

LIVRES BLANCS • ÉDITION 2026

Gouverner l'IA : de l'usage toléré à la preuve de maîtrise

Agents, identités machines, données et droit : ce qu'une direction doit pouvoir démontrer en 2026, une grille d'évaluation neutre et une feuille de route en 90 jours.

29 octobre 2026 • 15 min de lecture

L'ESSENTIEL

- Selon le playbook 2026 de l'éditeur français Dust, la question des directions n'est plus de savoir si l'IA est utilisée, mais de pouvoir prouver qu'elle est maîtrisée.
- Le rapport d'Entro Security sur le premier semestre 2025 compte 144 identités non humaines pour une identité humaine dans les environnements analysés, contre 92 pour 1 un an plus tôt.
- La « triade létale » décrite par Simon Willison le 16 juin 2025 réunit l'accès à des données confidentielles, l'exposition à du contenu non fiable et la capacité de communiquer vers l'extérieur.
- L'obligation de maîtrise de l'IA (article 4 de l'AI Act) s'applique depuis le 2 février 2025 ; le règlement (UE) 2026/1744 a reporté au 2 décembre 2027 les obligations des systèmes à haut risque de l'annexe III.

- Une plateforme d'IA s'évalue sur des preuves : pistes d'audit, connecteurs réservés aux administrateurs, accès par groupes (SSO, SCIM), cloisonnement, trafic sortant limité et réversibilité.

En 2024, les directions se demandaient si leurs équipes utilisaient l'IA. En 2026, la réponse est connue : oui, souvent en dehors des outils officiels. La question a donc changé. Selon le playbook de l'éditeur français Dust (France · Dust), publié dans une édition 2026, l'« IA fantôme » est désormais un fait admis dans les grandes entreprises ; ce qu'un comité de direction doit désormais établir, c'est sa capacité à démontrer qu'il garde la main sur l'IA.

Ce livre blanc répond à cette question pour les comités de direction, les DSI, les RSSI, les DPO et les acheteurs. Il s'appuie sur ce playbook, sur les textes en vigueur au 29 octobre 2026 et sur les recommandations des autorités européennes et françaises. Il ne recommande aucun produit.

1. Pourquoi c'est urgent : de l'« IA fantôme » à la preuve de maîtrise

Trois évolutions rendent la preuve urgente.

Les agents agissent. Un assistant conversationnel produit du texte. Un agent, lui, lit une boîte mail, interroge une base, ouvre un ticket, envoie un message. Le 20 juillet 2026, la CNIL et le Conseil de l'IA et du numérique (France · CNIL et CIANum) ont publié une note exploratoire sur l'IA agentique. Elle relève que la circulation des données entre agents, mémoires et services rend plus difficile d'identifier qui est responsable de quoi.

Les identités machines se multiplient. Comptes de service, clés d'API, jetons d'accès : chaque automatisme a une identité. Selon le rapport « NHI & Secrets Risk Report » du premier semestre 2025 (Israël · Entro Security), on compte 144 identités non humaines pour une identité humaine dans les environnements d'entreprise analysés par l'éditeur, contre 92 pour 1 au premier semestre 2024. L'étude porte sur

plus de 27 millions d'identités observées par un éditeur de sécurité : c'est un ordre de grandeur, pas une statistique représentative. Chaque agent d'IA ajoute ses propres comptes et jetons à cette population.

Le droit demande des preuves. Depuis le 2 février 2025, l'AI Act (UE · règlement (UE) 2024/1689) impose des mesures de maîtrise de l'IA. Le RGPD exige de pouvoir démontrer la conformité (article 5, paragraphe 2). NIS2 et DORA rendent les dirigeants comptables de la gestion du risque numérique, y compris chez les fournisseurs. Une charte ne suffit plus : il faut des journaux, des registres et des contrats.

La gouvernance de l'IA ne se juge plus à la qualité d'une charte, mais à la capacité de produire une preuve en quelques heures.

