



1

Prof. Dr. Jacques Folon

C O N T A C T

Managing Partner Folon & Partners
Founder GDPRFolder Belgium
Chairman GDPRFolder France

Professor Ichec Brussels Management School
Visiting Prof. UCL Saint Louis
Visiting Prof. HEC Liège
Visiting Prof. Rennes School of Business

<https://www.folon.com>
<https://gdprfolder.com>
<https://www.linkedin.com/company/gdprfolder>
<https://readmylips.be/en/speakers/jacques-folon>

jacques@gdprfolder.eu
www.linkedin.com/in/folon
+ 32 475 98 21 15

2

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

3



4

ChatGPT

2022

Capabilities

- Remembers what user said earlier in the conversation
- Allows user to...

What were the key AI developments in 2022?

- First came DALL-E,
- Next there was ChatGPT,

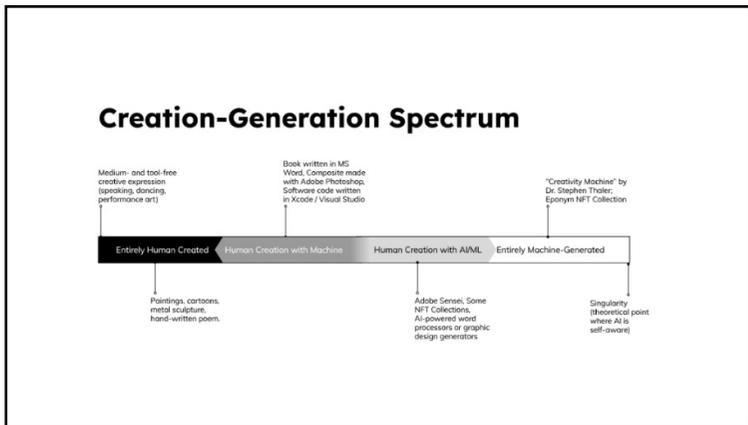
5

2022

THALER CASE (FED. CIR. 2022)

The core issue was whether an artificial intelligence system could be listed as an inventor on a patent application. Thaler, who developed AI systems that generated inventions, filed two patent applications, listing an AI system called DABUS as the sole inventor. The USPTO denied the applications, asserting that a machine cannot qualify as an inventor.

6



7

SORA

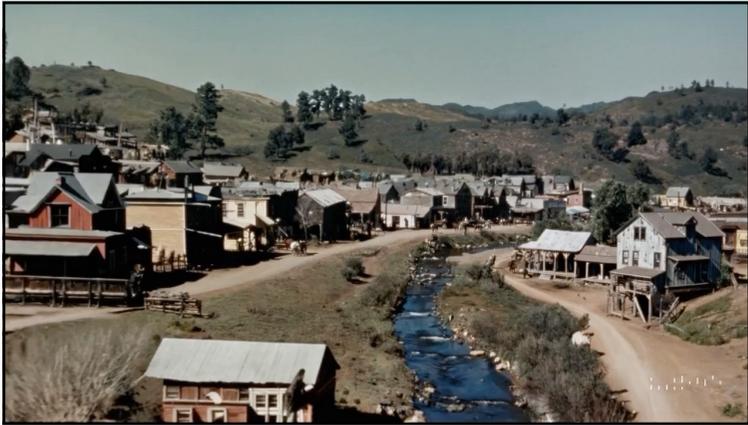
Text to video

Prompt:
Historical footage of California during the gold rush.

