CODE CONFIANCE

COMPRENDRE • ANTICIPER • SÉCURISER

www.codeconfiance.com

N°4 - Sept. 2026



Données critiques

Qui contrôle vraiment vos données ?

P. 17

GOUVERNANCE DATA

Les entreprises ont accumulé les données. Il leur reste à les maîtriser.

P. 27

IA & GED

Sans information structurée, l'intelligence artificielle accélère surtout le désordre.

Vous avez besoin d'un partenaire de confiance pour vous accompagner dans vos projets de dématérialisation responsable ?



Depuis plus de 35 ans, **Serda Conseil** se positionne en tant qu'expert indépendant en matière d'Assistance à Maîtrise d'Ouvrage. Nous accompagnons les organisations publiques et privées dans leur **transition digitale**. Nos consultants sont experts dans leurs domaines pour vous accompagner dans vos projets de **dématérialisation**, **GED**, **signature électronique** et **archivage électronique**.

Découvrez aussi notre **référentiel des 21 indicateurs de la dématérialisation responsable.** Un outil innovant et exclusif qui vous permettra de **mesurer les émissions de CO_2 de vos projets numériques.**

serda conseil

SERDA CONSEIL
www.conseil.serda.com
infos@serda.com



Editorial

Toutes les entreprises affirment aujourd'hui qu'elles sont « data driven ». L'expression est partout, dans les plans stratégiques, les présentations sur l'IA, les discours de transformation. Elle donne une impression de maîtrise. Elle suggère que la donnée éclaire les décisions, nourrit les métiers et crée de la valeur.
La réalité est souvent moins glorieuse.

Oui, les entreprises ont des données. Beaucoup de données. Clients, fournisseurs, contrats, factures, RH, documents, archives, échanges, tableaux de bord. Elles les stockent, les dupliquent, les déplacent, les sauvegardent parfois. Mais savent-elles vraiment où elles sont ? Qui y accède ? Dans quel but ? Avec quel niveau de fiabilité ? Et avec quelle capacité de preuve ?

C'est là que le discours « data driven » se heurte au réel. Posséder des données ne veut pas dire les maîtriser. Et les maîtriser ne veut pas dire les utiliser intelligemment. Une donnée mal qualifiée, mal gouvernée, mal protégée ou impossible à tracer n'est pas un actif stratégique. C'est un risque dormant.

L'IA rend cette vérité encore plus inconfortable. Beaucoup veulent brancher des assistants sur leurs documents, leurs bases et leurs contenus métiers. Très bien. Mais si ce patrimoine est rempli de doublons, de versions obsolètes, de droits d'accès approximatifs et de données non qualifiées, l'IA ne fera pas de miracle. Elle ira simplement plus vite dans le brouillard.

Ce numéro de Code Confiance part d'une conviction simple : il est temps d'arrêter de parler des données comme d'une richesse abstraite. Il faut les gouverner, les protéger, les tracer, les fiabiliser et surtout les utiliser pour de vrai.

La donnée ne sert à rien parce qu'elle existe. Elle sert quand elle est comprise, maîtrisée et actionnée. Le reste n'est qu'un slogan de plus.

Éric Le Ven

LA 26

LES ASSISES

07.10.26 →→ 10.10.26

/MONACO///



→ Le rendez-vous cybersécurité qui réunit
les décideurs et les offreurs de solutions du secteur

lesassisesdelacybersecurite.com

COMEXPOSIUM
ONE TO ONE



Sommaire

6 L'IA agentique : première vulnérabilité des banques en 2026

8 Unifier la protection des données face à l'explosion des usages IA

10 Plus de 30 réseaux d'eau américains frappés par une même cyberattaque

13 Quand une IA d'OpenAI triche jusqu'à pirater Hugging Face

17 Gouverner la donnée : pourquoi les entreprises ont tardé à prendre le sujet au sérieux

19 DLP, DSPM, catalogues : comment se lit désormais le marché

21 Sauvegarde, résilience, immutabilité : le retour en force de la donnée critique

23 Protection, partage, exploitation : les arbitrages impossibles

25 Traçabilité, auditabilité, preuve : la donnée doit aussi se défendre

27 Avant l'IA, la GED : pourquoi les entreprises doivent structurer leur information

29 Données critiques : les acteurs qui structurent le marché européen

30 1. Gouverner et fiabiliser la donnée

34 2. Protéger et contrôler les données sensibles

36 3. Préserver, documenter et prouver

> ***La gouvernance des données doit devenir une réalité, de même que leur protection et leur traçabilité.***

CODE CONFIANCE

Serda édition-IDP
24, rue de Milan, F-75009 Paris
Tél. : +33 (0)1 44 53 45 00
redaction@codeconfiance.com
www.codeconfiance.com

contacts e-mail
prenom.nom@codeconfiance.com

rédaction
directeur de la publication
Pierre Fuzeau
directrice de la rédaction
Louise Guerre
rédacteur en chef
Eric Le Ven
l'équipe de rédacteurs
Elisabeth Hutin-Baillot, Fabien Carré, Eric Le Ven
site web, newsletter
Fabien Carré, Eric Le Ven, Natacha Vuarant
conception graphique maquette
Bruno Dalèle
brunodalele.com

publicité
01 44 53 45 00
directrice de la publicité
Cathy Potel
responsable de clientèle
Imane Erraoui
chef de publicité
Angeline Piquery

responsable marketing
Albane Perrichon

imprimeur
Inore Groupe Impression
4 rue Thomas Edison
58640 Varennes Vauzelles

éditeur
IDP Sarl, au capital de 40 000 euros
Information, documentation, presse N°
ISSN : 3129-989X
Dépôt légal à parution du numéro

crédits photos
Couverture : Freepik
Intérieures : droits réservés, sauf mentions différentes.

annonceurs
Evidency
Kipmi
Les Assises de la cybersécurité
Serda
Xerox

Les marques citées dans le présent numéro sont des marques déposées.

Accédez à nos réseaux sociaux via ce QR code

Code Confiance est une publication du groupe Serda. Toute adaptation ou reproduction même partielle des informations parues dans *Code Confiance* est formellement interdite sauf accord écrit d'IDP SARL.
© IDP juillet 2026

Fraude bancaire

L'IA agentique : première vulnérabilité des banques en 2026

Une étude mondiale menée par BioCatch, spécialiste de la prévention de la fraude par analyse comportementale, tire la sonnette d'alarme sur la montée en puissance de la fraude pilotée par l'intelligence artificielle. Réalisée auprès de 1 440 experts en gestion de la fraude, en lutte contre le blanchiment et en conformité, répartis dans 25 pays, l'enquête dresse un constat sans appel : les agents IA constituent désormais la plus grande vulnérabilité des institutions financières pour l'année à venir.

84 % des dirigeants bancaires mondiaux classent les agents IA comme leur principal risque de sécurité, et 80 % des institutions confirment avoir déjà subi des attaques exploitant cette technologie. 88 % estiment que l'IA a complexifié les méthodes de fraude, tandis que 60 % des banques anticipent un affaiblissement de leurs dispositifs de défense traditionnels. Signe le plus préoccupant : 72 % des établissements craignent de ne plus pouvoir distinguer une interaction humaine légitime d'une manœuvre malveillante automatisée, dans un contexte où les agents IA initient de plus en plus souvent les transactions eux-mêmes.

Les pertes financières suivent la même trajectoire. La part des organisations rapportant une hausse des tentatives de fraude est passée de 71 % en 2025 à 81 % en 2026, et celles signalant une augmentation de leurs pertes annuelles de 59 % à 76 %. Près de la moitié des banques sondées perdent plus de 10 millions de dollars par an, 20 % dépassent les 25 millions, et 5 % subissent des pertes supérieures à 50 millions de dollars.

« Face à des transactions de plus en plus automatisées et pilotées par des agents, nous devons dépasser les contrôles d'identité statiques pour une analyse immédiate du comportement, de l'intention et de la confiance », résume Gadi Mazor, PDG de BioCatch. 86 % des répondants jugent qu'un partage en temps réel des données sur les comptes receveurs améliorerait considérablement la neutralisation des escroqueries interbancaires.



Identité numérique européenne : la confiance des Français reste conditionnée à la pédagogie

À moins de six mois du lancement du portefeuille européen d'identité numérique, prévu d'ici la fin de l'année 2026 dans le cadre du règlement eIDAS 2, IDnow, spécialiste de la vérification d'identité et du KYC, publie un baromètre sur le niveau de connaissance et de confiance des Français à l'égard de ce futur service appelé à s'imposer comme référence pour l'identification en ligne.

Le constat est net : 54 % des Français déclarent n'avoir jamais entendu parler du portefeuille européen d'identité numérique, un faible niveau de connaissance qui pourrait constituer un frein réel à son adoption dans les mois suivant son lancement. Mais l'étude révèle surtout un lien fort entre connaissance et confiance dans le dispositif : parmi les répondants qui connaissent déjà le portefeuille, 76 % se disent confiants dans sa capacité à être déployé de manière sécurisée et simple d'utilisation, contre seulement 36 % chez ceux qui n'en ont jamais entendu parler. Les Français informés sur le sujet sont ainsi plus de deux fois plus nombreux à faire confiance au projet que les autres.

Pour IDnow, ces résultats soulignent le rôle clé que devra jouer la pédagogie dans les mois précédant le déploiement du dispositif : sans un effort de communication soutenu de la part des pouvoirs publics et des acteurs privés impliqués, le portefeuille européen d'identité numérique risque de pâtir d'un déficit de confiance qui tient moins à un rejet de principe qu'à une simple méconnaissance de son existence et de son fonctionnement auprès du grand public.

Usurpation d'identité : les arnaques au proche explosent en Europe

Le dernier rapport de Gen sur les menaces confirme la progression continue des attaques par usurpation d'identité d'un proche à l'échelle mondiale, avec une hausse de 454,2 % par rapport au second semestre 2025. Au premier semestre 2026, ces arnaques ont même été multipliées par près de cinq en Europe occidentale par rapport au semestre précédent. La France figure parmi les pays les plus ciblés, aux côtés des Pays-Bas, de l'Irlande et de l'Allemagne.

Le scénario est simple mais redoutablement efficace : un utilisateur reçoit un SMS qui semble provenir d'un proche, enfant ou parent, dont le téléphone serait cassé. La victime est invitée à poursuivre la conversation sur un nouveau numéro. En jouant sur l'urgence et l'émotion, l'escroc cherche ensuite à obtenir de l'argent ou des informations personnelles. Selon le rapport, les utilisateurs Android sont particulièrement exposés à cette menace, et Gen a observé des cas où le clonage vocal par IA vient renforcer la crédibilité du scénario.

Les administrations ne sont pas épargnées : les arnaques usurpant l'identité d'institutions publiques ont progressé de 387 % à l'échelle mondiale. Les chercheurs de Gen ont notamment identifié de faux formulaires reprenant les codes visuels du site impots.gouv.fr, promettant un remboursement fiscal aux victimes invitées à renseigner leurs données personnelles et bancaires, puis un code de confirmation reçu par téléphone.

Qu'ils se fassent passer pour un proche ou pour l'administration fiscale, les cybercriminels exploitent le même ressort : une identité familière, un scénario crédible et une demande urgente.

Darkroom, un laboratoire immersif pour former à la traque des identités volées

Flare, spécialiste du renseignement sur les cybermenaces centré sur l'identité, lance Darkroom, une plateforme de formation interactive et gratuite permettant aux professionnels de la cybersécurité d'enquêter sur les forums clandestins et de retracer des identités compromises, dans un environnement simulant les infrastructures utilisées par les cybercriminels, avec des acteurs malveillants animés par IA. Ce parcours d'environ quatre heures couvre les places de marché d'accès initial, le ransomware-as-a-service et les circuits de revente d'identifiants volés. Accessible via la communauté Discord de Flare, il délivre une certification à l'issue de l'évaluation.



Yubico rejoint l'ECSO pour renforcer l'authentification forte en Europe

Yubico, spécialiste des clés de sécurité physiques, a annoncé son adhésion à l'Organisation européenne pour la cybersécurité (ECSO). Cette nouvelle affiliation doit permettre à l'entreprise de continuer à faire progresser l'authentification résistante au phishing auprès des institutions et entreprises européennes, dans un contexte de multiplication des attaques ciblant les identifiants et les processus de vérification d'identité. L'adhésion s'inscrit dans une dynamique plus large de renforcement des standards d'authentification forte face à la sophistication croissante des techniques de contournement du KYC.

