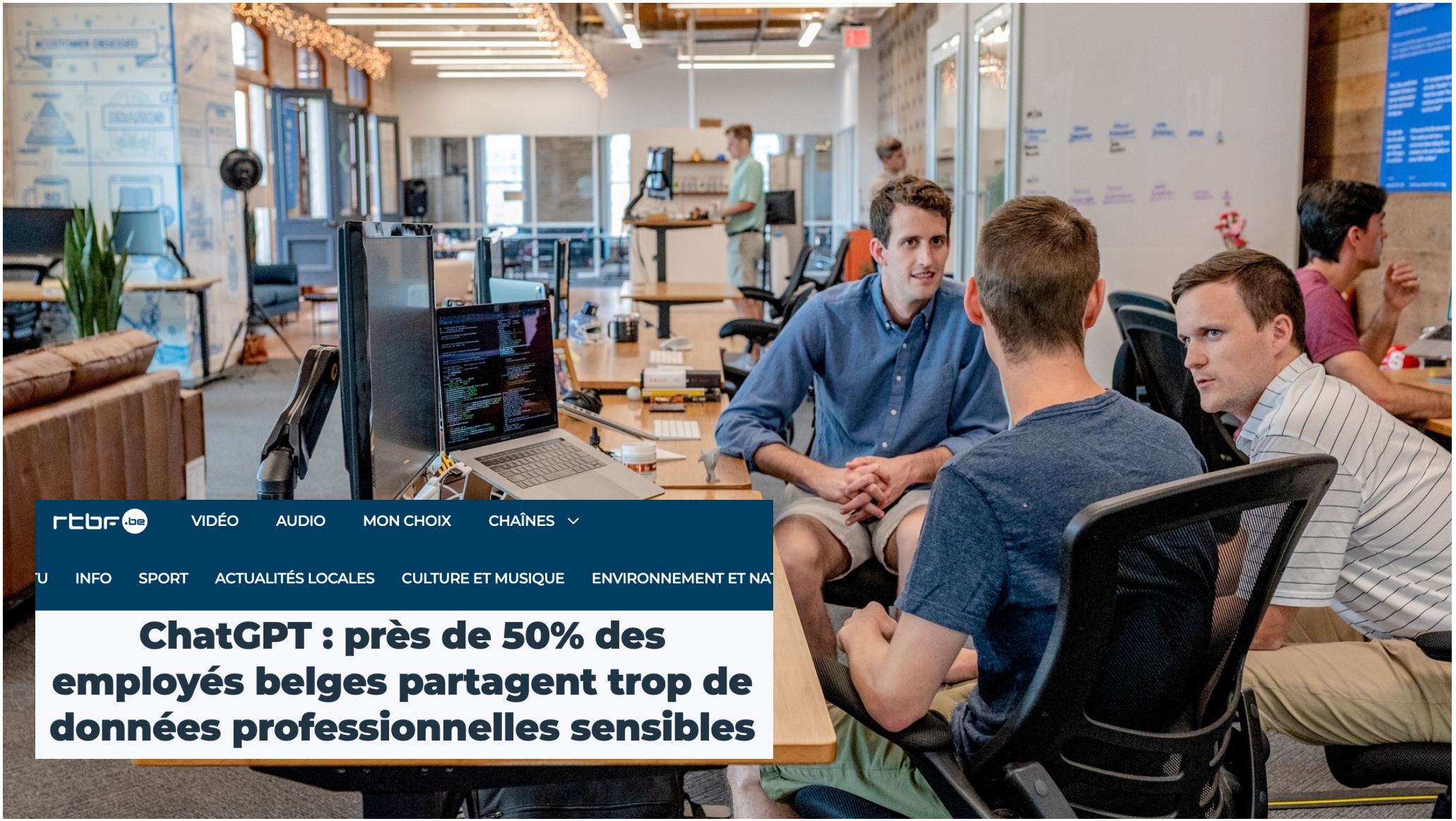
In the EU, the GDPR requires that information about individuals is accurate and that they have full access to the information stored, as well as information about the source. Surprisingly, however, OpenAI openly admits that it is unable to correct incorrect information on ChatGPT. Furthermore, the company cannot say where the data comes from or what data ChatGPT stores about individual people. The company is well aware of this problem, but doesn't seem to care. Instead, OpenAI simply argues that "*factual accuracy in large language models remains an area of active research*". Therefore, *noyb* today filed a complaint against OpenAI with the Austrian DPA.