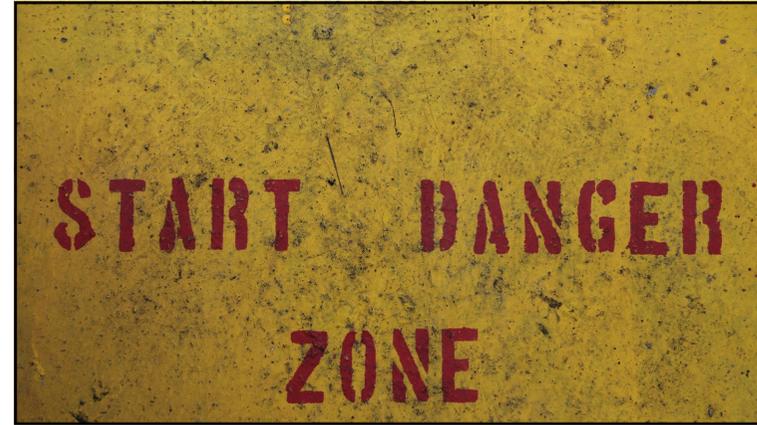
MARCH 2024

Clapperboard text: 01 7 9, 16 2 13 4 2 1, Roadside, Jakob & Ryan, Thomas Tupper

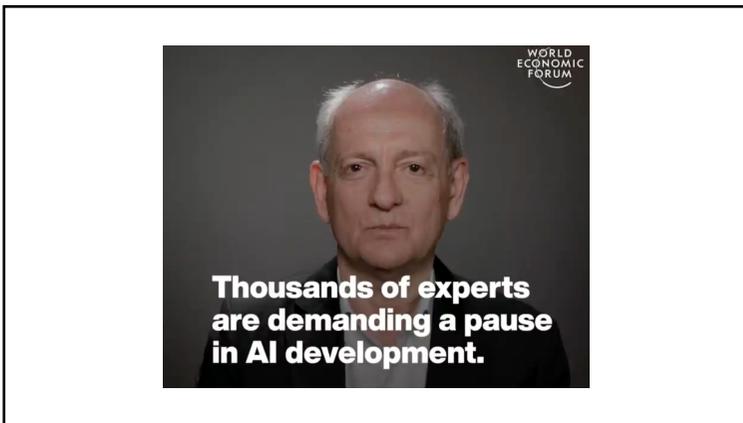
8



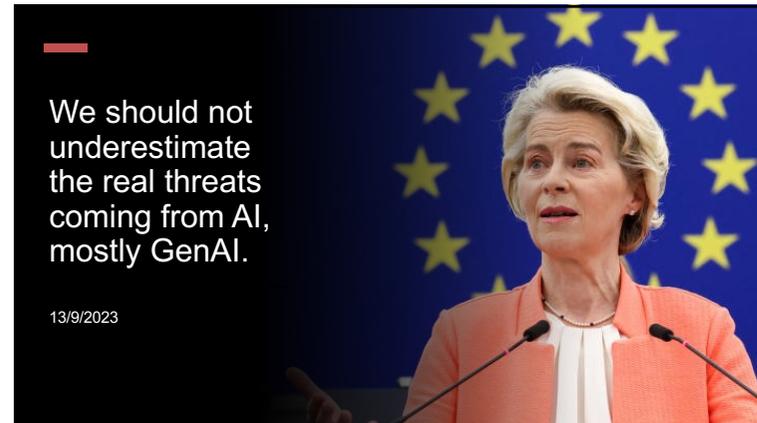
9



10



11



12



13



14



15



16



Leonardo Cervera Navas
Director of the European Data Protection Supervisor.



“Nous devons 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

17

“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

18



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

19



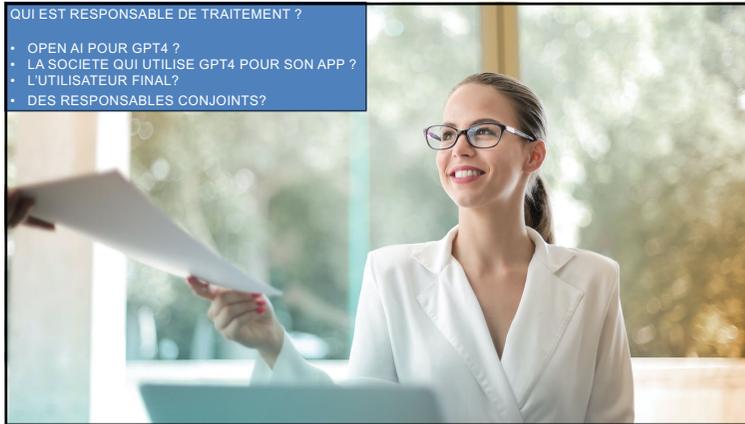
IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D’HISTOIRE
- **QUEL 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

20

QUI EST RESPONSABLE DE TRAITEMENT ?

- OPEN AI POUR GPT4 ?
- LA SOCIETE QUI UTILISE GPT4 POUR SON APP ?
- L'UTILISATEUR FINAL?
- DES RESPONSABLES CONJOINTS?



21

IA ET RGPD

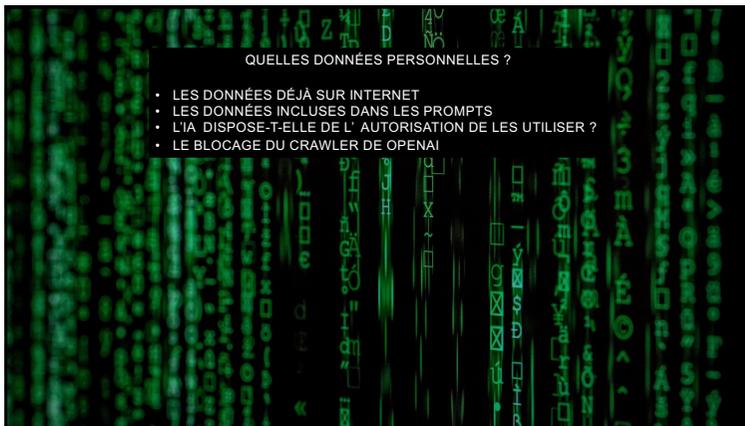
- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- QUI EST RESPONSABLE DE TRAITEMENT ?
- **QUELLES DONNÉES PERSONNELLES ?**
- QUELLE EST LA BASE LÉGALE ?
- QUELLE EST LA FINALITÉ ?
- PRIVACY BY DESIGN
- MINIMISATION ET MACHINE LEARNING
- ARCHIVAGE ET DURÉE DE CONSERVATION
- MESURES TECHNIQUES ET ORGANISATIONNELLES
- DROITS DES PERSONNES CONCERNÉES
- PRISES DE DÉCISIONS AUTOMATISÉES
- LES BIAIS DES ALGOS
- LES CRAINTES DES ENTREPRISES
- NÉCESSITÉ DE FORMATION AU RGPD MAIS PAS QUE...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS



22

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



23

LA COLLECTE DES DONNÉES SANS AUTORISATION !



24

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

25

QUELLE EST LA BASE LÉGALE ?

- CONSENTEMENT ?
- CONTRAT ?
- INTÉRÊT LÉGITIME ?

26

I Agree

- Quid de la validité du consentement individuel à la collecte, l'utilisation et la communication des données primaires ?
- Quid de la validité d'un consentement quand personne ne lit les privacy policies ?
- Les personnes comprennent-elles l'utilisation de données indirectes comme les likes, partages, cookies tiers, etc. ?
- Les personnes peuvent-elles comprendre les modalités du traitement algorithmique de l'information ?

27

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

28

QUELLE EST LA FINALITÉ DU TRAITEMENT ?