2. Les cinq questions qu'une direction doit pouvoir trancher

Le playbook de Dust regroupe les inquiétudes des RSSI en trois familles : l'attribution, la fuite de données, le contrôle. Nous les reprenons et y ajoutons deux questions que les directions sous-estiment : la manière de déployer et la chaîne d'approvisionnement.

Question 1 : l'attribution

Qui a fait quoi, et qui en répond ? Quand un agent agit avec les identifiants d'un salarié, les journaux enregistrent le salarié. Le playbook de Dust souligne qu'alors, la part de l'agent disparaît des traces : on ne distingue plus une erreur humaine d'une action automatique, ni la consigne qui l'a déclenchée. La note de la CNIL et du CIANum fait le même constat sur le plan juridique : établir une responsabilité suppose de pouvoir retracer chaque étape du processus.

Ce qu'il faut exiger : une véritable piste d'audit, qui relie chaque action à une personne, à un agent, à la configuration de cet agent et aux données lues. Le

playbook oppose cette piste d'audit à la simple observabilité, qui compte les requêtes et mesure les délais sans dire qui a décidé quoi.

Question 2 : la fuite de données et l'exposition juridique

Deuxième inquiétude relevée par Dust : la donnée qui sort. Vers un modèle externe, vers un outil non autorisé, vers un tiers. L'exposition est juridique autant que technique : le playbook cite le RGPD en Europe et le CCPA en Californie (États-Unis · Californie). S'y ajoutent, pour une entreprise française, le secret des affaires, le secret professionnel et les règles propres aux données de santé.

Quatre réponses doivent être écrites : quelles données peuvent entrer dans un outil d'IA, lesquelles jamais ; si le fournisseur réutilise les données pour entraîner ses modèles ; où elles sont traitées et stockées ; combien de temps elles sont conservées. La CNIL (France · CNIL) recommande depuis 2024 de vérifier dans quelle mesure le fournisseur peut réutiliser les données qui lui sont confiées, et d'adapter les usages en conséquence.

Question 3 : le contrôle des accès et les identités non humaines

Le playbook de Dust résume le contrôle en quelques gestes : ajouter, retirer, accorder, révoquer. Puis vérifier que la carte des accès que la direction a en tête correspond à la réalité. Son exemple : s'assurer qu'aucun chemin ne mène des équipes financières vers des données de santé.

Chaque agent, chaque connecteur et chaque clé d'API est une identité. Chacune doit avoir un propriétaire nommé, un périmètre minimal, une date d'expiration et une procédure de révocation. Avec plus de cent identités machines par identité humaine, la revue manuelle ne tient plus : l'inventaire doit être outillé.

Question 4 : le déploiement maîtrisé

Le playbook recommande trois principes. Les connecteurs, notamment les serveurs MCP (Model Context Protocol), les outils, les secrets et les points de terminaison

restent réservés aux administrateurs. L'accès aux agents se donne par appartenance à des groupes de l'annuaire, avec authentification unique (SSO) et provisionnement automatique (SCIM), et non adresse e-mail par adresse e-mail. Enfin, les frontières de connaissance sont appliquées par des espaces restreints.

Le bénéfice est concret : quand un salarié quitte l'entreprise ou change de poste, sa sortie de l'annuaire retire ses accès à tous les agents, sans intervention manuelle.

Question 5 : le trafic sortant et la chaîne d'approvisionnement

Le playbook recommande de limiter le trafic sortant aux seules adresses autorisées, et rappelle que les serveurs MCP distants et les composants tiers sont une cible d'attaques fréquente. Un cas l'illustre. En septembre 2025, un paquet imitant le serveur MCP d'un service d'envoi d'e-mails a ajouté, dans sa version 1.0.16, une copie cachée de chaque message vers une adresse externe (Royaume-Uni · The Register).

Un serveur MCP, un skill téléchargé, un modèle, une bibliothèque ou un sous-traitant du fournisseur sont autant de maillons. Chacun doit être recensé, validé et surveillé comme un fournisseur.