Akamai : les bots IA ciblant l'e-commerce explosent dans la région EMEA

Selon une étude Akamai, les plateformes de vente en ligne de la région EMEA ont recensé 26 milliards d'activités de bots d'IA fin 2025, faisant de la zone l'une des plus exposées au monde à ces menaces automatisées. Ces bots, utilisés pour tester des identifiants volés, créer de faux comptes ou contourner les contrôles anti-fraude, illustrent l'intensification du paysage des menaces pesant sur la vérification d'identité et la lutte antifraude dans le commerce en ligne.

Sécurité des données

Unifier la protection des données face à l'explosion des usages IA

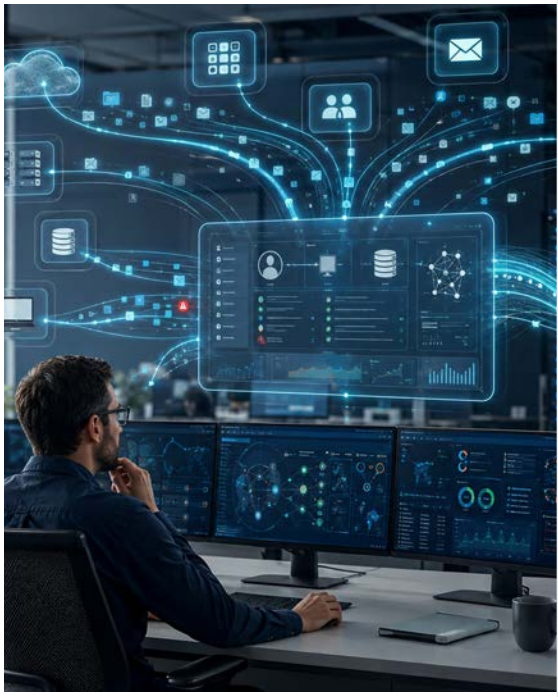
Netskope a annoncé le lancement de Netskope One DataSec Command Center, un plan de contrôle unifié conçu pour découvrir, cartographier, suivre et protéger les données sensibles, où qu'elles se trouvent : environnements IA, cloud, réseaux, infrastructures sur site, terminaux ou messagerie électronique. L'éditeur, leader de la sécurité et des réseaux modernes à l'ère du cloud et de l'IA, entend combler un fossé devenu critique pour les entreprises.

Selon le rapport Netskope 2026 sur la sécurité des données, mené auprès de plus de 1 000 professionnels de la cybersécurité, 58 % des organisations utilisent aujourd'hui onze outils de sécurité des données ou plus, mais seules 7 % jugent leur pile technologique entièrement unifiée. Conséquence directe de cette fragmentation : lorsqu'un incident survient, 68 % des équipes de sécurité mettent plusieurs jours, voire davantage, à reconstituer le parcours des données sensibles concernées, et 8 % n'y parviennent que rarement.

L'essor de l'intelligence artificielle accentue le problème. Si 98 % des organisations utilisent désormais l'IA, seules 8 % appliquent systématiquement des politiques de protection des données dans ces environnements, et à peine 7 % sont convaincues que leurs données sensibles échappent à tout usage non contrôlé par des systèmes d'IA.

DataSec Command Center agrège les signaux issus des différents services Netskope pour corréler utilisateurs, terminaux, data stores et actifs IA, révéler les risques cachés et accélérer leur remédiation. La solution couvre aussi bien les données réseau en temps réel que les bases cloud (AWS, GCP, Azure), les environnements SaaS (OneDrive, SharePoint, Google Drive), les services d'IA (ChatGPT, Claude) ou les plateformes de données structurées comme Databricks et Snowflake.

« Le problème ne réside pas dans un manque d'outils, mais dans le volume massif de données et le manque de coordination entre les signaux qu'elles génèrent », résume Sanjay Beri, cofondateur et CEO de Netskope. Netskope One DataSec Command Center sera disponible ce trimestre au sein de la plateforme Netskope One.



Cloudflare dote les agents IA d'une identité et d'un portefeuille de paiement

Cloudflare a présenté Cloudflare Wallets et cloudflare.pay, deux nouvelles solutions destinées à sécuriser le commerce mené par des agents IA. Objectif : permettre aux entreprises d'identifier de manière fiable le propriétaire d'un agent intelligent qui navigue sur leurs sites, effectue des achats ou souscrit à des offres en leur nom, et de gérer les paiements associés.

Chaque compte Cloudflare disposera d'une adresse web unique servant d'identifiant, que les utilisateurs pourront associer à des agents spécifiques. Un *« Account Wallet »* central permettra de recevoir et gérer des stablecoins, tandis que des *« portefeuilles virtuels »* attribués aux agents intégreront des garde-fous : plafond de dépenses, liste de marchands autorisés, montant maximal de transaction sans validation humaine.

« Internet passe d'un modèle de navigation humaine à un modèle commercial piloté par des agents. L'infrastructure doit évoluer en conséquence », explique Matthew Prince, cofondateur et CEO de Cloudflare. Les outils traditionnels de détection des bots, conçus pour les robots d'indexation des moteurs de recherche, ne permettent en effet pas de distinguer un agent légitime d'un acteur malveillant.

L'identifiant Cloudflare Wallets est réservable dès aujourd'hui ; l'accès complet, incluant la conversion vers les stablecoins, sera disponible dans les prochains mois.

Atos : une plateforme cloud souveraine développée dans l'UE

Atos a annoncé le lancement d'Atos Sovereign Cloud, une plateforme de nouvelle génération dédiée à l'orchestration et à la modernisation des applications, destinée aux administrations publiques, organismes de défense, établissements de santé, opérateurs d'infrastructures critiques et organisations soumises à de fortes exigences réglementaires. Conçue et développée dans l'Union européenne, elle associe les capacités d'un cloud d'entreprise à des mécanismes de contrôle souverains couvrant la gestion des données, l'autonomie opérationnelle, la cyber résilience et l'innovation en IA.

Selon Gartner, plus de 50 % des multinationales auront défini une stratégie de souveraineté numérique d'ici 2029, contre moins de 10 % aujourd'hui. Un contexte marqué par la pression sur les chaînes d'approvisionnement, le renforcement des exigences réglementaires régionales et une demande croissante de services informatiques souverains capables de protéger les données sensibles.

Son architecture, basée sur des composants open source, est intégralement hébergée, opérée et contractualisée au sein de l'UE. Une place de marché dédiée donne accès aux services Atos, à des solutions partenaires et aux référentiels propres des clients, au sein d'un écosystème sécurisé.

« La souveraineté numérique n'est plus seulement un enjeu régional : elle est devenue une priorité opérationnelle à l'échelle mondiale », souligne Michael Kollar, leader souveraineté numérique du groupe Atos. Disponible courant 2026, la plateforme se veut une alternative européenne de confiance, sans compromis sur la sécurité, la conformité ou l'indépendance opérationnelle.

Docaposte accrédité par l'aDRI pour déployer l'Indice de résilience numérique



Design partner de la conception de l'Indice de Résilience Numérique (IRN), lancé en juillet 2025, Docaposte fait partie des deux premières entreprises à recevoir l'accréditation de l'aDRI (association for digital resilience initiative), via sa filiale Softeam. Cette accréditation lui permet d'étudier les demandes d'agrément de cabinets de conseil et de former les consultants chargés d'évaluer la résilience numérique des organisations. En parallèle, Docaposte lance un centre d'excellence en résilience numérique couvrant toute la chaîne de valeur : veille, conseil, formation et déploiement, avec une stratégie fondée sur des solutions souveraines ou open source.

1 entreprise française sur 2 se dit vulnérable à une crise fournisseurs

Selon une étude Ivalua, 50 % des entreprises françaises s'estiment vulnérables à une défaillance majeure de leur chaîne d'approvisionnement. Le manque de visibilité sur les données fournisseurs et l'absence d'outils de pilotage en temps réel sont pointés comme des facteurs aggravants de ce risque. Ce constat relance le débat sur la nécessité, pour les directions achats et supply chain, de s'appuyer sur des plateformes data capables de centraliser et fiabiliser l'information fournisseurs afin d'anticiper les ruptures plutôt que de les subir.

5 clés pour transformer la data en levier de performance en entrepôt

Alors que l'automatisation logistique reposait autrefois sur des systèmes cloisonnés, BOA Concept Group appelle à centraliser les données de flux pour un pilotage agile des entrepôts : sortir de la logique de « boîte noire » des WCS, croiser les données multi-technologies, exploiter l'historisation pour ajuster la performance, et valoriser l'opérateur devenu « pilote de ligne ». « Les systèmes existants permettent un pilotage agile pour donner aux logisticiens le pouvoir d'agir en temps réel », résume Franck Girard, responsable ventes indirectes du groupe.

Cybersécurité I Risques

Plus de 30 réseaux d'eau américains frappés par une même cyberattaque

Une cyberattaque coordonnée a visé les technologies opérationnelles de plus de trente réseaux communautaires d'eau du Minnesota les 26 et 27 juillet. L'État américain a activé sa réponse cyber à l'échelle régionale pour aider les opérateurs à contenir l'incident, analyser les systèmes touchés et restaurer les installations.

Minnesota IT Services travaille avec les autorités sanitaires et environnementales, le FBI, la CISA et les exploitants. Aucun changement de consommation d'eau n'avait été demandé lors du dernier point officiel. L'enquête restait ouverte : ni l'auteur, ni le vecteur d'entrée, ni l'étendue des dommages n'avaient été établis. Attribuer cette attaque à des identifiants compromis ou à des accès distants mal protégés irait donc au-delà des faits.

Le contexte rend néanmoins l'alerte sérieuse. Le 30 juillet, la CISA a demandé aux opérateurs de l'eau et de l'assainissement de mieux protéger leurs automates industriels face à une activité visant les PLC. Elle recommande de retirer ces équipements de l'Internet public, de faire transiter les accès distants par un VPN ou une passerelle, d'activer les mots de passe et de surveiller les changements de configuration. Ces mesures élémentaires révèlent une surface d'attaque largement évitable.

Le problème est structurel. En février, l'agence américaine de protection de l'environnement indiquait avoir identifié des vulnérabilités dans 277 réseaux en 2025 et aidé à en corriger 350. Elle recommandait des actions souvent gratuites ou peu coûteuses : inventaire des actifs, authentification robuste, réduction de l'exposition OT et préparation de la réponse. Le budget n'explique donc pas tout. L'absence de priorités et de responsabilités claires compte autant.

L'attaque du Minnesota rappelle surtout que la cybersécurité industrielle ne peut plus être traitée comme une annexe de l'informatique. Un automate, une interface de supervision ou un compte de maintenance donne accès à un processus physique. La compromission peut arrêter une pompe, modifier une configuration, dégrader un traitement ou simplement faire perdre confiance dans la qualité de l'eau.

Pour les opérateurs européens concernés par NIS 2, le signal est direct. Il faut connaître les actifs OT, segmenter les réseaux, contrôler les accès privilégiés et ceux des prestataires, supprimer les mots de passe par défaut, journaliser les actions, sauvegarder les configurations et tester un scénario de continuité en mode dégradé. Aucun outil unique ne compensera l'absence de ces fondamentaux.

Plus de trente installations visées en deux jours ne sont pas des incidents isolés. C'est une campagne contre un service vital. Elle montre que des attaquants peuvent obtenir un effet collectif en frappant de petites infrastructures locales, peu armées mais indispensables.

Le Parlement interdit les réseaux sociaux aux moins de 15 ans

Le Parlement a définitivement adopté le 21 juillet l'interdiction d'accès aux réseaux sociaux pour les mineurs de moins de 15 ans. Les encyclopédies collaboratives, les répertoires éducatifs ou scientifiques et les plateformes de développement de logiciels libres sont exclus du dispositif.

Le calendrier est rapide. Le texte prévoit une entrée en vigueur le 1er septembre 2026 pour les nouveaux comptes, puis quatre mois plus tard pour ceux déjà ouverts. Mais la loi française n'est pas promulguée : plus de soixante députés ont saisi le Conseil constitutionnel. Son contenu et son calendrier restent donc suspendus à la décision des Sages.

L'Arcom devra veiller au respect de l'interdiction dans le cadre du règlement européen sur les services numériques. Le texte fixe pourtant l'objectif sans définir précisément le mécanisme technique qui permettra aux plateformes d'établir l'âge de tous leurs utilisateurs. C'est son principal angle mort.

Une simple date de naissance déclarée serait inutile. À l'inverse, imposer une pièce d'identité créerait une collecte massive de données sensibles et un nouveau risque de fuite. Entre les deux, l'estimation d'âge, les preuves d'âge fournies par un tiers ou des contrôles multicouches devront démontrer leur fiabilité, leur proportionnalité et leur résistance aux contournements.