1. APPRENTISSAGE DE L'IA
 1. QUELLES DONNÉES SONT UTILISÉES ?
 2. COMMENT ONT-ELLES ÉTÉ COLLECTÉES
 3. ONT-ELLES ÉTÉ COLLECTÉES POUR CETTE FINALITÉ ?
2. MISE EN PRODUCTION
 1. QUID DES DONNÉES DES UTILISATEURS ?
 2. TRANSPARENCE ?

TOUT CELA DOIT ÊTRE DÉFINI EN AMONT



29

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS



30

PRIVACY BY DESIGN & BY DEFAULT

- IMPORTANCE DE LA DOCUMENTATION
- REFLEXIONS PREALABLES
- ANTICIPER LA DPIA



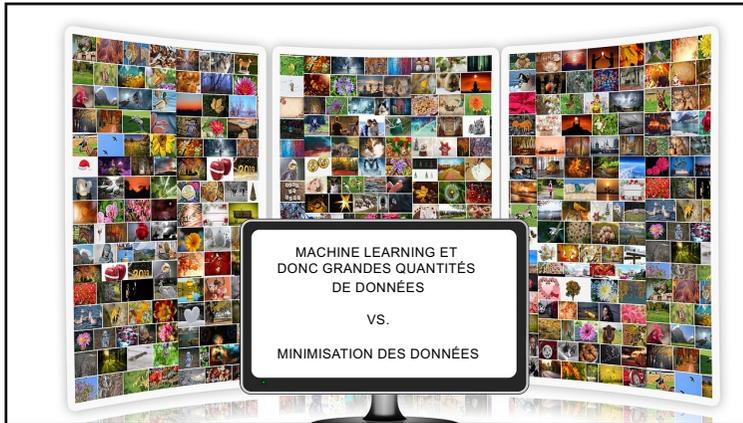
31

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS



32



33

La question de la quantité des données livrées à l'IA est délicate.

D'un côté, le principe de minimisation, consacré par le RGPD, implique de limiter la collecte de données personnelles à ce qui est strictement nécessaire au regard des finalités pour lesquelles elles sont traitées.

Mais, de l'autre, il pourrait être opportun de livrer à l'IA autant de données que possible afin, d'une part, de la rendre plus efficace et, d'autre part, d'éviter les biais statistiques qui pourraient découler d'un mauvais choix dans l'échantillonnage de données.

Ainsi que la Commission nationale de l'informatique et des libertés (CNIL) le relève dans la synthèse des débats publics menés sous son autorité sur le sujet, il n'est pas interdit de se demander si le développement de l'IA ne doit pas conduire à repenser l'équilibre général de la législation au regard du principe de minimisation

<https://www.cairn.info/revue-pouvoirs-2019-3-page-95.htm>

34

Selon la CNIL, un usage raisonné des données doit donc être fait. En pratique, il est ainsi préconisé, et cela de façon non-exhaustive :

- d'évaluer de manière critique la nature et la quantité des données à utiliser ;
- de vérifier les performances du système lorsqu'il est alimenté par de nouvelles données ;
- de distinguer clairement les données utilisées lors des phases d'apprentissage et de production ;
- de recourir à des mécanismes de pseudonymisation ou de filtrage des données ;
- d'établir et tenir à disposition une documentation concernant les modalités de constitution du jeu de données utilisé et de ses propriétés (source des données, échantillonnage des données, vérification de leur intégrité, opérations de nettoyage réalisées, etc.) ;
- de réévaluer de manière régulière les risques pour les personnes concernées (vie privée, risque de discrimination/biais, etc.) ;
- de veiller à la sécurité des données et notamment d'encadrer précisément les habilitations d'accès pour limiter les risques.

35

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

36



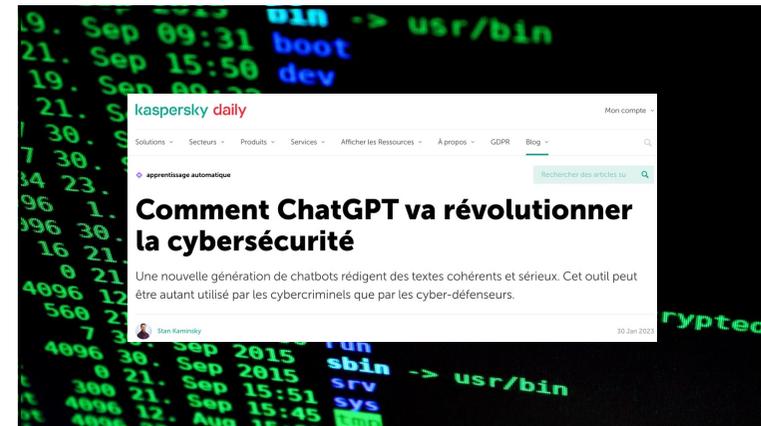
37



38



39



40



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 ?

41



Piratage ChatGPT : des hackers détournent l'IA pour créer des malwares

Maurine Briantais
18/01/23 12:44

ChatGPT est devenu un objet de convoitise pour les hackers, qui s'en servent pour créer facilement du code malveillant et mettre au point de nouvelles attaques. Le début d'une ère de piratage assisté par intelligence artificielle...

42



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.

43

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.



44

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)
Phase de production	Attaques par évitement (evasion attacks) Attaques de reprogrammation (reprogramming attacks) Attaques par déni de service		Attaques par inversion (model inversion attacks) Attaques d'extraction de modèle (model extraction attacks)

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

Petite taxonomie des attaques des systèmes d'IA

- Attaques par manipulation 8
- Attaques par évitement (evasion attacks) 9
- Attaques par reprogrammation (adversarial reprogramming attacks) 13
- Attaques par déni de service 14
- Attaques par infection 14
- Attaques 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

https://inc.cnil.fr/sites/default/files/atoms/files/inc_cnil_dossier-securite-systemes-ia.pdf

45

VIOLATIONS DE DONNÉES

OpenAI, a en effet confirmé une violation de données le 20 mars 2023 causée par un bug dans une bibliothèque open source, alors qu'une société de cybersécurité avait remarqué qu'un composant récemment introduit a été affecté par une vulnérabilité activement exploitée.