3. Le risque propre aux agents : la triade et comment la casser

Le 16 juin 2025, le développeur Simon Willison (international · Simon Willison) a nommé le risque central des agents : la « lethal trifecta », que nous traduisons par « triade létale ». Un agent devient dangereux quand il réunit trois capacités :

INGRÉDIENT	EXEMPLES	CE QU'IL PERMET À UN ATTAQUANT
Accès à des données confidentielles	Messagerie, gestion documentaire, fichier clients, base RH	Atteindre l'information à voler
Exposition à du contenu non fiable	Page web, e-mail entrant, pièce jointe, ticket client	Glisser des instructions cachées
Capacité d'agir ou de communiquer vers l'extérieur	Envoi d'e-mail, appel d'une URL, publication	Faire sortir l'information

Le mécanisme est simple. Un modèle de langage suit les instructions qu'il lit, y compris celles cachées dans un document qu'on lui demande de résumer : c'est l'injection de consignes. Un attaquant qui place un texte piégé dans une page web ou un e-mail peut faire envoyer des données internes vers une adresse qu'il contrôle. Willison souligne que les protections des fournisseurs ne couvrent pas les combinaisons d'outils assemblées par les utilisateurs, que le protocole MCP encourage justement à mélanger. Il juge aussi les filtres insuffisants : en sécurité, bloquer 95 % des attaques reste un échec. Sa conclusion : éviter la combinaison. **Un agent qui réunit les trois ingrédients doit être traité comme une fuite en attente, quel que soit le fournisseur.**

Le playbook de Dust propose une parade d'architecture : séparer les rôles. Un agent de recherche lit le web, mais n'a aucun accès aux données internes. Un agent rédacteur travaille sur des données internes, mais ne reçoit que des entrées structurées, et non du texte libre venu de l'extérieur. Un orchestrateur, sous garde, détient seul les droits d'action. Entre les agents, les échanges passent par des sorties structurées (champs définis, listes fermées), qui laissent peu de place à une instruction cachée.

Les autorités vont dans le même sens. La note de la CNIL et du CIANum propose de cloisonner la mémoire des agents, de les déployer dans des environnements isolés, de prévoir un bouton d'arrêt d'urgence et d'imposer une validation humaine pour les

décisions les plus critiques. L'ANSSI (France · ANSSI), dans ses recommandations sur l'IA générative publiées le 29 avril 2024, conseille d'éviter autant que possible les actions automatisées entre une IA et un système applicatif quand des données externes circulent (web, e-mail), et de ne pas laisser la machine prendre seule des décisions critiques.

Règle pratique : pour chaque agent, cochez les trois cases. Si les trois sont cochées, l'agent ne passe pas en production sans être redécoupé ou soumis à une validation humaine systématique.

4. Ce que dit le droit au 29 octobre 2026

UE · AI Act

- **Maîtrise de l'IA** (article 4) : depuis le 2 février 2025, fournisseurs et déployeurs prennent des mesures pour que leur personnel et les personnes qui utilisent l'IA pour leur compte aient un niveau suffisant de maîtrise. Le règlement (UE) 2026/1744, dit « omnibus IA », entré en vigueur le 27 juillet 2026, a reformulé l'article : il s'agit désormais de mesures pour soutenir le développement de cette maîtrise, sans garantir un niveau individuel. L'obligation demeure ; la Commission et les États membres doivent appuyer les efforts des entreprises.
- **Pratiques interdites** (article 5) : depuis le 2 février 2025. Pour un employeur, la plus concrète vise la reconnaissance des émotions sur le lieu de travail, interdite sauf raisons médicales ou de sécurité.
- **Transparence** (article 50) : depuis le 2 août 2026, le déployeur signale les hypertrucages, ainsi que les textes générés publiés pour informer le public sur des questions d'intérêt général, sauf relecture humaine sous responsabilité éditoriale. Les fournisseurs d'outils génératifs déjà sur le marché ont jusqu'au 2 décembre 2026 pour marquer les contenus produits.

