Tribune stratégique

cyber-régulation européenne

Du millefeuille normatif à la puissance de la convergence

David Pauillac

mars 2026

Table des matières

À l'attention des membres de Boards, Dirigeants et Décideurs des entreprises soumises aux réglementations numériques européennes NIS2, DORA, IA Act, RGPD, CRA, FIDA, DSP2, DSA, Solvabilité II…

9+	30%	70%	1
Règlements EU actifs	Budget audit récupérable	Temps RSSI perdu en reporting	Cadre unifié possible

> Le vrai risque pour votre entreprise n'est plus seulement la cyberattaque. C'est l'asphyxie normative : cette accumulation silencieuse de réglementations qui détourne vos équipes de la défense réelle pour les plonger dans une bureaucratie de la conformité sans fin. Il est temps de choisir entre subir le millefeuille et orchestrer la convergence.

Le constat d'échec : L'inefficience par la saturation normative

« On ne protège pas une forteresse en multipliant les règlements d'entrée. On la protège en renforçant ses murs. »

Il existe une conviction profondément ancrée dans la culture réglementaire européenne, et plus encore française, selon laquelle la sécurité s'obtient par l'accumulation de normes. Cette conviction, aussi compréhensible soit-elle dans son intention, produit aujourd'hui un effet inverse à celui recherché. À mesure que les textes se multiplient — NIS2, DORA, AI Act, RGPD, CRA, FIDA, sans oublier les déclinaisons nationales qui viennent s'y superposer —, les organisations ne deviennent pas plus résilientes. Elles deviennent plus occupées. Et l'occupation n'est pas la protection.

Ce premier chapitre pose un diagnostic que beaucoup ressentent sans toujours oser le formuler : le millefeuille réglementaire français et européen en matière de cybersécurité est en train de produire une saturation normative qui paralyse l'action défensive réelle.

« Plus nous réglementons, moins nous sécurisons réellement. »

Il ne s'agit pas ici de plaider pour moins de régulation, mais pour une régulation intelligente et surtout une mise en œuvre opérationnelle et efficace. Avant d'envisager les solutions — qui feront l'objet des chapitres suivants —, il convient de regarder le problème en face, avec lucidité et sans complaisance.
Trois phénomènes cristallisent ce constat.

Le paradoxe de la Compliance Fatigue : quand la règle devient l'ennemi de la défense

Qu'est-ce que la Compliance Fatigue ?

L'accumulation de réglementations redondantes sature les équipes de sécurité. La cybersécurité se transforme en pur exercice de « cochage » de cases administratif, au détriment d'une défense active et d'une véritable résilience.

La *Compliance Fatigue*, que l'on peut traduire librement par **fatigue de conformité**, désigne l'état d'épuisement organisationnel qui survient lorsque les équipes chargées de la sécurité consacrent l'essentiel de leurs ressources — humaines, financières et cognitives — à répondre à des obligations réglementaires au détriment de leur mission première : *détecter, prévenir et neutraliser les menaces*.
Ce phénomène n'est pas un simple inconfort opérationnel. C'est une **déformation structurelle** des organisations de sécurité, qui transforme progressivement des fonctions de défense active en fonctions de production documentaire. La cybersécurité, dans ce contexte, cesse d'être une discipline technique tournée vers l'adversaire pour devenir un exercice administratif tourné vers le régulateur.

Le mécanisme est presque mécanique dans sa logique : chaque nouveau règlement impose de nouveaux rapports, de nouvelles cartographies, de nouveaux plans de remédiation, de nouvelles preuves à conserver. Lorsque plusieurs règlements coexistent — chacun avec ses propres exigences de notification, ses propres formats, ses propres délais — les mêmes informations doivent être produites plusieurs fois, dans des formes différentes, pour des destinataires différents, selon des calendriers qui ne sont pas coordonnés entre eux.

Un exemple concret : le RSSI devenu greffier

Considérons la situation, loin d'être hypothétique, d'un Responsable de la Sécurité des Systèmes d'Information — le RSSI, figure centrale de la cybersécurité de toute organisation de taille significative — confronté à un incident de sécurité affectant à la fois des données personnelles, des systèmes financiers et une infrastructure considérée comme essentielle au sens de la directive NIS2.
Cet incident unique devra être notifié à l'ANSSI au titre de NIS2, à la CNIL au titre du RGPD, à l'ACPR ou à l'AMF au titre de DORA si l'organisation relève du secteur financier — le tout dans des délais distincts, avec des niveaux de détail distincts et selon des formulaires distincts. Il est documenté que dans de telles configurations, un RSSI peut consacrer plus de 70 % de son temps de réponse à incident à la production de rapports réglementaires, plutôt qu'à l'analyse technique de la menace, à la recherche de l'origine de l'attaque ou à la coordination des équipes de remédiation.
Le paradoxe atteint ici son paroxysme : au moment précis où l'organisation est sous attaque — c'est-à-dire au moment où l'expertise du RSSI a le plus de valeur — celui-ci est retenu loin de la ligne de front par des obligations de reporting qui, dans leur conception initiale, étaient destinées à améliorer la transparence et la coordination, mais qui, dans leur application cumulée, produisent exactement l'inverse. **L'adversaire, lui, ne remplit aucun formulaire**.

Ce que cela coûte réellement

La *Compliance Fatigue* n'est pas seulement un problème d'efficacité individuelle. Elle engendre des coûts systémiques qui méritent d'être nommés clairement. Elle conduit à une priorisation implicite de la forme sur le fond : une organisation sera davantage exposée à un risque juridique si elle ne notifie pas un incident dans les 72 heures que si elle ne l'a pas détecté à temps. Elle crée une concurrence interne pour des ressources rares : chaque heure passée à documenter est une heure qui ne sera pas investie dans la mise à jour des systèmes, l'entraînement des équipes ou la surveillance des flux réseaux. Elle génère enfin une démotivation des talents — les professionnels de la cybersécurité choisissent ce métier pour défendre des systèmes, pas pour rédiger des rapports — ce qui aggrave un marché du travail déjà structurellement en tension.

Le piège de la surtransposition française : le zèle qui pénalise

La surtransposition : définition et mécanisme

Lorsque l'Union européenne adopte un règlement ou une directive en matière de cybersécurité, les États membres disposent d'une marge de manœuvre variable dans sa mise en œuvre. Les règlements européens s'appliquent directement, sans transposition. Les directives, en revanche, doivent être intégrées dans le droit national, ce qui laisse aux législateurs et régulateurs locaux une latitude — parfois explicitement prévue — pour adapter, compléter, voire renforcer les exigences européennes. La surtransposition désigne le phénomène par lequel un État membre — par zèle réglementaire, par souci d'afficher une ambition souveraine, ou parfois par défaut de coordination entre les différentes administrations — ajoute des couches d'exigences nationales supplémentaires au-delà de ce que le texte européen requiert. En France, ce réflexe est historiquement ancré. Il participe d'une tradition juridique qui valorise la complétude du dispositif normatif, et d'une ambition politique légitime de faire de la France un modèle en matière de souveraineté numérique. Mais en cherchant à être le « bon élève » européen, la France superpose des exigences locales supplémentaires aux textes communautaires. Résultat : **une complexité accrue qui pénalise la compétitivité face aux acteurs non-européens, sans gain de sécurité mesurable.**

Quand être le « bon élève » devient un handicap compétitif

Prenons l'exemple de la certification souveraine. Dans le cadre du développement de l'AI Act européen — le premier règlement mondial sur l'Intelligence Artificielle (IA), adopté en 2024 et entré progressivement en application —, un cadre de qualification des systèmes d'IA à haut risque a été défini au niveau européen. Ce cadre prévoit des évaluations de conformité, des exigences de transparence et des mécanismes de surveillance du marché.
Or, parallèlement à ce cadre, la France a développé ou envisagé des exigences de certification spécifiques pour certains usages de l'IA dans des secteurs sensibles — santé, défense, administration — en superposant des critères de souveraineté technique (hébergement sur sol français, utilisation de solutions qualifiées SecNumCloud[1], audits supplémentaires) à des services ou systèmes déjà soumis aux évaluations prévues par l'AI Act ou par NIS2.
Le résultat est une **double charge de conformité** qui pèse essentiellement sur les acteurs français et européens — ceux qui, précisément, cherchent à respecter les règles —, tandis que les acteurs non-européens opérant en mode transfrontalier ou depuis des juridictions moins contraignantes peuvent contourner, déléguer ou simplement ignorer une partie de ces exigences dans un premier temps, avant d'être rattrapés — parfois — par la régulation.
Ce différentiel de contrainte n'est pas théorique. Il se traduit par des délais de mise sur le marché[2] plus longs pour les entreprises françaises, par des coûts de certification qui obèrent les budgets d'innovation, et par une complexité juridique qui décourage les investissements étrangers dans l'écosystème numérique français.
La souveraineté, mal calibrée, peut devenir un obstacle à la compétitivité qu'elle prétend défendre.

La confusion entre protection et protectionnisme

Il convient de distinguer deux logiques qui se présentent parfois sous le même habillage. La protection souveraine vise à garantir que des systèmes critiques ne dépendent pas de technologies ou d'infrastructures sur lesquelles la France n'aurait aucun levier de contrôle en cas de crise. Cette ambition est légitime, stratégiquement fondée et doit être poursuivie avec

1. Voir `https://cyber.gouv.fr/enjeux-technologiques/cloud/faq-qualification-secnumcloud/`
2. le fameux Time-to-Market

détermination. Le protectionnisme normatif, en revanche, consiste à utiliser la réglementation comme une barrière à l'entrée déguisée, au profit d'acteurs nationaux qui ne sont pas nécessairement les plus performants techniquement.
La ligne de partage entre ces deux logiques est parfois ténue. Mais la surtransposition française, dans plusieurs épisodes récents, a franchi cette ligne — souvent sans le vouloir — en produisant des complexités qui servent moins la sécurité nationale que la charge administrative de toutes les parties prenantes.