Selon l'enquête d'OpenAI, les titres de l'historique des conversations des utilisateurs actifs et le premier message d'une conversation nouvellement créée ont été exposés lors de cette violation de données. Le bug a également révélé des informations relatives au paiement appartenant à 1,2 % des abonnés de ChatGPT ainsi que le nom et le prénom, l'adresse électronique, l'adresse de paiement, la date d'expiration de la carte de paiement et les quatre derniers chiffres du numéro de la carte du client.

46

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

47

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 ACCEPTABLE ?

48

Des audits de la CNIL en trois étapes
 "Les investigations doivent se dérouler à trois niveaux"

Le premier doit se situer "au niveau de l'application" afin de s'assurer que les utilisateurs sont informés, "sur la façon dont les données qu'ils soumettent sont traitées, au'ils peuvent s'opposer au traitement ultérieur de leurs données d'entrée et exercer leur droit d'accès sur les données fournies au système".

»En 2025" au mieux, la Cnil doit apporter des réponses concrètes aux entreprises innovantes (...) ainsi qu'aux citoyens qui disposent de droits".

Le second concerne "la base de données d'entraînement utilisée pour le modèle" pour vérifier que "les personnes concernées par les données de bases (...) peuvent opérationnellement exercer leurs droits".

Le troisième niveau porte sur "le modèle sous-jacent", "la partie la plus complexe à mettre en oeuvre pour les modèles déjà entraînés", en particulier pour les IA génératives comme ChatGPT.

"Il est techniquement impossible de mettre en oeuvre un droit de rectification sur les données incluses dans le modèle entraîné".

A la place, il faudrait recourir à "d'autres solutions comme l'utilisation de modules permettant de corriger les erreurs ou inexactitudes du modèle".

Incertitude juridique en attendant 2025...

Source: https://www.usine-digitale.fr/article/voici-le-plan-d-action-de-la-cnil-pour-encadrer-l-intelligence-artificielle.N2171947?utm_source=dlvr.it&utm_medium=linkedin

49



IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

50



DÉCISION AUTOMATISÉE FAIRE INTERVENIR UN HUMAIN ? PLUSIEURS CAS EN MATIÈRE DE RH

51



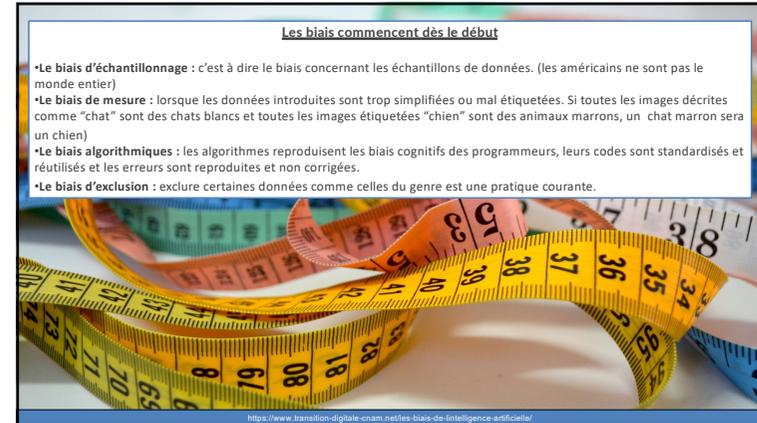
IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

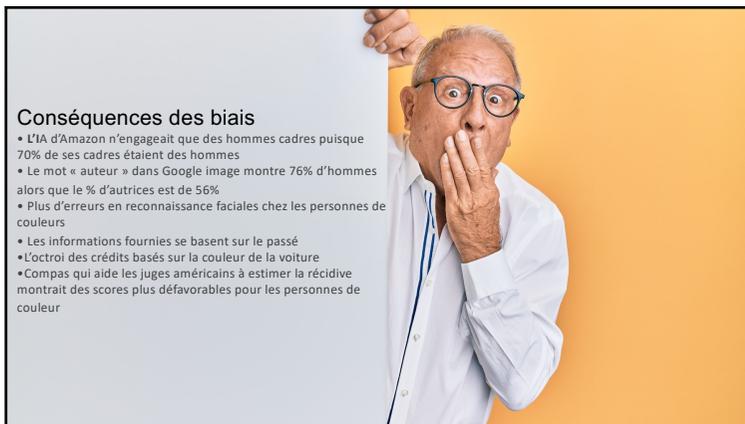
52



53



54



55



56

Top Reasons Organizations Are Banning ChatGPT

- **Potential risk to data security and privacy is the biggest reason (67%)** survey respondents cited for moving to block ChatGPT and similar generative AI tools.
- The next greatest concern (57%) is risk to corporate reputation.

WE RESPECT YOUR Privacy!