RGPD ET AI : AMIS OU ENNEMIS?

L'AVENIR NOUS LE DIRA…

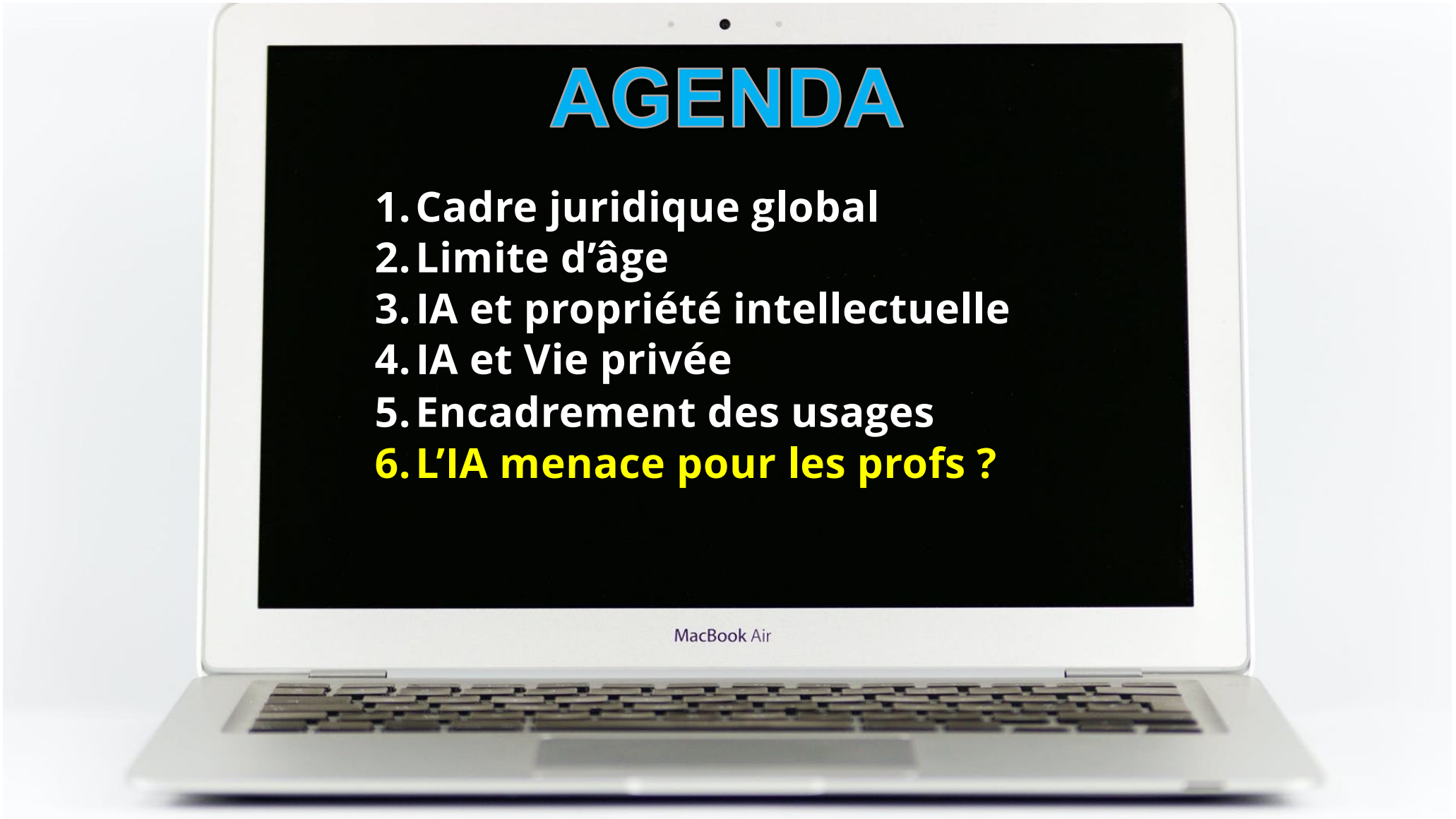
MAIS LORSQUE LA TECHNOLOGIE S'OPPOSE AU DROIT C'EST TOUJOURS LA TECHNOLOGIE QUI GAGNE