L'illusion de la sécurité par le texte : la conformité n'est pas la résilience

Une confusion conceptuelle aux conséquences graves

C'est sans doute le malentendu le plus fondamental — et le plus dangereux — que porte le paradigme réglementaire actuel. Il existe une confusion, parfois inconsciente, parfois entretenue par des intérêts bien compris, entre **conformité réglementaire** et **sécurité effective**. Or ces deux notions, si elles peuvent se renforcer mutuellement dans une architecture bien pensée, ne sont pas synonymes. Et les traiter comme tels expose les organisations à des risques qu'elles croient avoir maîtrisés.

La conformité est un *état administratif* : une organisation est conforme lorsqu'elle peut démontrer, à un instant donné et selon des critères prédéfinis, qu'elle a mis en place les processus, les politiques et les contrôles requis par un cadre normatif.
La sécurité est un *état dynamique* : une organisation est sécurisée dans la mesure où sa surface d'attaque est maîtrisée, ses vulnérabilités sont détectées et corrigées en temps utile, ses équipes sont formées à répondre aux menaces actuelles — et non à celles qui existaient au moment de la rédaction du règlement.

La différence est fondamentale, parce que les menaces évoluent en permanence, à une vitesse qui n'est pas celle du droit.

L'attaque qui ignorait la certification

Illustrons ce point par un scénario qui n'a rien d'exceptionnel. Une entreprise du secteur de la distribution, soumise au RGPD pour la gestion des données de ses millions de clients et à NIS2 pour la sécurité de sa chaîne logistique numérique, consacre depuis deux ans l'essentiel de ses ressources cybersécurité à l'obtention et au maintien de ses certifications. Elle dispose d'une politique de sécurité documentée, d'un registre des traitements à jour, d'un plan de réponse aux incidents validé par ses juristes et de preuves de conformité prêtes à être présentées à tout régulateur.

Un mardi matin, elle est victime d'une attaque par ransomware — un logiciel malveillant qui chiffre les données de l'entreprise et en bloque l'accès jusqu'au paiement d'une rançon. Le vecteur d'attaque : une vulnérabilité sur un système de supervision industrielle, dont le fabricant avait publié un correctif six semaines plus tôt. Ce correctif n'avait pas été appliqué, faute de ressources disponibles — les équipes techniques étant mobilisées sur la préparation du dernier audit de conformité.

L'attaque paralyse les opérations pendant onze jours. Le coût direct dépasse plusieurs dizaines de millions d'euros. L'entreprise est, à la date de l'attaque, **100 % conforme** aux exigences qui lui étaient applicables.

Ce scénario illustre une vérité que les professionnels de la cybersécurité connaissent bien : un attaquant n'interroge jamais le registre des traitements avant de lancer son exploit. Il cherche une porte d'entrée technique ou humaine. Et les portes d'entrée techniques se trouvent dans les configurations, les versions logicielles, les droits d'accès, les humaines dans les comportements des utilisateurs — pas dans les politiques de sécurité archivées dans un serveur documentaire.

Pourquoi ce malentendu persiste-t-il ?

La persistance de cette confusion n'est pas accidentelle. Elle s'explique par plusieurs dynamiques convergentes qu'il serait naïf d'ignorer.

Les **régulateurs**, confrontés à l'impossibilité pratique d'évaluer le niveau de sécurité réel de milliers d'organisations, se replient sur des indicateurs vérifiables : la présence de documents, l'existence de processus, la réalisation d'audits. Ce sont des approches imparfaites de la sécurité, mais ce sont des approches mesurables et quantifiables.

Les **conseils d'administration et les directions générales**, pour leur part, trouvent dans la conformité certifiée une forme de confort juridique et réputationnel. Être certifié conforme offre une protection partielle en cas d'incident : elle démontre la bonne foi de l'organisation et peut limiter les sanctions. Elle ne prévient pas l'incident lui-même, mais elle en réduit les conséquences juridiques. Ce calcul, aussi rationnel soit-il à l'échelle individuelle, est collectivement désastreux : il détourne des ressources de la prévention effective vers la gestion du risque juridique.

Enfin, un **écosystème de conseil et d'audit** s'est développé autour de la conformité réglementaire, dont la valeur commerciale repose précisément sur la complexité et la prolifération des normes. Chaque nouveau règlement génère une nouvelle demande de conseil, de formation, d'audit et de certification. Il serait excessif d'affirmer que cet écosystème est responsable de la saturation normative — les régulateurs ont leurs propres logiques. Mais il contribue à entretenir l'équation implicite selon laquelle *plus de conformité équivaut à plus de sécurité.*

> L'illusion la plus coûteuse : confondre conformité et sécurité. Une entreprise peut être 100 % conforme au RGPD et à DORA, et succomber le lendemain à un ransomware — parce que ses ressources étaient mobilisées sur la documentation juridique plutôt que sur l'hygiène informatique de base.

Nommer le problème pour mieux le résoudre

Les trois dynamiques analysées dans cette partie — la Compliance Fatigue, la surtransposition française et l'illusion de la sécurité par le texte — ne sont pas des phénomènes indépendants. Ils sont les manifestations d'une même pathologie systémique : **la substitution de la forme à la substance** dans la gouvernance de la cybersécurité.

Cette pathologie n'est pas une fatalité. Elle est le produit de choix — de conception réglementaire, de politique publique, de gouvernance d'entreprise — qui peuvent être revisités. Mais elle ne peut être corrigée que si elle est d'abord nommée clairement, sans euphémisme et sans déférence excessive pour des institutions qui, malgré leur bonne foi, ont produit un système qui dessert les objectifs qu'il prétend servir.

La question qui se pose au Législateur n'est pas : faut-il moins réguler mais comment réguler mieux, pour que la régulation serve effectivement la sécurité nationale, la résilience des organisations et la compétitivité de l'économie française ?

Cette tribune s'adressant aux dirigeants d'entreprise, la vraie question est comment satisfaire aux exigences et contraintes réglementaires tout en étant réellement résilient ?

La réponse exige un changement de para-

digme. Ce changement doit être fondé sur la convergence plutôt que sur l'accumulation, sur l'opérationnel plutôt que sur le déclaratif, sur la confiance construite plutôt que sur la conformité affichée.

Et si le Comité Exécutif se posait 3 bonnes questions

— Quelle proportion du budget cybersécurité est aujourd'hui consacrée à la conformité documentaire vs. à la protection opérationnelle ?

— Combien de régulateurs différents imposent des rapports distincts sur les mêmes incidents ?

— Votre RSSI pilote-t-il votre résilience réelle, ou votre bureaucratie réglementaire ?

La vision : Fusionner pour régner — le « Single Compliance Stack »

« La complexité est l'ennemie de l'exécution. Et dans le domaine de la sécurité, l'inexécution coûte des systèmes, des données, et parfois des vies. »

La partie précédente a établi un diagnostic sans concession : la prolifération normative, loin de renforcer la résilience des organisations françaises, crée une saturation qui détourne les ressources de la défense active, pénalise la compétitivité et entretient une illusion de sécurité fondée sur la conformité documentaire plutôt que sur la robustesse technique.
Ce constat appelle une réponse à la hauteur de l'enjeu. Non pas un allégement de la régulation — qui laisserait le champ libre aux comportements opportunistes et affaiblirait la protection collective —, mais une refondation architecturale de la manière dont les exigences réglementaires sont conçues, structurées et opérationnalisées au sein des organisations.

Cette refondation repose sur une idée centrale, aussi simple dans sa formulation qu'ambitieuse dans sa mise en œuvre : **unifier plutôt qu'empiler**. Là où le système actuel accumule des silos normatifs qui s'ignorent mutuellement, la vision défendue dans ce chapitre propose de construire un socle commun — un Single Compliance Stack, ou référentiel de conformité unifié — sur lequel toutes les exigences réglementaires pertinentes viendraient s'articuler de manière cohérente, lisible et efficiente.

Cette vision s'articule autour de trois transformations complémentaires et une approche holistique :

1. L'harmonisation des contrôles selon le principe Control Once, Comply Many
2. La création d'un Registre Universel des Actifs Numériques offrant une cartographie unifiée et dynamique
3. L'émergence d'une véritable *ingénierie de gouvernance intégrée* incarnée par une nouvelle fonction stratégique, celle de Chief Trust & Resilience Officer[3].

L'harmonisation des contrôles : « Control Once, Comply Many »

Une évidence technique que la régulation n'a pas encore intégrée

3. Voir mes différents articles sur LinkedIn

Tout professionnel de la sécurité informatique qui travaille au quotidien avec plusieurs cadres réglementaires finit par observer la même chose : *les exigences se répètent*. La gestion des identités et des accès est requise par le RGPD pour protéger les données personnelles, par NIS2 pour sécuriser les systèmes essentiels, par DORA pour garantir la résilience opérationnelle des entités financières, et demain par le CRA pour les produits connectés. La journalisation des événements de sécurité, le chiffrement des données sensibles, la gestion des correctifs, la détection des incidents — tous ces contrôles techniques fondamentaux apparaissent, sous des formulations variées et avec des nuances de périmètre, dans la quasi-totalité des textes réglementaires en vigueur.
Cette redondance n'est pas en soi problématique, mais elle reflète une réalité : les bonnes pratiques de sécurité sont universelles, et les régulateurs, chacun depuis son périmètre sectoriel, convergent naturellement vers les mêmes exigences techniques. Le problème n'est pas dans la convergence des exigences, mais dans l'**absence d'architecture commune** qui permettrait de capitaliser sur cette convergence. Faute d'un référentiel unifié, chaque réglementation impose sa propre terminologie, ses propres preuves, ses propres formats d'audit — et les organisations se retrouvent à produire plusieurs fois le même effort pour démontrer ce qui est, au fond, la même réalité.
Le principe **Control Once, Comply Many** — que l'on peut traduire par « contrôler une fois, satisfaire plusieurs exigences » — vise à corriger cette inefficience structurelle. Il postule qu'un contrôle technique bien documenté, réalisé selon des standards ouverts et reconnus, devrait pouvoir servir de preuve simultanée pour l'ensemble des régulateurs auxquels l'organisation est soumise. En d'autres termes : **une seule réalité technique, une seule démonstration, une reconnaissance croisée par l'ensemble des autorités compétentes**.