Source: <https://blogs.blackberry.com/en/2023/08/why-companies-ban-chatgpt>

57

Considérations sur la protection de la vie privée des chatbots d'IA

- ChatGPT met actuellement en garde les utilisateurs contre la fourniture ou la saisie d'informations sensibles ou personnelles, telles que les noms ou les adresses électroniques.
- Cependant, on ignore comment les créateurs de cet outil se conforment au RGPD, ou si des contrôles appropriés sont en place pour protéger les données personnelles et respecter les droits des individus à l'égard de leurs données.
- Risques
 - ces données sont réutilisées à d'autres fins, ce qui pourrait entraîner une utilisation abusive et nuire à la réputation de l'entreprise
 - violer la confiance des personnes qui ont fourni leurs informations à votre organisation (employés, clients et partenaires)

58

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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
- **NECESSITÉ DE FORMATION AU RGPD MAIS PAS QUE.**
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

59

« ChatGPT est sujet à des "hallucinations", des réponses fabriquées qui sont fausses, et des citations juridiques ou scientifiques inexistantes », a déclaré M. Friedmann (Gartner). Les responsables juridiques et de la conformité devraient émettre des directives exigeant des employés qu'ils vérifient l'exactitude, la pertinence et l'utilité réelle de tout résultat généré par ChatGPT avant de l'accepter.»

<https://blogs.blackberry.com/en/2023/08/why-companies-ban-chatgpt>

60



61



62

D'après la publication, le groupe avait autorisé des ingénieurs de la branche Samsung Semiconductor, en charge de la conception de composants électroniques comme la mémoire vive, le stockage, les processeurs ou les capteurs photo, d'utiliser ChatGPT pour corriger des problèmes de code source.

Pour accomplir sa tâche, ChatGPT avait bien entendu besoin de connaître ce code source, sans quoi il ne pouvait pas l'améliorer. Samsung a donc sciemment révélé le code source d'un nouveau programme à l'agent conversationnel, un contenu critique qui est désormais conservé sur les serveurs d'OpenAI, l'entreprise qui a développé ChatGPT. (source clubic.com)

ChatGPT est un outil formidable, mais qu'il faut savoir utiliser avec prudence. Il est, par exemple, fortement déconseillé de lui soumettre des informations confidentielles. Et ce n'est pas Samsung qui vous dira le contraire.

Des employés de Samsung Electronics ont fait fuiter des données confidentielles de la société en ayant recours à **ChatGPT**, rapporte le média coréen Economist.

63

Fuite de données et considérations relatives à la sécurité des chatbots d'IA

- Si des informations sensibles sur des tiers ou sur l'entreprise sont saisies dans ChatGPT, elles seront intégrées au modèle de données de ChatGPT et pourront être partagées avec d'autres personnes qui posent des questions pertinentes, ce qui entraînera une fuite de données.
- Toute divulgation non autorisée d'informations confidentielles dans ChatGPT (ou dans toute autre source en ligne) peut constituer une violation des politiques de sécurité de l'organisation.

64

Accueil » Actualité » ChatGPT risque-t-il d'être banni en France ? Premières plaintes déposées auprès de la CNIL

ChatGPT risque-t-il d'être banni en France ? Premières plaintes déposées auprès de la CNIL

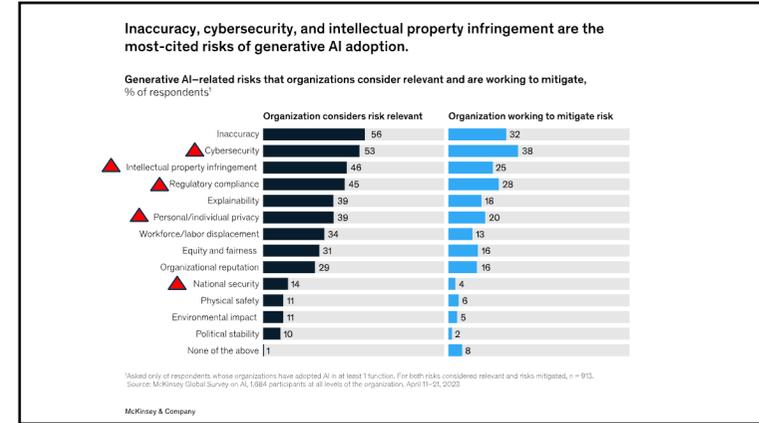
AURIANE POLÉE, le 6 avril 2023 08:00

La CNIL n'envisageait donc pas d'interdire ChatGPT, mais c'était avant de recevoir deux plaintes cette semaine. La première plainte a été déposée par l'avocate Zoé Vilain. Elle est la présidente de l'association de sensibilisation aux enjeux du numérique Janus International. Selon elle, « on n'est pas anti-tech, mais on souhaite une technologie éthique ». Elle reproche notamment à OpenAI de ne pas avoir une quelconque politique de confidentialité en place.

La deuxième plainte a été déposée par David Libeau, un développeur spécialisé dans la protection des données personnelles. Il accuse ChatGPT d'inventer de fausses informations personnelles à son sujet. « L'algorithme a commencé à affabuler et à m'attribuer la création de sites web ou l'organisation de manifestations en ligne », a-t-il expliqué.

En fin de compte, l'interdiction de ChatGPT en France n'est pas totalement impossible même si elle ne semble pas encore réalisable. L'Allemagne envisagerait aussi de son côté de bannir ChatGPT et d'autres pays européens pourraient bientôt lui emboîter le pas.

65



66

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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 BIAS DES ALGOS
- LES CRAINTES DES ENTREPRISES
- NÉCESSITÉ DE FORMATION AU RGPD MAIS PAS QUE...
- **AI ACT**
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- CONCLUSION ET RECOMMANDATIONS

67



68

Quels systèmes seraient interdits ?

Dans le projet certaines IA seront purement et simplement interdites. Sont concernés :

- **Les systèmes établissant une « note sociale »**, qui classifient les personnes selon leur fiabilité, par exemple, et peuvent conduire à « un traitement préjudiciable ou défavorable » ;
- **Les systèmes d'identification biométrique à distance et en temps réel** « dans des espaces accessibles au public à des fins répressives », y compris par les autorités ;
- **Les systèmes qui visent à manipuler par des techniques subliminales** agissant sur l'inconscient ;
- **Les systèmes ciblant les personnes vulnérables** comme les enfants ou les personnes handicapées.

