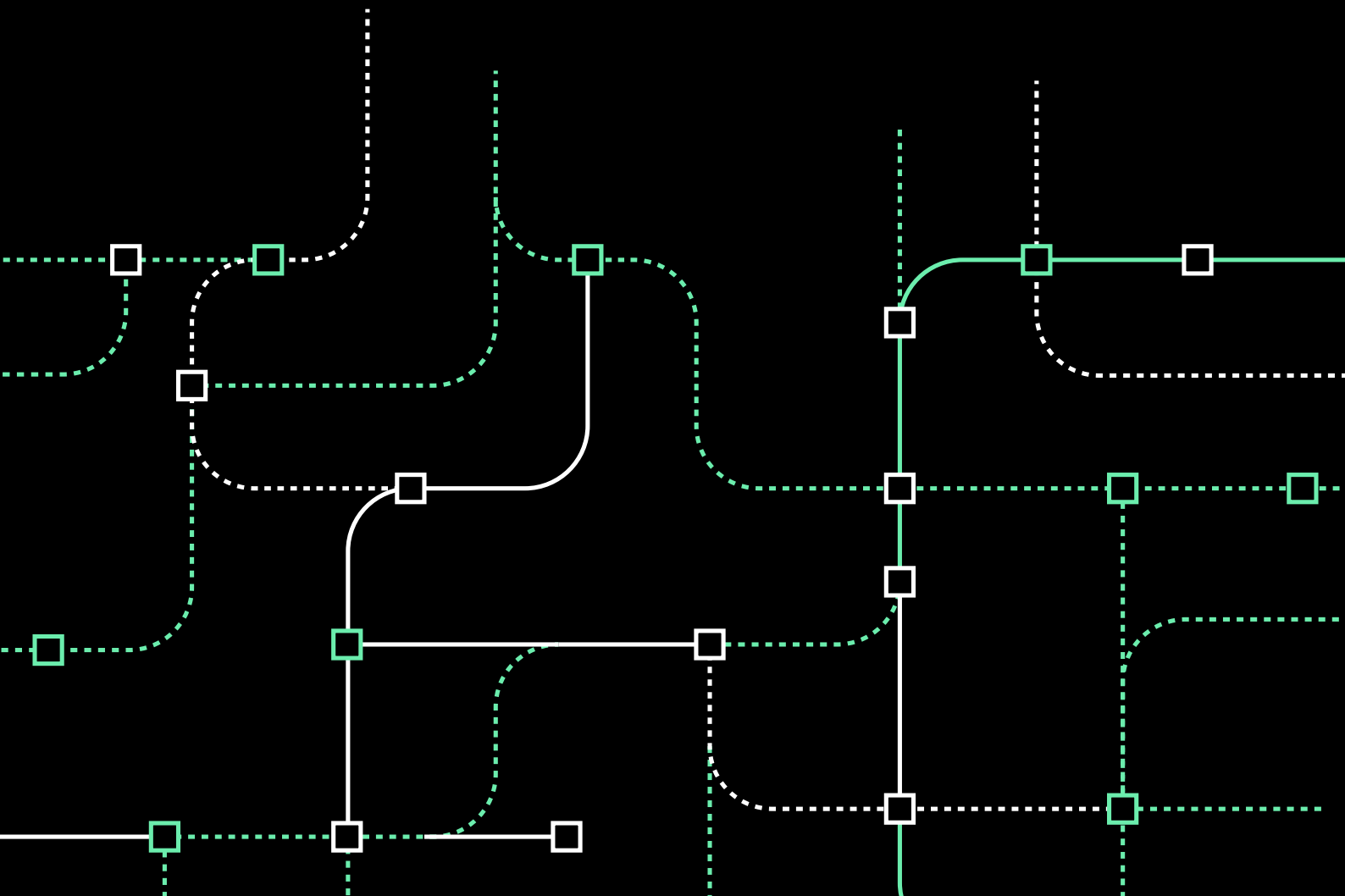
OneTrust

Rapport prévisionnel OneTrust 2027

Concevoir la gouvernance de l'IA :

planifier dans un contexte mouvant

Rapport



Sommaire

Introduction : Quand l'accès est accordé, les prérogatives doivent être encadrées et la confiance établie. 3

Prévision 1 : Sans garantie, il faut avoir un blocage. Les garanties sur l'IA sont incontournables 5

Prévision 2 : Les feux verts peuvent mener à la mauvaise destination : des agents validés peuvent effectuer des tâches non autorisées 9

Prévision 3 : Le parc d'IA dépasse le cadre des validations. Les changements importants sur l'IA doivent être accompagnés de garanties 13

Prévision 4 : Une autorisation n'est pas un laissez-passer inconditionnel. Les conversations avec l'IA font des choix d'utilisation des données une partie intégrante du parcours 17

La réglementation de l'IA en 2027, vue des experts 21

Contre-prévisions : 3 éléments qui n'auront pas lieu en 2027 29

Clause de non-responsabilité
Aucune partie du présent document ne peut être reproduite sous aucune forme que ce soit sans l'autorisation écrite du détenteur des droits d'auteur. Le contenu de ce document peut faire l'objet de révisions sans préavis en raison de progrès continus en matière de méthodologie, de conception et de fabrication. OneTrust LLC décline toute responsabilité pour toute erreur ou tout dommage résultant de l'utilisation de ce document. Les produits, contenus et supports OneTrust sont uniquement fournis à titre informatif et ne sont pas destinés à fournir de conseils juridiques. Veuillez consulter votre avocat pour toute question spécifique. Les informations fournies par OneTrust ne garantissent pas la conformité aux lois et aux réglementations applicables.

Copyright © 2026 OneTrust LLC. Tous droits réservés. Exclusif et confidentiel.

Introduction

Quand l'accès est accordé, les prérogatives doivent être encadrées et la confiance établie.



Blake Brannon
Chief Innovation Officer
OneTrust

Le débat sur le rythme de progression de l'IA frontière soulève immédiatement une question pour les entreprises : jusqu'où sommes-nous prêts à laisser ces systèmes aller ? Cette question devient lourde de conséquences lorsqu'un agent peut modifier un registre d'entreprise, utiliser des informations client ou lancer une opération dans un autre système.

Nous savons déjà comment y répondre pour les humains. Une nouvelle recrue reçoit un badge, on lui indique ce qu'elle peut décider et elle gagne progressivement la confiance de l'entreprise. Les agents ont besoin des mêmes trois éléments, mais avec un fonctionnement différent.

Un agent obtient ses droit d'accès dès qu'il est connecté à un système et il hérite souvent de tous les accès de son concepteur, ce qui dépasse souvent les besoins de la tâche confiée. Cette partie est simple et se produit déjà. Dans l'enquête OneTrust 2026 sur la gouvernance adaptée à l'IA, 87 % des personnes interrogées déclaraient que leur organisation encourageait l'utilisation des agents, avec 47 % qui disposent d'une gouvernance et de mesures de contrôle claires, et 40 % dont les capacités sont encore en cours de développement. Encourager l'utilisation est la bonne approche. Le risque réside dans ce qui est implicite. L'accès est accordé.

Ce qu'un agent peut faire avec cet accès relève d'une décision distincte, que quelqu'un doit prendre. L'accès correspond à ce qu'un système peut atteindre, les prérogatives à ce qu'il peut en faire, dans quel but et dans quelles limites. Un agent ayant accès au système de commandes peut être capable de récupérer les registres associés. Son niveau de prérogatives pourrait lui permettre d'effectuer des remboursements allant jusqu'à 200 $ sur des commandes datant de moins de 30 jours, tout montant dépassant ces limites étant soumis à une validation humaine. Ces limites doivent être consignées et respectées, et non être implicitement liées à la connexion, car le rôle d'un agent peut s'étendre de façon insidieuse : en établissant une autre connexion, en apprenant au cours d'une conversation un élément qu'un formulaire n'aurait jamais demandé, puis en le réutilisant pour une autre finalité, le tout avec la même autorisation initiale. L'agent ne fera aucun signalement. Seuls 5 % des répondants font état d'une coordination et d'une responsabilité claires sur l'ensemble du cycle de vie de l'IA ; sans cela, des étapes autorisées séparément peuvent se combiner pour aboutir à un résultat que personne n'a autorisé. Les prérogatives doivent être encadrées.

Pour qu'un agent soit digne de confiance, il doit prouver au fil du temps qu'il s'est limité à ce qu'il était autorisé à faire, et rien d'autre, et une personne autre que l'agent doit pouvoir le vérifier. Un agent peut fonctionner sous les identifiants d'un humain et utiliser son nom dans tous les systèmes auxquels il accède, mais il ne dispose pas de l'historique qui a rendu ces identifiants dignes de confiance. L'identité se transmet, pas la confiance. Et l'agent ne peut pas être son propre témoin : son compte rendu de ses actions n'est qu'un résultat de plus issu du système. L'historique doit être conservé hors du contrôle de l'agent et conservé en tant qu'élément probant pouvant faire l'objet d'une revue indépendante. Seules 28 % des