Comment cela fonctionne-t-il concrètement ?

Prenons l'exemple de la gestion des accès privilégiés à un système d'information — ce que les spécialistes appellent le *Privileged Access Management*, ou PAM. Ce contrôle consiste à s'assurer que seules les personnes autorisées peuvent accéder aux ressources les plus sensibles d'une organisation, que ces accès sont tracés, limités dans le temps, et révoqués dès qu'ils ne sont plus nécessaires. Ce contrôle est requis, sous des angles légèrement différents, par le RGPD (protection des données personnelles accessibles par des administrateurs), par NIS2 (sécurisation des systèmes essentiels contre les compromissions de comptes privilégiés), par DORA, et par les référentiels techniques de l'ANSSI[4]. Dans le système actuel, une organisation soumise à ces quatre cadres devra, dans bien des cas, produire quatre séries de preuves distinctes, participer à quatre processus d'audit potentiellement non coordonnés, et maintenir quatre cartographies de ses droits d'accès en format différent.

Dans l'architecture *Control Once, Comply Many*, cette même organisation réalise un **seul audit de sa gestion des accès privilégiés**, selon un référentiel de contrôles commun — par exemple, en s'appuyant sur les standards internationaux ISO 27001 ou sur le Cybersecurity Framework du NIST[5], enrichis des spécificités européennes. Les conclusions de cet audit, structurées selon une taxonomie partagée par les différentes autorités de régulation, sont ensuite **reconnues simultanément** comme preuve de conformité par l'ensemble des régulateurs concernés.

Un exemple particulièrement parlant pour illustrer les gains opérationnels : imaginez un audit unique du service d'annuaire d'entreprise — le système qui gère les identités numériques et les droits d'accès dans les entreprises — dont les conclusions seraient valables à la fois pour répondre aux exigences prudentielles de

4. Agence Nationale de la Sécurité des Systèmes d'Information
5. Cadre normatif s'imposant aux administrations fédérales américaines

l'ACPR[6]/AMF[7] dans le cadre de DORA, aux critères de gouvernance des systèmes algorithmiques imposés par l'AI Act, et aux obligations de sécurité des systèmes d'information essentiels prévues par NIS2. Un seul audit, une seule mobilisation des équipes techniques, une seule production documentaire — et trois exigences réglementaires satisfaites simultanément.

Les conditions de réussite

Ce principe, aussi séduisant soit-il, ne peut fonctionner que sous certaines conditions qui relèvent autant de la volonté politique que de l'ingénierie réglementaire.

La première condition est l'**existence d'un référentiel de contrôles commun**, reconnu par l'ensemble des autorités compétentes — ANSSI, CNIL, ACPR, AMF — et aligné sur les standards européens et internationaux. Ce référentiel doit être suffisamment précis pour être auditable, suffisamment flexible pour s'adapter à des contextes organisationnels variés, et suffisamment stable pour ne pas nécessiter une révision permanente.

La deuxième condition est la **reconnaissance mutuelle des preuves** entre régulateurs. Cela suppose un accord institutionnel fort, potentiellement formalisé dans un texte législatif ou réglementaire, qui définit les conditions dans lesquelles un audit réalisé selon le référentiel commun vaut preuve de conformité vis-à-vis de chacune des autorités signataires. Sans cet accord, le référentiel commun risque de s'ajouter aux exigences existantes plutôt que de les remplacer — reproduisant exactement le problème qu'il est censé résoudre.

La troisième condition est **la formation et l'acculturation** des équipes d'audit et d'inspection des régulateurs eux-mêmes, afin qu'ils soient en mesure d'interpréter des preuves produites selon un format unifié plutôt que selon leurs propres formats sectoriels habituels. Ce point, souvent négligé dans les réflexions sur l'harmonisation, est pourtant déterminant pour le succès opérationnel de la démarche.

Le Registre Universel des Actifs Numériques

Le problème de la cartographie fragmentée

On ne peut pas protéger ce qu'on ne voit pas. Cette maxime, universellement admise dans la communauté de la cybersécurité, devrait être le point de départ de toute réflexion sur la gouvernance des risques numériques. Or, dans la grande majorité des organisations françaises soumises à plusieurs cadres réglementaires, la connaissance de leurs propres actifs numériques est fragmentée entre plusieurs inventaires qui ne se parlent pas.

Le délégué à la protection des données — le DPO — maintient un **registre des traitements** qui recense les données personnelles collectées, les finalités de leur traitement, les durées de conservation et les destinataires. Ce registre est exigé par le RGPD et constitue un outil précieux pour la gouvernance des données. Mais il ne contient pas d'information sur les systèmes techniques qui hébergent ces données, ni sur les interconnexions entre ces systèmes.

Le RSSI, de son côté, maintient une **cartographie des systèmes d'information** qui recense les serveurs, les applications, les flux de données et les points d'interconnexion. Cette cartographie est indispensable à la gestion des vulnérabilités et à la réponse aux incidents. Mais elle intègre rarement les qualifications réglementaires des données traitées par chaque sys-

6. Autorité de contrôle prudentiel et de résolution
7. Autorité des Marchés Financiers

tème.

Le responsable de la conformité à l'AI Act, dans les organisations qui utilisent des systèmes d'intelligence artificielle à haut risque, tient un **inventaire des algorithmes** qui recense les modèles déployés, leurs finalités, leurs données d'entraînement et leurs performances. Cet inventaire, encore souvent embryonnaire dans les organisations françaises, est généralement déconnecté des deux précédents.

Enfin, dans les organisations soumises à DORA, un **registre des fonctions critiques ou importantes et des tiers TIC**[8] recense les processus métiers essentiels et les prestataires qui en assurent la continuité. Ce registre obéit à sa propre logique et à ses propres formats.

Le résultat de cette fragmentation est prévisible : lorsqu'un incident survient, ou lorsqu'une décision stratégique doit être prise sur un système donné, les équipes doivent reconstituer en urgence une vision d'ensemble à partir de sources dispersées, souvent incohérentes entre elles, parfois contradictoires. C'est une perte de temps considérable dans des situations qui n'en tolèrent pas.

La vision : une cartographie unique, dynamique et partagée

Le **Registre Universel des Actifs Numériques** — que l'on peut abréger en RUAN — est la réponse structurelle à cette fragmentation. Il s'agit d'une base de données unifiée qui recense l'ensemble des actifs numériques d'une organisation — données, systèmes, algorithmes, interconnexions, prestataires — en leur associant simultanément leurs qualifications selon chaque cadre réglementaire applicable.

L'ambition du RUAN n'est pas de créer un nouveau silo qui viendrait s'ajouter aux précédents, mais de **fusionner les inventaires existants** en une source de vérité unique, mise à jour en temps réel, et accessible à l'ensemble des fonctions qui en ont besoin — DPO, RSSI, Risk Manager, TPRM[9], auditeurs internes, et, en lecture adaptée, régulateurs.
Concrètement, chaque actif numérique enregistré dans le RUAN se voit attribuer un ensemble de **tags réglementaires** qui indiquent, pour cet actif spécifique, les régimes applicables et les niveaux d'exigence correspondants. Une base de données clients, par exemple, sera taguée simultanément comme actif critique au sens de DORA (si son indisponibilité compromet une fonction critique ou importante), comme traitement de données sensibles au sens du RGPD (car elle contient des données à caractère personnel), et comme jeu d'entraînement potentiel au sens de l'AI Act (si elle est utilisée pour entraîner ou affiner des modèles algorithmiques).

Ce *tagging* croisé transforme la cartographie d'un exercice administratif en **outil de pilotage stratégique**. Lorsqu'une décision est prise de migrer cette base de données vers un nouveau prestataire cloud, le RUAN permet d'identifier instantanément l'ensemble des implications réglementaires de cette décision — et donc d'anticiper les diligences nécessaires, d'informer les bonnes fonctions, et de planifier les actions de mise en conformité sans avoir à reconstituer le puzzle à chaque fois.

Un registre vivant, pas un document figé

La différence fondamentale entre le RUAN et les inventaires existants ne tient pas seulement à son caractère unifié, mais à son caractère **dynamique**. Les inventaires réglementaires actuels sont, dans la plupart des organisations, des documents mis à jour périodiquement —

8. Technologies de l'Information et de la Communication
9. Third Party Risk Manager

souvent annuellement, parfois plus fréquemment pour les organisations les plus matures — mais qui restent des photographies d'un état à un instant donné.

Or, les environnements numériques évoluent en permanence. De nouveaux systèmes sont déployés, des données migrent d'un système à l'autre, des prestataires changent, des algorithmes sont mis à jour. Un inventaire statique est donc structurellement en retard sur la réalité qu'il est censé décrire. Le RUAN, dans sa conception cible, s'appuie sur des **mécanismes d'alimentation automatisée** — interfaces avec les outils de gestion du patrimoine applicatif, avec les plateformes de gestion des vulnérabilités, avec les outils de découverte des données — pour maintenir une cartographie qui reflète en temps quasi-réel l'état effectif du système d'information. Cette automatisation réduit considérablement la charge de maintenance qui, dans les systèmes actuels, est l'une des principales raisons pour lesquelles les inventaires finissent par être abandonnés ou négligés.

La technologie nécessaire à la mise en œuvre de cette vision existe aujourd'hui. Des plateformes de *Security Asset Management*, combinées à des outils de *Data Discovery* et à des référentiels de *Configuration Management Database* (CMDB), permettent d'approcher cette vision à un niveau de maturité satisfaisant. Ce qui manque n'est pas la technologie, mais la **décision organisationnelle et politique** d'unifier des inventaires qui ont été construits séparément, par des fonctions différentes, selon des logiques différentes, et dont les propriétaires respectifs peuvent percevoir la fusion comme une perte d'autonomie ou de périmètre.