- **Haut risque** : après le règlement (UE) 2026/1744, les obligations s'appliquent le 2 décembre 2027 pour les systèmes de l'annexe III (recrutement, gestion des salariés, crédit, éducation, accès aux services essentiels...) et le 2 août 2028 pour ceux de l'annexe I, intégrés à des produits réglementés.
- **Obligations du déployeur d'un système à haut risque** (article 26) : l'utiliser conformément à sa notice, confier le contrôle humain à des personnes compétentes et dotées de l'autorité nécessaire, surveiller son fonctionnement, conserver les journaux au moins six mois, informer les représentants du personnel et les salariés concernés avant une mise en service au travail. Les organismes publics et certains déployeurs privés, notamment en crédit et en assurance vie ou santé, réalisent en outre une analyse d'impact sur les droits fondamentaux (article 27).

UE · RGPD

- **Base légale** (article 6) et finalité définie pour chaque usage qui touche des données personnelles.
- **Analyse d'impact** (article 35) quand le traitement est susceptible d'engendrer un risque élevé : c'est fréquent dès qu'une IA porte sur des salariés, des clients ou des données sensibles. L'AI Act prévoit que le déployeur s'appuie sur les informations du fournisseur pour la réaliser (article 26, paragraphe 9).
- **Décisions automatisées** (article 22) : une personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé qui l'affecte de manière significative. La note de la CNIL et du CIANum rappelle qu'une validation humaine purement formelle ne suffit pas.
- **Sous-traitants** (article 28) : contrat écrit, sous-traitants ultérieurs soumis à autorisation préalable, droit d'audit, assistance en cas de violation.
- **Transferts** (chapitre V) : hors de l'Espace économique européen, une décision d'adéquation ou des garanties appropriées, comme les clauses contractuelles types.

UE · NIS2 et DORA

- **NIS2** (directive (UE) 2022/2555) : pour les entités essentielles et importantes, les organes de direction approuvent les mesures de gestion des risques et peuvent voir leur responsabilité engagée (article 20). Les mesures incluent la sécurité de la chaîne d'approvisionnement, le contrôle des accès et l'authentification multifacteur (article 21). En France, la loi de transposition n'était pas définitivement adoptée au 29 octobre 2026.
- **DORA** (règlement (UE) 2022/2554) : applicable depuis le 17 janvier 2025 aux entités financières. Une plateforme d'IA est un prestataire de services TIC tiers : elle entre dans le registre d'informations sur les contrats, et son contrat doit contenir les clauses de l'article 30 (localisation des données, accès et restitution des données, résiliation), complétées par l'audit et la stratégie de sortie si elle soutient une fonction critique ou importante.

France · CNIL

- **IA générative** : depuis juillet 2024, les questions-réponses de la CNIL demandent aux organismes qui déploient un outil d'IA générative de partir d'un besoin précis, d'encadrer les usages par une charte, de privilégier un déploiement local pour les données sensibles, de former les utilisateurs et d'associer le DPO, en lien avec le RSSI.
- **IA agentique** : la note du 20 juillet 2026, rédigée avec le CIANum, juge que les agents restent pleinement soumis au RGPD et propose des garde-fous techniques (cloisonnement, environnements isolés, arrêt d'urgence, validation humaine).

Normes volontaires

- **ISO/IEC 42001:2023** (international · ISO et IEC) : la norme de système de management de l'IA, certifiable, bâtie sur la même structure que l'ISO/IEC 27001. Un certificat ISO/IEC 42001 ne vaut pas, à lui seul, présomption de conformité à l'AI Act ; ce rôle revient aux normes harmonisées européennes, dont la première a été référencée au Journal officiel en octobre 2026.

- **AI RMF** (États-Unis · NIST) : cadre publié le 26 janvier 2023, organisé en quatre fonctions (gouverner, cartographier, mesurer, gérer), complété le 26 juillet 2024 par un profil consacré à l'IA générative. Le NIST indique qu'il est en cours de révision. Il n'a pas de valeur juridique en Europe, mais fournit un vocabulaire commun avec les fournisseurs américains.