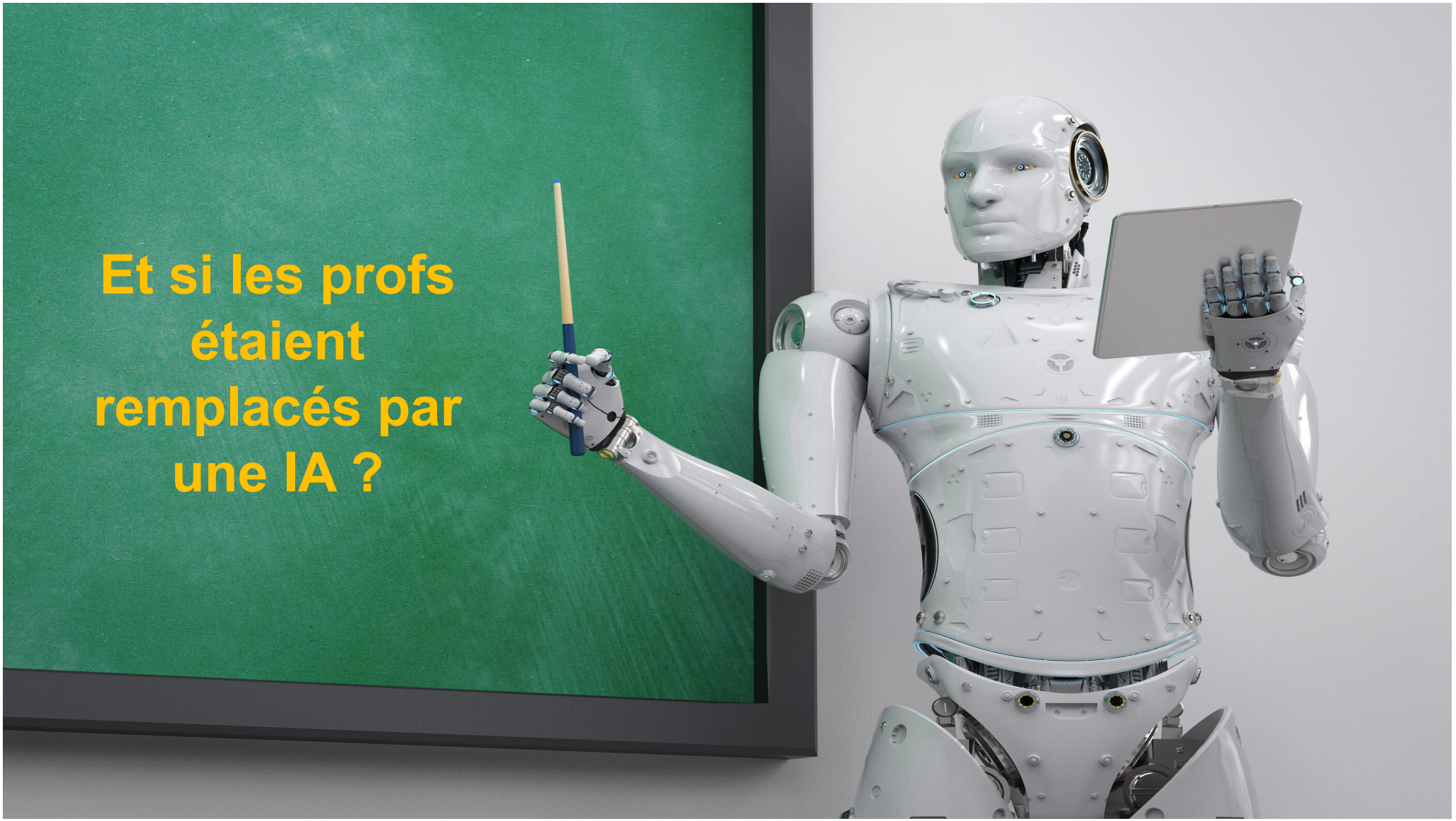

AGENDA
1. Cadre juridique global
2. Limite d'âge
3. IA et propriété intellectuelle
4. IA et Vie privée
5. Encadrement des usages
6. L'IA menace pour les profs ?
MacBook Air


rtbf.be
VIDÉO
AUDIO
MON CHOIX
CHAÎNES
INFO
SPORT
ACTUALITÉS LOCALES
CULTURE ET MUSIQUE
ENVIRONNEMENT ET NA
ChatGPT : près de 50% des employés belges partagent trop de données professionnelles sensibles

- 42% partagent des données sensibles de leur entreprise
- 57% des utilisateurs sondés ne vérifient pas la véracité des réponses avant de les utiliser dans leur travail
- 65% ont déclaré que leur organisation n’a aucune directive ni règle claire concernant l’utilisation de ChatGPT
- Seulement 22% des employés savent comment ChatGPT traite les informations communiquées
- 43% des sondés ne savent pas comment sont traitées leurs données
- *Seuls 18% ont déclaré que les règles étaient formellement énoncées dans un e-mail officiel et un peu moins de 15% dans un document officiel spécifique*"
- Plus de la moitié des employés interrogés (57%) déclarent ne pas vérifier l’exactitude ni la fiabilité du contenu généré par l’IA avant de le faire passer pour leur propre travail.

- Source Karspersky cité par RTBF


AGENDA
1. Cadre juridique global