La Gouvernance Intégrée : vers le « Chief Trust & Resilience Officer »

Le morcellement gouvernemental comme miroir du morcellement normatif

L'organisation des fonctions de conformité et de sécurité au sein des entreprises françaises reflète fidèlement — et aggrave — le morcellement du paysage réglementaire. Dans une grande organisation soumise à l'ensemble des cadres évoqués dans ce livre blanc, on trouve généralement au moins quatre fonctions distinctes dont les périmètres se chevauchent sans jamais véritablement se coordonner.

Le Délégué à la Protection des Données — DPO — est le gardien du RGPD. Nommé par obligation légale dans les organisations qui traitent des données personnelles à grande échelle, il rapporte souvent à la direction juridique et dispose d'une ligne directe avec la CNIL. Sa préoccupation centrale est la licéité et la proportionnalité des traitements de données.

Le **Responsable de la Sécurité des Systèmes d'Information — RSSI** — est le gardien de la sécurité des systèmes d'information. Il rapporte tantôt à la direction des systèmes d'information, tantôt à la direction des risques et beaucoup plus rarement à la direction générale. Sa préoccupation centrale est la protection des systèmes contre les menaces. Il interagit principalement avec l'ANSSI et, dans les secteurs régulés, avec les autorités sectorielles.

Le **Risk Manager** gère le cadre global de gestion des risques opérationnels et financiers. Il rapporte généralement à la direction des risques, et sa préoccupation centrale est la quantification et la mitigation des risques susceptibles d'affecter la performance ou la solvabilité de l'organisation.

Enfin, dans les organisations ayant développé des usages significatifs de l'intelligence artificielle, un **responsable de la conformité IA** — parfois intégré à la fonction juridique, parfois rattaché à la direction de l'innovation — commence à émerger pour gérer les implications de l'IA Act.

Ces quatre fonctions, dans la configuration actuelle, opèrent le plus souvent en **silos parallèles**. Elles partagent peu de données, se réunissent rarement ensemble, et peuvent parfois développer des positions contradictoires sur des sujets d'intérêt commun. Un exemple fréquemment observé : le RSSI préconise le chif-

frement systématique de certaines catégories de données pour des raisons de sécurité, tandis que le DPO s'interroge sur la compatibilité de ce chiffrement avec les droits d'accès des personnes concernées ; pendant ce temps, le Risk Manager intègre le risque de chiffrement défaillant dans son modèle sans coordination avec les deux autres ; et le responsable IA n'a pas été consulté alors que les données concernées servent à l'entraînement d'un algorithme.

Ce morcellement gouvernemental n'est pas seulement une source d'inefficience. Il est une source de risque : les angles morts naissent précisément dans les espaces entre les silos, là où personne ne regarde parce que chacun croit que l'autre s'en charge.

La figure du « Chief Trust & Resilience Officer »

La réponse à ce morcellement est l'émergence d'une nouvelle fonction stratégique : **le Chief Trust & Resilience Officer**, ou CTRO [10]. Cette appellation, encore peu répandue en France mais qui gagne du terrain dans les organisations les plus avancées en matière de gouvernance intégrée, désigne un **dirigeant** dont la responsabilité est de **piloter de manière transverse l'ensemble des risques numériques** de l'organisation, en décloisonnant les fonctions qui les gèrent.

Le CTRO n'est pas un super-RSSI, ni un DPO élargi, ni un Risk Manager rebaptisé. C'est une **fonction de synthèse et d'arbitrage stratégique**, qui dispose d'une autorité fonctionnelle sur l'ensemble des responsables de conformité et de sécurité, et qui répond directement au Directeur Général ou au Conseil d'Administration. Son rôle est de s'assurer que les différentes fonctions travaillent à partir d'une vision commune des risques, que leurs arbitrages sont cohérents entre eux, et que les ressources allouées à la conformité et à la sécurité sont optimisées à l'échelle de l'organisation plutôt que défendues de manière silotée par chaque fonction.

Il est utile de préciser ici ce que **ce rôle n'est pas** : il ne s'agit pas de supprimer les fonctions existantes de DPO, RSSI ou Risk Manager — chacune dispose d'une expertise irremplaçable et, pour certaines d'entre elles, d'obligations légales d'indépendance qui doivent être préservées. Il s'agit de créer au-dessus d'elles — ou mieux, autour d'elles — une fonction d'intégration qui permette à chacune de rester experte dans son domaine tout en contribuant à une vision collective de la résilience organisationnelle.

Une instance de décision unique pour le Board

L'une des manifestations les plus concrètes de la gouvernance intégrée est la **transformation de la structure des comités de pilotage réglementaires**. Dans la configuration actuelle, les conseils d'administration et les comités exécutifs des grandes organisations françaises reçoivent régulièrement des rapports distincts — et souvent non coordonnés — de leurs différentes fonctions de conformité et de sécurité. Un comité des risques traitera du risque de cybersécurité selon la grille du RSSI. Un comité de conformité traitera des risques RGPD selon la grille du DPO. Un comité d'audit traitera des risques opérationnels selon la grille du Risk Manager.

Il n'est pas rare que ces trois comités se réunissent dans le même mois et présentent des évaluations contradictoires sur le même sujet — par exemple, le niveau de risque associé à un prestataire cloud — sans que quiconque soit en mesure de synthétiser ces évaluations en une position cohérente sur laquelle le Board puisse prendre une décision éclairée.

10. Ou, en bon français, Directeur de la Confiance et de la Résilience Numériques

La gouvernance intégrée propose de **fusionner ces instances en un comité unique de résilience numérique**, qui présente au Board une vision consolidée des risques numériques de l'organisation — couvrant simultanément les dimensions technique, réglementaire, opérationnelle et stratégique — et qui formule des recommandations d'arbitrage cohérentes, hiérarchisées et directement actionnables.

Ce faisant, elle résout un problème que les dirigeants connaissent bien : la difficulté à prendre des décisions sur des sujets techniques complexes lorsque les experts qu'ils consultent leur fournissent des éclairages partiels et parfois contradictoires. En disposant d'une instance unique, pilotée par un CRO dont le mandat est précisément d'intégrer ces perspectives, le Board gagne en **clarté décisionnelle** sans perdre en profondeur d'analyse.

Un exemple concret illustre ce gain : une organisation envisage d'adopter une solution d'intelligence artificielle pour automatiser certaines décisions de crédit. Dans le système actuel, cette décision sera analysée séparément par le responsable IA (conformité à l'AI Act), le DPO (impacts RGPD sur les décisions automatisées), le RSSI (risques de sécurité de la solution), et le Risk Manager (risques opérationnels et réputationnels). Ces analyses arrivent au Board de manière séquentielle ou simultanée mais non synthétisée, créant une confusion pour les dirigeants.

Dans le modèle de gouvernance intégrée, le CTRO présente une **analyse unique et consolidée**, qui intègre l'ensemble de ces dimensions, identifie les arbitrages nécessaires — par exemple, l'équilibre entre la performance du modèle et les exigences d'explicabilité imposées par l'AI Act — et propose une recommandation qui tient compte simultanément de toutes les contraintes.
Le Board décide. La décision s'exécute.

Une architecture de la cohérence

Les trois piliers de la vision présentée dans ce chapitre — le référentiel de contrôles unifié, le Registre Universel des Actifs Numériques, et la gouvernance intégrée portée par le Chief Resilience Officer — ne sont pas des innovations technologiques. Ce sont des **innovations organisationnelles et institutionnelles**, qui requièrent davantage de volonté managériale et politique que d'investissement technologique.

Leur point commun est de substituer à la logique d'accumulation — empiler des textes, multiplier les inventaires, proliférer les comités — une logique de cohérence architecturale : moins de couches, mais des couches qui fonctionnent ensemble ; moins de preuves, mais des preuves qui valent pour tous ; moins d'instances de pilotage, mais des instances qui voient l'ensemble.

Cette vision est-elle utopique ? Certains le diront. Ils invoqueront les résistances institutionnelles, les prérogatives des régulateurs, les cultures organisationnelles silotées, la complexité juridique d'une reconnaissance mutuelle entre autorités. Ces objections sont réelles. Elles ne sont pas insurmontables.

> Il existe déjà des convergences normatives analogues : un SMSI (ISO 27001 – sécurité des SI) et un SMIA (ISO 42001 – systèmes d'IA) peuvent être conçus et gérés de manière entièrement mutualisée — même équipe, même documentation socle, même cycle d'audit. La convergence n'est pas un idéal, c'est une réalité opérationnelle.

Rationaliser l'opérationnel : Mutualiser pour gagner en agilité

« Une contrainte bien organisée devient une discipline. Une discipline bien automatisée devient un avantage compétitif. »

Les deux parties précédents ont posé le diagnostic et esquissé la vision. La première a démontré que la saturation normative produit des effets inverses à ceux qu'elle recherche. La seconde a proposé une architecture de cohérence — un socle commun de contrôles, un registre unifié des actifs, une gouvernance intégrée — capable de transformer le millefeuille en levier de résilience. Il reste maintenant à répondre à la question la plus immédiate, celle que posent les directeurs opérationnels, les responsables de conformité et les équipes de terrain : *concrètement, par où commencer, et comment faire ?*

Cette troisième partie descend au niveau de l'exécution. Il ne s'agit plus d'architecture conceptuelle, mais de **transformation opérationnelle** — des processus à réorganiser, des outils à déployer, des cultures à faire évoluer. Il s'adresse autant aux équipes qui vivent au quotidien le poids de la conformité qu'aux dirigeants qui cherchent à comprendre comment convertir une contrainte réglementaire croissante en source d'efficience et, à terme, en différenciateur compétitif. Trois leviers opérationnels structurent cette transformation : la mutualisation de la gestion des risques liés aux tiers — fournisseurs, prestataires, partenaires — à travers un cadre unifié ; la refonte de la culture de sécurité au sein des organisations, pour en faire un programme intégré plutôt qu'une succession de formations cloisonnées ; et l'automatisation de la conformité, qui permet de passer d'une photographie périodique et coûteuse à un tableau de bord vivant, utile au pilotage business en temps réel.