France · hébergement des données sensibles

Un arrêté du 12 août 2026, publié au Journal officiel du 14 août, approuve le référentiel SecNumCloud 3.2 de l'ANSSI pour les données d'une sensibilité particulière de l'État, de ses opérateurs et de certains groupements d'intérêt public. La conformité se prouve par une qualification de l'ANSSI ou par une certification européenne reconnue équivalente. Les entreprises privées n'y sont pas tenues, mais le référentiel sert de repère pour les données exposées aux lois extra-européennes. L'ANSSI recommande, dans son guide de 2024, de privilégier un hébergement qualifié quand un système d'IA générative est déployé dans le cloud.

Le report du haut risque à décembre 2027 ne reporte ni la maîtrise de l'IA, ni la transparence, ni le RGPD.

5. Les données, socle de la gouvernance

Une plateforme d'IA ne vaut que ce que valent les données qu'elle atteint et les droits qui les protègent. Six chantiers conditionnent tout le reste.

Classification. Quatre niveaux suffisent souvent : public, interne, confidentiel, réglementé (données de santé, données bancaires, secrets protégés). À chaque niveau correspond une règle d'usage pour chaque catégorie d'outil.

Registre. Le registre des traitements RGPD (article 30) peut accueillir les systèmes d'IA : finalité, données, agents, connecteurs, fournisseurs, durée de conservation. Un registre unique, revu à chaque changement, évite deux inventaires qui divergent.

Droits d'accès hérités. Un assistant qui interroge des documents internes, selon la technique dite RAG (génération augmentée par la recherche), doit appliquer à

chaque question les droits des documents sources. Sinon, n'importe quel utilisateur obtient en une phrase le résumé d'une note réservée à la direction. Cet héritage se teste avec plusieurs profils d'utilisateurs avant l'ouverture.

Conservation. Consignes, réponses, journaux et mémoire des agents sont des données. Chacune doit avoir une durée de conservation. La note de la CNIL et du CIANum signale que la mémoire persistante des agents tend à accumuler des données et à constituer des profils très précis des utilisateurs.

Hébergement et souveraineté. Lieu de traitement, lieu de stockage, sous-traitants ultérieurs, droit applicable au fournisseur et à sa maison mère : ces quatre informations figurent dans le dossier d'achat. Pour les données de santé, la certification HDS s'ajoute.

Réversibilité. Depuis le 12 septembre 2025, le Data Act (UE · règlement (UE) 2023/2854) encadre le changement de fournisseur de services de traitement de données ; à partir du 12 janvier 2027, les frais de changement et de sortie des données seront interdits. Pour une plateforme d'IA, la réversibilité couvre aussi les consignes des agents, les bases de connaissance, les historiques et les journaux.

6. Grille d'évaluation d'une plateforme d'IA

Cette grille est neutre vis-à-vis des éditeurs. Elle s'applique à un assistant du marché, à une plateforme d'agents ou à un développement interne.

CRITÈRE	PREUVE À DEMANDER	OÙ LA TROUVER
Pistes d'audit	Un extrait de journal pour une action d'agent : demandeur, agent, version, droits utilisés, données lues, action, horodatage ; durée de conservation ; export vers votre outil de supervision	Démonstration sur un environnement de test ; documentation d'administration ; annexe sécurité du contrat
Connecteurs sous contrôle	Liste des connecteurs, serveurs MCP et outils activables ; qui peut les ajouter ; circuit de validation ; portée des jetons	Console d'administration ; politique de sécurité de l'éditeur
SSO et SCIM	Authentification unique sur votre annuaire ; attribution des accès par groupes ; déprovisionnement automatique	Documentation d'intégration ; test de départ d'un salarié fictif
Cloisonnement	Espaces restreints ; héritage des droits des sources ; séparation entre agents	Démonstration avec plusieurs profils ; rapport de test d'intrusion
Trafic sortant	Liste des destinations sortantes ; liste d'autorisation configurable ; blocage des liens et images externes dans les réponses	Schéma d'architecture ; paramètres d'administration
Choix du modèle et absence de dépendance	Modèles disponibles ; possibilité d'en changer, d'en héberger un en Europe ou sur site ; engagement de non-entraînement sur vos données	Contrat ; conditions des fournisseurs de modèles
Hébergement et sous-traitants	Lieux de traitement et de stockage ; liste des sous-traitants ultérieurs ; exposition aux lois extra-européennes ; qualifications (SecNumCloud, HDS)	Liste publiée des sous-traitants ; attestations ; centre de confiance de l'éditeur