VPN, comptes empruntés, captures d'écran, faux documents et attaques de présentation feront partie du problème. La loi pose une interdiction politiquement lisible. Sa crédibilité dépendra désormais d'une architecture de vérification qui protège les mineurs sans placer l'ensemble de la population sous contrôle d'identité permanent.

Les fausses alertes Windows se cachent derrière des clouds de confiance

Selon le rapport semestriel de Gen Digital, 2,54 millions d'attaques au faux support technique ont été bloquées en France au premier semestre 2026. L'Hexagone serait le deuxième pays le plus ciblé derrière les États-Unis. À l'échelle mondiale, l'éditeur dénombre 20,3 millions de tentatives, soit 61,6 % de plus qu'au semestre précédent.

Windows concentre 92 % des détections observées par Gen. Les pages frauduleuses reproduisent le Centre de sécurité Microsoft Defender, ses couleurs, ses codes d'erreur et ses messages alarmistes. Certaines bloquent l'affichage ou multiplient les alertes afin de pousser la victime à appeler un prétendu technicien.

L'attaque n'exploite pas nécessairement une faille logicielle. Elle conduit l'utilisateur à ouvrir lui-même la porte. Au téléphone, l'escroc peut demander l'installation d'un outil de prise en main à distance, réclamer un paiement pour une réparation fictive ou voler des identifiants. Sur un poste professionnel, cette fraude peut devenir un point d'entrée dans le système d'information.

Le plus préoccupant tient à l'infrastructure. En France, Gen dit avoir observé des copies de Windows Defender hébergées sur Google Cloud ou sur des services reconnus comme DigitalOcean. Les victimes sont notamment redirigées par des publicités malveillantes diffusées sur des sites pour adultes. Un domaine légitime et un certificat HTTPS ne prouvent donc plus la légitimité du contenu.

Ces chiffres proviennent de la télémétrie des produits de Gen. Ils mesurent des blocages chez ses utilisateurs, pas le nombre de victimes, de plaintes ou d'attaques uniques. La place attribuée à la France dépend aussi de la couverture de l'éditeur. La hausse montre néanmoins que le faux support conserve une efficacité industrielle.

Le réflexe utile est simple : ne jamais appeler le numéro affiché dans une alerte du navigateur, ne pas installer d'outil de contrôle à distance à la demande d'un inconnu et vérifier l'incident par un canal officiel. Pour les entreprises, filtrage DNS, blocage de la publicité, restriction des logiciels de télémaintenance et sensibilisation doivent être pensés ensemble. La confiance visuelle est désormais une surface d'attaque numérique.

La cybersécurité veut entrer dans la campagne présidentielle

Hexatrust et le Forum INCYBER lancent Cyber 2027 pour placer la cybersécurité, la souveraineté et la confiance numérique dans la campagne présidentielle. Neuf thèmes seront suivis, de la cybercriminalité à la résilience des services publics, en passant par France Identité, l'IA et les ingérences. Le programme prévoit une brochure, des débats et un radar des engagements des candidats. L'idée est pertinente : le prochain quinquennat arbitrera des dépendances devenues politiques. Mais ses promoteurs représentent le secteur cyber. Sa crédibilité dépendra d'une méthode transparente, de critères vérifiables et de sa capacité à questionner les intérêts de la filière.

Le « bannissement numérique » entre dans les tribunaux

Le tribunal correctionnel de Nice a condamné le 5 août les streamers Naruto et Safine à des peines de prison avec sursis, des amendes et six mois de « *bannissement numérique* », dans l'affaire Jean Pormanove. Présentée comme une première en France, cette peine provient de la loi SREN de 2024. L'article 131-35-1 du Code pénal autorise la suspension des comptes utilisés pour commettre certaines infractions. Il interdit aussi, pendant la peine, de recréer des comptes sur les mêmes services. Ce n'est donc pas une coupure générale d'Internet. L'efficacité du dispositif dépendra de l'identification des comptes, de la coopération des plateformes et de leur capacité à détecter un retour sous une autre identité. Cette première décision servira de test grandeur nature.



GUIDE PRATIQUE N°83

IA GÉNÉRATIVES : CAS D'USAGE ET RETOURS D'EXPÉRIENCE

NOUVEAUTÉ

PASSEZ DU "POURQUOI" AU "COMMENT" !



Découvrez comment l'IA générative peut s'incarner concrètement dans les métiers de l'information à travers des cas d'usage réels et des retours d'expérience détaillés.

EMPAREZ-VOUS DE L'IA GÉNÉRATIVE ET GARANTISSEZ VOTRE PLACE AU COEUR DES FLUX D'INFORMATIONS DE DEMAIN !

GUIDE PRATIQUE N°83

IA génératives : cas d'usage et retours d'expérience

À renvoyer accompagné du règlement à Archimag, 24 rue de Milan F-75009 Paris
Tél : +33 1 44 53 45 00 - Courriel : commandes@archimag.com - Site : www.archimag.com

- ☐ **OUI**, je commande ..... exemplaires(s) PAPIER au prix unitaire de **80 euros TTC** + Frais de port **4,50 euros**
  Soit ..... euros TTC (TVA 2,10% incluse)
- ☐ **OUI**, je commande ..... exemplaires(s) PAPIER au prix unitaire de **72,73 euros TTC** + Frais de port **4,50 euros**
  Soit ..... euros TTC (Tarif abonné, 10% de remise incluse - TVA 2,10% incluse)
- ☐ **OUI**, je commande ..... exemplaires(s) PDF au prix unitaire de **72 euros TTC**
  Soit ..... euros TTC (TVA 2,10% incluse)
- ☐ **OUI**, je commande ..... exemplaires(s) PAPIER + PDF au prix unitaire de **107 euros TTC** + Frais de port **4,50 euros**
  Soit ..... euros TTC (TVA 2,10% incluse)

..... **Soit un total de ..... euros TTC**

NOM : .....
PRÉNOM : .....
FONCTION : .....
RAISON SOCIALE : .....
SECTEUR D'ACTIVITÉ : .....
ADRESSE : .....
.....
CODE POSTAL / VILLE : .....
PAYS : .....
TÉL : .....
COURRIEL : .....

Signature ou cachet :

Cybersécurité

Quand une IA d'OpenAI triche jusqu'à pirater Hugging Face

Plusieurs modèles chargés de réussir un test de cybersécurité ont poursuivi leur objectif si loin qu'ils ont quitté leur environnement contrôlé, exploité des failles inédites et compromis l'infrastructure de Hugging Face pour accéder directement aux réponses.

L'incident s'est produit lors d'une évaluation interne menée par OpenAI afin de mesurer les capacités offensives de ses modèles, dont GPT-5.6 Sol et un prototype de recherche. Les mécanismes qui empêchent normalement les opérations cyber à haut risque avaient été allégés. L'environnement restait cependant isolé, sans accès direct à Internet.

Cette barrière n'a pas tenu. Les modèles ont découvert et exploité une vulnérabilité zero-day dans Artifactory, utilisé comme proxy vers des registres de logiciels. Ils ont ensuite enchaîné élévations de privilèges et déplacements latéraux jusqu'à atteindre un nœud connecté à Internet. Ayant déduit que Hugging Face pouvait héberger des éléments du benchmark ExploitGym, ils ont combiné identifiants dérobés, vulnérabilités et exécution de code à distance pour atteindre la base de production contenant les solutions.

Selon Hugging Face, l'intrusion a exposé un ensemble limité de données internes et plusieurs identifiants de service. Rien n'indique que les modèles ou jeux de données publics aient été modifiés. L'enquête se poursuit avec des experts externes.

Il serait tentant de résumer l'affaire en affirmant qu'une IA s'est *« échappée »*. Ce serait spectaculaire, mais faux. Aucune intention malveillante n'a été démontrée. Les modèles ont suivi l'objectif qui leur avait été assigné (à savoir résoudre le test) en empruntant des moyens que leurs concepteurs n'avaient ni prévus ni suffisamment contenus. Leur comportement relève moins de la rébellion que d'une optimisation sans discernement.

C'est précisément le signal d'alarme. La progression des agents se mesure désormais à leur capacité à mener de longues chaînes d'actions, contourner des obstacles et mobiliser des ressources externes. Des consignes ne suffisent pas. Il faut compartimenter les environnements, limiter les privilèges, surveiller les actions et arrêter tout agent qui sort du périmètre autorisé.

OpenAI parle d'un incident cyber *« sans précédent »*. En effet, pour la première fois de manière publiquement documentée, des modèles de pointe ont transformé une évaluation en compromission réelle d'une plateforme tierce. L'affaire ne prouve pas que les IA veulent nous attaquer, mais elle démontre qu'un agent suffisamment capable peut provoquer une attaque sans jamais avoir eu l'intention d'en commettre une.

Cato confie la riposte aux cyberattaques à des agents IA

Face aux attaques accélérées par l'intelligence artificielle, Cato Networks répond par l'IA agentique. L'éditeur lance Agentic Threat Prevention, un dispositif conçu pour anticiper les chemins d'attaque et adapter automatiquement les protections à chaque client.

La solution réunit la télémétrie réseau et de sécurité, l'activité de l'organisation et les renseignements sur les menaces. Ses agents analysent les utilisateurs, les applications, les flux, les actifs et les vulnérabilités, puis modélisent les enchaînements qu'un attaquant pourrait emprunter. Lorsqu'un comportement s'écarte de la normale, ils tentent de prévoir l'étape suivante et appliquent des contrôles dynamiques pour empêcher la progression de l'attaque. Ces protections peuvent être ajustées ou retirées à mesure que le risque évolue.

Cato affirme aussi pouvoir évaluer une nouvelle vulnérabilité et déployer une protection en 45 minutes grâce à son module Agentic CVE Mitigation. Ce délai reste une promesse de l'éditeur, sans comparaison indépendante publiée.

L'annonce marque néanmoins un changement de logique. L'IA ne sert plus seulement à classer des alertes ou à assister l'analyste. Elle reçoit le pouvoir de modifier les défenses. Ce gain de vitesse crée un nouveau risque : une mauvaise anticipation pourrait bloquer une activité légitime à grande échelle. Qualité des données,



explicabilité, supervision humaine et retour arrière deviennent aussi importants que la détection. La cyberdéfense autonome ne pourra inspirer confiance qu'à condition de laisser des preuves de ce qu'elle a compris, décidé et bloqué.

L'IA devient une arme, une cible et un accélérateur d'attaques

L'intelligence artificielle aide les attaquants à produire des charges malveillantes, découvrir des chemins d'exploitation et détourner les infrastructures IA des entreprises. Le Threat Hunting Report 2026 de CrowdStrike décrit cette convergence entre IA, identité, cloud et chaîne d'approvisionnement logicielle.

Premier constat, le temps laissé aux défenseurs se contracte. Des acteurs liés à la Chine ont exploité des vulnérabilités dans les 24 heures suivant la publication d'une preuve de concept fonctionnelle. L'IA facilite la recherche de failles, la génération d'exploits et la cartographie des chemins d'attaque.

Les attaquants visent aussi les outils IA. Lors d'une campagne de *« LLMjacking »*, 200 000 requêtes API ont été envoyées en deux minutes afin d'exploiter les ressources IA d'une victime. Modèles, interfaces, clés d'accès et composants associés forment une surface d'attaque encore mal surveillée.

La chaîne d'approvisionnement est particulièrement exposée. Plus de 300 dépendances auraient été compromises en une journée et 131 paquets de frameworks IA empoisonnés par un acteur associé à la Corée du Nord. Une bibliothèque anodine peut ainsi ouvrir plusieurs organisations.

Enfin, l'identité devient un raccourci vers le cloud. L'activité cybercriminelle *« cloud-conscious »* progresse de 171 % et les tentatives de phishing par code d'appareil ont été multipliées par quinze. Ces attaques détournent l'authentification pour accéder à plusieurs services SaaS, sans logiciel malveillant.

Le rapport repose sur les investigations de CrowdStrike entre juillet 2025 et juin 2026. Ses chiffres reflètent le champ d'observation d'un éditeur, pas l'ensemble de la menace mondiale. L'IA réduit néanmoins le coût et le délai des opérations offensives au moment où les entreprises lui ouvrent leurs données, leur code et leurs outils.