La gestion unifiée du risque tiers : mettre fin au harcèlement *questionnairiste*

Le fournisseur sous le feu croisé des questionnaires

Il existe, dans la relation entre grandes organisations et leurs fournisseurs de services numériques, une pratique aussi répandue qu'inefficace : le **questionnaire de sécurité**. Chaque client adresse à chaque fournisseur son propre questionnaire, élaboré selon sa propre interprétation des réglementations applicables, dans son propre format, selon son propre calendrier. Un fournisseur de services cloud de taille intermédiaire, qui dessert plusieurs centaines de clients relevant de secteurs régulés différents — finance, santé, énergie, administration publique — peut se retrouver à répondre simultanément à plusieurs dizaines de questionnaires distincts par an, portant tous, au fond, sur les mêmes sujets : la sécurité de ses infrastructures, la protection des données qu'il héberge, la résilience de ses services, et la conformité de ses pratiques aux principales réglementations européennes.

Ce phénomène a un nom dans la communauté professionnelle : le questionnaire fatigue, ou *fatigue questionnairiste*. Il désigne l'état d'épuisement administratif des équipes conformité des fournisseurs, condamnées à passer une part considérable de leur temps à répondre à des questionnaires redondants plutôt qu'à améliorer effectivement leur niveau de sécurité. Pour les fournisseurs de taille modeste — les PME et ETI du tissu numérique français —, cette charge peut représenter un frein réel à leur développement commercial, voire une barrière à l'entrée sur certains marchés. Et pour les clients qui envoient ces questionnaires, la valeur reçue en retour est souvent décevante : des réponses génériques, produites à la chaîne, qui ne reflètent pas nécessairement la réalité de la sécurité du fournisseur.

Le contexte réglementaire accentue ce problème. La directive NIS2 impose aux opérateurs d'entités essentielles et importantes de gérer

les risques liés à leur chaîne d'approvisionnement numérique. DORA impose aux entités financières des exigences détaillées de diligence sur leurs prestataires tiers de services informatiques. Le CRA impose aux fabricants et distributeurs de produits connectés des exigences de sécurité tout au long du cycle de vie. Le RGPD impose des contrats de traitement de données avec chaque sous-traitant.FIDA impose des exigences supplémentaires sur les prestataires manipulant des données financières sensibles.

Chacune de ces réglementations impose, de manière indépendante, des diligences sur les tiers. En l'absence de coordination, chaque client interprète ces diligences à sa manière et produit son propre questionnaire. Le fournisseur répond à chacun séparément. Tout le monde perd du temps.
Personne n'est plus en sécurité.

Le passeport de conformité fournisseur : une solution à portée de main

La réponse opérationnelle à ce problème est le **passeport de conformité fournisseur** — ou, dans une terminologie plus technique, le cadre unifié de Third Party Risk Management, abrégé en TPRM. L'idée est d'une simplicité désarmante : **un fournisseur ne devrait remplir qu'une seule auto-évaluation standardisée**, structurée autour d'un référentiel de contrôles commun, reconnue par l'ensemble de ses clients pour satisfaire simultanément leurs obligations de diligence respectives.

Ce passeport couvrirait, selon une taxonomie commune et reconnue, l'ensemble des dimensions réglementaires pertinentes : la sécurité des produits au titre du CRA, la protection des données au titre du RGPD, la résilience opérationnelle au titre de NIS2 et de DORA, et les exigences d'accès aux données au titre de FIDA. Il serait structuré de manière à ce que chaque client puisse extraire, depuis cette évaluation unique, les éléments de preuve correspondant à ses propres obligations réglementaires spécifiques.

Le gain est immédiat et concret pour toutes les parties. **Pour le fournisseur**, la charge administrative est drastiquement réduite : une seule évaluation, mise à jour périodiquement et complétée en cas d'incident significatif, remplace des dizaines de questionnaires disparates. Les ressources libérées peuvent être réinvesties dans l'amélioration effective de la posture de sécurité. **Pour le client**, la qualité de l'information reçue s'améliore : une évaluation approfondie, réalisée dans un cadre rigoureux et vérifiable, vaut infiniment plus que cent questionnaires remplis à la hâte. **Pour le régulateur**, la lisibilité du marché s'améliore : lorsque l'ensemble des acteurs utilisent le même référentiel, il devient possible d'identifier des tendances systémiques, de détecter des vulnérabilités communes et d'orienter les actions de supervision de manière plus ciblée.

Concrètement, un prestataire cloud soumis au CRA pour ses produits et à NIS2 pour ses services ne remplit plus qu'une seule auto-évaluation standardisée. Celle-ci couvre simultanément ses exigences de sécurité produit au titre du CRA — gestion des vulnérabilités, mises à jour de sécurité, documentation technique —, et ses obligations de résilience de service au titre de NIS2 — continuité, gestion des incidents, sécurité de la chaîne d'approvisionnement. Le client, en accédant à cette évaluation unique via une plateforme partagée, peut valider en quelques minutes ce qu'il lui faudrait auparavant plusieurs semaines de questionnaires pour établir.

Les modèles existants dont s'inspirer

Cette vision n'est pas sans précédent. Plusieurs initiatives ont déjà démontré la faisabilité du concept, à différentes échelles. Le programme **CAIQ** (*Consensus Assessments Initiative Questionnaire*) de la **Cloud Security Alliance** propose un questionnaire standardisé pour les fournisseurs cloud, reconnu par un nombre croissant d'organisations mondiales. Le cadre **Shared Assessments** aux États-Unis a développé une méthodologie d'évaluation mutualisée des tiers, adoptée par plusieurs centaines de grandes organisations financières. En Europe, le programme **GAIA-X** a entrepris de définir des référentiels communs pour la qualification des fournisseurs cloud européens, même si son déploiement opérationnel reste à consolider.

Ce que la France — et l'Europe — doit faire, c'est **passer de l'initiative sectorielle à la norme institutionnelle** : mandater ou fortement inciter les régulateurs sectoriels à reconnaître mutuellement un référentiel commun d'évaluation des tiers, et créer les conditions d'une adoption généralisée par les acteurs du marché. L'ANSSI, en tant qu'autorité nationale de cybersécurité, est naturellement positionnée pour porter ce chantier, en coordination avec la CNIL, l'ACPR et les autres autorités compétentes.

La culture de sécurité « All-in-One » : former une fois, comprendre tout

Le désert pédagogique des formations cloisonnées

La sensibilisation des collaborateurs aux risques numériques est, dans la quasi-totalité des organisations françaises, organisée selon une logique qui reproduit fidèlement — et aggrave — le morcellement réglementaire dénoncé dans ce livre blanc. Les collaborateurs reçoivent, au fil de l'année, une formation RGPD dispensée par le DPO ou son équipe, une formation de sensibilisation à la cybersécurité organisée par le RSSI, une formation sur les risques de l'intelligence artificielle portée par la direction juridique ou la direction de l'innovation, et peut-être, dans les secteurs financiers, une formation spécifique sur les obligations DORA.

Chacune de ces formations est conçue de manière indépendante, avec ses propres supports, ses propres intervenants, ses propres modalités pédagogiques et ses propres indicateurs de réussite. Elles se succèdent dans le calendrier des collaborateurs sans que jamais personne ne leur explique les liens qui les unissent. Le résultat est prévisible : une **saturation pédagogique** qui produit une mémorisation faible, une application encore plus faible, et une conviction croissante chez les collaborateurs que ces formations sont des obligations administratives à traverser plutôt que des apprentissages utiles à leur travail quotidien.

Cette fragmentation pédagogique a une conséquence opérationnelle grave : elle crée des **angles morts comportementaux**. Un collaborateur correctement formé au RGPD peut ignorer qu'envoyer un fichier client dans un outil d'intelligence artificielle grand public constitue simultanément une violation de données personnelles, un risque de sécurité et une infraction aux obligations de l'AI Act. Il n'a pas fait le lien parce que personne ne lui a montré que ces trois dimensions étaient, dans sa réalité quotidienne, inséparables.

Un programme intégré d'acculturation numérique

La vision alternative est celle d'un **programme unique et intégré d'acculturation au numérique**, qui traite la protection des données, la cybersécurité et les risques de l'intelligence artificielle comme un continuum cohérent plutôt que comme trois disciplines juxtaposées. Ce programme ne supprime pas la profondeur thématique — il est toujours nécessaire que les collaborateurs comprennent les spécificités de chaque domaine — mais il les inscrit dans une

narration commune centrée sur les comportements attendus dans des situations de travail réelles.

La clé pédagogique de cette approche est le **scénario intégré** : plutôt que d'enseigner le RGPD en tant que corpus juridique, la cybersécurité en tant que discipline technique et l'AI Act en tant que régulation sectorielle, le programme place le collaborateur dans des situations concrètes qui font apparaître simultanément les trois dimensions. L'apprentissage se construit autour de la réalité du risque, pas autour de la structure administrative des textes.

L'exercice de simulation d'hameçonnage illustre parfaitement ce potentiel pédagogique intégré. Un hameçonnage est une technique d'attaque qui consiste à tromper un collaborateur pour qu'il clique sur un lien malveillant ou divulgue des informations sensibles, en se faisant passer pour un expéditeur de confiance. Ces simulations sont déjà largement utilisées dans les programmes de sensibilisation à la cybersécurité. Mais leur potentiel pédagogique est généralement limité à la détection du message frauduleux et au signalement à l'équipe de sécurité.

Un scénario de simulation enrichi pourrait faire bien davantage. Imaginez un exercice dans lequel un collaborateur reçoit un message frauduleux l'invitant à partager un document client via une plateforme non approuvée. La simulation enseigne simultanément : la détection du message suspect et le signalement à l'équipe de sécurité — compétence requise par DORA pour la gestion des incidents ; l'identification des données personnelles contenues dans le document et la compréhension du risque de fuite — compétence requise par le RGPD ; et la sensibilisation au risque que représente le partage de données avec des outils d'IA non maîtrisés, notamment des modèles de langage grand public — risque émergent couvert par l'AI Act et les politiques internes sur l'usage de l'IA.

Un seul scénario, trente minutes de formation, trois dimensions réglementaires couvertes. Le gain est non seulement quantitatif — moins de temps de formation pour une couverture équivalente ou supérieure — mais surtout qualitatif : le collaborateur comprend la cohérence de ces risques dans sa vie professionnelle quotidienne, ce qui ancre les comportements appris bien plus efficacement qu'une succession de modules abstraits.