CRITÈRE	PREUVE À DEMANDER	OÙ LA TROUVER
Contrat de sous-traitance RGPD	Clauses de l'article 28 ; notification des violations ; droit d'audit ; encadrement des transferts	Accord de traitement des données annexé au contrat
Réversibilité	Export des agents, consignes, bases de connaissance, historiques et journaux dans un format ouvert ; délai ; coût	Plan de réversibilité contractuel ; test de sortie partiel
Coûts	Mode de tarification (par siège, à l'usage) ; plafonds et alertes ; coût total sur trois ans, intégration comprise	Grille tarifaire ; simulation sur vos volumes réels

Une preuve qui n'existe que dans une présentation commerciale n'est pas une preuve. Demandez la démonstration, l'extrait, la clause.

7. Feuille de route en 90 jours

Jours 1 à 30 : inventaire, règles, rôles

- **Inventaire** : outils d'IA utilisés, officiels ou non ; agents ; connecteurs ; identités non humaines ; fonctions d'IA ajoutées à vos logiciels existants.
- **Politique d'usage** : deux pages au plus. Données autorisées par niveau de classification, outils autorisés, usages interdits, cas où une validation humaine est obligatoire.
- **Rôles** : un sponsor au comité de direction, qui arbitre ; le RSSI, pour les identités, les journaux et les tests ; le DPO, pour la base légale, l'analyse d'impact et le registre ; un propriétaire métier par cas d'usage ; les achats, pour la grille, les clauses et la réversibilité.
- **Maîtrise de l'IA** : un premier module de formation, adapté aux rôles, dont la participation est tracée.

Jours 31 à 60 : un pilote gouverné

- Deux ou trois cas d'usage, sur une seule plateforme évaluée avec la grille.
- Accès par groupes (SSO, SCIM), connecteurs validés, espaces restreints.
- Contrôle de la triade pour chaque agent ; redécoupage si nécessaire.
- Analyse d'impact quand le cas d'usage l'exige ; journaux activés et exportés.
- Indicateurs suivis chaque semaine : usage, qualité des réponses, incidents, coûts.

Jours 61 à 90 : contrôle, preuves, passage à l'échelle

- **Exercice de preuve** : tirer au hasard trois actions d'agents et reconstituer, en vingt-quatre heures, qui a demandé quoi, avec quels droits, sur quelles données.
- **Tests** : départ d'un salarié fictif, contenu piégé soumis à un agent, export partiel des données.
- **Dossier de preuves** : registre, analyses d'impact, contrats, extraits de journaux, attestations de formation.
- **Décision** : extension, correction ou arrêt, présentée au comité de direction avec ses indicateurs.

Le passage à l'échelle se décide sur un dossier de preuves, pas sur un taux d'adoption.

8. Dix questions à poser lundi matin

1. Pouvons-nous lister tous les outils et agents d'IA utilisés chez nous, y compris en dehors des outils officiels ?
2. Pour une action réalisée hier par un agent, pouvons-nous dire qui l'a demandée, avec quels droits et sur quelles données ?
3. Combien d'identités non humaines avons-nous, et chacune a-t-elle un propriétaire et une date d'expiration ?
4. Qui peut ajouter un connecteur, un serveur MCP ou un skill, et qui valide cet ajout ?