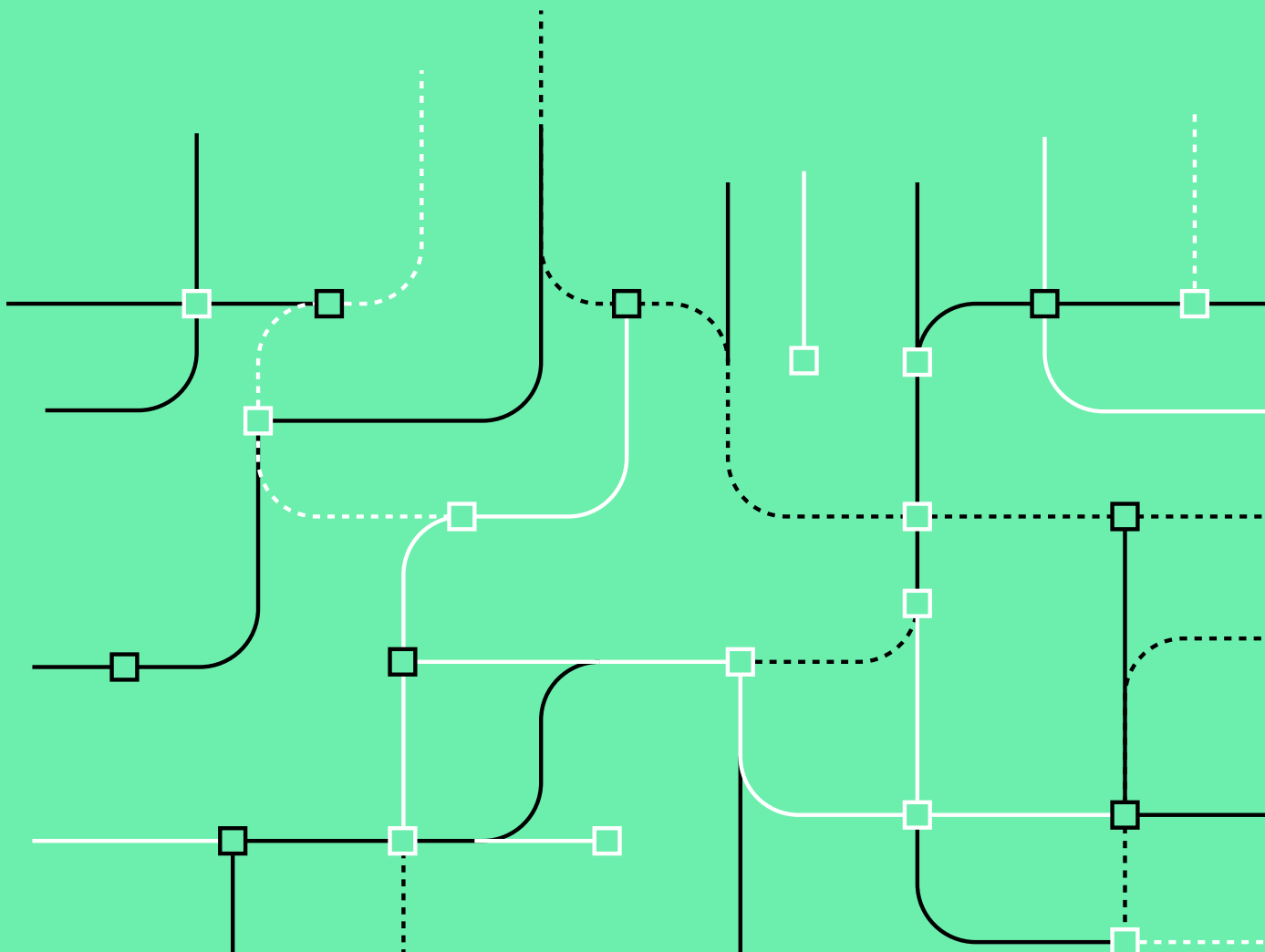
personnes interrogées parlent de preuves de gouvernance et de pistes d'audit : c'est l'activité la moins courante de l'enquête. La première prévision de ce rapport indique qui demandera ces preuves, et à quel moment. La confiance doit être prouvée.

Rien de tout cela ne plaide en faveur d'un ralentissement. Des limites claires éliminent les retards évitables, et la gouvernance existe pour prendre les décisions les plus difficiles au bon rythme et pour désigner qui assume le risque résiduel.

Les quatre prévisions qui suivent examinent comment l'accès, les prérogatives et les éléments probants vont façonner l'adoption et les résultats commerciaux en 2027, des garanties commerciales aux limites du travail délégué, en passant par l'évolution du parc d'IA et les données propres aux clients. Avant d'étendre les prérogatives d'un agent, votre organisation est-elle capable d'expliquer la finalité autorisée, d'empêcher les actions non autorisées et de reconstituer ce qui s'est passé ? C'est l'épreuve à laquelle ce rapport invite les dirigeants à se préparer.

Prévision 1

Sans garantie, il faut avoir un blocage. Les garanties sur l’IA sont incontournables.



Prévision 1

Sans garantie, il faut avoir un blocage. Les garanties sur l'IA sont incontournables.

En 2027, les acheteurs de services intégrant une IA à fort impact exigeront de plus en plus des éléments probants à jour et pertinents pour le déploiement avant d'activer ou d'étendre leur utilisation. Le niveau de garantie requis tiendra compte de l'autonomie des fonctionnalités, de leur impact sur l'activité et des possibles dommages. Cette pression pourrait s'étendre aux décisions sur les contrats, les renouvellements et les budgets.

Imaginons qu'un fournisseur lance une nouvelle fonctionnalité d'IA. Le développement est terminé, la fonctionnalité est disponible et le client peut l'activer. Pourtant, il attend. La question qui reste en suspens est de savoir si les garanties déjà fournies couvrent ce dont le service est désormais capable.

Pour le fournisseur, la maturité technique ne s'est pas encore traduite par l'acceptation du client. La valeur commerciale du lancement dépend en partie de la résolution des questions de risque qui se posent entre la disponibilité et l'activation.

Nous nous attendons à ce que ce lien devienne plus explicite au cours de l'année 2027. Les acheteurs se demanderont si les garanties existantes s'appliquent aux fonctionnalités, aux connexions de données et au déploiement qu'on leur demande d'accepter. Des éléments de preuve manquants ou obsolètes peuvent retarder l'activation, restreindre le champ d'application ou limiter l'expansion.

Les études de OneTrust révèlent un niveau inégal d'éléments probants : 28 % des entreprises déclarent disposer d'éléments probants en matière de gouvernance et de pistes d'audit, ce qui constitue l'activité la moins répandue parmi celles répertoriées. Parallèlement, 38% d'entre elles donnent la priorité à la préparation aux réglementations, aux normes ou aux audits au cours des 12 prochains mois.

Les éléments probants doivent permettre de prendre les décisions. Les tests d'intrusion identifient les vulnérabilités dans leur périmètre. Évaluer les mesures de contrôle

« Les clients ont besoin de garanties correspondant aux fonctionnalités qu'on leur demande d'utiliser. Lorsque les fonctionnalités changent, les tests antérieurs peuvent laisser de nouvelles questions sans réponse. Les éléments probants pertinents les aident à comprendre l'exposition au risque et à déterminer s'ils sont à l'aise avec l'idée de les activer. »

Tim Mullen
Chief Information Officer
OneTrust



permet de vérifier si les limites sont respectées. Les acheteurs et les responsables métier doivent néanmoins savoir ce qui a été examiné, quelles protections sont efficaces et qui peut accepter le risque résiduel.

Une étude récente de Gartner identifie la gouvernance de l'IA comme un critère d'achat émergent, avec des demandes de preuves de traçabilité, de surveillance et de mécanismes de prise de contrôle de la part des clients. L'analyse établit également un lien entre les réponses incomplètes, un processus de due diligence plus long et d'éventuelles contraintes sur les garanties. Cela confirme la prévision, sans toutefois établir dans quelle mesure ces demandes déterminent déjà les résultats commerciaux.

La pression touche également les équipes dirigeantes. Gartner estime que les dirigeants doivent comprendre quelles décisions commerciales sont influencées par l'IA et qui est responsable des conséquences.
Nous nous attendons à ce que cet examen confère davantage de poids aux éléments probants lorsque les organisations décident d'activer une fonctionnalité ou d'étendre ses prérogatives.

La vérification des fournisseurs assistée par l'IA constitue une autre possibilité pour 2027. Les politiques publiées et les documents sur les garanties pourraient influencer la sélection préliminaire. La question de savoir si cela modifiera à grande échelle les décisions de présélection reste ouverte pour 2027.

Quant aux CFO et aux investisseurs, ils chercheront à savoir si une fonctionnalité génère suffisamment de valeur pour justifier ses coûts d'exploitation et son niveau d'exposition au risque. Nous nous attendons à ce que les décisions concernant la poursuite des investissements s'appuient plus explicitement sur ces mesures, parallèlement aux mécanismes de garanties. Une fonctionnalité peut rester dans les limites validées sans pour autant devoir être étendue.

Pour les fournisseurs, résoudre les questions relatives aux garanties devient une étape de la mise en service d'une fonctionnalité d'IA. Les équipes commerciales doivent déterminer quelles preuves font défaut et qui peut prendre les décisions. Pour les acheteurs, la question concrète est de savoir s'il faut activer la fonctionnalité, imposer des conditions ou attendre.

Ce qui pourrait changer la prévision

Il est possible que les acheteurs continuent à accepter les questionnaires habituels et les contrôles périodiques. Les exclusions d'assurance pourraient modifier l'exposition au risque sans entraîner d'investissement dans la gouvernance, tandis que les contentieux évoluent de manière inégale. La prévision perd de sa pertinence si de nouveaux éléments de preuve ne modifient que rarement l'activation, les conditions ou l'extension des fonctionnalités.

Vraisemblance :
Modérée.



Impact sur le secteur :

Élevé lorsque les garanties influencent l'acceptation ou l'extension. La conséquence peut affecter l'adoption du produit, les conditions commerciales et la confiance nécessaire pour engager des ressources.

Priorités pour les leaders de la gouvernance

- Sécurité et produit : correspondance entre les garanties et la fonctionnalité et la version proposées.
- Équipes commerciales : suivi des demandes qui retardent l'acceptation ou modifient le périmètre du déploiement.
- Risques et juridique : identification des questions pertinentes relatives aux contrats, à la couverture et aux informations à divulguer.

[1] Lorsque la gouvernance de l'IA n'est pas à la hauteur, le chiffre d'affaires et les dirigeants en pâtissent, Gartner, 2026

- Finance et responsables métier : définition de la valeur attendue, des coûts d'exploitation et des éléments probants de garantie requis avant tout investissement ou toute extension supplémentaire.