Construire une culture, pas remplir des obligations

Cette approche pédagogique intégrée n'est pas seulement plus efficiente. Elle vise un objectif plus ambitieux que la simple conformité : **construire une culture organisationnelle de la résilience numérique**, dans laquelle chaque collaborateur comprend son rôle dans la chaîne de protection collective et agit en conséquence, non par obligation réglementaire, mais par conscience professionnelle.

La différence entre une organisation qui « fait de la sensibilisation » et une organisation qui a développé une culture de sécurité est fondamentale. Dans la première, les collaborateurs savent ce qu'ils sont censés faire parce qu'on le leur a dit. Dans la seconde, ils savent *pourquoi* ils doivent le faire, et cette compréhension les rend capables d'adapter leur comportement à des situations nouvelles que le programme de formation n'avait pas anticipées — y compris face à des menaces émergentes, des usages technologiques inédits ou des contextes de travail qui évoluent rapidement.

Dans un environnement numérique où les menaces se renouvellent plus vite que les formations ne peuvent être mises à jour, cette capacité d'adaptation culturelle est un **actif stratégique** dont la valeur dépasse largement le coût du programme qui la forge.

L'automatisation de la conformité : du tableau de bord statique au pilotage en temps réel

La conformité comme photographie : une métaphore dépassée

La manière dont la conformité réglementaire est traditionnellement évaluée et démontrée repose sur une métaphore implicite : celle de la photographie. À intervalles réguliers — annuellement pour la plupart des certifications, trimestriellement pour certains reporting réglementaires —, l'organisation mobilise ses équipes pour produire une évaluation de son état de conformité à un instant donné. Cette évaluation est documentée, validée, présentée aux auditeurs et archivée. Jusqu'à la prochaine.

Cette approche présente une limite fondamentale qui est rarement explicitée : **elle mesure le passé, pas le présent**. Un rapport de conformité produit en décembre ne dit rien sur l'état de sécurité de l'organisation en mars. Entre ces deux dates, des systèmes ont été modifiés, des configurations ont évolué, des correctifs n'ont pas été appliqués, des comptes d'accès n'ont pas été révoqués. L'organisation croit être conforme parce qu'elle l'était il y a trois mois. Elle ne l'est peut-être plus.

Cette déconnexion entre la réalité opérationnelle et son image réglementaire est l'une des causes les plus fréquentes des incidents de sécurité dans des organisations apparemment bien conformes : l'écart s'est creusé, silencieusement, entre deux photographies.

Le « *Compliance-as-Code* » : une conformité qui se surveille elle-même

La réponse technologique à ce problème porte un nom qui peut sembler abstrait mais dont le contenu est très concret : le *Compliance-as-Code*, que l'on peut traduire par **conformité codifiée** ou *conformité automatisée*. Il s'agit de traduire les exigences réglementaires en règles vérifiables automatiquement par des outils informatiques, qui surveillent en permanence l'état des systèmes et alertent en temps réel lorsqu'un écart de conformité est détecté.

L'idée sous-jacente est puissante dans sa logique : si une exigence réglementaire peut être exprimée de manière suffisamment précise pour être auditée, elle peut être exprimée de manière suffisamment précise pour être **vérifiée automatiquement**. Un contrôle qui requiert aujourd'hui une demi-journée d'audit humain peut, lorsqu'il est traduit en règle automatisée, être vérifié en quelques secondes sur l'ensemble du parc de systèmes de l'organisation, et répété aussi fréquemment que nécessaire — idéalement en continu.

Prenons un exemple précis. L'une des exigences fondamentales du RGPD est le chiffrement des données personnelles sensibles, notamment lorsqu'elles sont stockées sur des systèmes exposés à un risque élevé de compromission. Cette même exigence se retrouve, sous des formulations différentes, dans les attentes prudentielles de l'EIOPA[11] pour les entités du secteur de l'assurance, et dans les exigences techniques de NIS2 pour les opérateurs d'entités essentielles.

Dans le système actuel, la conformité à cette exigence est vérifiée lors d'audits périodiques, au cours desquels un auditeur échantillonne un nombre limité de systèmes et vérifie manuellement l'état du chiffrement. Ce processus est coûteux, lent, et ne couvre qu'une fraction du parc système.

Dans une approche *Compliance-as-Code*, un script automatisé — une séquence d'instructions informatiques, accessible à tout professionnel informatique de niveau intermédiaire —

11. Autorité Européenne des Assurances et des Pensions Professionnelles

vérifie quotidiennement, voire en continu, l'état du chiffrement sur l'ensemble des systèmes identifiés comme hébergeant des données sensibles. Lorsqu'un écart est détecté — une base de données récemment déployée sans chiffrement activé, un disque dont le certificat de chiffrement a expiré —, une alerte est générée instantanément, assignée à l'équipe responsable et tracée dans un journal d'incidents. Le tableau de bord de conformité est mis à jour en temps réel pour refléter l'état effectif des systèmes. Le régulateur, en cas de contrôle, accède non plus à une photographie statique mais à un historique dynamique qui démontre non seulement la conformité actuelle, mais la continuité de la surveillance et la réactivité aux écarts détectés.

De la contrainte au pilotage : le tableau de bord de résilience

L'automatisation de la conformité a une vertu qui dépasse son seul bénéfice réglementaire : elle transforme la conformité en **outil de pilotage opérationnel**. Un tableau de bord de conformité automatisé ne sert plus seulement à démontrer aux régulateurs que l'organisation respecte les règles. Il devient un instrument de visibilité en temps réel sur l'état de santé numérique de l'organisation — un instrument que les dirigeants, les conseils d'administration et les équipes opérationnelles peuvent utiliser pour prendre des décisions éclairées.

Ce tableau de bord peut afficher, en un coup d'œil, le niveau de conformité de chaque système aux principales exigences réglementables, les tendances d'évolution sur les dernières semaines ou les derniers mois, les écarts détectés et leur statut de remédiation, et les zones de risque qui méritent une attention prioritaire. Il peut être décliné en vues adaptées à différents publics : une vue technique pour les équipes de sécurité et informatiques, une vue réglementaire pour le DPO et le responsable conformité, une vue stratégique pour le CTRO et le Board.

Cette capacité de pilotage intégré transforme profondément la relation entre la direction générale et les fonctions de sécurité et de conformité. Au lieu de recevoir périodiquement des rapports rétrospectifs qui décrivent ce qui s'est passé, les dirigeants disposent d'une **visibilité prospective** sur ce qui est en train de se passer — et peuvent agir avant que les écarts ne se transforment en incidents.

Les prérequis et les limites à ne pas ignorer

L'enthousiasme pour l'automatisation doit toutefois être tempéré par une lucidité sur ses prérequis et ses limites.

L'automatisation ne fonctionne que sur des **exigences suffisamment précises et mesurables** pour être traduites en règles informatiques. Certaines exigences réglementaires — notamment celles qui portent sur des notions qualitatives comme la proportionnalité des mesures de sécurité, l'adéquation des politiques de gouvernance ou la maturité d'une culture organisationnelle — résistent à l'automatisation et continueront de requérir une évaluation humaine. Le *Compliance-as-Code* est un complément à l'audit humain, pas un substitut.

L'automatisation requiert également une **qualité élevée de la cartographie des systèmes et des données**, c'est-à-dire, précisément, le Registre Universel des Actifs Numériques décrit au chapitre précédent. Un outil de monitoring automatisé ne peut surveiller que ce qu'il connaît. Si la cartographie est incomplète ou obsolète, des systèmes entiers peuvent échapper à la surveillance sans que personne ne s'en aperçoive.

Enfin, l'automatisation doit être accompagnée d'une **organisation des flux d'alerte et de remédiation**. Un système qui génère des centaines d'alertes quotidiennes sans proces-

sus clair pour les trier, les prioriser et les traiter reproduit, à l'échelle des outils techniques, la même saturation que le millefeuille réglementaire produit à l'échelle organisationnelle. L'automatisation bien conçue réduit le bruit ; mal conçue, elle l'amplifie.

L'opérationnel comme moteur de la transformation

Les trois leviers opérationnels présentés dans ce chapitre — la gestion unifiée des risques tiers, la culture de sécurité intégrée et l'automatisation de la conformité — partagent une même philosophie : **faire de la contrainte réglementaire un catalyseur d'efficience plutôt qu'un fardeau administratif**.

Cette transformation n'est pas immédiate. Elle requiert des investissements initiaux — en outils, en processus, en formation — et une volonté organisationnelle de bousculer des habitudes bien ancrées. Elle requiert également une coordination entre acteurs qui n'ont pas toujours l'habitude de travailler ensemble : régulateurs, entreprises, fournisseurs, associations professionnelles. Mais les gains, une fois la transformation engagée, sont réels et mesurables. Des ressources libérées, réinvesties dans la défense active. Des fournisseurs mieux évalués, avec moins d'effort. Des collaborateurs mieux formés, avec plus d'impact. Une conformité surveillée en continu, avec moins de surprise. Et une direction générale enfin dotée d'une visibilité en temps réel sur la résilience numérique de son organisation.

Ces gains ne sont pas seulement opérationnels. Ils sont stratégiques. Dans un environnement où la cybersécurité est devenue un enjeu de compétitivité, de réputation et de souveraineté, les organisations qui auront réussi cette transformation disposeront d'un **avantage structurel** sur celles qui continueront à subir le millefeuille sans chercher à en sortir.