2. Limite d'âge
3. IA et propriété intellectuelle
4. IA et Vie privée
5. Encadrement des usages
6. L'IA menace pour les profs ?
MacBook Air


Et si les profs étaient remplacés par une IA ?

Les 20 emplois que le GPT-4 peut potentiellement remplacer ainsi que les caractéristiques humaines dévelopées par le logiciel.

	Professions	Caractéristiques humaines
1	Gestionnaire de données	vitesse et précision
2	Représentant(e) commerciale	communication, empathie
3	Correcteur(trice)	sens du détail
4	Assistant(e) juridique	recherche et organisation
5	Comptable	compétences mathématiques
6	Traducteur(trice)	compétences linguistiques
7	Rédacteur(trice)	créativité et écriture
8	Analyste d'études de marché	capacités analytiques
9	Gestionnaire des médias sociaux	création de contenu
10	Planificateur(trice) de rendez-vous	gestion du temps
11	Télévendeur(euse)	communication et persuasion
12	Assistant(e) virtuel	polyvalence et organisation
13	Secrétaire	capacité d'écoute et dactylographie
14	Journaliste	vérification des faits et rédaction
15	Agent de voyage	planification et coordination
16	Professeur(e)	connaissance et enseignement

ChatGPT 4 et les 20 métiers le plus menacés

Amid Faljaoui

17-03-2023, 13:39 • Mise à jour le: 17-03-2023, 13:39 • Source : Trends-Tendances •