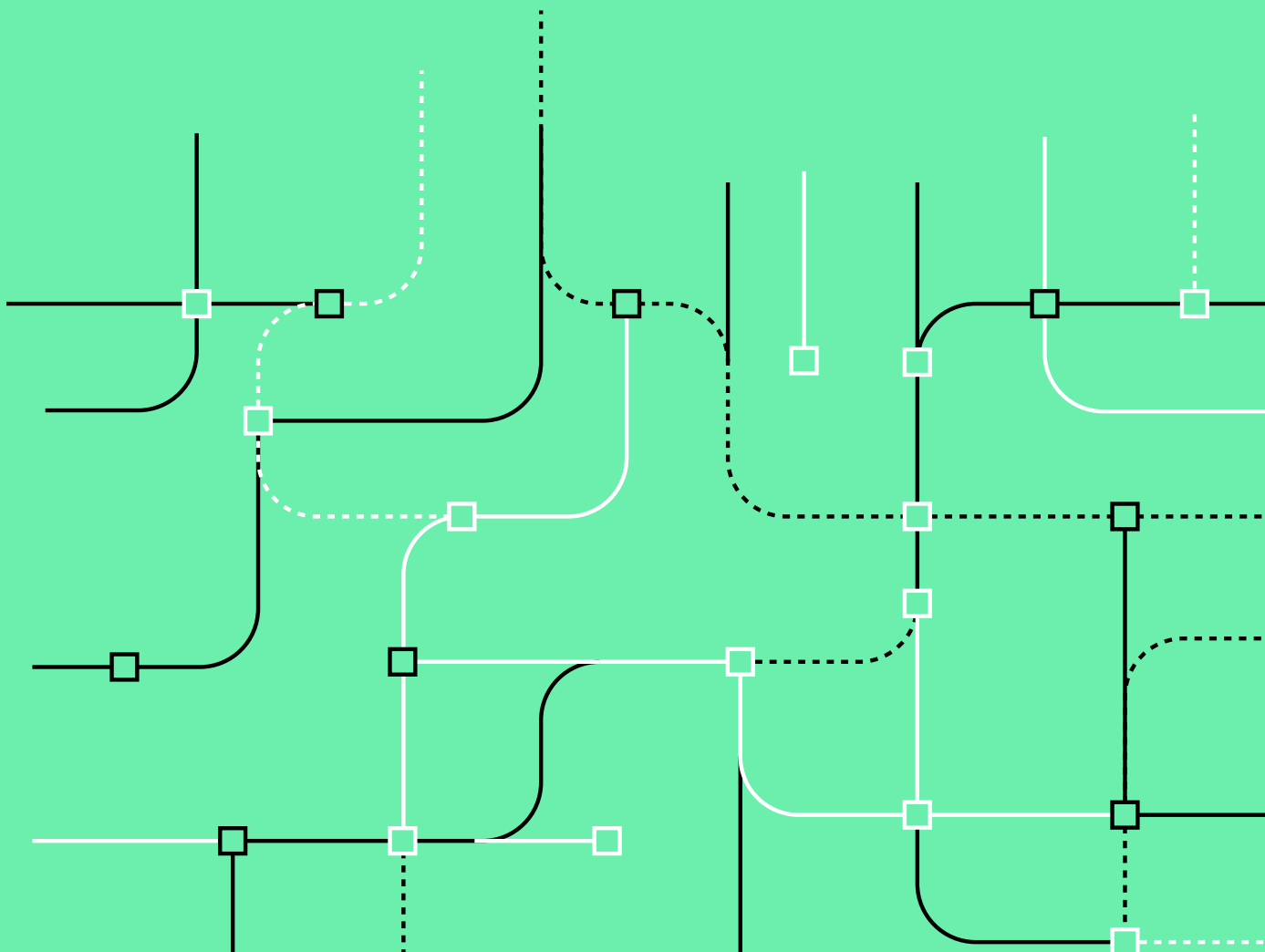
À surveiller en 2027

- Des acheteurs qui retardent l'activation ou l'extension jusqu'à ce que de nouveaux éléments probants soient fournis.
- Des dispositions contractuelles qui exigent des garanties pour tout changement important sur l'IA.
- Des questions de garanties spécifiques à l'IA liées aux conditions de couverture ou aux exclusions.
- Des décisions de financement et d'extension qui prennent explicitement en compte la valeur fournie et les coûts d'exploitation, parallèlement aux éléments probants de contrôle.



Prévision 2

Les feux verts peuvent mener à
la mauvaise destination.
Les agents validés peuvent
effectuer des tâches non autorisées



Prévision 2

Les feux verts peuvent mener à la mauvaise destination : des agents validés peuvent effectuer des tâches non autorisées

En 2027, les principaux programmes consacrés aux agents à fort enjeu ajouteront aux critères de déploiement les prérogatives liées à chaque tâche, les interventions testées et les registres protégés. Les premiers programmes évalueront également les résultats combinés d'actions autorisées séparément.

> « Les utilisateurs veulent que l'agent en fasse plus : accéder à Internet, lire et écrire dans Salesforce, déclencher des workflows et envoyer des messages à leurs collègues. Mais l'agent peut avoir les accès de son créateur, sans sa capacité de discernement. Une fois que ses prérogatives s'étendent, est-ce le même agent que celui que vous avez validé ? »

DV Lamba
Chief Technology and Product Officer
OneTrust

Imaginons un agent chargé de réduire les dépenses liées au cloud tout en respectant les délais de traitement des commandes. Il réduit la capacité inutilisée et repousse certaines activités par lots. Il est autorisé à faire ces deux opérations.

La facture s'allège, mais le traitement des commandes de la nuit ne respecte pas le délai. Chaque action a réussi, mais leur effet combiné a enfreint une règle initiale.

Le problème du déploiement consiste à définir ce qu'un agent est autorisé à accomplir, notamment les conséquences métier inacceptables. L'autorisation technique de réduire la capacité ou de repousser une tâche n'autorise pas tous les compromis. Les limites de la tâche doivent pouvoir être appliquées là où le travail est effectué, avec un moyen d'intervenir lorsqu'elles sont atteintes.

Le rôle d'un agent peut également s'élargir après la validation. Un workflow utile acquiert une autre connexion ou responsabilité, modifiant ce sur quoi l'agent peut agir. L'organisation doit déterminer à quel moment ces ajouts dépassent les prérogatives initialement accordées.

> « Une revue de gouvernance doit définir des conditions qui peuvent être appliquées dans le workflow. Un agent autorisé à résumer les tickets du service client peut avoir besoin d'une autorisation distincte pour mettre à jour le registre client ou effectuer des remboursements. L'organisation devrait pouvoir tester ces limites après le déploiement et les revoir lorsque la tâche ou la politique change. »

Sriram Iyer
SVP and GM AI Strategy & Products
OneTrust

«

L'humain dans la boucle ne peut pas être un simple spectateur. La question est de savoir s'il dispose des connaissances et du discernement critique nécessaires pour remettre en question l'IA, plutôt que de se laisser convaincre par un résultat soigné et bien structuré. Le contrôle doit permettre d'établir si la finalité est valable, si l'orientation est correcte et si les erreurs sont réduites au minimum. »

Odia Kagan
Partner & Co-Chair, Privacy & Data Security
Fox Rothschild LLP

Un registre indiquant que chaque action a réussi sa vérification technique ne peut pas établir que le résultat global reste dans les limites prévues. La validation doit définir la tâche autorisée avec suffisamment de clarté pour que les équipes puissent en tester les limites et évaluer ce qui s'est passé tout au long du workflow.

48 % des personnes interrogées dans le rapport d'étude OneTrust signalent au moins un incident impliquant des actions non validées effectuées par des systèmes ou des agents d'IA au cours de l'année passée. Seuls 28 % déclarent avoir des preuves de gouvernance et des pistes d'audit. Les prérogatives et la reconstruction sont des préoccupations opérationnelles actuelles.

Les examinateurs ont également besoin de registres indépendants du contrôle de l'agent exécutant, qui relient les actions à fort enjeu aux prérogatives accordées. Ces registres doivent permettre de mener des investigations sur différents systèmes, notamment sur les exceptions pertinentes et sur les retouches faites par des humains. Ils peuvent établir ce qui s'est passé, tandis qu'évaluer le résultat global nécessite toujours de porter un jugement au regard de la finalité et des limites de la tâche.

La vérification doit se poursuivre après le déploiement. Les équipes doivent examiner les processus métier dans lesquels l'IA intervient, identifier les comportements inacceptables qui apparaissent concrètement et utiliser ces constatations pour revoir la tâche ou les mesures de contrôle. Un test de validation ne peut pas prévoir toutes les combinaisons d'actions à fort enjeu.

En 2027, on aboutit donc à une limitation plus claire de l'autonomie déployable. Si une entreprise ne peut pas faire respecter les limites des tâches ou reconstituer le résultat, elle devra peut-être restreindre l'accès aux données, supprimer des outils ou maintenir un contrôle humain. Des prérogatives élargies doivent découler de mesures de contrôle démontrées et d'une décision responsable concernant le risque résiduel.

Ce qui pourrait changer la prévision

La vérification humaine peut être suffisante pour des tâches circonscrites. L'évaluation de la tâche dans son ensemble peut augmenter les coûts et la latence sans détecter de manière fiable les conséquences néfastes. L'adoption peut donc progresser plus rapidement pour ce qui est des prérogatives et de l'intervention explicites que pour l'évaluation fiable des résultats.

Vraisemblance :
Modérée



pour des critères de déploiement stricts. Émergente pour une évaluation fiable de tâches complètes.

Impact sur le secteur :

Élevé lorsque les prérogatives de l'agent ont une incidence sur la livraison des services, les transactions ou les décisions sensibles.

Priorités pour les leaders de la gouvernance

- Responsables métier : définition des résultats inacceptables, examen des comportements dans les processus live et attribution de la responsabilité des mesures correctives.
- Sécurité et ingénierie : tests des processus de refus, d'expiration, de remontée et de révocation.

- Protection de la vie privée et gouvernance de l'IA : traduction de la finalité et de l'appétence au risque en conditions exécutoires.
- Audit : établissement de la façon dont une tâche peut être reconstituée à partir de différents systèmes.