La France est-elle en Europe ?

JO 2024 : la Cnil appelle les parlementaires à ne pas introduire de la reconnaissance faciale dans la loi

Publié le 24/02/2023 08:52 | Mis à jour le 24/02/2023 08:54

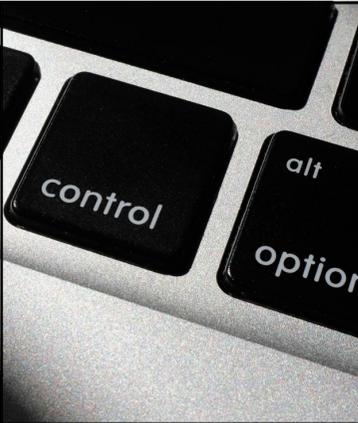
Science | 10/06/2023 19:00 | Actualisé le 17/06/2023 13:30

Bientôt tous scrutés ? Un vote du Sénat sur la reconnaissance faciale ravive nos pires peurs

Les sénateurs ont adopté un projet de loi autorisant la reconnaissance faciale dans un cadre bien précis. De quoi susciter des inquiétudes sur la possibilité d'une surveillance généralisée.

Par Le HuffPost

69



- Quels systèmes seraient permis sous conditions ?
- **Les systèmes à « hauts risques »**, car ayant une « *incidence préjudiciable significative sur la santé, la sécurité et les droits fondamentaux des citoyens* », comme les machines médicales, les systèmes de reconnaissance faciale ou les voitures autonomes, par exemple.
- Ces IA, classifiées comme très risquées, seront autorisées sous réserve de contrôles effectués par des agences nationales. Ces audits seront menés par des tiers indépendants.
- **Les systèmes présentant des « risques spécifiques de manipulation »**, c'est-à-dire qui interagissent avec des humains, sont utilisés pour analyser des émotions ou identifier des catégories sociales grâce à des données biométriques, ou génèrent des contenus tels que des « *trucages vidéo ultra-réalistes* ».
- Ces systèmes devront être assortis d'obligations de transparence spécifiques, en l'occurrence, un avertissement sur le fait que leur contenu est « *généralisé par des moyens automatisés* »

70

- **Quels systèmes seraient autorisés sans réserve ?**
- **Tous les autres types d'IA ne nécessiteront pas d'évaluation ou de mesures particulières.**
- **C'est le cas, par exemple, des objets connectés recourant à l'IA.**

Ces systèmes devront simplement respecter les droits fondamentaux et la loi européenne, et en particulier le RGPD



71

IA ACT bonne ou mauvaise nouvelle ?

■ LE FIGARO (FR) / 14 juin 2023

Innové plutôt que régulé

Réguler l'IA ne saurait suffire, estime Fabien Versaveu, PDG de Rakuten France, dans les colonnes de Figaro :

« Avec l'IA Act en discussion à Bruxelles, l'Europe se targue d'être victorieuse : être, au milieu d'une effervescence technologique sans pareille, la première puissance mondiale à concevoir une régulation pour l'intelligence artificielle. Peut-être... Mais ne sommes-nous pas en train de nous précipiter dans le piège de réguler à l'aveugle ce qui semble être la nouvelle frontière technologique, ne devons-nous pas mettre toute l'énergie européenne au service d'une stratégie offensive et créative, plutôt que défensive et normative ? Oui, en matière de technologie, réguler et protéger c'est bien, innover et concevoir c'est mieux »

■ LA REPUBBLICA (IT) / 15 juin 2023

Dans le bon sens

La Repubblica se réjouit :

« L'Europe est connue pour édicter de nombreuses règles. Trop selon certains, qui considèrent que c'est la raison pour laquelle l'innovation progresse ailleurs, aux États-Unis ou en Chine. Mais sur la question de l'IA, la technologie qui promet de tout changer, ce sont les innovateurs eux-mêmes qui réclament des règles. Et c'est, finalement, la stratégie européenne même rend. Le Parlement de Strasbourg a voté hier sa version de l'AI Act. ... La tâche finale sera discutée négociée avec les gouvernements, dans le but évident d'être approuvé à la fin de la législature européenne. Et de faire de l'Union la première puissance démocratique à se doter d'une législation sur l'IA. »

■ FRANKFURTER ALLGEMEINE ZEITUNG (DE) / 14 juin 2023

Un coup de frein trop brutal

Le Parlement européen veut imposer des règles beaucoup trop strictes, critique Frankfurter Allgemeine Zeitung :

« La plupart des applications sont sans risque. ... ChatGPT n'est pas un danger lorsqu'il est utilisé comme assistant pour des recherches sur Internet. Il en va autrement lorsque des IA sont amenés à décider d'intérêts humains, que ce soit lors de la conduite autonome ou de l'octroi de crédits. Dans ces cas-là, il faut s'assurer qu'elles ont été entraînées avec des données solides et non discriminatoires. Le Parlement aurait dû s'en rendre compte. Mais visiblement, le choc ChatGPT a été trop grand. Les élus demandent une vérification globale des risques liés à l'IA générative, quel que soit le domaine d'application. C'est exactement le coup de frein dont l'Europe n'a pas besoin. L'UE doit sans tarder veiller à corriger le processus législatif. »

■ NDR 2023

AI Act : une régulation européenne prometteuse ?

Le Parlement européen a adopté hier la première réglementation mondiale visant à réguler l'intelligence artificielle (IA). Cette loi classe les applications en fonction de différents niveaux de risque. Elle est jugée particulièrement dangereuse, comme les applications de reconnaissance faciale, doivent être interdites, tandis que d'autres seront autorisées sous conditions. Si certains craignent même la décision, d'autres saluent une régulation essentielle.