Levier 1 **Gestion unifiée du risque tiers** TPRM mutualisé	Arrêter de harceler les fournisseurs avec des questionnaires redondants. Créer un passeport de conformité fournisseur unique, couvrant simultanément DORA, CRA, RGPD, NIS2 et FIDA. → Un fournisseur Cloud remplit une seule auto-évaluation standardisée, valable pour ses obligations CRA (produit) et NIS2 (service) auprès de tous ses clients.
Levier 2 **Culture de sécurité All-in-One** Sensibilisation unifiée	Remplacer les multiples sessions de sensibilisation cloisonnées par un programme unique d'acculturation numérique, traitant l'IA, la cyber et la vie privée comme un tout cohérent. → Une simulation de phishing enseigne simultanément le signalement d'incident (DORA), la protection des données (RGPD) et les risques de fuite via les LLM (IA Act).
Levier 3 **Compliance-as-Code** Automatisation en temps réel	Utiliser la technologie pour monitorer les contrôles en temps réel. Transformer la conformité statique en tableau de bord dynamique, utile au pilotage business et directement présentable au Conseil. → Un script vérifie automatiquement le chiffrement des données et met à jour en temps réel le statut de conformité RGPD et EIOPA, sans intervention manuelle.

> Le principe directeur : la conformité doit être un sous-produit automatique de la bonne architecture de sécurité — pas une activité parallèle qui consomme des ressources sans créer de résilience.

Conclusion : De la contrainte à l'avantage compétitif

« Les nations qui prospèrent ne sont pas celles qui ont les règles les plus nombreuses. Ce sont celles qui ont les règles les plus intelligentes. »

Cette tribune stratégique est partie d'un constat inconfortable mais incontestable : la France, comme la plupart de ses partenaires européens, a répondu à la croissance des menaces numériques par une croissance symétrique des textes réglementaires. Elle l'a fait avec de bonnes intentions — protéger les citoyens, sécuriser les infrastructures critiques, préserver la souveraineté technologique — et avec une rigueur juridique qui lui est caractéristique. Mais elle a, ce faisant, produit un millefeuille normatif dont le poids commence à écraser précisément ceux qu'il était censé protéger. Le paradoxe est saisissant, et il mérite d'être énoncé une dernière fois avec toute la clarté qu'il requiert : **nous avons construit un système de protection si complexe qu'il consomme les ressources nécessaires à la protection elle-même**. Les RSSI rédigent des rapports au lieu d'analyser des menaces. Les équipes juridiques interprètent des textes au lieu de structurer des défenses. Les conseils d'administration arbitrent entre des expertises contradictoires au lieu de prendre des décisions stratégiques éclairées. Et les fournisseurs remplissent des questionnaires au lieu d'améliorer leur sécurité.

Les parties qui précèdent ont proposé une voie de sortie. Non pas la déréglementation — qui serait une capitulation devant des risques réels —, mais la **convergence** : un socle commun de contrôles, un registre unifié des actifs, une gouvernance intégrée, une gestion mutualisée des risques tiers, une culture de sécurité cohérente, une conformité automatisée et dynamique. Ces propositions ne sont pas des utopies théoriques. Ce sont des transformations techniquement réalisables, économiquement justifiables et politiquement nécessaires.

Il reste à répondre à la question ultime que tout dirigeant, tout membre de conseil d'administration et tout décideur public est en droit de poser : *pourquoi faire cet effort ? Quel est le bénéfice tangible, mesurable, stratégique, de cette transformation ?* La réponse se déploie sur trois dimensions qui, ensemble, dessinent le contour d'un avantage compétitif national dont la France aurait tort de se priver.

La réallocation du capital : financer l'innovation avec les économies de la bureaucratie

Ce que coûte réellement le millefeuille

Il n'existe pas, à ce jour, de comptabilité nationale précise du coût total de la saturation normative en matière de cybersécurité pour les entreprises françaises. Mais les ordres de grandeur que l'on peut reconstituer à partir des études sectorielles disponibles sont éloquents. Dans les grandes organisations soumises à l'ensemble des cadres réglementaires évoqués dans cette tribune — NIS2, DORA, RGPD, AI Act, CRA —, la part des budgets cybersécurité consacrée à des activités de conformité documentaire, d'audit et de reporting représente couramment entre 30 et 45 % des dépenses totales. Dans certains secteurs particulièrement régulés — banque, assurance, santé —, cette proportion peut dépasser 50 %.

Ces chiffres ne signifient pas que la conformité est inutile. Ils signifient qu'une fraction considérable des ressources allouées à la conformité est absorbée par des redondances évitables : le même contrôle vérifié trois fois, le même incident notifié à quatre régulateurs, la même évaluation fournisseur conduite douze fois par douze clients différents. Ce sont ces redondances — et seulement elles — que la convergence normative vise à éliminer.

Si la rationalisation proposée dans cette tribune permettait de réduire ne serait-ce que de 30 % seulement la part des budgets consacrée à ces redondances — une hypothèse conservatrice au regard des gains observés dans les organisations qui ont déjà engagé des démarches d'harmonisation partielle —, les ressources libérées seraient considérables. Pour une grande entreprise dont le budget cybersécurité annuel atteint vingt millions d'euros, cela représente six millions d'euros réallouables. Pour l'ensemble des entreprises françaises soumises aux principales réglementations numériques, on peut estimer que le gain se chiffre en milliards.

Réinvestir dans la défense active et l'innovation

La question n'est pas seulement combien, mais vers quoi ces ressources pourraient être réorientées. La réponse mérite d'être précisé, parce qu'elle détermine la nature de l'avantage compétitif à construire.

La première destination naturelle de ces ressources est la **cybersécurité offensive** — entendue non pas comme une capacité d'attaque, mais comme la posture de sécurité proactive qui cherche activement les vulnérabilités avant que les attaquants ne les trouvent. Les programmes de Bug Bounty — littéralement, prime à la faille — en sont l'illustration la plus concrète. Ces programmes rémunèrent des chercheurs en sécurité indépendants pour identifier et signaler de manière responsable les vulnérabilités dans les systèmes d'une organisation. Ils sont parmi les mécanismes de détection les plus efficaces connus, précisément parce qu'ils mobilisent une diversité de profils et d'approches qu'aucune équipe interne ne peut reproduire seule.

Or, les programmes de Bug Bounty permanents sont aujourd'hui réservés aux grandes organisations technologiques qui disposent des budgets suffisants. La grande majorité des entreprises françaises ne peuvent pas se les permettre — non par manque de volonté, mais par manque de ressources, absorbées par la bureaucratie de la conformité. Réduire de 30 % le budget d'audit redondant pour financer un programme permanent de recherche de vulnérabilités, **c'est substituer une dépense rétrospective et défensive à un investissement prospectif et actif**. C'est passer de la démonstration de la conformité à la construction de la résilience.

La deuxième destination est **la recherche et développement en sécurité**. Les entreprises françaises de la cybersécurité — dont plusieurs figurent parmi les leaders mondiaux dans leurs niches respectives — ont besoin d'un écosystème dans lequel leurs clients disposent des ressources et du temps pour tester, déployer et industrialiser des solutions innovantes. Un marché domestique asphyxié par la bureaucratie réglementaire est un marché qui ne peut pas se permettre l'innovation. Un marché libéré de ses redondances est un marché qui devient un terrain d'expérimentation et de déploiement pour les technologies de sécurité de demain.

L'accélération du Time-to-Market : la conformité comme moteur, non comme frein

Le paradoxe du premier entrant réglementé

Dans l'économie numérique, la vitesse est une dimension compétitive fondamentale. La capacité à lancer un nouveau service, à explorer un nouveau marché, à répondre à une opportunité émergente avant ses concurrents détermine souvent qui capture la valeur et qui la laisse passer. Or, dans l'environnement réglementaire actuel, le processus de validation de la conformité d'un nouveau service numérique — notamment lorsqu'il touche à des données personnelles, à des fonctions financières ou à des algorithmes d'intelligence artificielle — peut s'étendre sur des mois, parfois sur une année entière.

Ce délai n'est pas intrinsèquement lié à la complexité du service ou à la rigueur légitime du régulateur. Il est, en grande partie, une conséquence directe de la fragmentation normative : l'organisation doit démontrer sa conformité séparément à chaque cadre applicable, selon des processus qui ne sont pas coordonnés, avec des experts différents pour chaque dimension réglementaire, et en produisant des documentations qui ne peuvent pas être mutualisées.

La conformité par design : un socle déjà validé

La vision de la convergence normative transforme radicalement cette dynamique. Lorsqu'une organisation dispose d'un *Single Compliance Stack* — un socle commun de contrôles déjà validés, un registre d'actifs à jour, une gouvernance intégrée opérationnelle et une automatisation de la conformité en temps réel —, le lancement d'un nouveau service ne part plus de zéro sur le plan réglementaire. Il s'appuie sur une **infrastructure de conformité préexistante** dans laquelle le nouveau service vient s'inscrire, plutôt que de construire son propre dossier de conformité from scratch.

C'est ce que l'on désigne par le concept de **conformité par design** — ou *compliance by design* — : l'intégration des exigences réglementaires dès la conception du service, de manière à ce que la conformité soit une caractéristique architecturale du produit plutôt qu'une validation externe ajoutée après coup. Lorsque ce principe est combiné avec un socle de conformité unifié et déjà opérationnel, les délais de mise sur le marché se compriment de manière spectaculaire.

L'exemple du secteur des services financiers est particulièrement illustratif. FIDA — le règlement européen sur l'accès aux données financières, qui constitue la prochaine étape de l'Open Finance en Europe — impose des exigences combinées en matière de sécurité des interfaces d'accès aux données, de protection des données personnelles des clients et de gouvernance algorithmique pour les services qui utilisent ces données à des fins de recommandation ou de décision. Dans le système actuel, une fintech qui souhaite lancer un service basé sur FIDA doit constituer trois dossiers de conformité distincts — cybersécurité, RGPD, AI Act —, les valider séquentiellement auprès de trois autorités différentes, et gérer les inévitables allers-retours entre des exigences qui peuvent se révéler contradictoires dans leur interprétation.

Avec un socle de conformité unifié, cette même fintech s'appuie sur un référentiel de contrôles déjà validé couvrant simultanément la cybersécurité, la protection des données et la gouvernance algorithmique. Elle n'a pas à reconstituer la preuve de sa conformité : elle l'a en permanence. Elle peut se concentrer sur **ce qui différencie son service** — l'expérience utilisateur, la pertinence algorithmique, la qualité des données — plutôt que sur la production documentaire. Le délai de mise sur le marché passe de douze à dix-huit mois à quelques semaines ou quelques mois. La différence n'est pas marginale : elle peut déterminer si l'entreprise capte ou manque une fenêtre d'opportunité de marché.