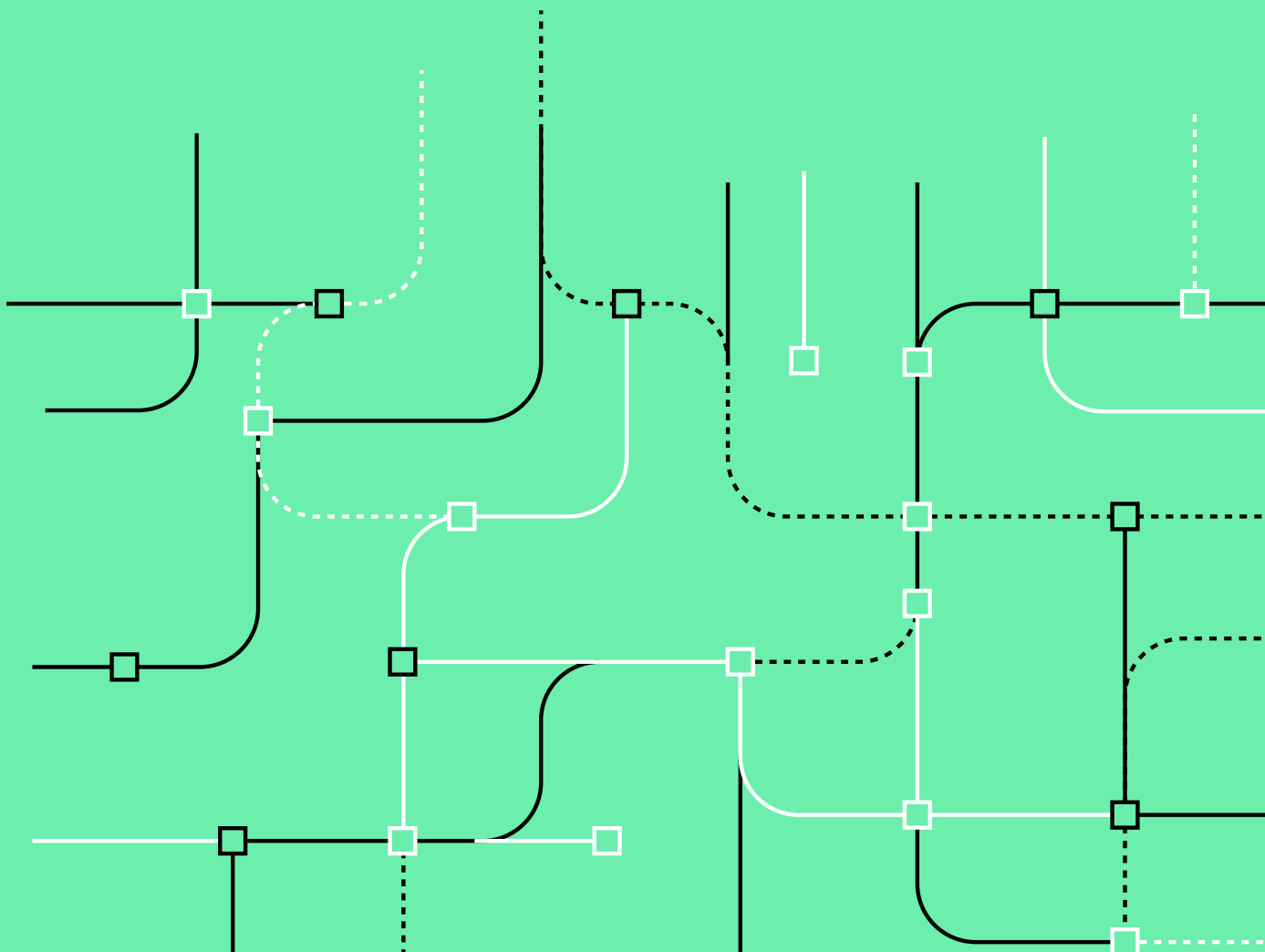
À surveiller en 2027

- Des revues de déploiement nécessitant la définition des limites des tâches et des tests d'intervention.
- Des registres protégés contre l'agent agissant.
- Des évaluations pour détecter les combinaisons d'actions autorisées préjudiciables.
- Parrainage et retrait de l'agent liés à des contrôles d'accès utilisables.
- Des preuves que les changements importants apportés aux politiques parviennent aux agents concernés et sont testés dans leurs workflows.
- Des constats post-déploiement entraînant une révision des limites des tâches, des contrôles ou des procédures opérationnelles.



Prévision 3

La validation n’est pas absolue. Les changements importants sur l’IA doivent être accompagnés de garanties



Prévision 3

La validation n'est pas absolue. Les changements importants sur l'IA doivent être accompagnés de garanties

En 2027, les entreprises les plus avancées commenceront à considérer les changements importants apportés à l'IA achetée, développée et intégrée comme de nouveaux événements de garanties, même lorsqu'aucun nouveau fournisseur n'est intégré. Les revues prendront en compte la fonctionnalité concernée, les outils connectés, l'accès aux données, la finalité et l'efficacité des mesures de contrôle.

Une équipe du service client utilise une application d'IA hébergée. Une équipe d'ingénierie exploite un modèle open-weight. Une plateforme d'entreprise validée ajoute un assistant qui se connecte aux registres internes.

Ce parc hétérogène comprend l'IA que l'organisation achète, développe et dont elle hérite dans les applications existantes. Les services hébergés, les modèles open-weight gérés et les modèles exploités en interne répartissent les responsabilités différemment. Les open-weight à eux seuls n'indiquent pas à l'organisation qui exploite ou prend en charge un déploiement.

« On ne peut pas gouverner ce que l'on ne peut pas voir. Tous les jours, des humains créent des agents qui ne se contentent pas de répondre à des messages. Ils effectuent des actions et accèdent à des données personnelles et sensibles. Nous devons avoir de la visibilité sur les agents qui sont créés et un moyen de déterminer quand ils doivent être évalués. »

Manuel Manuel
AI and Data Protection Specialist
Scania Sweden

« L'IA ne crée pas une catégorie entièrement nouvelle de gouvernance. Elle s'ajoute aux structures de gouvernance dont les organisations ont déjà besoin. À mesure que l'IA est adoptée parallèlement aux exigences de protection de la vie privée et de réglementation croissantes dans le monde, la gouvernance dans son ensemble se rapprochera du cœur du fonctionnement des entreprises. »

Damian Apone
Director, Global Retail Cybersecurity
Genuine Parts Company

Un parc d'IA plus diversifié ne signifie pas qu'il faut créer un programme de gouvernance distinct pour chaque modèle, outil ou déploiement, mais qu'il faut étendre les responsabilités déjà établies en matière de sécurité, de protection de la vie privée, de risque, d'achats et de responsabilité métier à de nouvelles combinaisons de technologies.

La question importante est de savoir quelles responsabilités incombent à chacun.

«

Le plus difficile est de maintenir une visibilité opérationnelle quand l'IA est utilisée dans les processus métier existants. Quand plusieurs acteurs sont impliqués, il peut être difficile d'établir les responsabilités. À mesure que les modèles, les fournisseurs et les cas d'usage évoluent, la conformité devient un travail continu : suivre les changements, surveiller les décisions et réévaluer le risque entre équipes. »

Olivia Roth
DPO / Gouvernance de l'IA
Yves Rocher Allemagne

Un fournisseur peut exploiter un service pendant que le client en contrôle la configuration. Une équipe interne peut exploiter un modèle tandis qu'un responsable métier détermine les conditions acceptables de son utilisation. Un connecteur, un outil ou l'intégration du Model Context Protocol peut donner un accès à des éléments qui n'avait pas été pensé initialement.

39 % des personnes interrogées estiment qu'avoir

«

Une évaluation formalise une décision concernant une fonctionnalité, une configuration et un profil de risque donnés. Un nouveau modèle, un nouveau connecteur ou une nouvelle source de données peut modifier les hypothèses sur lesquelles cette décision s'appuie. Une notification peut aider à identifier le changement. L'organisation doit encore décider si la validation initiale tient toujours ou si la fonctionnalité concernée doit être réévaluée, limitée ou désactivée. »

Sriram Iyer
SVP and GM AI Strategy & Products
OneTrust

une visibilité limitée sur les composants IA tiers, les fournisseurs ou les sources de données cause des retards. Par ailleurs, 28 % déclarent que certains outils d'IA tiers ont été adoptés avant évaluation complète. Il faut avoir ces relations à l'esprit pour déterminer quelles modifications doivent relancer un processus de validation.

«

Les clients demanderont des garanties, mais revérifier régulièrement chaque fournisseur par des revues conventionnelles n'est pas viable. Nous devons donner la priorité aux systèmes présentant le plus grand potentiel de nuisance et comprendre leurs résultats. L'enjeu consiste à faire de la conformité un processus capable de s'adapter au changement, plutôt qu'une réponse qui deviendra éculée. »

Ojas Rege
SVP Emerging Products and Technologies
OneTrust

Un changement est important quand il modifie une hypothèse sur laquelle la validation initiale s'appuyait. Un nouveau connecteur peut exposer des données clients supplémentaires. Des autorisations plus étendues peuvent permettre à un assistant de mettre à jour des registres qu'il pouvait auparavant uniquement consulter. Une modification du modèle ou de la configuration peut avoir une incidence sur le fonctionnement d'une mesure de contrôle existante. La revue doit porter sur l'évolution de l'exposition au risque et réutiliser les éléments probants qui restent applicables.

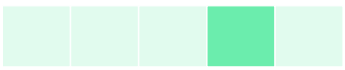
Une modification substantielle peut rouvrir une décision commerciale dans un contrat existant. Si la fonctionnalité concernée prend en charge un workflow critique, la restreindre peut interrompre les opérations. Continuer sans réévaluation peut exposer l'entreprise à des risques que la validation initiale n'avait jamais pris en compte. La répartition des responsabilités et les modalités de repli déterminent la capacité de réaction de l'organisation.

La revue manuelle répétée de chaque composant sera difficile. La priorisation doit tenir compte des préjudices potentiels, de la sensibilité des données et de la dépendance de l'entreprise. Chaque usage à fort enjeu a besoin d'une responsabilité clairement établie pour détecter le changement et décider de la suite. Toutes les mises à jour ne justifient pas une réévaluation complète.