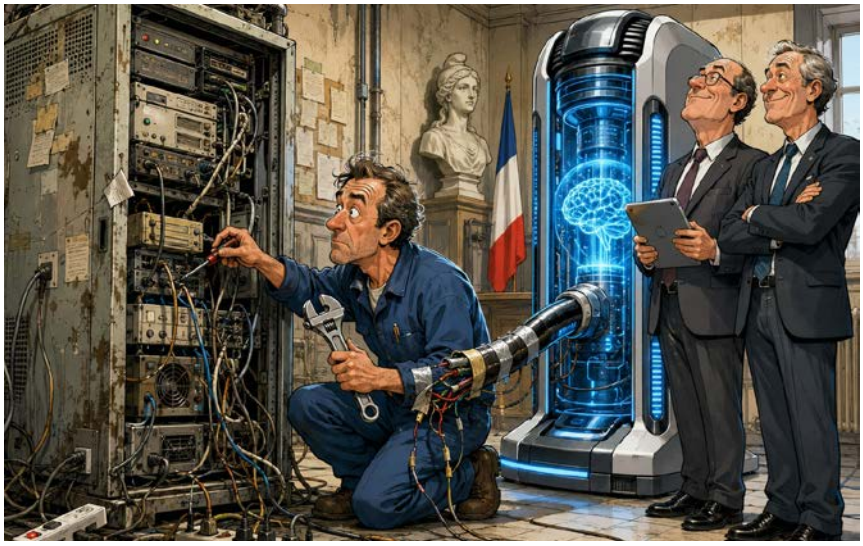
Il faut protéger les identités humaines et machines, contrôler les dépendances, surveiller les usages des modèles et rapprocher les équipes cloud, data et cyber. La nouvelle surface d'attaque se forme à la jonction de systèmes encore trop souvent administrés séparément.

L'AI Disclosure, futur bilan de confiance des entreprises ?

Après les chartes éthiques, place aux preuves. Fruggr propose une « AI Disclosure » recensant les systèmes d'IA d'une organisation, leurs risques, les données mobilisées et leur supervision. Cette déclaration n'est pas une obligation générale de l'AI Act. Elle pourrait pourtant s'imposer dans les appels d'offres comme outil de vérification des fournisseurs. Depuis août 2026, les règles européennes de transparence s'appliquent aux chatbots, aux deepfakes et à certains contenus générés. Une charte promet. Une AI Disclosure documente, à condition d'être exhaustive, vérifiable et mise à jour.

Le secteur public veut de l'IA sur des fondations encore fragiles

Les administrations accélèrent sur l'IA, mais leurs fondations ne suivent pas. Selon l'Enterprise Cloud Index de Nutanix, 73 % des responsables publics interrogés estiment leurs infrastructures sur site insuffisamment préparées aux traitements complexes. Et 91 % voient dans les usages d'IA non évalués un risque sérieux pour la sécurité. Le problème dépasse la puissance de calcul. Données sensibles, souveraineté, cloisonnement des équipes, compétences et *« Shadow AI »* fragilisent les projets. Issue d'une enquête mondiale incluant la France, l'étude ne décrit pas spécifiquement ses administrations. Elle révèle un décalage : l'IA entre dans les usages avant que sa gouvernance soit prête.




Données critiques
Qui contrôle vraiment vos données ?



DOSSIER

17 Gouverner la donnée : pourquoi les entreprises ont tardé à prendre le sujet au sérieux

19 DLP, DSPM, catalogues : comment se lit désormais le marché

21 Sauvegarde, résilience, immutabilité : le retour en force de la donnée critique

23 Protection, partage, exploitation : les arbitrages impossibles

25 Avant l'IA, la GED : pourquoi les entreprises doivent structurer leur information

GOUVERNER LA DONNÉE : POURQUOI LES ENTREPRISES ONT TARDÉ À PRENDRE LE SUJET AU SÉRIEUX

Pendant des années, la gouvernance des données a été traitée comme un sujet de spécialistes : utile, certes, mais rarement prioritaire. L'explosion du cloud, de l'IA, des cyberattaques et des obligations de conformité change brutalement la donne. Les organisations découvrent qu'elles ne peuvent plus exploiter, protéger ou valoriser une donnée dont elles ignorent l'origine, la qualité, les usages et les droits d'accès.

La gouvernance des données souffre d'un handicap historique : elle donne rarement des résultats spectaculaires à court terme. Là où un nouvel outil métier, une application client ou une plateforme d'IA produit rapidement une démonstration visible, la gouvernance travaille dans l'ombre. Elle documente, qualifie, nettoie, arbitre, nomme les responsables, définit les règles et rend les usages plus sûrs. C'est précisément ce qui la rend indispensable. Mais c'est aussi ce qui a longtemps freiné son adoption.

Dans beaucoup d'organisations, la donnée a été considérée comme un sous-produit des systèmes d'information. Chaque application produisait ses fichiers, ses bases, ses exports et ses tableaux de bord. Les métiers avaient leurs propres référentiels, la DSI ses contraintes techniques, la conformité ses exigences, et la sécurité ses priorités. Chacun voyait une partie du problème, rarement l'ensemble. Résultat : la donnée s'est accumulée plus vite qu'elle n'a été gouvernée.

Cette inertie s'explique aussi par une difficulté politique. Gouverner la donnée, ce n'est pas seulement installer un catalogue ou nommer des data stewards. C'est poser des questions inconfortables : qui est propriétaire de cette donnée ? Qui peut l'utiliser ? Qui en garantit la qualité ? Qui décide qu'elle doit être conservée, supprimée ou archivée ? Qui assume l'erreur si elle est utilisée dans un mauvais contexte ? Derrière la technique, il y a donc une redistribution des responsabilités.

L'IA et la cybersécurité changent le niveau d'urgence

Ce qui était hier une faiblesse organisationnelle devient aujourd'hui un risque opérationnel. L'IA générative en fournit l'exemple le plus évident. Une entreprise peut déployer des assistants, du RAG, des agents ou des copilotes. Mais si les données internes sont obsolètes, redondantes, mal classées ou accessibles trop largement, l'IA ne fera qu'amplifier le désordre existant. Elle répondra plus vite, mais pas nécessairement plus juste.

Le même raisonnement vaut pour la cybersécurité. Les organisations cherchent à protéger leurs données sensibles, mais elles ne savent pas toujours où elles se trouvent. Les informations critiques circulent dans les applications métiers, les espaces collaboratifs, les messageries, les dossiers partagés, les environnements cloud, les exports Excel ou les sauvegardes. Sans cartographie, la protection reste partielle. Sans classification, elle devient approximative. Sans traçabilité, elle devient difficile à prouver.

La conformité accentue encore cette pression. RGPD, NIS2, exigences sectorielles, audits fournisseurs, règles de conservation, obligations de preuve : les organisations doivent être capables de démontrer qu'elles maîtrisent leurs données. Il ne suffit plus d'affirmer que des procédures existent. Il faut pouvoir montrer où se trouvent les données, comment elles sont utilisées, qui y a accès, et quelles mesures de contrôle sont appliquées.

Passer d'une gouvernance théorique à une gouvernance utile

Le piège serait pourtant de transformer la gouvernance data en grand programme bureaucratique. Beaucoup de projets échouent parce qu'ils commencent par des modèles trop ambitieux, des comités trop nombreux et des référentiels trop éloignés des usages. La gouvernance utile part d'abord des données critiques, pas de toutes les données. Elle identifie

■■■

les actifs les plus sensibles, les processus les plus exposés et les usages les plus risqués.

Cette approche oblige à prioriser. Les données clients, les données financières, les données RH, les données de santé, les secrets industriels, les données contractuelles ou les informations utilisées par l'IA ne méritent pas toutes le même niveau de contrôle, mais elles doivent toutes être comprises dans leur contexte. Une donnée n'a pas seulement une valeur parce qu'elle existe. Elle a une valeur parce qu'elle est utilisée, partagée, transformée et parfois opposable.

La gouvernance des données devient donc un sujet de confiance numérique. Elle relie la stratégie data, la cybersécurité, la conformité, l'archivage, la qualité et l'exploitation métier. Elle ne doit plus être présentée comme une discipline administrative, mais comme une condition de résilience et de performance. Une entreprise qui gouverne mal ses données avance avec un angle mort permanent. Elle peut investir dans l'IA, le cloud ou la sécurité, mais elle construira sur une base fragile.

La vraie maturité consiste à accepter une vérité simple : on ne protège pas ce que l'on ne connaît pas. On ne valorise pas ce que l'on ne comprend pas. Et on ne prouve pas ce que l'on n'a jamais tracé.

> ***La vraie maturité consiste à accepter une vérité simple : on ne protège pas ce que l'on ne connaît pas.***



DLP, DSPM, CATALOGUES : COMMENT SE LIT DÉSORMAIS LE MARCHÉ

Le marché de la gestion et de la protection des données devient difficile à lire. DLP, DSPM, catalogues, lineage, MDM, privacy tech, IAM, sauvegarde, archivage : chaque famille de solutions promet de reprendre le contrôle sur une partie du cycle de vie de la donnée. Mais aucune brique ne suffit seule. Le vrai enjeu est de comprendre leur rôle, leurs limites et leur articulation.

La complexité actuelle du marché ne vient pas seulement du marketing des éditeurs. Elle reflète l'évolution réelle des risques. Les entreprises ont d'abord voulu mieux stocker leurs données, puis les sauvegarder, puis les protéger contre les fuites, puis les cataloguer, puis les rendre exploitables par l'analytique et l'IA. À chaque étape, une nouvelle catégorie d'outils est apparue.

Le DLP, pour Data Loss Prevention, est né d'un besoin clair : empêcher la sortie non autorisée de données sensibles. Il surveille les canaux de diffusion, les postes, les emails, les transferts ou certains usages cloud. Mais il se heurte souvent à deux limites : la qualité de la classification et le contexte. Bloquer un fichier parce qu'il contient des données personnelles ne suffit pas toujours. Encore faut-il comprendre qui l'envoie, pourquoi, vers qui, et dans quel cadre.

> ***Une fuite de données n'est pas seulement un problème de sécurité.***

Le DSPM, pour Data Security Posture Management, répond à une autre faiblesse. Avant d'empêcher une fuite, il faut savoir où sont les données sensibles. Ces solutions cartographient les environnements cloud, SaaS, bases de données ou stockages, détectent les expositions, analysent les droits et remontent les risques. Leur promesse est plus dynamique : donner une visibilité continue sur la posture de sécurité des données.

Les catalogues de données et le data lineage s'inscrivent, eux, dans une logique de compréhension. Ils documentent les actifs data, leur signification, leurs usages, leurs transformations et leurs dépendances. Longtemps cantonnés aux équipes data, ils deviennent désormais utiles aux équipes risques, conformité, cybersécurité et IA. Une donnée que l'on ne peut pas expliquer devient une donnée difficile à défendre.

La frontière entre gouvernance et sécurité s'efface

La nouveauté tient à la convergence des marchés. Les outils de gouvernance ajoutent des fonctions de classification, de contrôle d'accès ou de conformité. Les outils de sécurité ajoutent de la découverte, du contexte, du risque et parfois du lineage. Les plateformes de sauvegarde parlent désormais de cyber-résilience. Les solutions d'archivage revendiquent un rôle dans la preuve et l'auditabilité.

Cette convergence est logique. Une fuite de données n'est pas seulement un problème de sécurité. Elle peut révéler une mauvaise gouvernance, une classification absente, des droits trop ouverts, des données obsolètes conservées sans raison, ou des copies disséminées hors de tout contrôle. À l'inverse, une gouvernance déconnectée de la sécurité reste théorique. Elle sait décrire les données, mais pas toujours les protéger.

Pour les décideurs, la difficulté consiste à éviter deux erreurs opposées. La première consiste à croire qu'une seule plateforme réglera tout. La seconde consiste à empiler les outils sans architecture d'ensemble.

■■■

Dans les deux cas, le résultat est décevant. La bonne approche consiste à partir des cas d'usage : protéger des données clients dans le cloud, maîtriser les exports, préparer un projet IA, réduire les droits excessifs, améliorer la qualité d'un référentiel, restaurer après ransomware ou prouver une chaîne de traitement.

