CYBERSÉCURITÉ

L'accélération technologique et le défi du Shadow Gen AI : l'effet Reine Rouge

La transformation digitale impose une perpétuelle adaptation des compétences au niveau individuel et organisationnel, provoquant une course effrénée des directions informatiques et juridiques pour maîtriser l'utilisation non autorisée des systèmes d'intelligence artificielle par les salariés. Confrontées au Shadow Gen AI, les organisations doivent gérer les risques et garantir le contrôle et la sécurité sans freiner les initiatives de leurs salariés. Cette dynamique illustre parfaitement le paradoxe de la Reine rouge. "Ici, vous voyez, il faut courir le plus vite possible pour rester au même endroit. Si vous voulez aller ailleurs, il vous faut courir encore deux fois plus vite ! » « De l'autre côté du miroir », Lewis Carroll

À l'origine, il n'était question que d'informatique fantôme ou de Shadow IT, ce phénomène s'est métamorphosé en Shadow Gen AI, créant une course effrénée des directions informatiques et juridiques pour maîtriser l'utilisation non autorisée des systèmes d'intelligence artificielle par les salariés.
L'informatique fantôme (Shadow IT) correspond à l'utilisation d'appareils, des services cloud ou des applications sans supervision explicite ni l'approbation des services support IT et partant de l'employeur. Ce phénomène déjà facilité avec la multiplication des applications SaaS, s'accélère dangereusement avec l'utilisation non autorisée et/ou connaissance explicite d'outils d'intelligence artificielle au sein des organisations, qualifiées d'IA fantômes (Shadow Gen AI).

L'utilisation de plateformes d'IA générative (Perplexity par exemple) ou de modèles de langage comme ChatGPT pour effectuer des tâches quotidiennes telles que la programmation, la rédaction ou la création d'images peut sembler de prime abord tout à fait anodine du fait de leur déconcertante accessibilité.

Le Shadow Gen AI se fait oublier : 83% des contenus juridiques (e.g documents légaux, code source, données RH) seraient partagés via des comptes non professionnels et injectés dans des IA non validées, selon une étude de Cyberhaven Labs[1], et ce sans autorisation de l'IT. C'est précisément la racine du mal : l'invisibilité et l'accélération technologique. La particularité et le danger majeur du Shadow Gen AI résultent en effet de son invisibilité : chaque utilisateur peut potentiellement dans cette course à l'adaptation devenir une source de risques, et ce sans compétences techniques particulières ou sans s'en apercevoir. Il s'inscrit ainsi dans une logique d'invisibilisation progressive et de banalisation où les employés normalisent l'usage non autorisé des outils d'IA, développent une dépendance aux solutions automatisées tout en perdant conscience des implications de leurs usages.

La transformation digitale impose une course perpétuelle à l'adaptation des compétences au niveau individuel et organisationnel, le recours à des « *assistants IA* » en mode Copilot et/ou des « *coding agent* » se banalise.

Alain Damasio souligne parfaitement cette naturalisation insidieuse du technococon : « *Il existe aujourd'hui plein de stratégies de contournement du rapport humain rendues possibles par ces technos. C'est pareil pour le rapport au monde et dans la construction du rapport à soi* ».

Le passage du Shadow IT au Shadow Gen AI ou "courir pour rester en place" concernent les salariés qui courent après des outils d'IA sans autorisation pour optimiser leur productivité et, par là même leur employabilité, les directions ou départements IT qui courent après la sécurisation des usages et les organisations font une course à l'adaptation et au contrôle pour préserver l'innovation.

Le Shadow Gen AI renouvelle ainsi la tension fondamentale entre innovation et contrôle. Les organisations doivent simultanément innover rapidement pour maintenir leur compétitivité et attractivité, respecter un cadre réglementaire de plus en plus strict en termes de gestion de risque et garantir le contrôle et la sécurité sans freiner les initiatives de leurs salariés.
Cette situation stimule la course aux armements technologiques, expose à des vulnérabilités de sécurité croissante, et génère une perte de contrôle sur les usages de l'IA et des problématiques de conformité réglementaire.
Cette dynamique illustre parfaitement le paradoxe de la Reine rouge : plus les organisations courent après la sécurisation du Shadow AI, plus elles doivent accélérer pour maintenir le contrôle, dans une course perpétuelle à l'adaptation. Ce besoin de maîtriser le Shadow Gen IA se conjugue avec l'intensification des obligations de sécurité by design mises à la charge des organisations, la nécessité de repenser la gouvernance et l'interface homme/machine, levier des organisations auto-apprenantes.