72

Un excès de réglementations ?

INFLATION NORMATIVE CONSTATÉE
 Le nombre de pages de nouvelles réglementations européennes a augmenté de 100% entre 2010 et 2020.

DANGER
 INFLATION LÉGISLATIVE
 QUAND TROP DE LOIS TUE LA LOI

Citation Georges Pompidou
 « Mais attention donc d'envoyer les Français à la mer, c'est un piège de règlementation dans ce pays. On en a eu assez ! Laissez-les vivre un peu en nous tenant que nous sommes ! Foncez-leur la pain ! Il faut bloquer ce pays ! »
 Georges Pompidou pour Chirac, 1994

73

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- **AUTRES RISQUES**
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
 - CONCLUSION ET RECOMMANDATIONS

74

THE WALL STREET JOURNAL

Help! My Political Beliefs Were Altered by a Chatbot!

- Des chercheurs de l'Université Cornell aux États-Unis ont réalisé une étude mettant en exergue les dangers de l'intelligence artificielle.
- D'après l'expérience menée, les IA sont en mesure d'**influencer les opinions** de leurs interlocuteurs
- En fonction des biais de leurs algorithmes, les chatbots, comme ChatGP, Bard ou encore Claude, peuvent modifier la façon de penser des utilisateurs à leur insu.
- Elon Musk regrette que ChatGPT soit programmé pour mettre en avant des idées « woke », reflétant les pensées de ses développeurs. En réponse, il souhaite mettre au point « TruthGPT ».

SOURCE : <https://www.wsj.com/articles/chatbot-herd-chinese-political-beliefs-151876d2modestemaietNEWS>

75

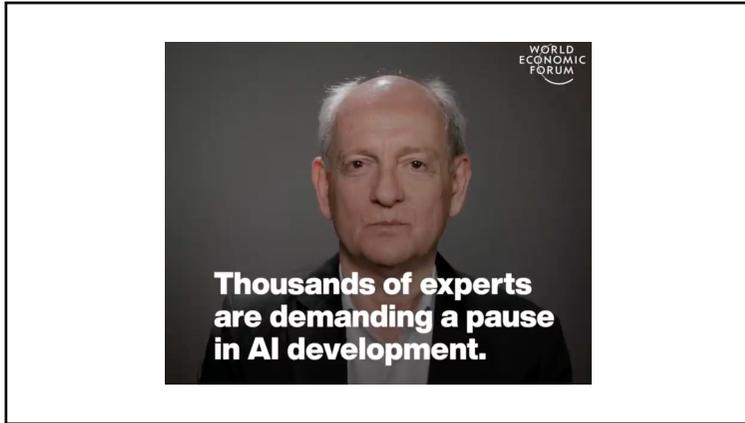
Intelligence artificielle : un Belge poussé au suicide par le chatbot Eliza

ACTUALITÉ

Autrefois des changes de six semaines avec une intelligence artificielle, un père de famille belge s'est donné la mort. « Sans cette IA, mon mari serait encore là », relate son épouse.

PAR LA RÉDACTEUR DE MATHY FAIR
 6 AVRIL 2022

76



77

IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
 - CONCLUSION ET RECOMMANDATIONS

78



79

LE SOIR

chat: Politique Société Monde Economie Vidéo Sports Culture MAD Plus

Chat GPT: si jeune et déjà hors la loi!

Si Chat GPT a fait le buzz depuis début décembre, à travers une série de 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 arrivés, ChatGPT serait-il déjà entré directement dans l'illégalité ?

ChatGPT est-il un vulgaire plagiaire ?

OpenAI

ChatGPT: Hello Chatbot ChatGPT

Hello! How can I assist you today?

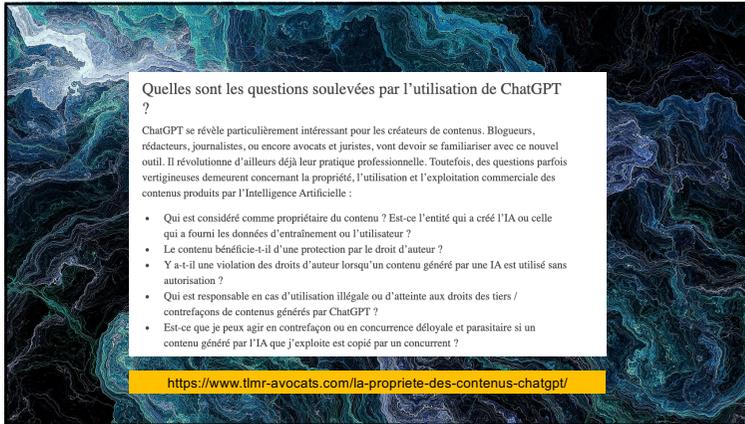
Can you help me with my homework?

Of course! What do you need help with?

Carla Mandel

The Human Rights Foundation is a 501(c)(3) non-profit organization.

80



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/ia-proprie-des-contenus-chatgpt/>

81



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

AI 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.

82



Le cœur du problème

Le New York Times concède depuis longtemps des licences sur son contenu dans le cadre d'ententes négociées, y compris avec les principales plateformes technologiques.