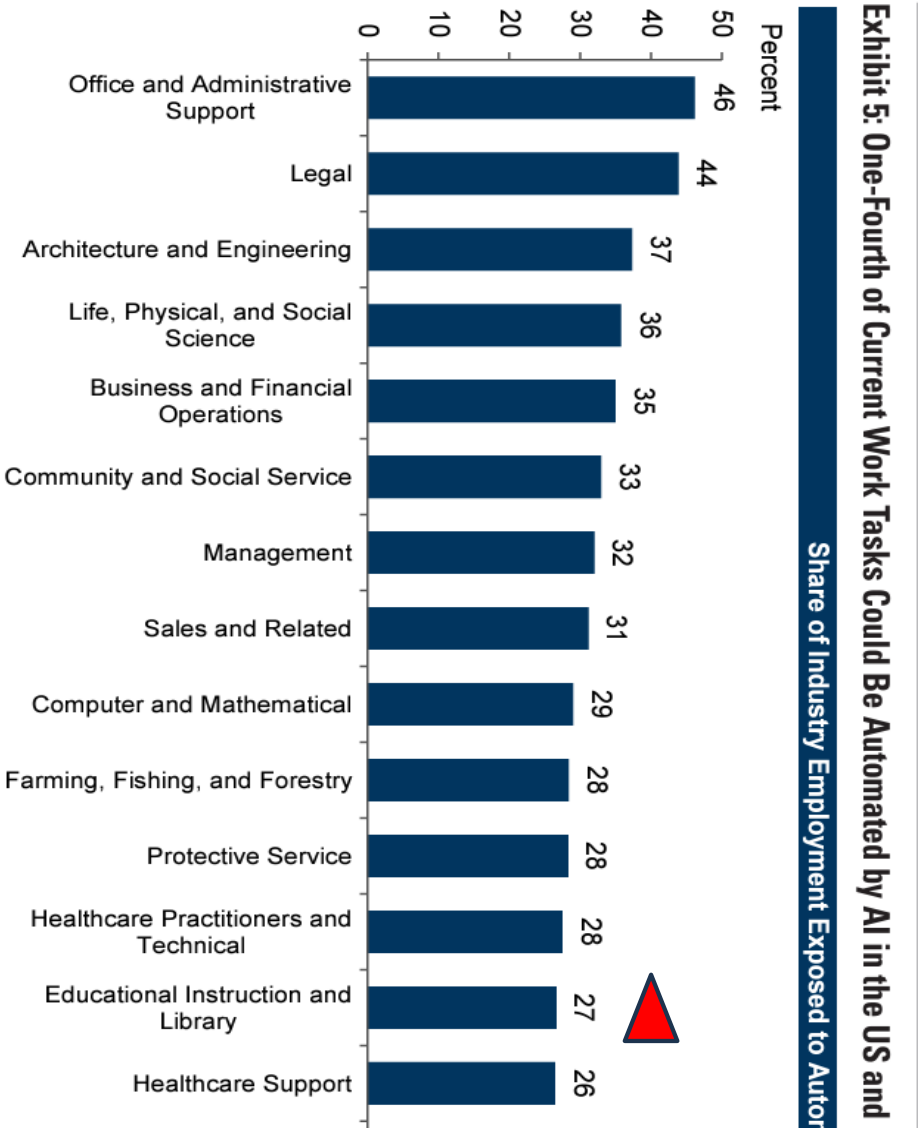
Goldman Sachs | Economics Research

26 March 2023 | 9:05

Global Economics Analyst

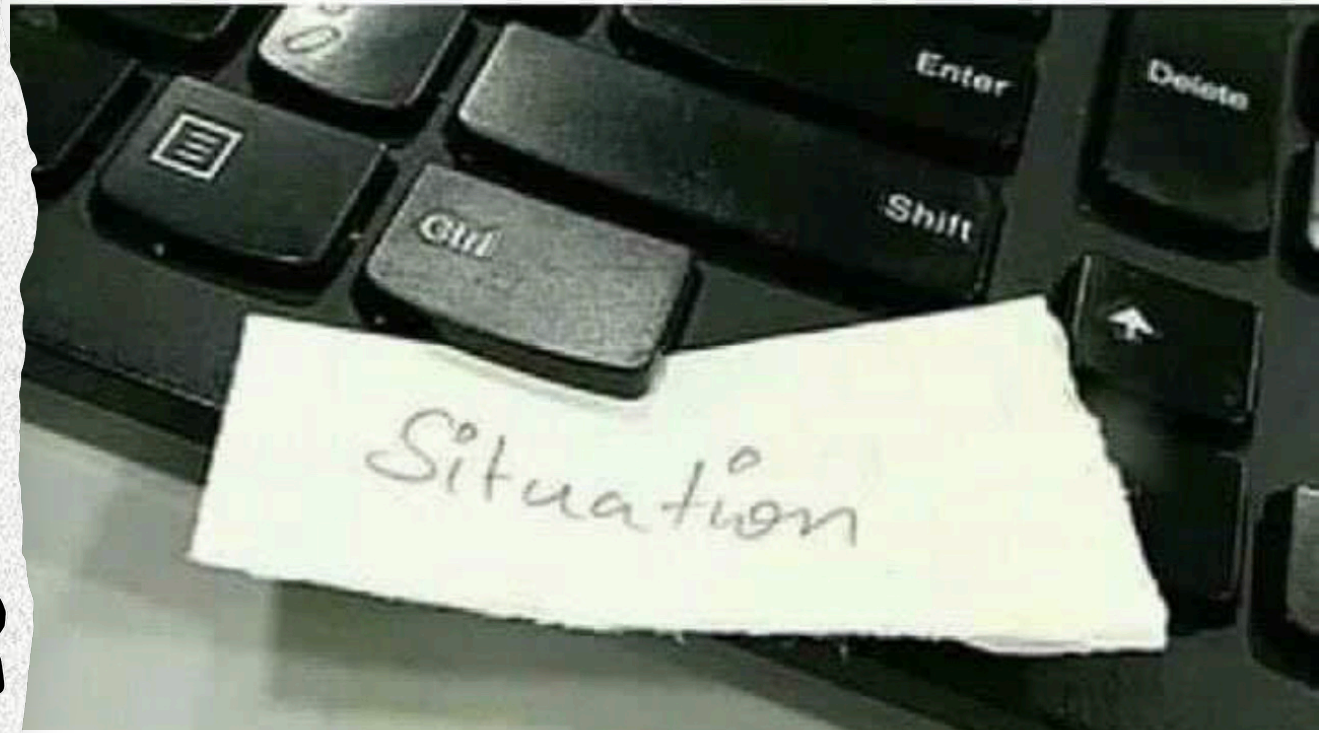
The Potentially Large Effects of Artificial Intelligence on Economic Growth (Briggs/Kodnani)

Importance de la valeur ajoutée !

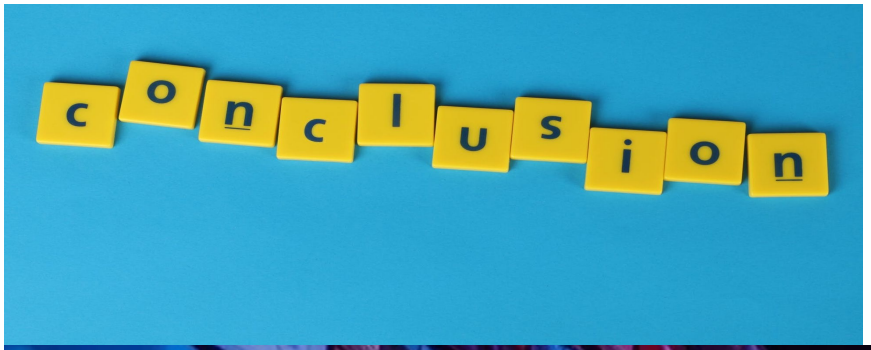


Devons-nous nous réjouir ou avoir peur ?

La situation est sous contrôle.




The Sky is not the Limit
It's just the Beginning



Importance de la veille permanente


THANK YOU

SOURCES

- ALAIN STROWEL, PRESENTATION EFFECTUEE LORS DE LA CONFERENCE ABILWAYS
- ANNE GABRIELLE HAIE,PARTNER STEPTOE, IDEM
- ELISABETH DEHARENG, PARTNER, BAKER, MCKENZIE, IDEM
- https://www.steptoe.com/en/news-publications/steptechtoe-blog.html?tab=blog_posts
- Perplexity (avec vérifications ;-)
- Gemini
- Beautiful AI
- Canva