La responsabilité des organisations à l'épreuve du Shadow AI

La problématique du Shadow AI / IT s'inscrit dans un cadre réglementaire renforcé :

- **l'obligation[2] de moyens renforcée[3]** contraignant les employeurs à prévenir les risques d'atteinte à la santé et à la sécurité de leurs travailleurs[4] ;
- **l'obligation générale d'assurer la sécurité du traitement** de données personnelles[5] aux termes de l'article 32 du RGPD au moyen de mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque[6] ;
- **la multiplication des obligations de sécurité sectorielles *« by design »*** en matière de cybersécurité et de résilience (e.g DORA, NIS 2, LPM, REC) et notamment l'obligation de mise en place d'une gouvernance des risques, de contrôles appropriés des systèmes, de détection de la menace et de reporting.

Ce panorama des obligations de sécurité a été complété récemment par la publication du :

- Cyber Resilience Act (CRA)[7], du 23 octobre 2024, imposant aux fabricants de produits comportant des éléments numériques des exigences de cybersécurité et résilience,
- Règlement d'exécution de la directive NIS 2[8], du 17 octobre 2024, établissant notamment des exigences techniques et méthodologiques, et celui du règlement DORA, du 29 novembre 2024.

Enfin, le projet de loi déposé le 15 octobre 2024 relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité viendra parachever cet arsenal juridique en transposant les directives REC, NIS 2 et celle accompagnant le règlement DORA[9]. Le texte prévoit notamment la publication d'un décret fixant les objectifs auxquels doivent se conformer les entités visées par la directive NIS 2 et d'un référentiel d'exigences techniques et organisationnelles.

Certaines précisions seront d'ailleurs bienvenues dans le cadre de la lutte contre le Shadow AI. En effet, parmi les nombreuses obligations désormais imposées en matière de résilience, le règlement d'exécution de la NIS 2 oblige les entités concernées à « *surveiller et journaliser les activités sur leurs réseaux et dans leurs systèmes d'information afin de détecter les événements qui pourraient être considérés comme des incidents et de réagir en conséquence pour en atténuer l'impact* ». Bien que le contenu des journaux soit détaillé par le texte, il faudra encore détailler les contours de l'obligation et ses modalités pratiques d'application.

Les obligations finalement établies devront en toute hypothèse être respectées et documentées dans le cadre du déploiement d'un système d'IA mais également, a priori, en cas d'autorisation, explicite ou implicite, d'un tel système.

Le Shadow Gen AI expose donc à des risques de non-conformités exponentiels et à des mises en cause de la responsabilité des employeurs du fait de leurs salariés (outre le risque de survenance de risques psychosociaux, de perte de contrôle sur les données fournies aux systèmes d'IA générative, de vulnérabilités cyber spécifiques à ces systèmes[10], etc...).

Il ne s'agit pas de remettre en cause les opportunités offertes par l'IA (automatisation des tâches et gains de productivité, amélioration des processus décisionnels, optimisation de l'organisation du travail, etc.), mais plutôt de rappeler qu'une utilisation non maîtrisée expose à des impacts préjudiciables à plusieurs niveaux :

- **Juridique**, avec la perte de contrôle sur les données personnelles, la divulgation d'informations confidentielles, les atteintes potentielles aux droits des tiers, les vulnérabilités sur le plan cyber, les atteintes à la santé et à la sécurité des salariés etc. ;
- **Environnemental**, notamment du fait de la consommation massive en électricité et en eau, de la multiplication des infrastructures cachées, etc. ;
- **Éthique et sociétal**, avec la désagrégation du lien social, la perte d'autonomie[11] décisionnelle, le renforcement de biais sans contrôle, le rapport au réel faussé, la dépendance accrue aux systèmes automatisés, la difficulté à établir les responsabilités, la manque de transparence dans les processus décisionnels, l'absence de contrôle sur les usages, etc.