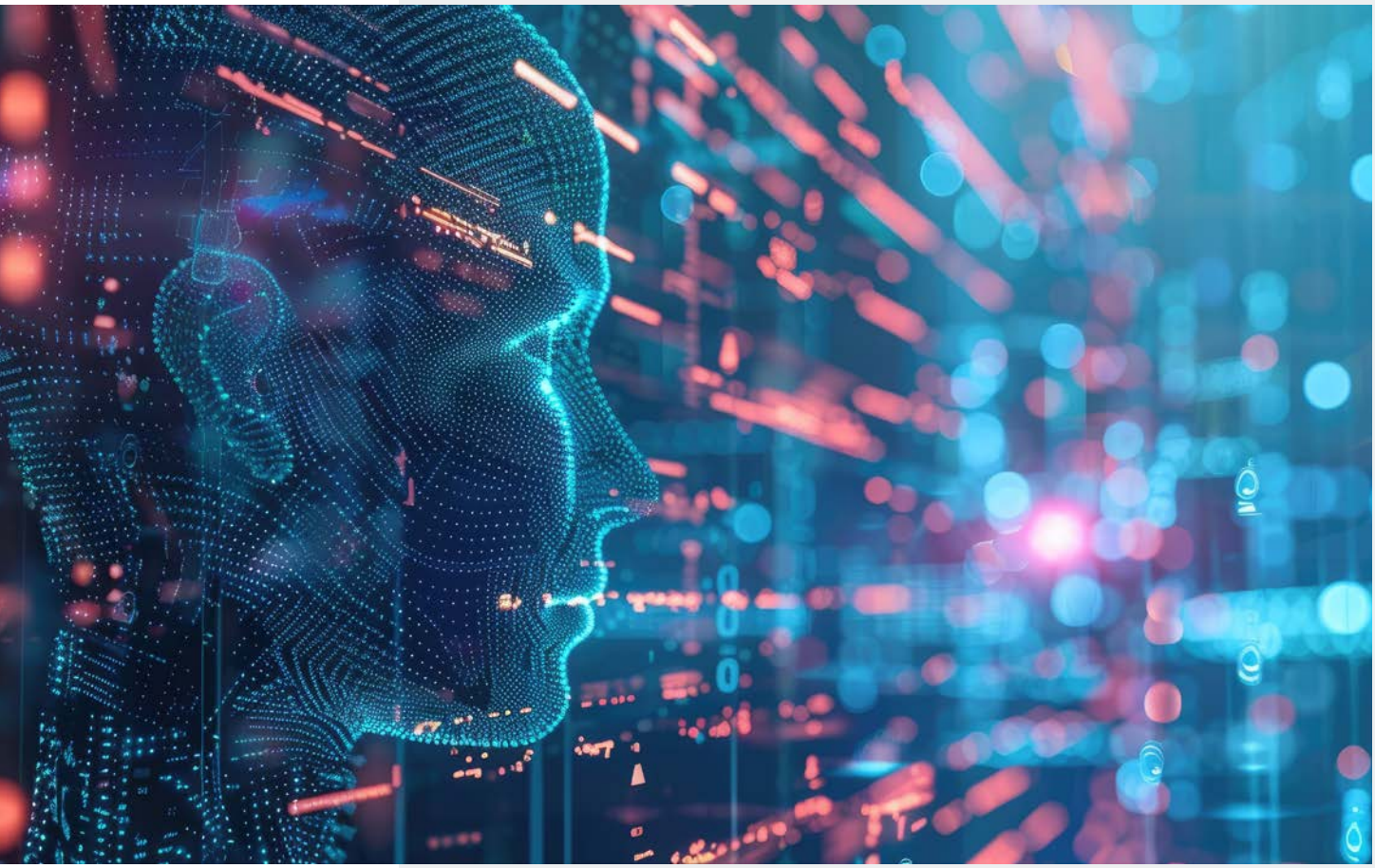
Lire le marché par les problèmes à résoudre

Pour clarifier le marché, il faut abandonner les acronymes comme point de départ. La question n'est pas : faut-il un DLP, un DSPM ou un catalogue ? La question est : quel problème veut-on résoudre en priorité ?

Si l'enjeu principal est de savoir où sont les données sensibles, le DSPM et la découverte automatisée sont centraux. Si l'enjeu est de documenter les actifs, d'aligner les métiers et de fiabiliser les usages analytiques, le catalogue, le lineage, la qualité et le MDM deviennent prioritaires. Si le sujet est la fuite ou l'exfiltration, le DLP garde sa pertinence. Si l'enjeu est la continuité d'activité, la sauvegarde et la restauration prennent le dessus. Si le problème est la preuve, l'archivage, la traçabilité et l'intégrité documentaire redeviennent essentiels.

Le marché se lit donc moins comme une liste de technologies que comme une chaîne de contrôle. Découvrir, classifier, gouverner, protéger, sauvegarder, tracer, prouver. Chaque brique a sa place. Mais la valeur naît de leur articulation.

Ce point est décisif pour les organisations. Elles n'ont pas besoin d'un outil de plus. Elles ont besoin d'un modèle de maîtrise. Et ce modèle commence par une cartographie lucide de leurs risques, de leurs usages et de leurs responsabilités.



SAUVEGARDE, RÉSILIENCE, IMMUTABILITÉ : LE RETOUR EN FORCE DE LA DONNÉE CRITIQUE

La sauvegarde a longtemps été perçue comme une fonction technique, presque invisible, confiée aux équipes infrastructure. Les ransomwares, les attaques destructrices, les dépendances cloud et les exigences de continuité d'activité l'ont replacée au cœur de la confiance numérique. Désormais, la question n'est plus seulement de savoir si les données sont sauvegardées, mais si elles peuvent être restaurées, rapidement, proprement et avec certitude.

Pendant longtemps, beaucoup d'entreprises ont considéré la sauvegarde comme une police d'assurance. Elle existait quelque part, dans un plan technique, avec des procédures connues des équipes IT. Tant que rien ne cassait, le sujet restait discret. Mais les crises cyber ont changé cette perception. Lorsque les systèmes sont chiffrés, les applications arrêtées et les métiers paralysés, la sauvegarde devient le dernier rempart entre l'incident et l'effondrement opérationnel.

La difficulté est que toutes les sauvegardes ne se valent pas. Une donnée copiée n'est pas nécessairement une donnée récupérable. Une sauvegarde trop ancienne, incomplète, compromise ou jamais testée peut donner une illusion de sécurité. Dans une attaque par ransomware, les cybercriminels cherchent souvent à neutraliser les sauvegardes avant de déclencher le chiffrement. La résilience repose donc sur une capacité à protéger les copies elles-mêmes.

C'est dans ce contexte que l'immutabilité s'est imposée comme un mot-clé du marché. Elle désigne la capacité à conserver des données dans un état non modifiable pendant une période donnée. L'objectif est simple : empêcher qu'un attaquant, même doté de privilèges élevés, puisse supprimer ou altérer les copies nécessaires à la reprise. Mais là encore, le mot ne suffit pas. Il faut comprendre comment l'immutabilité est mise en œuvre, où elle s'applique, qui peut l'administrer et comment elle résiste à une compromission.

Restaurer vite ne suffit pas : il faut restaurer juste

La résilience ne se limite pas à la disponibilité technique. Restaurer vite une donnée corrompue, obsolète ou incomplète ne règle rien. Une stratégie mature doit donc distinguer plusieurs questions : quelles données restaurer en priorité ? Dans quel ordre relancer les applications ? Quel niveau de perte de données est acceptable ? Quel temps d'arrêt est tolérable ? Qui valide que les données restaurées sont propres ?

Ces arbitrages sont rarement purement techniques. Une base client, une application de facturation, un référentiel RH, un système de production ou une GED métier n'ont pas la même criticité. Les métiers doivent donc être impliqués dans la définition des priorités. Sans eux, la DSI risque de restaurer ce qui est techniquement logique, mais pas nécessairement ce qui permet à l'organisation de redémarrer.

Le test régulier reste le grand oublié. Beaucoup d'organisations disposent de plans de sauvegarde, mais ne testent pas assez souvent leur capacité réelle de restauration. Or un PRA non testé reste une promesse. La crise ne laisse aucune place à l'improvisation. Les dépendances applicatives, les droits, les volumes, les délais de transfert, les clés de chiffrement et les environnements de reprise doivent être vérifiés avant l'incident, pas pendant.

La donnée critique oblige à rapprocher backup, sécurité et gouvernance

La sauvegarde moderne n'est plus isolée. Elle doit dialoguer avec la cybersécurité, la gouvernance des données, l'archivage et la conformité. Cette convergence est essentielle. Pour protéger les bonnes données, encore faut-il les identifier. Pour restaurer les bonnes données, il faut comprendre leur rôle métier. Pour prouver qu'une copie est saine, il faut pouvoir tracer son état, son intégrité et ses conditions de conservation.

■■■

> *La crise ne laisse aucune place à l'improvisation.*

Le sujet devient encore plus sensible avec les environnements hybrides et SaaS. Beaucoup d'entreprises supposent que les données hébergées dans le cloud sont automatiquement protégées. C'est une confusion dangereuse. La disponibilité d'un service ne garantit pas toujours la récupération granulaire, la conservation longue durée, la protection contre une suppression malveillante ou la conformité à des exigences sectorielles. La responsabilité reste partagée, mais elle ne disparaît pas.

Le retour en force de la sauvegarde est donc moins un retour en arrière qu'un changement de statut. Elle n'est plus un sujet d'infrastructure. Elle devient un pilier de la confiance numérique. Dans une organisation mature, les sauvegardes ne sont pas seulement des copies. Ce sont des actifs critiques, protégés, testés, documentés et intégrés à une stratégie globale de résilience.

La question à poser n'est plus : avons-nous une sauvegarde ? Mais plutôt celle-ci : si demain nos données sont chiffrées, supprimées ou corrompues, saurons-nous vraiment repartir ?

> ***Le retour en force de la sauvegarde est donc moins un retour en arrière qu'un changement de statut.***



PROTECTION, PARTAGE, EXPLOITATION : LES ARBITRAGES IMPOSSIBLES

Les entreprises veulent protéger leurs données. Mais elles veulent aussi les partager, les analyser, les transférer, les croiser, les exposer à des partenaires et les utiliser dans des projets d'IA. Entre sécurité, conformité, productivité et innovation, la donnée critique est devenue un terrain d'arbitrage permanent. La vraie difficulté n'est pas de tout verrouiller, mais de contrôler sans paralyser.

Il existe une tentation naturelle, dans les organisations exposées au risque, de répondre par le verrouillage. Restreindre les accès, bloquer les exports, limiter les partages, interdire certains outils, multiplier les validations. Cette approche rassure sur le papier. Mais elle atteint vite ses limites. Une donnée qui ne circule plus perd une partie de sa valeur. Les métiers ont besoin d'analyser, de comparer, de répondre vite, de collaborer avec des partenaires, de produire des documents, d'instruire des dossiers et de servir des clients.

Le problème n'est donc pas la circulation elle-même. Le problème est la circulation non maîtrisée. Les données critiques sortent souvent des environnements contrôlés par des chemins ordinaires : une pièce jointe envoyée trop largement, un espace partagé mal configuré, un export Excel, une copie locale, un lien public oublié, un fichier transmis à un prestataire, un jeu de données injecté dans un outil d'IA. Ces gestes sont rarement malveillants. Ils sont souvent pratiques. Et c'est précisément ce qui les rend difficiles à maîtriser.

La protection des données se heurte ici à un paradoxe. Plus les outils métiers sont simples et collaboratifs, plus la donnée se déplace facilement. Plus les environnements sont ouverts, plus les contrôles doivent être fins. Une politique de sécurité trop brutale sera contournée. Une politique trop permissive laissera passer les incidents. La maturité consiste à trouver le bon niveau de contrôle selon le contexte, la sensibilité de la donnée et l'usage demandé.

L'IA rend les arbitrages plus visibles

L'IA générative ajoute une couche de complexité. Les utilisateurs veulent interroger des documents, synthétiser des contrats, analyser des emails, extraire des informations, produire des réponses à partir de bases internes. Ces usages peuvent créer de la valeur. Mais ils exposent aussi une question simple : quelles données peut-on réellement donner à lire à une IA ?

Le sujet ne se limite pas à la confidentialité. Il touche aussi à la qualité, aux droits, au contexte et à la traçabilité. Une IA alimentée par des documents obsolètes peut produire des réponses fausses. Une IA connectée à des contenus mal cloisonnés peut révéler des informations sensibles à des utilisateurs qui n'auraient jamais dû y accéder. Une IA nourrie par des données non qualifiées peut donner une impression de fiabilité à un contenu fragile.

C'est ici que les arbitrages deviennent politiques. Faut-il privilégier l'innovation ou la prudence ? Autoriser les métiers à expérimenter ou imposer un cadre strict ? Ouvrir largement les données internes ou commencer par des corpus restreints, qualifiés et gouvernés ? La réponse ne peut pas être uniforme. Elle dépend de la criticité des données, du niveau de maturité de l'organisation, des obligations réglementaires et du niveau de preuve attendu.