5. Un salarié qui part perd-il automatiquement l'accès à tous les agents et à leurs données ?
6. Lesquels de nos agents réunissent les trois ingrédients de la triade ?
7. Vers quelles destinations nos agents peuvent-ils envoyer des données ?
8. Quels fournisseurs et sous-traitants traitent nos consignes et nos documents, et dans quel pays ?
9. Pouvons-nous changer de modèle ou de plateforme en moins de trois mois, avec nos agents et nos historiques ?
10. Quelles mesures de maîtrise de l'IA avons-nous prises au titre de l'article 4 de l'AI Act, et pouvons-nous le prouver ?

Une direction qui répond à ces dix questions avec des documents, et non avec des intentions, gouverne son IA.

Questions fréquentes

Qu'est-ce que la « triade létale » des agents d'IA ? +

L'obligation de maîtrise de l'IA de l'article 4 de l'AI Act a-t-elle été supprimée ? +

Quand s'appliquent les obligations des systèmes d'IA à haut risque ? +

Une certification ISO/IEC 42001 suffit-elle pour être conforme à l'AI Act ? +

SOURCES

1. France · Dust — La gouvernance de l'IA : concilier performance et sécurité dans les grandes entreprises (playbook, édition 2026) (<https://dust.tt>)

2. International · Simon Willison — The lethal trifecta for AI agents: private data, untrusted content, and external communication (16 juin 2025) (<https://simonwillison.net/2025/Jun/16/the-lethal-trifecta/>)
3. Israël · Entro Security — NHI & Secrets Risk Report, premier semestre 2025 (<https://lp.entro.security/nhi-secrets-risk-report-h1-2025>)
4. UE · Journal officiel — Règlement (UE) 2024/1689 sur l'intelligence artificielle, AI Act (13 juin 2024) (<https://eur-lex.europa.eu/eli/reg/2024/1689/oj>)
5. UE · Journal officiel — Règlement (UE) 2026/1744, omnibus numérique sur l'IA (24 juillet 2026) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202601744)
6. UE · Journal officiel — Règlement (UE) 2016/679, RGPD (27 avril 2016) (<https://eur-lex.europa.eu/eli/reg/2016/679/oj>)
7. UE · Journal officiel — Directive (UE) 2022/2555, NIS2 (14 décembre 2022) (<https://eur-lex.europa.eu/eli/dir/2022/2555/oj>)
8. UE · Journal officiel — Règlement (UE) 2022/2554, DORA (14 décembre 2022) (<https://eur-lex.europa.eu/eli/reg/2022/2554/oj>)
9. France · CNIL — IA agentique et données personnelles : note exploratoire avec le Conseil de l'IA et du numérique (20 juillet 2026) (<https://www.cnil.fr/fr/ia-agentique-cnil-cianum-note>)
10. France · CNIL — Les questions-réponses de la CNIL sur l'utilisation d'un système d'IA générative (18 juillet 2024) (<https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur-lutilisation-dun-systeme-dia-generative>)
11. France · ANSSI — Recommandations de sécurité pour un système d'IA générative (29 avril 2024) (https://cyber.gouv.fr/sites/default/files/document/Recommandations_de_s%C3%A9curit%C3%A9_pour_un_syst%C3%A8me_d_IA_g%C3%A9n%C3%A9rative.pdf)
12. France · Légifrance — Arrêté du 12 août 2026 portant approbation du référentiel d'exigences SecNumCloud (JO du 14 août 2026) (<https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000054678082>)
13. International · ISO et IEC — ISO/IEC 42001:2023, système de management de l'intelligence artificielle (<https://www.iso.org/standard/42001>)
14. États-Unis · NIST — AI Risk Management Framework, AI RMF 1.0 (26 janvier 2023) et profil IA générative (26 juillet 2024) (<https://www.nist.gov/itl/ai-risk-management-framework>)
15. Royaume-Uni · The Register — Postmark MCP server code hijacked : copie cachée des e-mails (29 septembre 2025) (https://www.theregister.com/2025/09/29/postmark_mcp_server_code_hijacked/)

Ce livre blanc est une analyse indépendante, pas un avis juridique. Faits vérifiés à la date d'édition ; chaque source est citée.