Ces enjeux, souvent intrinsèques à l'IA et au fonctionnement du machine learning, auront au surplus tendance à se multiplier ou à s'accentuer du fait du Shadow AI :

- **L'absence de supervision** : contournement des structures de gouvernance formelles, risques accrus en matière de sécurité et conformité, inefficacité décisionnelle.
- **Le développement décentralisé** : solutions développées par des non-spécialistes IT (e.g. coding agent), création de silos de données compromettant la prise de décision globale, manque de robustesse et de scalabilité.
- **Le déploiement rapide** : contournement des processus d'approbation formels, défaut de

contrôle et de surveillance des systèmes d'IA, vulnérabilités non identifiées, et non-conformité réglementaire.
- **La tentation de la flexibilité à tout prix** : expérimentation aléatoire, fragmentation et fragilisation des systèmes, incohérence des données.
- **La surexposition aux accès non autorisés aux données personnelles ou confidentielles** : traitement de données clients sensibles sans respect des protocoles de sécurité, risque de régurgitation des données, perte de contrôle sur les données (Quid des demandes d'exercice de droit ?).

Toutes ces circonstances sont de nature à engager la responsabilité administrative, civile et pénale[12] des organisations et de leurs dirigeants[13], a fortiori en cas de négligence ou de manquement à une obligation de prudence ou de sécurité[14].

Tenues pour responsable des faits commis par leurs préposés, les organisations n'ont d'autres choix que de rappeler aux collaborateurs leur obligation de loyauté, qui implique notamment le respect des politiques internes (charte informatique, process, etc.), et de mener une stratégie proactive pour maîtriser le Shadow AI. Non le code ne fait pas la loi[15], et il appartient à chaque organisation de contrôler les pratiques de l'IA pour en limiter les risques.

Repenser la gouvernance au service de la lutte contre le Shadow GenAI

Pour prévenir efficacement les risques liés au Shadow GenAI, les entreprises doivent privilégier une approche multidimensionnelle et multidisciplinaire, de la protection des données, au droit social, en passant par des concepts de Gestion des Ressources Humaines (GRH)[16]. Mais comment faire ?

La solution semble devoir passer par une gouvernance transparente qui refuse l'illusion du "tout-automatique" imperceptible, par des mesures de contrôle et, surtout, par une réappropriation consciente des technologies, par exemple au travers de ces questionnements :
- **D'abord, quelle posture adopter face à l'IA ?** L'interdire ? L'autoriser sous conditions ? L'encadrer et/ou faciliter son utilisation avec des politiques claires et des alternatives sécurisées aux systèmes sur étagère disponibles en ligne ?
- **Comment identifier les signes avant-coureurs du Shadow AI ?** Il peut s'agir de pics anormaux d'activité, de tentatives d'accès multiples à des données auxquelles les utilisateurs n'ont jamais accédé auparavant, de trafic important ou de transfert de données vers des plateformes d'IA tierces non autorisées, etc.
- **Quelle gouvernance face aux usages et mésusages de l'IA ?** La gestion des risques, les analyses d'impact à mener en continu, la documentation de la conformité (RGPD[17], RIA), le contrôle interne, la création de comités éthiques, la documentation des processus décisionnels, l'adaptation des mesures de sécurité, la supervision humaine, les audits externes, le plan de développement des compétences, la veille réglementaire, etc. sont autant de mesures visant à encadrer et sécuriser l'utilisation des systèmes d'IA.
- **Comment prévenir les menaces cyber ?** Et notamment celles spécifiques aux systèmes d'IA générative (e.g. les attaques par manipulation du système, par injection des données, par exfiltration) ? Comment adapter les mesures de protection selon l'évolution des risques ? Quels outils de supervision et de détection de la menace (e. g. la mise en place de DLP et d'outils de détection de fuites de données) ? Quelle formation aux risques ?
- **Quelle responsabilité ?** Par exemple en cas de dommages causés par un système d'IA occulte (atteintes à la protection des données, aux droits des tiers, biais algorithmiques et discriminations, incidents de sécurité et violations de données, etc.).
- **Quelles garanties assurantielles en cas de dommage ?** Que faire pour répondre aux éventuelles conditions assurantielles (charte informatique, BYOD, BYAP, outils de gouvernance des risques et de détection, etc.) ?