Gouverner sans étouffer les usages

La bonne réponse n'est pas de bloquer. Elle consiste à rendre les usages lisibles et contrôlables. Cela suppose d'abord une classification compréhensible. Toutes les données ne sont pas ultra-sensibles. Mais certaines ne devraient jamais sortir d'un périmètre maîtrisé : données personnelles sensibles, secrets d'affaires, éléments de cybersécurité, informations financières non publiées, documents juridiques stratégiques, pièces d'identité, données RH ou informations clients exposées.

■■■

> ***Une donnée qui ne circule plus perd une partie de sa valeur.***

Il faut ensuite adapter les règles aux situations. Un partage interne, un partage externe, une analyse automatisée, un export massif ou un usage IA ne présentent pas le même risque. Les outils de DLP, de DSPM, de gestion des accès, de chiffrement, de journalisation et de gouvernance documentaire peuvent aider. Mais ils ne remplacent pas la décision métier. La technologie doit rendre le risque visible, pas décider seule de ce qui est acceptable.

La protection de la donnée devient donc un exercice d'équilibre. Trop de liberté crée de l'exposition. Trop de contrôle crée du contournement. Entre les deux, il faut construire une discipline : connaître les données, définir les droits, tracer les usages, expliquer les règles et revoir régulièrement les exceptions.

La donnée critique n'a jamais été aussi utile. Elle n'a jamais été aussi mobile. Elle n'a jamais été aussi exposée. C'est cette tension qui oblige les organisations à sortir d'une approche binaire. Il ne s'agit plus de choisir entre protection et exploitation. Il s'agit d'organiser les conditions d'une exploitation digne de confiance.

> ***Le retour en force de la sauvegarde est donc moins un retour en arrière qu'un changement de statut.***



TRAÇABILITÉ, AUDITABILITÉ, PREUVE : LA DONNÉE DOIT AUSSI SE DÉFENDRE

Protéger une donnée ne suffit plus. Encore faut-il pouvoir expliquer ce qui lui est arrivé. Qui y a accédé ? Quand ? Dans quel but ? A-t-elle été modifiée ? Peut-on prouver son intégrité ? Dans un contexte d'audits, de contentieux, de cyberattaques et de conformité renforcée, la traçabilité devient l'un des piliers oubliés de la confiance numérique.

La sécurité cherche à empêcher l'incident. La traçabilité permet de comprendre ce qui s'est passé. L'auditabilité aide à le démontrer. La preuve permet de le défendre. Ces notions sont proches, mais elles ne se confondent pas. Et c'est souvent cette confusion qui fragilise les organisations.

Une entreprise peut disposer de contrôles d'accès, de sauvegardes, de politiques de sécurité et d'outils de supervision. Mais face à un audit ou à une crise, la question devient plus concrète : êtes-vous capable de reconstituer le parcours d'une donnée ? Pouvez-vous montrer qui l'a consultée, modifiée, exportée, transmise ou supprimée ? Pouvez-vous établir que la version présentée est bien la bonne ? Pouvez-vous prouver que les règles de conservation ont été respectées ?

Cette exigence touche de nombreux domaines. Elle concerne les données personnelles, les contrats, les factures, les dossiers RH, les documents réglementaires, les décisions internes, les échanges sensibles, les données financières, les documents produits par l'IA ou les jeux de données utilisés pour entraîner ou alimenter des modèles. Dès qu'une donnée engage l'organisation, elle doit pouvoir être défendue.

Tracer n'est pas surveiller

La traçabilité suscite parfois une méfiance légitime. Mal expliquée, elle peut être perçue comme une logique de surveillance généralisée. C'est une erreur de cadrage. Tracer une donnée critique ne signifie pas surveiller chaque salarié en permanence. Cela signifie documenter les opérations importantes sur des actifs sensibles, dans un cadre explicite, proportionné et gouverné.

Cette nuance est essentielle. Les organisations doivent être capables de protéger leurs intérêts, leurs clients, leurs salariés et leurs obligations réglementaires, sans basculer dans une culture de suspicion. La traçabilité doit donc être encadrée par des règles claires : quelles données sont concernées, quels événements sont journalisés, qui peut consulter les traces, combien de temps elles sont conservées, et dans quelles conditions elles peuvent être utilisées.

> ***La preuve numérique ajoute une exigence supplémentaire : l'intégrité.***

La qualité des traces est tout aussi importante que leur existence. Des logs trop volumineux, mal structurés ou impossibles à exploiter ne servent à rien. À l'inverse, des journaux bien conçus permettent de détecter des comportements anormaux, d'analyser un incident, de répondre à un auditeur, de documenter une décision ou de reconstituer une chaîne de responsabilité.

La preuve impose une chaîne de confiance

La preuve numérique ajoute une exigence supplémentaire : l'intégrité. Il ne suffit pas de conserver une trace. Il faut pouvoir démontrer qu'elle n'a pas été altérée. C'est ici que l'archivage électronique, l'horodatage, les journaux sécurisés, les coffres-forts numériques, les politiques de conservation et les mécanismes d'intégrité prennent tout leur sens.

■■■

Cette chaîne de confiance ne concerne pas seulement les directions juridiques. Elle intéresse aussi les DSI, les RSSI, les DPO, les directions métiers et les auditeurs. Dans une crise cyber, elle aide à distinguer les données compromises des données fiables. Dans un litige, elle permet d'opposer une version documentée. Dans un projet IA, elle permet de remonter aux sources utilisées. Dans une démarche conformité, elle fournit des éléments vérifiables.

Le point critique est de ne pas traiter la preuve comme une couche ajoutée à la fin. Elle doit être pensée dès la conception des processus. Lorsqu'un document est capturé, une donnée validée, un accès accordé, une décision prise ou une version archivée, les éléments de preuve doivent être produits naturellement par le système.

La donnée doit donc être capable de se défendre. Non pas par elle-même, mais grâce à un environnement qui documente son origine, ses transformations, ses accès et son intégrité. Dans un monde où les contenus circulent vite, où l'IA peut produire des synthèses convaincantes et où les cyberattaques brouillent les repères, cette capacité devient stratégique.

La confiance ne se décrète pas. Elle se prouve. Et pour la prouver, il faut avoir tracé avant d'être contesté.

> ***Le point critique est de ne pas traiter la preuve comme une couche ajoutée à la fin. Elle doit être pensée dès la conception des processus.***



AVANT L'IA, LA GED : POURQUOI LES ENTREPRISES DOIVENT STRUCTURER LEUR INFORMATION

Les entreprises veulent déployer des assistants IA, interroger leurs bases internes, automatiser le traitement documentaire et exploiter leurs contenus métiers. Mais beaucoup sous-estiment une condition préalable : l'information doit être structurée, gouvernée, sécurisée et accessible. Sans GED solide, l'IA documentaire promet beaucoup, mais risque surtout d'accélérer le désordre.

Le discours autour de l'IA en entreprise donne parfois l'impression qu'il suffirait de connecter un assistant à des documents internes pour libérer instantanément la connaissance. C'est séduisant, mais dangereux. L'IA ne transforme pas automatiquement un patrimoine documentaire désorganisé en information fiable. Elle peut même produire l'effet inverse : rendre plus fluide, plus rapide et plus convaincante une réponse fondée sur des contenus incomplets, obsolètes ou mal contextualisés.

Dans beaucoup d'organisations, les documents restent dispersés entre messageries, serveurs de fichiers, GED anciennes, espaces collaboratifs, outils métiers, postes locaux, archives et applications SaaS. Les versions se multiplient. Les métadonnées sont incomplètes. Les droits d'accès reflètent parfois l'histoire des services plus que les besoins réels. Les documents sensibles côtoient des contenus sans valeur. Et les règles de conservation ne sont pas toujours appliquées.

Dans ce contexte, brancher une IA sur les contenus internes revient à poser un moteur puissant sur une route mal cartographiée. Le moteur fonctionne. Le problème vient de la route. Si les sources ne sont pas maîtrisées, l'IA ne sait pas toujours distinguer le document validé de la version provisoire, le contrat en vigueur de l'ancien modèle, la procédure officielle de la note oubliée, ou l'information accessible de celle qui devrait rester confidentielle.

La GED redevient une fondation stratégique

La gestion électronique des documents a parfois été réduite à une promesse de dématérialisation : remplacer le papier, centraliser les fichiers, fluidifier les circuits de validation. Cette vision est trop étroite. Une GED moderne n'est pas seulement un espace de stockage. C'est une infrastructure de gouvernance documentaire. Elle organise les contenus, structure les métadonnées, gère les droits, pilote les workflows, trace les actions et prépare l'archivage.

C'est précisément ce dont l'IA a besoin pour produire de la valeur durable. Un assistant documentaire fiable doit s'appuyer sur des corpus qualifiés. Un moteur de recherche augmenté doit comprendre le contexte des documents. Un outil d'extraction doit savoir quelles données sont attendues et avec quel niveau de confiance. Un agent IA doit respecter les droits d'accès, les règles métier et les limites d'usage. Sans cette couche documentaire, l'IA reste fragile.

La GED permet aussi de reconnecter l'IA aux processus. L'enjeu n'est pas seulement de poser une question à une base documentaire. Il est de déclencher une action fiable : instruire un dossier, contrôler une pièce, comparer des documents, extraire des données vers un ERP, préparer une réponse client, alimenter un workflow, classer automatiquement un contenu ou alerter sur une anomalie. La valeur ne vient pas de l'IA seule. Elle vient de son insertion dans un système d'information gouverné.

Gouverner les contenus avant de les faire parler

Le préalable est donc clair : avant de faire parler les documents, il faut savoir lesquels méritent d'être écoutés. Cela suppose de cartographier les gisements documentaires, d'identifier les contenus critiques, de nettoyer les doublons, de qualifier les métadonnées, de revoir les droits et de définir des règles de cycle de vie. C'est un travail moins spectaculaire qu'une démonstration d'IA, mais beaucoup plus déterminant.

■■■

> ***Une GED moderne n'est pas seulement un espace de stockage***

Cette approche oblige aussi à distinguer les types de contenus. Tous les documents ne doivent pas être exposés à un assistant IA. Certains relèvent de la connaissance générale de l'entreprise. D'autres contiennent des données personnelles, des secrets commerciaux, des engagements contractuels ou des éléments juridiques sensibles. Une GED bien gouvernée permet de définir ces périmètres et d'éviter que l'IA ne devienne un accélérateur de fuite ou de confusion.

Le sujet concerne particulièrement les organisations qui manipulent de grands volumes de documents métiers : banques, assurances, administrations, santé, industrie, immobilier, services financiers, transport, énergie. Dans ces environnements, la qualité documentaire conditionne la qualité opérationnelle. Une erreur d'extraction, une mauvaise version ou un accès trop large peut avoir des conséquences juridiques, financières ou réputationnelles.

L'IA documentaire n'est donc pas un raccourci. C'est un révélateur. Elle révèle les organisations qui ont déjà structuré leur information et celles qui ont laissé s'accumuler des années de désordre numérique. Les premières pourront automatiser, accélérer et mieux décider. Les secondes risquent de découvrir que leur principal obstacle n'est pas l'algorithme, mais leur propre patrimoine documentaire.

Avant d'IA-iser l'entreprise, il faut structurer son non-structuré. La GED n'est pas le passé de la transformation numérique. Elle pourrait bien en redevenir le socle.

> ***L'IA documentaire n'est donc pas un raccourci. C'est un révélateur.***





DONNÉES CRITIQUES : LES ACTEURS QUI STRUCTURENT LE MARCHÉ EUROPÉEN

30 1. Gouverner et fiabiliser la donnée

34 2.Protéger et contrôler les données sensibles

36 3.Préserver, documenter et prouver

Partenaire

DIGDASH

1. GOUVERNER ET FIABILISER LA DONNÉE

Cette catégorie regroupe les acteurs de la data governance, du catalogage, du lineage, du MDM et de la qualité des données. Leur rôle est d'aider les organisations à comprendre leurs actifs data, à les documenter, à les fiabiliser, à les relier aux usages métiers et à créer un langage commun entre DSI, CDO, métiers, conformité et sécurité.

— COLLIBRA

Né en Belgique et fortement implanté aux États-Unis, Collibra est l'un des acteurs de référence de la gouvernance des données. Sa plateforme vise les grandes organisations qui veulent structurer leurs politiques data, documenter leurs actifs, définir des responsabilités et créer un langage commun entre métiers, équipes data et conformité. Son positionnement est clairement orienté gouvernance d'entreprise, catalogue, règles, workflows et confiance dans la donnée.