Ce qui pourrait changer la prévision

Les fournisseurs gérés peuvent fournir suffisamment d'informations et de mesures de contrôle pour permettre aux programmes existants de s'adapter. Une visibilité limitée peut aussi empêcher une réévaluation efficace. La prévision dépend du fait que les changements importants produisent des décisions documentées, plutôt que de simples notifications.

Vraisemblance :
Modérée.



Les lacunes existantes en termes de visibilité sur les tiers et d'évaluation justifient la nécessité d'une revue déclenchée par le changement. Nous prévoyons une adoption plus large dans les usages à fort enjeu en 2027, tandis que la réévaluation systématique de l'ensemble du parc d'IA reste moins mature.

Impact sur le secteur :

Élevé pour la continuité, la sécurité et la responsabilité dans les déploiements existants.

Priorités pour les leaders de la gouvernance

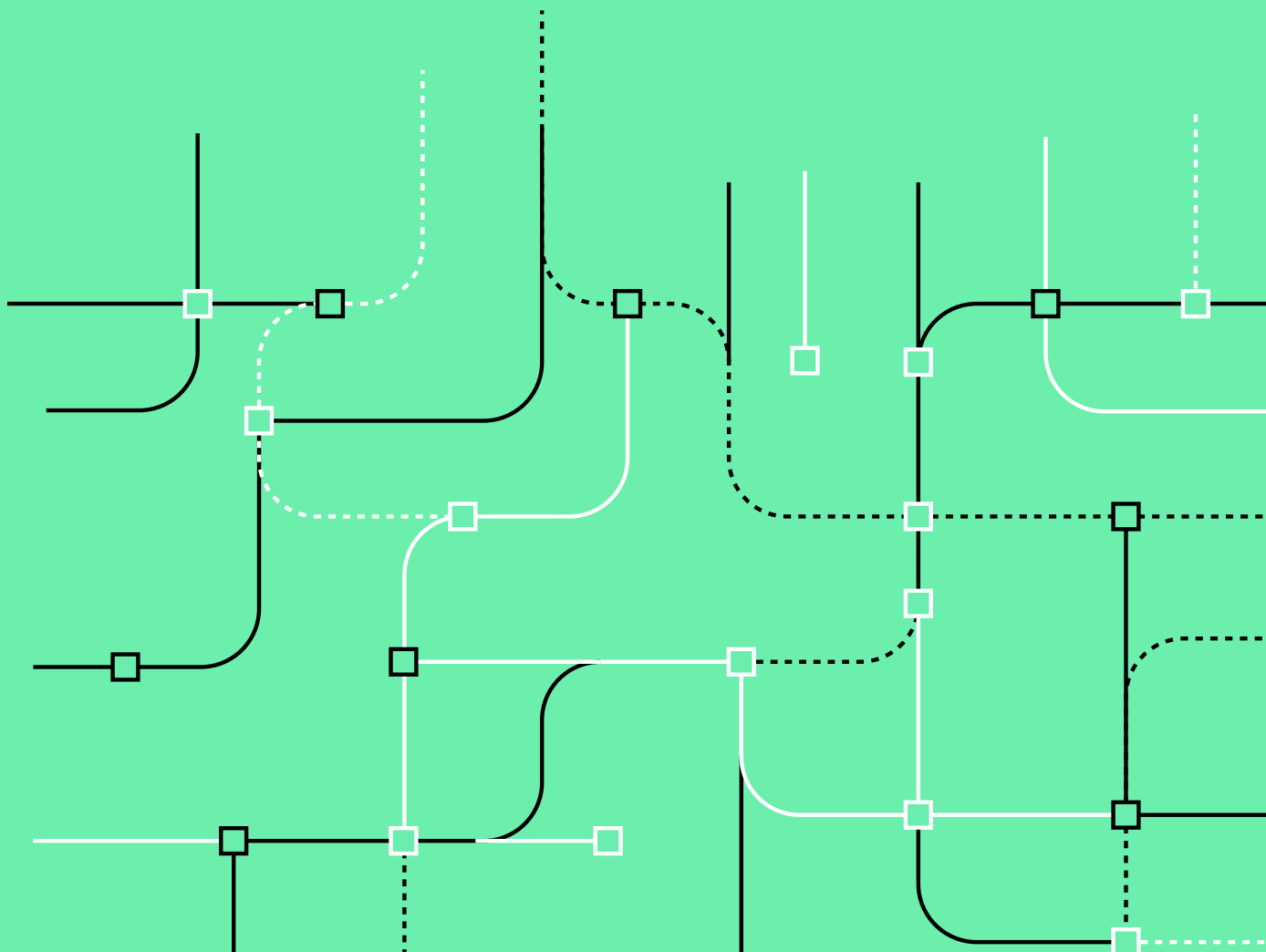
- Technologie et données : cartographie des modèles, applications, connecteurs et flux de données à fort enjeu.
- Achats et juridique : notification des changements et établissement des droits de restriction ou de désactivation pertinents.
- Sécurité : réévaluation de l'efficacité des mesures de contrôle et des accès modifiés.
- Responsables métier : définition de qui peut poursuivre, limiter, corriger ou interrompre une utilisation, avec un dispositif de repli si nécessaire.

À surveiller en 2027

- Des réévaluations lancées sans nouvel appel d'offres.
- Des notifications de changement reliées aux usages et dépendances concernés.
- Des revues déclenchées par une baisse de l'efficacité des mesures de contrôle ainsi que par de nouvelles fonctionnalités.
- Des décisions documentées pour poursuivre, restreindre, corriger ou remplacer un service modifié.
- Des dispositifs de repli testés pour les workflows critiques.

Prévision 4

Une autorisation n’est pas un laissez-passer inconditionnel. Les conversations avec l’IA font des choix d’utilisation des données une partie intégrante du parcours



Prévision 4

Une autorisation n'est pas un laissez-passer inconditionnel. Les conversations avec l'IA font des choix d'utilisation des données une partie intégrante du parcours

En 2027, les premiers utilisateurs des parcours clients assistés par l'IA relieront des choix plus clairs d'utilisation des données aux traitements qu'ils autorisent. Les conversations peuvent révéler des informations allant au-delà de ce dont un service a besoin pour traiter la demande, et un workflow d'IA peut les réutiliser au-delà de la finalité comprise par le client. Nous nous attendons à ce que les premières mises en œuvre s'attaquent à ces limites dans chaque service. Une application cohérente entre fournisseurs prendra plus de temps.

Prenons un acheteur demandant à un assistant de réserver un manteau dans une taille donnée dans un magasin local. Au cours de la conversation, il indique qu'il s'agit d'un cadeau et décrit les préférences du destinataire. L'échange fournit un contexte de service utile, notamment des détails qu'un formulaire de réservation n'aurait peut-être jamais demandés.

La finalité immédiate reste de trouver l'article et de le mettre de côté pour retrait. Réutiliser ces détails conversationnels à des fins publicitaires introduit une décision distincte sur l'usage autorisé. Lorsqu'un choix supplémentaire est requis, le service doit l'expliquer et faire en sorte que la réponse du client soit prise en compte lors des traitements ultérieurs.

Pour l'entreprise, l'enjeu consiste à préserver une personnalisation utile sans laisser les clients dans l'incertitude quant à ce que leur conversation a autorisé. Des prompts répétés peuvent interrompre le processus d'achat, tandis qu'une réutilisation inattendue peut saper la confiance des clients. Le moment où un choix intervient et ses effets deviennent ainsi une composante de l'expérience client.

Le choix doit modifier ce qui se passe ensuite. Si l'acheteur refuse l'utilisation publicitaire facultative, ce choix doit être respecté, tout en finalisant l'achat si possible. Si un choix est ultérieurement retiré, le traitement concerné doit être identifié et la modification appliquée là où elle est nécessaire.

L'organisation a besoin d'un moyen de comparer les traitements ultérieurs avec la finalité et les utilisations autorisées consignées dans sa cartographie des données et dans les évaluations de protection de la vie privée concernées. Une utilisation proposée en dehors de cette

> « À première vue, une notification préalable à l'utilisation peut sembler constituer une simple obligation de déclaration. En pratique, sa production exige des organisations qu'elles cartographient précisément à l'avance ce que fait la prise de décision automatisée, comment les informations personnelles contribuent à son résultat et comment ce résultat façonne la décision. Les équipes juridiques doivent se coordonner avec les équipes produit, d'ingénierie, des ressources humaines et des opérations pour rédiger la notification. »
>
> **Jake Harrison**
> Associate
> Crowell & Moring LLP

«

La question de la confidentialité revient à savoir ce qu'il advient des informations après leur intégration dans le workflow. L'IA peut les combiner ou les utiliser à des fins qui dépassent les finalités initiales. Il faut examiner l'usage ultérieur des informations et s'assurer que les conditions qui leur sont appliquées restent pertinentes à mesure que le processus évolue. »

Brett Tarr
Head of Privacy & AI Governance
OneTrust

portée doit déclencher une revue. Lorsque le contexte initial ne peut pas être reconstitué de manière fiable, cette incertitude doit être levée avant de procéder à la nouvelle utilisation.

En Californie, les exigences relatives aux usages couverts de la prise de décision automatisée illustrent un défi opérationnel connexe : expliquer une décision exige que les équipes comprennent comment le workflow utilise les informations personnelles et produit son résultat. Cela confirme la nécessité de contexte et de responsabilité transversale.

L'étude OneTrust met en évidence le défi plus vaste lié aux données : 52 % des personnes interrogées identifient la qualité, l'accès, la protection de la vie privée ou la sécurité des données comme des facteurs de retard, tandis que 39 % donnent la priorité à une meilleure visibilité sur les risques et l'usage des données.

Les préférences des clients, les autorisations techniques et le consentement légal restent des éléments distincts. Une instruction donnée à un assistant n'est pas automatiquement un consentement légal, et une autorisation enregistrée ne constitue pas à elle seule un traitement licite.