La multitude d'interrogations donne un indice de la complexité de l'équation que les organisations doivent désormais résoudre : développer des mécanismes de gouvernance équilibrés permettant de protéger les droits fondamentaux, tout en exploitant le potentiel productif de l'IA.

Si chaque organisation devra ainsi, selon sa stratégie d'IA, son activité ou encore sa culture d'entreprise, se livrer à son propre « *numéro d'équilibriste* », ces quelques mesures générales nous semblent incontournables pour susciter l'innovation tout en maintenant le contrôle :
- **Identifier et cartographier les outils et usages des systèmes d'IA** au sein de l'organisation et se positionner face à l'IA : créer un catalogue d'outils d'IA approuvés et facilement accessibles, mettre en place des processus d'approbation accélérés pour les outils d'IA, développer des guidelines spécifiques par fonction ;
- **Mener des actions de sensibilisation et de formation** des salariés sur les risques liés à l'utilisation de l'IA, qu'il s'agisse de la protection des données, mais également de l'ensemble des aspects éthiques entourant l'utilisation des systèmes d'IA (durabilité, développement de l'esprit critique, vigilance sur le biais d'automatisation, prévention des risques psychosociaux (RPS), etc.). En règle générale, la prise de conscience et l'acceptation des enjeux permet une meilleure adhésion aux politiques internes et limite les dérives ;
- **Mettre en place une charte informatique** afin d'encadrer l'usage des nouvelles technologies, en prévenir les abus, et de s'assurer, dans certains cas, de la preuve à des fins disciplinaires ; Y adjoindre une charte d'utilisation des systèmes d'IA pour les mêmes fins et encadrer les BYOD et BYAP ;
- **Maintenir une supervision humaine significative**, parce que l'« *IA de confiance ne saurait être celle d'une confiance aveugle dans la machine* »[18]. Il s'agira en particulier de contrôler et d'auditer le fonctionnement des systèmes et de renforcer les procédures internes telles que les délégations

et sub-délégations de pouvoirs, notamment pour les DSI ou les RSSI. Il s'agit d'aligner les responsabilités de chacun sur les pouvoirs détenus, de sensibiliser les personnes concernées et ainsi de limiter les éventuelles négligences. Cette responsabilisation s'avérera particulièrement centrale dans la lutte, au quotidien et sur le terrain, contre le Shadow AI ;

- **Développer une gouvernance transparente de l'IA, des processus de contrôle organisationnels et un monitoring technique** visant à déceler et rapporter les usages non autorisés des systèmes d'IA et engager les mesures subséquentes (outils de DLP, blocage informatique, éventuelles sanctions, etc.) : mettre en place des outils de détection des accès non autorisés, surveiller les flux de données vers les plateformes d'IA, implémenter des solutions de monitoring spécifiques à l'IA, auditer régulièrement les comptes et droits d'accès, établir des rapports sur les comptes inactifs, appliquer le principe du moindre privilège ;
- **Impliquer le Délégué à la Protection des Données (DPO)** dans la gouvernance globale de l'IA (intégration dans un éventuel comité, surveillance humaine des systèmes, gouvernance des données, dialogue social, etc.) afin que ce dernier poursuive, en collaboration avec les DSI, RSSI et direction métiers, la maintenance du programme de conformité RGPD, son suivi dynamique et sa mise à jour conformément à la stratégie de l'organisation.
- **Développer une culture de l'éthique numérique** et assurer une veille réglementaire proactive afin d'être en mesure de déterminer les évolutions du modèle de gouvernance interne.

L'interface Homme-machine : les 5 disciplines, levier des organisations apprenantes

Le Shadow Gen AI nous conduit à une logique de redevabilité et de développement des compétences de manière autonome mais également à des nouveaux modèles mentaux tenant compte des enjeux de l'interface homme/machine, de la « *normalisation des comportements par une régulation technologique insidieuse et ubiquitaire* »[19] et considérant « *l'homme sous le salarié* »[20].