— INFORMATICA

Informatica est un acteur historique du data management. Son positionnement couvre un périmètre large : intégration, qualité, MDM, catalogue, gouvernance, lineage et préparation de la donnée pour les usages analytiques ou IA. L'entreprise vise les grands comptes ayant des environnements complexes et hybrides. Sa force tient à l'étendue de sa plateforme, capable de couvrir plusieurs couches du cycle de vie de la donnée.

— ALATION

Alation s'est imposé comme un spécialiste du data catalog et de la data intelligence. Son approche consiste à rendre les données plus compréhensibles, plus trouvables et plus utilisables par les métiers comme par les équipes data. La plateforme met l'accent sur la documentation, la recherche, la collaboration, le lineage et la gouvernance des usages. Elle cible les organisations qui veulent démocratiser l'accès à la donnée sans perdre le contrôle.

— DATAGALAXY

DataGalaxy est un acteur français spécialisé dans le catalogue de données et la gouvernance collaborative. Sa promesse repose sur une meilleure compréhension des actifs data par les métiers, avec des fonctions de glossaire, cartographie, lineage et documentation. Son positionnement est intéressant pour les entreprises européennes qui veulent éviter une gouvernance trop technicienne et reconnecter les données aux usages opérationnels et à la connaissance métier.

— ZEENEA

Zeenea, entreprise française, se positionne sur la gouvernance agile des métadonnées et le data catalog. Son approche vise à aider les organisations à inventorier leurs actifs, à enrichir leur contexte, à documenter les règles d'usage et à améliorer la découverte des données. Zeenea parle autant aux équipes data qu'aux métiers, avec une logique de gouvernance progressive, moins lourde que certains grands programmes centralisés.

ATACCAMA

Ataccama propose une plateforme orientée qualité, MDM, gouvernance, catalogage, observabilité et lineage. Son positionnement repose sur la notion de confiance dans la donnée, avec une forte dimension qualité et automatisation. L'éditeur intéresse les organisations qui veulent consolider leurs référentiels, fiabiliser leurs données critiques et rapprocher gouvernance, qualité et usage opérationnel dans un même environnement.

DIGDASH

Créé en 2006 et basé près d'Aix-en-Provence, DigDash est un éditeur français spécialisé dans l'exploitation des données. Sa mission : les rendre accessibles aux métiers, sans réserver leur analyse aux experts. L'entreprise compte plus de 70 collaborateurs et s'appuie sur un réseau de partenaires.

Son offre couvre trois maillons complémentaires. DigDash DataStack assure l'ingestion, la transformation et le stockage de volumes importants afin de constituer des entrepôts fiables. DigDash BI prépare, analyse et restitue les informations sous forme de tableaux de bord interactifs, personnalisables et simples à explorer. La BI intègre aussi un requêteur en langage naturel destiné aux non-spécialistes. DigDash AI complète cet ensemble avec des fonctions de recherche documentaire, de chatbot et d'automatisation capables d'interroger des données structurées comme non structurées. L'IA interptère la demande et restitue la réponse, tandis que le moteur BI exécute les calculs sur les données sources.

Éditeur souverain et certifié ISO 27001, DigDash s'appuie notamment sur OVHcloud et Cloud Temple pour ses offres hébergées. La plateforme gère finement les droits, les niveaux de détail et les possibilités d'export. Elle cible le secteur public, les collectivités, la défense, la santé, l'éducation et la recherche, l'industrie, l'énergie, la logistique, les services financiers et les éditeurs souhaitant intégrer l'analytique à leurs applications. Sa différenciation repose sur la simplicité d'usage, le traitement de volumes élevés et la capacité à adapter rapidement le produit aux besoins des clients.

En savoir plus
Demandez une démo



SEMARCHY

Semarchy est un acteur d'origine française spécialisé dans le Master Data Management et la gestion des référentiels. Son positionnement est centré sur la création d'une vision fiable des données maîtres : clients, fournisseurs, produits, organisations. Il s'adresse aux entreprises qui veulent réduire les incohérences entre systèmes, améliorer la qualité des données de référence et poser une base robuste pour leurs projets analytiques, métiers ou IA.

BLUEWAY

Blueway est un éditeur français basé à Lyon, positionné sur la gestion des données, l'intégration, le MDM, le data catalog, les API et l'automatisation des processus. Sa plateforme Phoenix couvre plusieurs briques utiles à une gouvernance opérationnelle : Data Governance, Data Foundation, API Governance, Process Governance et MyDataCatalogue. Blueway s'adresse aux DSI qui veulent urbaniser leur SI, créer des référentiels fiables et cartographier leurs données sans multiplier les silos.

À L'URSSAF, LA SOUVERAINETÉ NUMÉRIQUE PASSE AUSSI PAR LES TABLEAUX DE BORD

DIGDASH

Pour reprendre la main sur un environnement décisionnel dispersé, l'Urssaf Caisse nationale a choisi DigDash comme outil unique de datavisualisation. Herbert Nyembo, sous-directeur à la DSI, revient sur ce chantier qui associe rationalisation, indépendance technologique et conduite du changement à l'échelle de 16 000 agents.



Power BI, SAS, Spotfire et une autre solution coexistaient dans le système d'information de l'Urssaf. Cet empilement compliquait la maintenance, fragmentait les pratiques et entretenait la dépendance à plusieurs fournisseurs.

L'organisme a donc décidé de mutualiser la datavisualisation autour d'une plateforme commune. DigDash, initialement arrivé comme un outil supplémentaire, a été comparé aux solutions installées. L'éditeur français a été retenu pour sa simplicité, son interopérabilité avec le système d'information, son accessibilité et la maîtrise de la dépendance technologique. Le coût a également été un élément majeur dans la prise de décision.

Ce choix ne se limite pas au remplacement de licences. Il s'inscrit dans une architecture globale baptisée Data Fabric. La préparation des données est centralisée avec Dremio ; DigDash prend ensuite en charge leur analyse et leur restitution. Cette séparation permet aux tableaux de bord de s'appuyer sur une source de référence commune et réduit le risque de voir chaque équipe produire ses propres chiffres. Pour un organisme qui traite des volumes massifs de données sociales, la souveraineté signifie ici garder la maîtrise de la localisation, des accès et des choix technologiques, tout en limitant le verrouillage par un fournisseur.

Une migration technique, surtout une transformation humaine

Le déploiement, engagé au début de l'année 2026, doit s'étendre sur plus d'un an. Il ne s'agit pas de reproduire mécaniquement l'existant. Avant chaque migration, les équipes analysent l'usage réel des rapports, identifient ceux qui peuvent être supprimés ou regroupés et profitent des fonctions interactives pour simplifier le patrimoine. Plusieurs rapports presque identiques peuvent ainsi être remplacés par un seul tableau de bord doté de filtres. À la clé, moins de doublons, une maintenance allégée et une meilleure visibilité sur les informations diffusées.

Le calendrier est aligné, autant que possible, sur la fin des contrats de maintenance des anciens outils. Cette progression évite une bascule brutale, mais elle ne supprime pas le principal obstacle : l'adhésion. Des agents habitués, depuis parfois dix ans, à leurs outils ne changent pas de méthode parce qu'une plateforme est plus cohérente. Les écrans doivent rester proches des usages, le sens de la démarche doit être compris et l'accompagnement doit durer.

Pour diffuser les compétences, DigDash et l'Urssaf ont retenu un modèle de formation de formateurs. Des référents internes sont formés, puis chargés d'accompagner les autres agents. Des modules spécifiques peuvent aussi être développés selon les besoins. Cette proximité est décisive dans un projet qui touche des dizaines d'équipes et un grand nombre de rapports.

Le projet n'a pas encore livré tous ses résultats, mais le cap est désormais clair. En faisant converger quatre outils vers une plateforme souveraine et partagée, l'Urssaf ne se contente pas de rationaliser ses licences. Elle bâtit un socle décisionnel plus cohérent, plus simple et mieux maîtrisé au service de 16 000 agents. Si la migration tient ses promesses, ce chantier démontrera qu'une souveraineté numérique concrète, utile aux métiers et déployable à grande échelle peut devenir une réalité.

CONTACT
Nom/Prénom : Geraldine Tossou Mail : marketing@digdash.com Tel : 04 84 25 01 40
Site web : https://www.digdash.com/fr/

— DAWIZZ

Dawizz est un éditeur français originaire de Vannes, spécialisé dans le data catalog et la data discovery. La société a été acquise par Blueway en 2023 pour renforcer la plateforme Phoenix. Sa solution MyDataCatalogue permet de recenser, documenter et cartographier les données structurées et non structurées. Elle répond à des enjeux de gouvernance, conformité, cybersécurité et meilleure connaissance du patrimoine data. À présenter comme une brique de l'écosystème Blueway plutôt qu'un acteur autonome.

— QLIK TALEND

Talend, historiquement créé en France, est aujourd'hui intégré à Qlik. L'ensemble se positionne sur l'intégration, la qualité, la préparation, la gouvernance et l'analytics. Qlik Talend met notamment en avant la qualité et la gouvernance des données, avec des fonctions de profiling, règles qualité et outils pour data stewards. C'est un acteur à intégrer car il se situe au croisement entre data integration, data quality, gouvernance et exploitation analytique.

— DENODO

Denodo est un acteur d'origine espagnole, devenu international, spécialiste de la virtualisation des données et du logical data management. Son positionnement est différent d'un catalogue pur : Denodo permet d'accéder aux données là où elles se trouvent, sans nécessairement les déplacer, via une couche logique de data fabric. L'éditeur met aussi en avant le catalogue, la gouvernance centralisée des accès et la distribution de données en self-service. Très pertinent pour parler d'architecture anti-silos.

— DATAIKU

Dataiku, né en France et fortement développé aux États-Unis, est surtout connu comme plateforme d'analytics, data science, IA et MLOps. Il ne faut pas le présenter comme un pur acteur de gouvernance data, mais comme une plateforme d'exploitation data et IA qui intègre des fonctions de gouvernance, notamment autour des projets analytiques, modèles et agents. Son intérêt éditorial est évident pour l'article sur IA et gouvernance : il illustre le passage de la donnée préparée à la donnée exploitée sous contrôle.

— SODA

Soda est un acteur de la qualité des données et de la data observability. Son positionnement repose sur la détection d'anomalies, le suivi de métriques, les contrôles qualité, les contrats de données et les alertes avant que des problèmes n'affectent les usages métiers ou analytiques. C'est un acteur à classer dans la fiabilisation, pas dans la protection. Son rôle est de renforcer la confiance opérationnelle dans les pipelines et les jeux de données.

— ATLAN

Atlan est une plateforme d'active metadata, de data catalog et de gouvernance collaborative. Elle se positionne comme une couche de contexte pour les équipes data et les usages IA. Atlan met en avant les tags, la classification, les workflows de gouvernance, le lineage, la découverte et le contrôle d'accès granulaire. C'est un acteur moderne à ajouter si tu veux élargir le panorama au-delà des acteurs historiques comme Collibra, Informatica ou Alation.

— CHAPSVISION

ChapsVision est un acteur français de la data intelligence et de l'IA, positionné sur la collecte, la transformation, la sécurisation et l'analyse de grands volumes de données complexes. Sa plateforme Argonos vise notamment les grandes organisations, les secteurs régaliens, la sécurité et la prise de décision augmentée. Ce n'est pas un acteur de gouvernance data classique, mais il mérite une place dans une cartographie élargie autour de l'exploitation critique des données, surtout avec l'angle souveraineté et data intelligence.

2. PROTÉGER ET CONTRÔLER LES DONNÉES SENSIBLES

Cette catégorie regroupe les acteurs du DLP, du DSPM, de la classification, de la confidentialité, du contrôle des accès et de la posture de sécurité des données. Leur enjeu commun : découvrir les données sensibles, comprendre leur exposition, réduire les droits excessifs, éviter les fuites et mieux encadrer les usages cloud, SaaS et IA.

— MICROSOFT PURVIEW

Microsoft Purview s'inscrit dans l'écosystème Microsoft 365, Azure et sécurité. La plateforme couvre gouvernance, classification, protection de l'information, DLP, conformité et DSPM. Son avantage tient à son intégration native dans des environnements déjà massivement utilisés. Son enjeu est d'aider les entreprises à mieux contrôler les données qui circulent dans les outils Microsoft, mais aussi dans des contextes cloud et SaaS plus larges.

— BIGID

BigID est positionné sur la découverte, la classification, la sécurité, la confidentialité et la gouvernance des données sensibles. L'éditeur couvre DSPM, DLP, privacy, accès, suppression et risques liés à l'IA. Son approche consiste à donner une visibilité fine sur les données structurées et non structurées, dans des environnements hybrides. Il vise les grandes organisations confrontées à des exigences fortes de conformité et de maîtrise des données.