Les transferts entre fournisseurs compliquent l'application, car le statut d'une autorisation peut ne pas préciser la finalité ou les limites qui le sous-tendent. Le service destinataire a besoin de suffisamment de contexte pour évaluer l'usage proposé. Lorsque ce contexte fait défaut, il peut être nécessaire de suspendre le nouvel usage ou de demander des précisions.

Nous nous attendons à ce que les premières mises en œuvre relient un choix effectué lors d'une interaction avec une IA à un traitement pour le même service. Leur valeur dépendra de la possibilité pour les clients de comprendre le choix proposé et du fait que le refus ou le retrait modifie le comportement du service. Une application cohérente entre les fournisseurs reste une extension moins aboutie.

Ce qui pourrait changer la prévision

Les notifications et confirmations existantes peuvent suffire pour de nombreux parcours. Des prompts supplémentaires peuvent perturber l'exécution, tandis que l'interprétation de l'autorisation par les fournisseurs peut différer. L'adoption pourrait rester limitée à des services isolés, avec peu de preuves d'une application en aval.

Vraisemblance :
Émergente.



Impact sur le secteur :

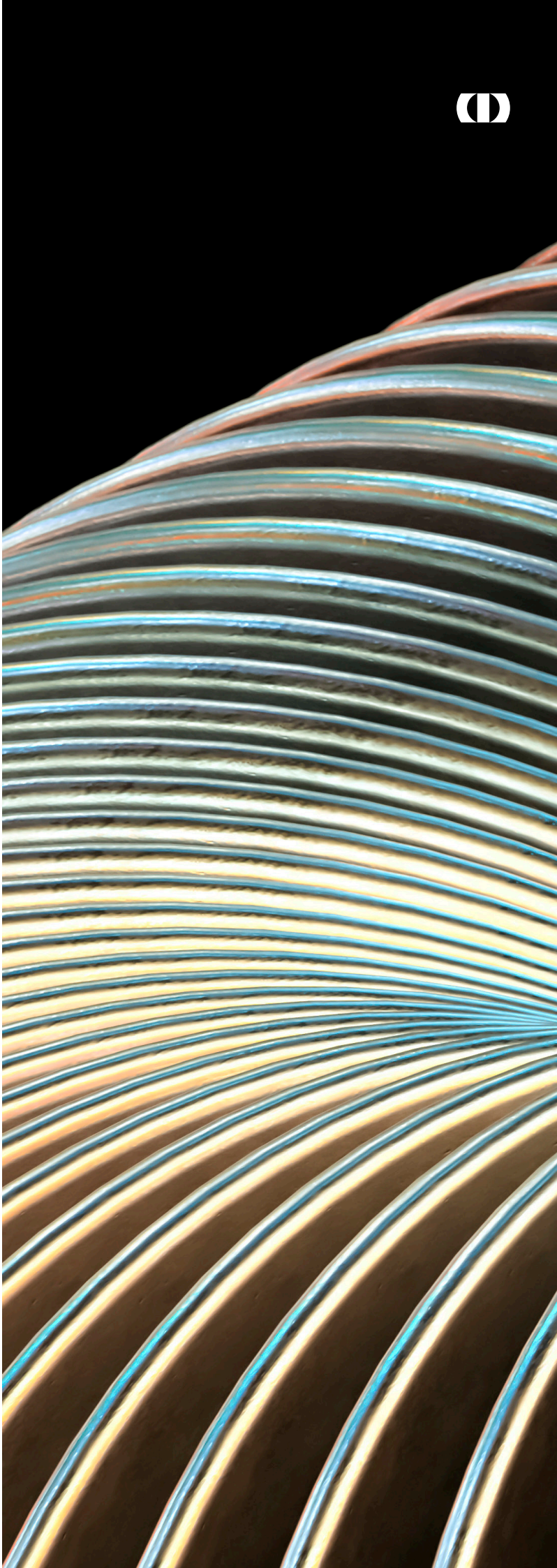
Élevé pour l'expérience client et l'usage des données, avec une adoption initialement limitée.

Priorités pour les leaders de la gouvernance

- Produit et marketing : identification des changements de finalité ou de destinataire dans les parcours prioritaires.
- Protection de la vie privée et juridique : établissement des choix et des exigences applicables.
- Ingénierie : tests de l'usage autorisé, du refus et du retrait en aval.
- Équipes data : préservation du contexte de finalité et de destinataire nécessaire aux décisions ultérieures.

À surveiller en 2027

- Des parcours identifiés demandant un choix pertinent au moment de l'utilisation proposée.
- Des registres précisant la finalité et le destinataire prévus.
- Des traitements qui changent lorsqu'une personne refuse ou retire son consentement.
- Des pilotes qui interrompent leur action ou demandent une nouvelle confirmation lorsqu'un transfert dépasse le périmètre initial.
- Des tests montrant comment le retrait atteint les systèmes en aval.



La réglementation de l'IA en 2027, vue des experts



La réglementation de l'IA en 2027, vue des experts

La réglementation de l'IA aborde 2027 avec des calendriers de mise en œuvre inégaux et des différences significatives entre juridictions. Certains gouvernements introduisent des exigences spécifiques à l'IA, tandis que d'autres appliquent des règles existantes de protection de la vie privée, de protection des consommateurs, relatives à l'emploi et à certains secteurs.

Le défi commun aux organisations devient de plus en plus opérationnel : déterminer où l'IA est utilisée, quelles obligations s'appliquent, qui contrôle ses actions et quels éléments probants peuvent démontrer la conformité.



États-Unis : les réglementations émergent

La situation aux États-Unis reste fragmentée, mais cette fragmentation ne réduit pas la charge opérationnelle : elle ne fait que la répartir.

Au niveau fédéral, le cadre de référence de la Maison-Blanche sur la politique en matière d'IA du 20 mars 2026 formule des recommandations législatives non contraignantes, notamment des propositions de préemption fédérale. Les pouvoirs existants des agences et les exigences des États continuent de façonner la conformité.

« J'estime très peu probable l'adoption de toute réglementation supplémentaire et exhaustive de l'IA au niveau des États ou au niveau fédéral en 2027. Plutôt que d'attendre la prochaine grande réglementation, les organisations devraient se concentrer sur des outils de gouvernance pérennes, tels que la transparence, et rester à l'écoute pour comprendre tout risque émergent de contentieux lié à l'IA. »

Tyler J. Thompson
Partner, Co-Chair, Global Artificial Intelligence Practice
Reed Smith LLP

Quelques repères réglementaires

- Californie : la réglementation relative à la prise de décision automatisée est entrée en vigueur le 1er janvier 2026. Les obligations importantes pour 2027 comprennent les avis préalables à l'usage, ainsi que les droits d'accès et d'opposition applicables aux décisions importantes.
- Colorado : le gouverneur a signé la loi sur la prise de décision automatisée, abrogeant la loi plus générale de l'État sur l'IA à haut risque. Les organisations doivent réévaluer leurs plans de conformité au regard de cette nouvelle législation.
- Illinois : les exigences en matière d'IA dans le domaine de l'emploi prévues par le projet de loi HB 3773 sont entrées en vigueur le 1er janvier 2026. Le gouverneur a également approuvé la loi sur les mesures de sécurité pour l'IA frontière (SB 315), qui introduit un axe distinct sur la gouvernance de la sécurité pour les principaux développeurs d'IA.

Ces exigences influencent de plus en plus les décisions d'achat et de déploiement.



« Les questions importantes sont beaucoup plus détaillées et doivent être abordées au cours du processus d'achat fournisseur, plutôt que pendant le processus de mise à jour de la conformité. Le modèle sous-jacent fourni par un tiers est-il autorisé à s'entraîner sur des données personnelles, et quels leviers contractuels sont en place pour garantir que ce n'est pas le cas ? Les administrateurs disposent-ils du contrôle et de l'autorité nécessaires pour déterminer si une nouvelle fonctionnalité intégrée est activée ? L'outil de transcription par IA utilise-t-il des données d'empreinte vocale, susceptibles de déclencher l'application de lois sur les données biométriques ? »

Abigail Walker
Associate, Emerging Technologies, Global Corporate Group,
Reed Smith LLP

L'Illinois montre aussi comment le contrôle de l'IA recoupe les droits individuels dans les décisions liées à l'emploi.

Pour les organisations, la réponse concrète consiste à relier les exigences juridiques aux achats, à la configuration des systèmes, aux décisions là fort enjeu et aux registres de contrôle avant qu'un problème ne survienne.

« D'ici 2027, l'Illinois devrait s'imposer comme un leader de la gouvernance de l'IA en mettant l'accent non seulement sur l'adoption de l'IA, mais aussi sur la responsabilité. En s'appuyant sur les lois existantes régissant l'utilisation de l'IA dans le recrutement, les employeurs feront face à des attentes croissantes en matière de transparence, d'explication de la prise de décision automatisée, d'évaluation des biais et d'offre de voies de recours significatives contre les résultats pilotés par l'IA. Parallèlement, la loi de l'Illinois sur les mesures de sécurité de l'IA frontière (SB 315) signale un basculement vers une gouvernance de la sécurité de l'IA, en exigeant des principaux développeurs qu'ils publient des référentiels d'atténuation des risques, signalent les incidents de sécurité importants et se préparent à des audits tiers indépendants d'ici 2028. Ensemble, ces évolutions mettent l'accent sur une innovation de l'IA responsable centrée sur l'humain. »

Megan M. Miller
Founder & Attorney, Miller Mosaic
The Identity Counsel



Union européenne : la mise en œuvre soulève la question des éléments probants

Le Règlement européen sur l'IA est entré en vigueur en 2024, avec une application générale depuis le 2 août 2026. Ses obligations échelonnées font de la mise en place de la classification des risques, de la documentation, de la transparence et de la supervision des priorités.