Un accord à l'amiable n'a pas abouti

Open AI plaide le fair use

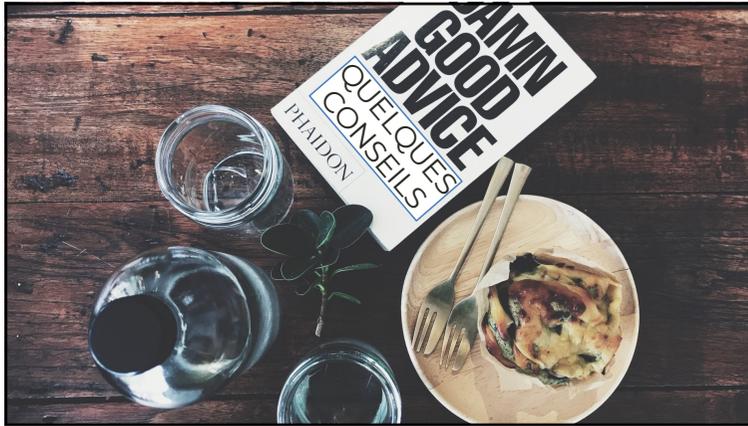
83



IA ET RGPD

- UN (PETIT) PEU DE CONTEXTE ET D'HISTOIRE
- 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...
- AI ACT
- AUTRES RISQUES
 - INFLUENCE SOURNOISE
 - PROPRIÉTÉ INTELLECTUELLE
- **CONCLUSION ET RECOMMANDATIONS**

84



85

- Importance du RGPD
- Transparence des algorithmes
- Formation à l'éthique pour les travailleurs du secteur
- Lutter contre les « boîtes noires »
- Créer des fonctions internes liées à l'éthique
- Vérification de l'objectivité des données
- Identifier les biais
- Privilégier la diversité dans les équipes




FORMATION DES COLLABORATEURS A L'IA
 FORMATION EN SECURITE DE L'INFORMATION
 FORMATION RGPD
 CODE DE CONDUITE
 CHOIX DES OUTILS
 ANALYSE DE RISQUES

86



87

- **AI TRISM**
- AI TRISM stands for Artificial Intelligence Trust, Risk, and Security Management. It is a framework that helps organizations manage the risks of developing and deploying AI models.
- AI TRISM addresses five key areas:
 - **Explainability:** AI TRISM helps organizations understand how their AI models make decisions and identify potential biases.
 - **ModelOps:** AI models need to be managed and maintained just like any other software system. AI TRISM provides tools and processes for automating and monitoring the lifecycle of AI models.
 - **Data anomaly detection:** AI models are trained on data; if the data is incorrect, the outputs won't be satisfying, too. AI TRISM helps organizations identify and address data anomalies that could lead to errors in AI models.
 - **Adversarial attack resistance:** AI TRISM provides tools and techniques for defending against adversarial attacks.
 - **Data protection:** AI models often contain sensitive personal data. AI TRISM helps organizations comply with data privacy regulations and protect the privacy of individuals.
- AI TRISM is becoming increasingly important as organizations adopt more AI. According to [insights by Gartner](#), by 2026, companies that use AI TRISM to manage their AI systems will make better decisions by removing 80% of inaccurate or fake data.



88

- **Augmented Working, BYOAI, & Shadow AI**
- BYOAI (Bring Your Own Artificial Intelligence) is a new workplace trend where **employees bring their own AI tools and applications to work**. The increasing availability of affordable and easy-to-use AI tools and the growing demand for AI skills in the workforce drive this trend. [Forrester reports](#) that 60% of workers will utilize their own AI to perform tasks.
- There are many benefits to BYOAI, including increased productivity and innovation, improved employee satisfaction, and reduced costs.
- While BYOAI is a great opportunity for workers, **it might easily get out of control**.
- **Shadow AI, also known as Shadow IT for AI**, refers to using artificial intelligence applications and tools within an organization without explicit knowledge or oversight from the IT department.
- It poses several risks, such as:
 - **Data privacy and security breaches:** Unsanctioned AI tools may not have the same protections as official ones, so sensitive information can be stolen or lost.
 - **Compliance violations:** Similarly, these tools might not follow important regulations which could lead to legal trouble.



89

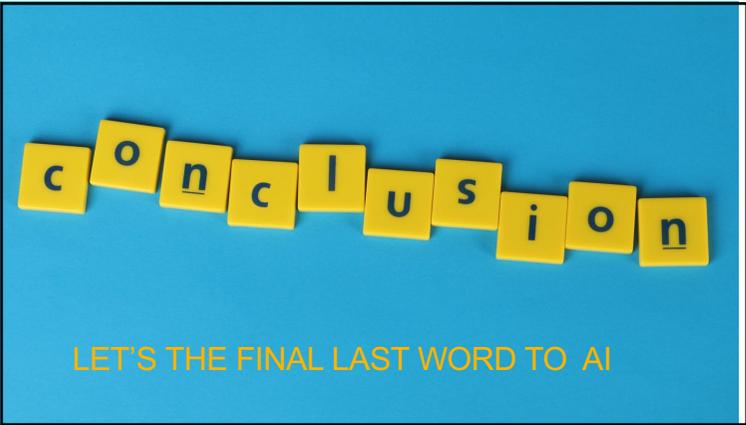
- **Ethical AI**
- Ethical AI is a branch of applied ethics that examines the ethical implications of artificial intelligence (AI). It encompasses a wide range of topics, including:
 - **Bias and fairness**
 - AI technology can reflect and amplify the biases of their creators. This, in turn, can lead to unfair outcomes for certain groups of people.
 - **Transparency and explainability**
 - The logic behind artificial intelligence can be difficult to understand, even for experts. This "black-box problem" can make it difficult to trust AI decisions and to hold AI developers accountable for their creations.
 - **Privacy**
 - AI often collects and uses large amounts of personal data, which raises concerns about privacy and data protection.
 - **Safety and Security**
 - AI systems can be misused to cause harm, such as by developing autonomous weapons or spreading misinformation.



90



91



92



93



94



95