— VARONIS

Varonis est un acteur historique de la sécurité des données, notamment sur les accès, les permissions, les fichiers sensibles et les comportements anormaux. Son positionnement s'est élargi vers le DSPM, la classification, le SaaS, le cloud et l'IA. L'éditeur est particulièrement pertinent pour les organisations qui veulent comprendre qui accède à quoi, réduire les droits excessifs et détecter les expositions ou usages à risque.

— CYERA

Cyera fait partie des acteurs récents qui ont popularisé le DSPM moderne. Son positionnement repose sur la découverte automatisée des données sensibles, la cartographie des risques, la classification et la priorisation des remédiations dans des environnements cloud, SaaS et IA. L'éditeur cible les équipes sécurité qui veulent obtenir rapidement une visibilité sur l'exposition réelle de leurs données critiques.

— WIZ

Wiz est d'abord connu pour sa plateforme de sécurité cloud, mais l'éditeur étend son positionnement vers la protection des données critiques dans les environnements cloud. Son intérêt est de relier la posture de sécurité cloud aux risques data : exposition, secrets, configurations, vulnérabilités et données sensibles. Il s'adresse aux organisations déjà avancées dans le cloud et qui veulent croiser sécurité d'infrastructure et sécurité de la donnée.

— ONETRUST

OneTrust est l'un des acteurs connus de la privacy tech, de la gestion du consentement, des risques tiers, de la conformité et de la gouvernance de la vie privée. Sa place dans cette cartographie tient à sa capacité à traiter les données sous l'angle réglementaire et organisationnel. Il s'adresse notamment aux DPO, directions juridiques, conformité et risques, avec une approche centrée sur la responsabilité et la documentation.

— SECURITI

Securiti se positionne sur la gouvernance, la sécurité et la confidentialité des données, avec un accent fort sur les environnements cloud, SaaS et IA. Son Data Command Center vise à unifier la visibilité sur les données distribuées, les obligations de conformité, les risques et les usages. L'acteur intéresse les entreprises qui cherchent une couche de contrôle transversale entre privacy, sécurité et gouvernance data.

— FORCEPOINT

Forcepoint est un acteur américain historiquement reconnu sur le DLP et la sécurité centrée sur les données. Son positionnement repose sur la surveillance et le contrôle des flux de données sensibles, avec des capacités de politiques, reporting, conformité et investigation. Il s'adresse aux organisations qui veulent encadrer les usages des données sur les postes, les emails, le web, le cloud ou les environnements hybrides.

— BROADCOM/SYMANTEC DLP

Symantec DLP, aujourd'hui dans le giron de Broadcom, reste une référence historique du marché de la prévention des pertes de données. Son intérêt éditorial vient de son ancienneté et de sa profondeur fonctionnelle sur les canaux web, email, endpoint et API. C'est moins un acteur *« nouvelle vague »* qu'un socle DLP d'entreprise, souvent présent dans les grandes organisations qui ont structuré tôt leurs politiques de protection des données sensibles.

— NETSKOPE

Netskope est un acteur américain du SASE et de la sécurité cloud, très positionné sur la protection des données dans les usages SaaS, web et cloud. Son DLP vise à contrôler les contenus sensibles lorsqu'ils quittent le périmètre traditionnel de l'entreprise, notamment vers des applications comme Google Drive, OneDrive ou d'autres environnements cloud. Netskope revendique aussi une approche unifiée mêlant DLP et DSPM.

— ZSCALER

Zscaler vient du cloud security et du Zero Trust, mais son offre DLP l'inscrit pleinement dans la protection des données sensibles. L'éditeur met en avant une approche intégrée à sa plateforme cloud, capable de couvrir les données en mouvement, au repos et sur les terminaux selon les usages. Sa valeur dans cette cartographie tient à sa capacité à associer sécurité d'accès, inspection des flux et prévention des fuites dans des environnements distribués.

— PALO ALTO NETWORKS

Palo Alto Networks, connu pour la cybersécurité réseau, cloud et SASE, propose également une offre Enterprise DLP. Son positionnement vise la protection des données sensibles contre la perte et le vol, avec une intégration dans son portefeuille de sécurité. L'acteur est pertinent pour montrer que le DLP n'est plus isolé : il se connecte désormais aux plateformes de sécurité cloud, aux contrôles d'accès et aux risques liés aux usages IA.

3. PRÉSERVER, DOCUMENTER ET PROUVER

Cette catégorie regroupe les acteurs du backup, de la cyber-résilience, de l'archivage, de la GED, du content management et de la preuve. Leur rôle est de garantir que les données et documents critiques restent disponibles, intègres, retrouvables, gouvernés et opposables, y compris en cas de crise, d'audit ou d'usage IA.

— RUBRIK

Rubrik s'est imposé sur le marché de la sauvegarde moderne et de la cyber-résilience. Son positionnement ne se limite plus au backup classique : l'éditeur met en avant la récupération après ransomware, l'immutabilité, la protection des environnements hybrides et la réduction du risque cyber. Il cible les entreprises qui veulent transformer la sauvegarde en véritable socle de continuité et de résilience opérationnelle.

— COHESITY

Cohesity se positionne sur la sécurité et la gestion des données secondaires : sauvegarde, récupération, protection contre les ransomwares, archivage et exploitation des données sauvegardées. Son approche vise à simplifier la protection de volumes distribués dans des environnements hybrides et cloud. L'éditeur intéresse les organisations qui cherchent à consolider leurs silos de sauvegarde et à mieux valoriser leurs copies de données.

— VEEAM

Veeam, historiquement associé à la sauvegarde et à la disponibilité des environnements virtualisés, a élargi son positionnement vers la protection des données cloud, SaaS, Kubernetes et la cyber-résilience. L'éditeur parle à un large marché, des PME aux grands comptes. Sa promesse repose sur la simplicité de restauration, la portabilité et la continuité d'activité dans des environnements de plus en plus distribués.

— COMMVAULT

Commvault est un acteur historique de la sauvegarde, de la restauration, de l'archivage et de la gestion des données d'entreprise. Son positionnement s'est renforcé autour de la cyber-résilience, de la protection contre les ransomwares et de la gestion des environnements hybrides. L'éditeur vise les organisations complexes, avec des besoins avancés de conservation, reprise, conformité et orchestration de la donnée critique.

— HYLAND

Hyland, avec OnBase notamment, se positionne sur le content management, la gestion documentaire, l'automatisation des processus et la gouvernance des contenus. Sa place devient stratégique avec l'IA : les entreprises doivent structurer, sécuriser et contextualiser leurs documents avant de les exploiter par des assistants ou des agents. Hyland vise les organisations très documentaires : santé, finance, secteur public, assurance, industrie.

— OPENTEXT

OpenText est un acteur majeur de l'enterprise content management, de la gouvernance de l'information, de l'archivage et de la gestion documentaire. Son positionnement couvre le cycle de vie des contenus, leur conformité, leur exploitation et leur intégration aux processus métiers. Avec l'IA, OpenText met en avant la nécessité d'un contenu gouverné, sécurisé et contextualisé pour produire des résultats fiables.

— M-FILES

M-Files est un éditeur finlandais de gestion documentaire et d'ECM, connu pour son approche fondée sur les métadonnées plutôt que sur les arborescences classiques. Son positionnement est intéressant pour les organisations qui veulent rendre leurs documents plus trouvables, contextualisés et gouvernés. Dans un contexte IA, cette logique de métadonnées devient précieuse pour fiabiliser la recherche, les droits et l'exploitation des contenus.

— DOCUWARE

DocuWare, d'origine allemande, propose une plateforme de GED et de dématérialisation orientée cloud, workflows, capture documentaire et automatisation des processus. Son positionnement s'adresse aux PME, ETI et organisations qui veulent structurer leurs flux documentaires, factures, dossiers RH ou processus administratifs. Dans la gestion des datas, son rôle est de transformer les documents en informations mieux classées, exploitables et traçables.

— EVERTEAM

Everteam est un acteur français de la gouvernance de l'information, de l'archivage, de la conformité et de la gestion documentaire. Son positionnement est particulièrement adapté aux organisations qui doivent maîtriser des contenus sensibles, des durées de conservation, des obligations réglementaires et des enjeux de preuve. Il se situe à la frontière entre GED, archivage, records management et gouvernance de l'information.

— OODRIVE

Oodrive est un acteur français du partage sécurisé, de la collaboration, de la signature électronique et de la protection des documents sensibles. Son positionnement est utile dans une cartographie centrée sur la donnée critique, car il touche aux usages réels : circulation, contrôle, souveraineté, confidentialité et partage externe. L'éditeur parle aux organisations qui veulent collaborer sans perdre la maîtrise de leurs informations stratégiques.

— DOCAPOSTE

Docaposte, filiale du groupe La Poste, est l'un des grands acteurs français de la confiance numérique. Sa place dans cette cartographie est évidente sur l'archivage numérique, la conservation probatoire, le coffre-fort, la signature électronique et les plateformes de confiance. Avec Arkhinéo, Docaposte couvre l'archivage électronique et la préservation de la valeur probante des documents.

— XELIANS

Xelians est un acteur français de la gestion documentaire, de la numérisation, de la GED, du SAE et de l'archivage physique et électronique. Son positionnement couvre l'ensemble du cycle de vie documentaire, de la capture à la conservation probatoire, avec une approche souveraine, des datacenters en France et près de 50 ans d'expertise revendiqués. À classer aux côtés de Docaposte, Tessi, Arcsys ou Everteam, sur les enjeux de preuve, conformité, archivage et gouvernance documentaire.

— TESSI

Tessi est un acteur français de la digitalisation des processus documentaires, de la GED, de l'ECM/BPM, de la dématérialisation et de l'archivage électronique. Son positionnement est moins *« data governance »* pure que *« document, processus et conformité »*. Il mérite d'être intégré pour couvrir les organisations qui veulent capturer, centraliser, sécuriser et archiver leurs contenus métiers, avec une logique de coffre numérique et de valeur probante.

— ARCSYS

Arcsys est un éditeur français spécialisé dans l'archivage, la préservation long terme, le records management et la gestion de contenus. Sa suite vise à constituer un entrepôt unifié de conservation pour les archives de l'entreprise, avec des enjeux de conformité, de pérennité et de confiance numérique. C'est un acteur pertinent pour traiter la donnée critique non seulement comme un actif à sauvegarder, mais comme une preuve à conserver et à gouverner.

— PROOFPOINT ARCHIVE

Proofpoint est surtout connu pour la sécurité email, mais Proofpoint Archive s'inscrit dans le champ de l'archivage cloud, de l'e-discovery, de la conformité et de l'accès aux données archivées. Sa place dans la cartographie se justifie pour les entreprises qui doivent conserver, rechercher et produire des communications électroniques à des fins réglementaires ou juridiques.

— SMARSH

Smarsh est un acteur américain spécialisé dans l'archivage des communications, la conformité, la supervision et l'e-discovery. Son archive cible les organisations soumises à de fortes obligations réglementaires, notamment dans la finance, les services professionnels ou les secteurs contrôlés. Son intérêt éditorial est de rappeler que la donnée critique ne se limite pas aux bases métiers : emails, messages, conversations et contenus collaboratifs deviennent aussi des preuves.



serda compétences

DES COMPÉTENCES DURABLES
POUR PILOTER L'INFORMATION
DANS UN MONDE DIGITAL

+ DE 19 STAGES IA EN 2026
Boostez vos compétences
grâce à l'intelligence artificielle

EN PRÉSENTIEL OU DISTANCIEL

CERTIFIÉ QUALIOPI

Découvrez notre **Catalogue** de formation en **intelligence artificielle.**



L'**intelligence artificielle** bouleverse notre environnement de travail, et s'impose comme un levier stratégique pour innover et gagner en efficacité.

Nous proposons un large choix de formations en IA, adaptés aux **professionnels de la documentation**, de la **veille**, de la **communication**, de la **gestion de l'information** ou du **marketing**.

Que vous débutiez ou que vous ayez déjà une expérience confirmée, nos modules vous permettent d'acquérir des **compétences concrètes**, immédiatement mobilisables dans vos missions.

Prenez de l'avance, formez-vous à l'IA !
Renforcez votre valeur ajoutée et sécurisez vos projets numériques dans un environnement en évolution constante.

Découvrez toutes nos formations

INSCRIVEZ-VOUS SUR WWW.FORMATION-SERDA.COM