Le Digital Omnibus sur l'IA, entré en vigueur le 27 juillet 2026, a révisé le calendrier pour les systèmes à haut risque. Les obligations applicables aux systèmes d'IA à haut risque visés à l'annexe III, notamment pour certains usages liés à l'emploi, à l'éducation et à la biométrie, s'appliquent à compter du 2 décembre 2027. L'IA à haut risque intégrée à des produits réglementés suivra le 2 août 2028.

Les dates révisées apportent davantage de clarté, même si l'état de préparation des normes harmonisées et des autorités nationales de contrôle continue de soulever des questions sur la mise en œuvre.

La distinction entre obligations différées et obligations existantes est importante. Les exigences du RGPD continuent de s'appliquer au traitement pertinent des données à caractère personnel, et les obligations applicables du règlement sur l'IA restent exécutoires conformément à leurs calendriers respectifs.

Les organisations ont besoin d'évaluations et d'une documentation qui correspondent aux systèmes réellement en fonctionnement après le déploiement. Un modèle modifié, un nouveau fournisseur ou une connexion étendue peut rouvrir des questions qu'une approbation antérieure semblait avoir réglées.



« Le changement le plus marquant dans l'IA en 2027 est l'intelligence infrastructurelle. L'IA n'est plus seulement une compétition technologique, militaire et énergétique entre les États-Unis, l'Europe et la Chine : elle est désormais intégrée dans le quotidien des populations, dans les soins médicaux, le contrôle des frontières, la recherche d'emploi et la distribution des ressources. »

Mahdi Barkabian Zanjani
Professionnel indépendant

Royaume-Uni : les régimes existants peuvent importer plus qu'une nouvelle législation sur l'IA

Le Royaume-Uni suit une voie différente, aucune loi transversale complète sur l'IA ne définissant actuellement l'approche réglementaire. Les exigences existantes en matière de supervision sectorielle et de cybersécurité pourraient entraîner des changements plus immédiats qu'une loi dédiée.

Le projet de loi sur la cybersécurité et la résilience reste soumis au processus législatif. Ses obligations potentielles doivent être distinguées des exigences de supervision existantes.

Pour les organisations opérant dans des secteurs réglementés, la priorité immédiate consiste à comprendre comment l'IA modifie les responsabilités existantes en matière d'accountability, de supervision des fournisseurs, de risque lié aux modèles et de résilience opérationnelle. Attendre une loi dédiée à l'IA pourrait laisser ces obligations insuffisamment traitées.

« Il est toujours très peu probable que le très médiatisé UK AI Bill se matérialise en 2027. Mais il est possible que le gouvernement ajoute au projet de loi sur la cybersécurité et la résilience (réseaux et systèmes d'information) des mesures de cybersécurité liées à l'IA. Cela pourrait inclure des mesures de signalement supplémentaires pour les incidents graves liés à l'IA et les quasi-incidents liés à l'IA dans les services essentiels, en plus des obligations de signalement des incidents et de supervision de la chaîne d'approvisionnement pour les fournisseurs critiques dans le champ d'application, tels que les fournisseurs de services gérés et de centres de données. »

Katie Hewson
Partner
Stephenson Harwood

Corée du Sud : la politique cède la place aux éléments probants opérationnels

La loi-cadre de la Corée du Sud sur l'IA est entrée en vigueur le 22 janvier 2026. Son approche d'application progressive met davantage l'accent sur la mise en œuvre, en particulier sur l'identification des systèmes d'IA à fort impact et la documentation des contrôles appliqués avant le déploiement.

L'exigence opérationnelle va de la découverte d'un système à l'explication de sa classification, des garanties choisies, de la supervision humaine et des éléments probants à l'appui.

« La charge la plus sous-estimée sera probablement l'inventaire et la classification de l'IA. Les fonctionnalités d'IA sont de plus en plus intégrées aux logiciels ordinaires et aux services tiers, tandis que le régime coréen applicable à l'IA à fort impact couvre des usages sensibles, notamment le recrutement, l'emprunt, la santé, l'éducation et certaines décisions gouvernementales. Les organisations peuvent donc découvrir que la difficulté consiste à identifier l'IA intégrée dans les processus métier existants et à déterminer quels systèmes déclenchent des obligations supplémentaires. »

Timothy Dickens
Partner
DR&AJU Law Group LLC

Brésil : le report de l'adoption d'une loi sur l'IA ne signifie pas qu'il n'y a pas de cadre réglementaire

Le projet de cadre global sur l'IA Brésil, PL 2338/2023, a été adopté par le Sénat en décembre 2024, mais exige encore une approbation législative.

La législation existante encadre déjà les activités liées à l'IA. La Loi générale sur la protection des données à caractère personnel (LGPD), notamment son article 20 relatif aux décisions automatisées, ainsi que le Code de défense des consommateurs, créent des obligations que les organisations ne peuvent différer pendant l'élaboration d'une législation exhaustive.

« Les entreprises doivent abandonner l'approche attentiste sur la loi PL 2338/2023 et mettre en place des architectures de gouvernance autour des lois qui encadrent actuellement le secteur, soient la LGPD, les directives de l'ANPD et les règles sectorielles de protection des consommateurs. L'ISO/IEC 42001 peut démontrer une diligence de base, mais ne peut pas remplacer les obligations légales ni protéger une entreprise de sa responsabilité en cas de conséquences préjudiciables liées à l'IA. »

Adriana Ruggeri Quinelo
Legal Counsel & Advisor
Ruggeri Quinelo

La distinction est particulièrement importante pour les organisations qui s'appuient sur des normes volontaires de gouvernance. La certification peut étayer des éléments attestant de la diligence, mais elle ne détermine pas si les décisions automatisées sont conformes au droit brésilien sur la protection de la vie privée et la protection des consommateurs.



Des régimes différents, des questions de gouvernance qui convergent

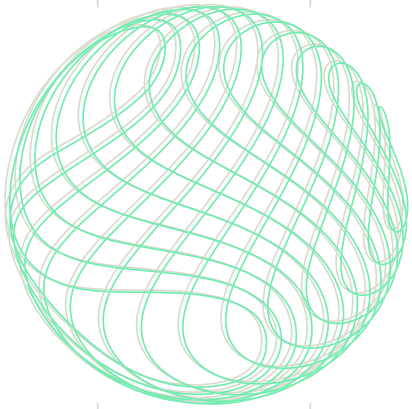
Ces juridictions ne convergent pas vers des règles identiques. Les contributions suggèrent quelque chose de plus utile : bon nombre des questions opérationnelles commencent à se ressembler.

Détection

Savons-nous où l'IA est utilisée, notamment les fonctionnalités intégrées aux logiciels courants et fournies par des tiers ?

Contexte

Comprenons-nous quelle personne, quelle décision, quelles données, quels processus opérationnels ou quelle obligation réglementaire l'IA peut affecter ?



Contrôle

L'organisation peut-elle montrer où s'appliquent les autorisations, l'intervention humaine significative, la transparence, la restriction et la remontée ?

Éléments probants

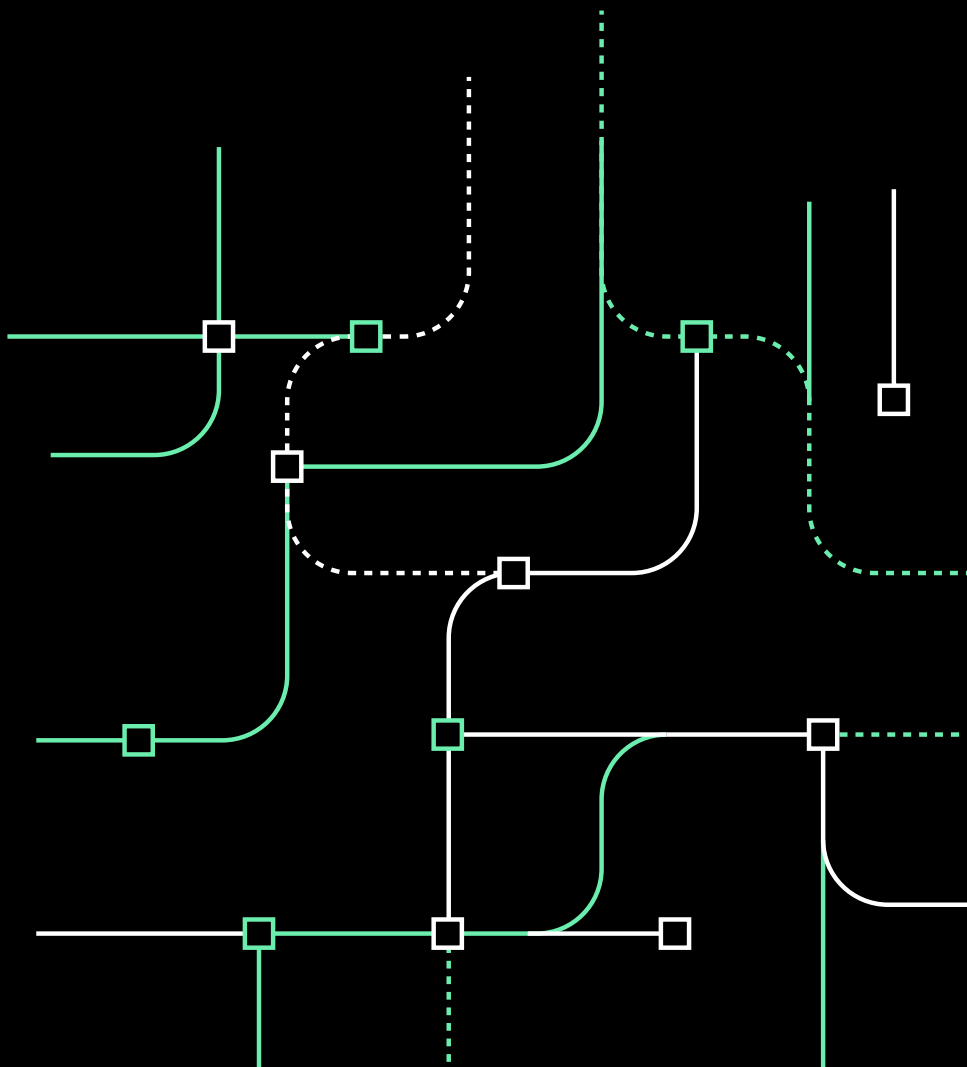
Les équipes peuvent-elles reconstituer ce qui a été évalué, quel système ou quelle version était en service, ce qui a changé, quelles mesures de contrôle s'appliquaient et qui en était responsable ?

