

Governance by Design : pourquoi votre "Policy IA" ne vous protège de rien

Par Laurent ASSOULY, Septembre 2026

Introduction

Les comités de direction pondent des chartes éthiques à un rythme frénétique et pensent naïvement avoir sécurisé le déploiement de l'intelligence artificielle dans l'entreprise, persuadés qu'un document de bonne conduite suffira à encadrer les nouveaux usages. Face à la pression médiatique et à la peur panique de rater le virage technologique de la décennie, les décideurs achètent des solutions génératives dans l'urgence tout en demandant à leurs juristes de rédiger un pare-feu juridique pour se couvrir. La réalité du terrain démontre pourtant qu'un simple texte publié sur l'intranet ne résiste pas une seule seconde à la pression opérationnelle d'un salarié pressé qui utilise un modèle de langage externe pour livrer son travail à temps. Face à l'explosion des outils génératifs, la véritable ligne de défense ne se trouve plus dans un règlement interne, puisqu'elle nécessite de transformer une consigne écrite en une barrière technique infranchissable. C'est l'opposition brutale entre l'illusion du papier et la réalité du code.

La Policy : le mirage du contrôle par le papier

La "Policy" représente exclusivement le cadre théorique de l'entreprise, c'est-à-dire les lois, les règles de conformité et les principes éthiques que l'organisation souhaite s'imposer pour encadrer ses équipes. Ce travail intellectuel est systématiquement produit par des avocats, des directeurs de la conformité ou des consultants externes qui conçoivent un monde parfait où les consignes sont scrupuleusement lues et respectées. Ces documents détaillent minutieusement l'interdiction absolue de partager des données personnelles identifiables ou l'obligation théorique de vérifier systématiquement les biais cognitifs des algorithmes, alors que les employés cherchent uniquement à automatiser leurs tâches rébarbatives pour rentrer chez eux plus tôt.

Le problème de la Policy réside dans son absence totale de matérialité informatique, car elle s'appuie uniquement sur la discipline humaine au lieu de bloquer physiquement les comportements à risque sur le réseau. Une entreprise ne peut pas protéger sa propriété intellectuelle ou se conformer aux exigences complexes de l'AI Act avec de simples promesses rédigées sur du papier à en-tête. Le salarié qui doit analyser un fichier Excel de dix mille lignes avant la réunion de dix heures ne lira jamais la charte de bonne conduite, parce que son seul impératif immédiat est de trouver un outil gratuit en ligne capable de faire le travail à sa place. Le document juridique se transforme alors en un simple alibi managérial qui protège la direction en cas de procès, mais qui ne sécurise absolument rien de manière concrète sur les serveurs de l'entreprise.

La Gouvernance : la réalité des tranchées informatiques

La “Gouvernance” désigne au contraire l’implémentation physique et technique des contraintes imaginées par la direction, un travail d’ingénierie complexe qui consiste à rendre le contournement des règles mécaniquement impossible. Les acteurs de cette gouvernance sont les administrateurs systèmes, les architectes cloud et les équipes de cybersécurité qui configurent des passerelles réseau ou tracent les requêtes via des systèmes de gestion des identités ultra-stricts. Ce n’est pas un exercice de rédaction juridique ou de philosophie d’entreprise, parce que c’est une architecture lourde qui exige de déployer des filtres de prévention des pertes de données (DLP) capables d’intercepter un numéro de sécurité sociale avant qu’il ne parte vers une intelligence artificielle publique.

L’équipe technique agit dans la mécanique pure des flux de données, ce qui exige des budgets matériels conséquents et une véritable expertise de développement interne. Gérer la gouvernance d’une intelligence artificielle signifie concrètement installer des proxys d’entreprise qui interceptent chaque prompt de chaque utilisateur, analyser la charge de la requête en temps réel, et appliquer une politique de filtrage dynamique avant de l’envoyer au modèle linguistique. Cela implique de gérer les droits d’accès avec une précision chirurgicale, afin qu’un stagiaire du service marketing n’ait pas techniquement la possibilité d’interroger un modèle connecté aux bases de données financières des ressources humaines. Cette barrière technologique demande des investissements massifs que la signature d’un PDF ne remplacera jamais.

L’émergence vitale de la Governance by Design

Une entreprise qui paie cher une Policy mais n’investit pas dans son département informatique pour l’implémenter se transforme instantanément en une cible immobile face aux cybermenaces modernes. À l’image du concept de “Security by Design” qui a révolutionné le développement logiciel en forçant les ingénieurs à coder la sécurité avant même de penser à l’interface, la seule solution viable consiste à adopter la “Governance by Design”. Ce concept impose l’intégration des règles de contrôle directement dans l’architecture des systèmes dès leur conception initiale, sans jamais laisser l’utilisateur final décider s’il doit ou non respecter la règle édictée par le service juridique.

Le dialogue permanent entre les avocats d’affaires et la direction des systèmes d’information devient une nécessité absolue, afin que chaque article de la charte éthique se traduise par une ligne de code restrictive sur le pare-feu de l’entreprise. Si le document juridique interdit formellement l’envoi de données de santé vers des serveurs hébergés en dehors de l’Union européenne, la Governance by Design traduit cette phrase par une règle de routage automatique qui bloque toute requête API vers un fournisseur américain non certifié. La règle métier n’est plus une simple suggestion à lire dans un manuel d’accueil le jour de l’embauche, puisqu’elle devient une contrainte codée en dur dans l’infrastructure de l’entreprise, ce qui rend l’erreur humaine techniquement impossible.

Conclusion

Le besoin de cadres techniques rigides devient une urgence existentielle face à l’arrivée massive des agents autonomes qui remplaceront très bientôt les simples générateurs de texte conversationnels. Ces futurs algorithmes ne se contenteront plus de rédiger des brouillons d’e-mails pour assister un humain, car ils agiront de manière totalement indépendante sur les bases de données internes

en enchaînant des milliers de requêtes à la vitesse du processeur, ce qui rendra toute tentative de supervision humaine manuelle définitivement obsolète.

Si un collaborateur peut lire une charte et décider de l'ignorer par fatigue ou par précipitation pour boucler un dossier, un agent logiciel exécutera ses instructions sans aucune conscience morale ni aucune notion du risque juridique. Une intelligence artificielle autonome qui reçoit l'ordre d'optimiser une campagne marketing n'hésitera pas une milliseconde à exporter toute la base clients vers un outil tiers non sécurisé si aucune barrière technique ne l'en empêche physiquement. L'entreprise survivra uniquement si elle a eu la lucidité d'automatiser ses contrôles de sécurité à la même vitesse que les outils qu'elle tente de maîtriser, parce que le papier n'a jamais arrêté une requête réseau.

Bibliographie

- MIT Sloan Management Review — « [The Real Question to Ask About AI Governance](#) »
- CIO.com — « [How the Senate's AI AGENT Act could reshape enterprise AI governance](#) »
- CIO.com — « [Your identity governance wasn't built for AI agents](#) »
- TechRepublic — « [Coupang's \\$409M Fine Shows the Real Cost of Weak AI Governance](#) »
- Enterprise AI Governance — « [How China is governing agentic AI](#) »