Pourquoi ne pas s'inspirer de la pensée systémique de Peter Senge et sa compréhension fine des interconnexions entre innovation et sécurité ?[21] Il s'agit de développer notre capacité à nous adapter avec de nouvelles façons de penser et d'agir : remplacer l'autorité et le contrôle par l'engagement de nos collaborateurs et le développement de l'apprentissage à tous les niveaux.

Pour illustrer, au sein de notre structure, nous avons fait le choix de nous impliquer en pro bono au sein de l'association d'intérêt général DataRing en allant à la rencontre de chercheurs, d'Universitaires, de scientifiques ou d'acteurs majeurs de l'IA (causeries Data[22]), et en participant à la création d'espaces d'expérimentation sécurisés pour les systèmes d'IA avec des prestataires informatiques. Nous avons ainsi constitué et participé à la constitution de comités d'IA en charge de mettre à jour en continu des chartes des usages des systèmes d'IA (avec un déploiement progressif de bots internes à usage de R&D) en y associant étroitement RSSI, DPO et services métiers. Nous avons fait le choix de nous former et de former à l'usage de l'IA générative avec notre petite legal tech de formation « *Trustbydesign* »[23].

Les organisations doivent apprendre à courir non pas pour rester sur place mais pour transformer l'entreprise en système auto-apprenant pour absorber les chocs, avancer de manière durable et pragmatique, en s'inspirant des 5 disciplines chères à Peter Senge. Pour y parvenir il nous faut apprendre collectivement et en permanence :

- **La maîtrise personnelle :** approfondir et clarifier notre approche de la réalité et en l'occurrence de l'intelligence artificielle, avec la compréhension des motivations individuelles d'utilisation de l'IA, des enjeux éthiques et sécuritaires, la responsabilisation des utilisateurs, etc.
- **Les modèles mentaux :** découvrir nos représentations du monde, nos préjugés, biais, la logique sous-jacente de la machine et la nôtre, la remise en question des pré supposés sur l'IA, les croyances limitantes sur les procédures officielles de validation des outils IT/IA, etc.
- **La vision partagée :** relier les individus autour d'une vision commune sur l'IA, la représentation du futur dans l'organisation, l'alignement des objectifs individuels et organisationnels sur les usages de l'IA, le cadre de gouvernance inclusif, le développement d'une culture de l'innovation responsable, etc.
- **L'« apprenance » en équipe :** réfléchir ensemble et expérimenter, partager les bonnes pratiques, se former en continu, élaborer un plan de développement de compétences, etc.
- **La pensée systémique :** comprendre les problèmes dans leur intégralité, les interdépendances, les attentes, une approche équilibrée entre innovation et contrôle, les impacts organisationnels.

Rien ne pourra se faire sans une vision partagée, un alignement des pratiques entre les besoins des employés et la stratégie IA de l'organisation, le partage des expériences afin de transformer la course effrénée du Shadow AI en opportunité d'apprentissage organisationnel structuré et sécurisé : établir des politiques d'utilisation de l'IA claires mais flexibles, créer des canaux de communication transparents, instaurer des mécanismes de validation agiles et sûrs et favoriser l'innovation responsable (privacy by design, durabilité, sécurité by design).

La vraie question n'est peut-être pas de savoir si l'intelligence artificielle (en mode Shadow ou pas) est une opportunité ou un désastre, mais plutôt de savoir sur quoi elle repose[24], sur la nature de sa fixation et de notre volonté/capacité à la contrôler pour un usage éthique, durable et sûr.

Nous avons un droit à l'explication et à la reddition de comptes pour réduire l'asymétrie informationnelle entre les acteurs de l'IA, les citoyens et les institutions démocratiques de contrôle. Il nous faut aller à la rencontre de la pratique (DPO, DSI, RSSI, Chercheurs, Directions métiers, Avocats) pour tisser des liens

précieux, comprendre la logique algorithmique et les mécanismes de prise de décisions et s'inscrire dans un apprentissage continu et créatif.