Ces fonctionnalités restent pertinentes même lorsque les calendriers réglementaires changent. Elles permettent aux organisations de réagir lorsqu'une nouvelle règle entre en vigueur, qu'une loi existante s'étend à l'IA ou qu'un organisme de réglementation demande ce qui s'est passé lors d'un déploiement particulier.

Les voies juridiques vont continuer à différer. L'exigence opérationnelle se clarifie : la gouvernance doit rester connectée à l'IA quand elle passe progressivement de la validation à l'utilisation.

Contre-prévisions :

3 éléments qui n’auront *pas* lieu en 2027



Contre-prévision 1

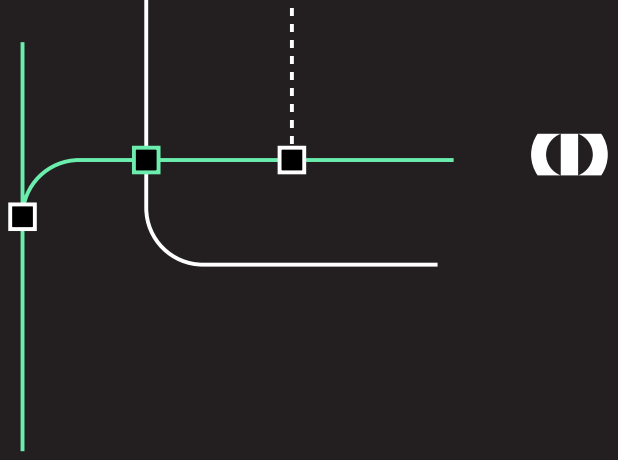
La garantie de référence ne suffira pas à trancher toutes les décisions de déploiement

Une évaluation peut rester valable dans son périmètre d'origine alors qu'un déploiement modifié n'est pas suffisamment examiné. La question est de savoir si les éléments probants couvrent toujours la fonctionnalité, l'utilisation prévue et les mesures de contrôle dont dépend la validation.

« La certification peut démontrer aux autorités de contrôle, aux investisseurs et aux partenaires commerciaux une diligence de base, mais elle ne constitue pas une protection juridique automatique. Les organisations doivent toujours comprendre les lois et les obligations sectorielles qui s'appliquent à l'IA qu'elles déploient. »

Adriana Ruggeri Quinelo
Legal Counsel & Advisor
Ruggeri Quinelo

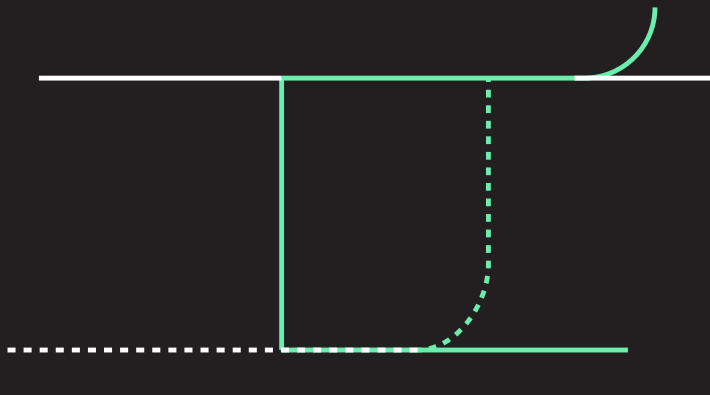
Un test d'intrusion réalisé en janvier peut ne pas couvrir les fonctionnalités introduites en mars. Le même principe s'applique aux hypothèses qui sous-tendent une validation. Une nouvelle connexion, des prérogatives augmentées ou une baisse de l'efficacité des mesures de contrôle peuvent rouvrir une décision, tandis que les garanties globales de l'organisation restent pertinentes.



« Un client peut accepter l'assurance concernant un service et néanmoins demander de nouveaux tests avant d'activer une fonctionnalité modifiée. La question est de savoir si les éléments probants couvrent ce qu'il s'apprête à utiliser. Les garanties existantes nous fournissent une base, et nous devons déterminer où le changement exige davantage. »

Tim Mullen
Chief Information Officer
OneTrust

En 2027, les organisations devront déterminer si les garanties existantes couvrent un déploiement d'IA modifié. La revue complémentaire devra se concentrer sur les hypothèses que la modification a remises en question, tout en conservant les éléments probants qui restent pertinents.



Contre-prévision 2

Augmenter les effectifs ne suffira pas à assurer un contrôle à grande échelle

Les organisations vont continuer à s'appuyer sur le jugement humain pour les politiques, les décisions sensibles et les exceptions. L'extension des workflows des agents rendra plus difficile l'affectation de personnes avant chaque étape d'exécution.

La décision opérationnelle consiste à déterminer les situations nécessitant un jugement humain et ce qui peut être fait dans des conditions définies. Un workflow limité peut rendre possible la validation avant toute action à fort enjeu. Un autre peut exiger des prérogatives déléguées plus restreintes, avec remontée lorsque les conditions changent.

La surveillance automatisée doit aussi être évaluée. Les dirigeants doivent vérifier qu'elle détecte les écarts pertinents, permet de joindre la personne responsable et facilite une intervention efficace.

L'objectif est de mettre en place une IA adaptée, au bon rythme. Le délai entre la demande et la mise en service de la fonctionnalité peut mettre en évidence des temps d'attente inutiles. La qualité des décisions, la gestion des exceptions et les incidents survenant après la validation permettent de déterminer si le processus fonctionne de manière responsable.

L'augmentation des effectifs ne peut pas permettre à la revue humaine de s'aligner sur la vitesse des machines. Un modèle de supervision qui dépend de personnes inspectant chaque action ne peut pas suivre le rythme lorsque des agents connectés agissent entre systèmes. Les organisations ont besoin de limites applicables et d'une surveillance permettant d'identifier les situations nécessitant un jugement humain, avec des personnes capables d'intervenir efficacement. Le recrutement peut renforcer cette supervision, mais ne peut pas se substituer à une modification de la gouvernance du travail.

« La surveillance humaine ne pourra pas s'accroître aussi vite que l'activité liée à l'IA. Je pense que la surveillance continue va être de plus en plus agentique. Cela change la manière dont les humains supervisent le travail et crée une nouvelle responsabilité qui consiste à évaluer le système de surveillance lui-même. »

Ojas Rege
SVP Emerging Products and Technologies
OneTrust

« Alors que les employés utilisent l'IA quotidiennement, chacun doit comprendre clairement comment le faire de manière responsable. L'enjeu consiste à rendre la gouvernance facile à appliquer tout en garantissant une utilisation sûre. »

Federico Sembolini
Senior Manager AI Transformation - AI Governance
BBVA

Contre-prévision 3

Vous n’aurez pas de certitude avant de devoir prendre une décision

La promesse la moins crédible que nous puissions faire pour 2027 serait de dire que nous savons exactement ce qui nous attend.

Les modèles vont changer. De nouveaux usages vont mettre à l’épreuve des décisions qui semblaient arrêtées. Certaines prévisions de ce rapport se concrétiseront plus rapidement que prévu. D’autres prendront plus de temps. L’environnement économique influencera également les fonctionnalités que les organisations choisiront d’adopter.

Les organisations devront toujours décider quels usages de l’IA autoriser et qui sera responsable des conséquences.

En 2027, ces décisions précéderont souvent l’établissement d’éléments probants sur la fonctionnalité suivante ou le modèle opérationnel suivant. Attendre un plan de gouvernance achevé laisse les équipes travailler avec les validations et les habitudes qu’elles ont déjà, même lorsque le travail a changé.

«

Il n’y a pas une unique bonne réponse. Les entreprises doivent comprendre ce qui fonctionne pour leur activité. Face à la pression croissante pour utiliser davantage d’outils d’IA, le défi consiste à déterminer qui est responsable de la gouvernance et comment celle-ci devrait fonctionner dans l’entreprise. »

Bruna Baccini
Responsable de la conformité et DPO
GOL Airlines

«

Nous ne devons pas avoir peur des possibilités de l’IA, mais nous ne devons pas non plus nous précipiter sur ce qu’elle peut faire. La technologie évolue peut-être à la vitesse de la lumière, mais les humains ont besoin de temps pour changer. Nous devons penser à l’aspect humain autant qu’à la technologie. »

Aaron Weller
Leader of Privacy Innovation and Assurance
HP

La réponse pragmatique consiste à rendre les décisions qui peuvent être révisées. Une validation doit définir les conditions dans lesquelles elle s’applique et ce qui déclenche une nouvelle revue. Les dirigeants doivent également savoir qui peut modifier la décision lorsque ces conditions ne s’appliquent plus.

Concevoir ce labyrinthe revient à prévoir la possibilité de réviser une décision tout en en restant responsable. Le véritable test de leadership pour 2027 est de savoir si votre organisation peut modifier les prérogatives d’un workflow d’IA tout en expliquant qui a validé le changement, ce qu’il permet et comment l’arrêter.



www.onetrust.fr

Clause de non-responsabilité
Aucune partie du présent document ne peut être reproduite sous aucune forme que ce soit sans l'autorisation écrite du détenteur des droits d'auteur. Le contenu de ce document peut faire l'objet de révisions sans préavis en raison de progrès continus en matière de méthodologie, de conception et de fabrication. OneTrust LLC décline toute responsabilité pour toute erreur ou tout dommage résultant de l'utilisation de ce document. Les produits, contenus et supports OneTrust sont uniquement fournis à titre informatif et ne sont pas destinés à fournir de conseils juridiques. Veuillez consulter votre avocat pour toute question spécifique. Les informations fournies par OneTrust ne garantissent pas la conformité aux lois et aux réglementations applicables.

Copyright © 2026 OneTrust LLC. Tous droits réservés. Exclusif et confidentiel.