Comme le souligne le manifeste du projet DialIA[25], l'intégration de l'IA devra également être abordée par les partenaires sociaux et par un dialogue social spécifique dans les entreprises[26], dit « *dialogue social technologique* »[27], pour favoriser son acceptabilité, générer des situations capacitantes de travail et organiser le partage de la valeur.

Il s'agit de faire le choix d'un numérique maitrisé et non subi avec des utilisateurs « *éclairés* », sans jamais céder à la tentation du panoptique de Bentham.

Le Shadow AI n'est peut-être qu'une leçon de vie en mode logique inversée, celle que nous donne Lewis Caroll dans « *De l'autre côté du miroir* », à propos de l'apprentissage, de la maitrise personnelle et de l'autre perspective critique.

« Qui marche plus lentement que toi ?
Personne !
— C'est faux, répliqua le Messager d'un ton maussade.
C'est tout le contraire : qui marche plus vite que moi ?
Personne !
— C'est impossible ! dit le Roi.
Si Personne marchait plus vite que toi, il serait arrivé ici le premier... »

France CHARRUYER
Avocat associé Altij & Oratio
Présidente de l'Association d'intérêt général Data-Ring

Notes

(1) Citation consultable ici : https://www.futura-sciences.com/planete/actualites/environnement-alain-damasio-decrochage-technologique-traduira-plaisir-vivre-beaucoup-plus-intense-86224/

(2) Article L.4121-1 du Code du travail.

(3) Cass. soc. 25 novembre 2015 pourvoi n°14-24.444, Publié au bulletin.

(4) Ses applications se sont d'ailleurs multipliées avec l'essor du numérique : cyberharcèlement, risques psychosociaux, etc.

(5) Article 32 du RGPD.

(6) Le manquement à cette obligation pouvant occasionner des sanctions administratives pouvant s'élever à 20 millions d'euros ou, s'il s'agit d'une entreprise, à 4% du chiffre d'affaires annuel.

(7) RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n° 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience).

(8) RÈGLEMENT D'EXÉCUTION (UE) 2024/2690 DE LA COMMISSION du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance.

(9) RÈGLEMENT D'EXÉCUTION (UE) 2024/2956 DE LA COMMISSION du 29 novembre 2024 définissant des normes techniques d'exécution pour l'application du règlement (UE) 2022/2554 du Parlement européen et du Conseil en ce qui concerne les modèles types pour le registre d'informations.

(10) Pour aller plus loin : https://cyber.gouv.fr/publications/recommandations-de-securite-pour-un-systeme-dia-generative

(11) LaborIA, Etude des impacts de l'IA sur le travail, Rapport d'enquête LaborIA Explorer, 2024.

(12) Article 121-3 du Code pénal.

(13) Article 121-2 du Code pénal.

(14) Pour en savoir plus : https://www.altij.fr/detail-actualites/en-periode-de-crise-plus-imprevisible-que-jamais-comment-gerer-les-cyber-risques

(15) En référence à l'expression « Code is law », provenant de l'article éponyme de Lawrence LESSIG, professeur de droit à Harvard, publié en janvier 2000 dans le Harvard Magazine.

(16) Pour aller plus loin : https://www.altij.fr/detail-actualites/faut-il-reglementer-lutilisation-de-lintelligence-artificielle

(17) Pour aller plus loin : https://www.cnil.fr/fr/les-fiches-pratiques-ia

(18) Conseil d'État, Intelligence artificielle et action publique : construire la confiance, servir la performance, 2022.

(19) Yves POULLET, La vie privée à l'heure de la société du numérique, Larcier, 2019.

(20) Gérard LYON-CAEN, Les libertés publiques et l'emploi, La Documentation française, 1992.

(21) Peter SEGE, The Fifth Discipline : the Art and Practice of the Learning Organization. New York :Doubleday/Currency, 1990.

(22) https://podcast.ausha.co/les-causeries-data

(23) https://www.trustbydesign.fr

(24) « IA washing » ou le retour du « Turc mécanique », célèbre mystification du XVIIIème siècle.

(25) https://dialia.alwaysdata.net

(26) Commission de l'intelligence artificielle, IA : notre ambition pour la France, rapport, 2024.

(27) LaborIA, précité.

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info