Un avantage pour toutes les tailles d'entreprise, mais vital pour les PME

Cet avantage du time-to-market bénéficie à toutes les organisations, mais il est vital pour **les PME et les ETI** qui constituent le tissu le plus dynamique de l'écosystème numérique français. Une grande entreprise peut absorber douze mois de processus réglementaire, même si c'est coûteux et frustrant. Une start-up en phase de croissance, une PME qui cherche à diversifier ses services, une ETI qui veut accélérer sa transformation numérique ne le peuvent souvent pas. Pour elles, la lenteur réglementaire n'est pas un inconfort : c'est parfois une menace existentielle. En simplifiant et en accélérant les processus de validation, la convergence normative ne fait pas seulement gagner du temps aux grandes organisations. Elle **ouvre le marché** à des acteurs qui en étaient structurellement exclus par la complexité et le coût de la conformité. Elle élargit la base de l'innovation numérique française. Et elle crée les conditions d'une compétition plus dynamique sur les marchés européens et mondiaux.

La souveraineté et l'attractivité de la place de France : la lisibilité comme argument de puissance

Repenser la souveraineté numérique

Le mot « souveraineté » est sans doute l'un des plus utilisés — et des plus galvaudés — dans les débats sur la politique numérique française. Il recouvre des réalités très différentes selon les contextes : souveraineté des données, souveraineté technologique, souveraineté réglementaire, souveraineté industrielle. Sa polysémie est parfois une force — elle permet de mobiliser des coalitions larges autour d'une ambition commune — mais elle est aussi une faiblesse, car elle autorise des interprétations qui peuvent se contredire mutuellement.

Cette tribune stratégique défend une conception précise de la souveraineté numérique, qui s'écarte délibérément du réflexe protectionniste pour embrasser une logique de **puissance par la lisibilité**. La France ne sera souveraine dans le numérique ni en multipliant les couches réglementaires pour rendre son marché inaccessible, ni en copiant les modèles américain ou chinois de concentration technologique qui ne correspondent ni à ses valeurs ni à ses capacités. Elle le sera en devenant le territoire européen où il fait le mieux sens de construire, d'investir et d'innover dans le numérique — parce que les règles y sont claires, cohérentes, prévisibles et opérationnellement efficientes.

Cette souveraineté par la lisibilité est une **souveraineté d'attraction**, pas de restriction. Elle ne cherche pas à enfermer les acteurs dans un périmètre national, mais à faire de la France le point de gravité naturel de l'écosystème numérique européen.

Paris, hub de la lisibilité réglementaire

La comparaison internationale est instructive. Les écosystèmes numériques les plus dynamiques du monde — Silicon Valley, Tel Aviv, Singapour, Londres avant le Brexit — ont tous en commun non pas l'absence de régulation, mais **la prévisibilité et la cohérence de leur environnement réglementaire**. Les entreprises technologiques, notamment celles qui cherchent à s'implanter sur le marché européen, n'ont pas peur des règles. Elles ont peur de l'incertitude, de l'incohérence et de la multiplication des interlocuteurs réglementaires.

Dans ce contexte, la France a une opportunité historique que sa tradition juridique et son ambition souveraine la préparent particulière-

ment bien à saisir : devenir **le laboratoire européen de la régulation numérique intelligente**. Non pas en renonçant à ses exigences de sécurité et de protection des données — qui sont, au contraire, des arguments de confiance — mais en les articulant dans un cadre unifié, lisible et opérationnellement efficace que les entreprises technologiques percevraient comme un avantage plutôt que comme un obstacle.

Imaginez une licorne étrangère — américaine, indienne, japonaise — qui cherche à établir son quartier général européen pour lancer ses services sur le marché de l'Union. Elle a le choix entre plusieurs capitales. Berlin lui offre un écosystème technologique dense mais un paysage réglementaire fragmenté entre le droit fédéral et les droits des Länder. Amsterdam lui offre une fiscalité attractive mais une taille de marché limitée. Dublin lui offre un environnement anglophone familier mais une réputation de laxisme réglementaire qui commence à peser sur les relations avec les autres États membres.

Paris lui offre quelque chose de différent : l'accès au premier marché continental de l'Union, un écosystème de talents parmi les meilleurs d'Europe, une administration qui — dans le scénario que ce livre blanc appelle de ses vœux — lui présente **un interlocuteur unique, un référentiel de conformité unifié et un calendrier de validation prévisible**. Pour une entreprise qui a besoin de certitude réglementaire pour planifier ses investissements, construire son architecture technique et rassurer ses investisseurs, cette lisibilité a une valeur économique réelle, mesurable en mois de délai gagnés et en millions d'euros de coûts de conformité évités.

C'est ce que nous appelons **la lisibilité réglementaire comme argument de puissance**. Et c'est, au fond, la forme la plus ambitieuse et la plus durable de la souveraineté numérique française.

Une responsabilité qui dépasse les entreprises

Il serait réducteur de conclure cette tribune stratégique en limitant la portée de ses propositions au seul monde de l'entreprise. La transformation [12] que nous décrivons est, en dernière analyse, une transformation de **la relation entre l'État et le secteur privé** dans le domaine numérique — une relation qui doit évoluer d'un rapport de contrôle bureaucratique vers un rapport de co-construction de la résilience nationale.

Cette évolution requiert des entreprises qu'elles cessent de traiter la conformité comme une contrainte externe à subir, et commencent à la traiter comme une dimension de leur stratégie à maîtriser. Elle requiert des régulateurs qu'ils acceptent de coordonner leurs exigences et de reconnaître mutuellement leurs preuves, au prix d'une partie de leur autonomie sectorielle. Elle requiert du législateur qu'il cesse d'additionner les textes sans en évaluer les effets cumulés, et commence à concevoir la régulation comme une architecture cohérente dont la complexité globale doit être activement gérée.

Et elle requiert des conseils d'administration et des comités exécutifs qu'ils cessent de déléguer la résilience numérique à des équipes techniques isolées, et commencent à la traiter comme ce qu'elle est devenue : **une dimension centrale de la gouvernance stratégique, au même titre que la performance financière, la gestion des talents ou la transition écologique**.

12. Un travail, à destination des décideurs politiques est en cours

Appel à l'action : trois engagements pour trois acteurs

Cette tribune stratégique ne prétend pas avoir réponse à tout. La transformation qu'elle décrit est complexe, progressive et politiquement exigeante. Mais il est possible d'identifier, pour chacun des acteurs clés, un engagement prioritaire qui permettrait d'enclencher la dynamique de convergence sans attendre que tous les obstacles soient levés.

Pour **les dirigeants d'entreprises et les conseils d'administration** : mandatez, dès aujourd'hui, une revue de l'architecture de votre gouvernance de la conformité numérique. Identifiez les redondances, les silos et les angles morts. Posez la question, peut-être inconfortable, de savoir quelle fraction de vos dépenses de conformité produit une amélioration réelle de votre résilience — et quelle fraction ne produit que de la documentation. Cette revue est le point de départ de toute transformation sérieuse.

Pour **les régulateurs et les autorités publiques** : engagez une concertation formelle et contraignante avec vos homologues sectoriels pour identifier les exigences redondantes et les conditions d'une reconnaissance mutuelle des preuves de conformité. Cette concertation n'exige pas de texte législatif pour commencer. Elle exige de la volonté institutionnelle et la conviction partagée que la coordination entre régulateurs est une condition de l'efficacité de la régulation elle-même.

Pour **les décideurs politiques** : faites de la simplification réglementaire numérique une priorité de politique industrielle, au même titre que le soutien à la filière de la cybersécurité ou l'investissement dans les infrastructures numériques souveraines. La rationalisation du paysage normatif n'est pas un recul de l'ambition française. C'est son accomplissement.

Épilogue : l'intelligence comme choix stratégique

L'intelligence artificielle comme allié structurel de la convergence

Il serait paradoxal de conclure une tribune stratégique sur la rationalisation de la régulation numérique sans évoquer l'outil qui, peut-être plus qu'aucun autre, est en mesure d'en accélérer concrètement la mise en œuvre : l'intelligence artificielle elle-même.

Alors que l'IA fait l'objet de régulations croissantes — l'AI Act en étant l'expression la plus aboutie —, elle constitue simultanément l'une des réponses les plus prometteuses à la surcharge réglementaire qu'elle contribue, par ailleurs, à complexifier. Des systèmes d'IA spécialisés sont aujourd'hui capables d'analyser en temps réel l'ensemble des obligations réglementaires applicables à une organisation, de les croiser avec l'état effectif de ses systèmes et de ses processus, et de générer automatiquement les reportings requis par chaque autorité compétente — dans le bon format, selon le bon calendrier, avec le bon niveau de granularité. Ce qui mobilisait autrefois plusieurs semaines de travail humain pour consolider des données éparses en rapports réglementaires cohérents peut désormais être produit en quelques heures, avec une traçabilité et une reproductibilité que le travail manuel ne peut pas garantir.

Au-delà du reporting, les outils d'IA sont capables de surveiller en continu la cohérence entre les contrôles en place et les exigences réglementaires, d'identifier les écarts avant qu'ils ne deviennent des incidents, et de prioriser les actions correctives selon leur criticité réglementaire et leur impact opérationnel réel. Ils peuvent également assister les équipes juridiques et de conformité dans la veille normative — en détectant automatiquement les évolutions des textes applicables, en évaluant leur impact sur les dispositifs existants et en proposant des plans de mise en conformité adaptés. L'IA

ne remplace pas le jugement humain dans l'interprétation des normes, ni la responsabilité des dirigeants dans les arbitrages stratégiques. Mais elle libère les équipes de la part la plus chronophage et la moins créatrice de valeur de leur travail de conformité — précisément celle que ce livre blanc a identifiée comme le principal gisement de ressources à récupérer au profit de la défense active.

En ce sens, l'intelligence artificielle n'est pas seulement un objet de régulation : elle est, bien déployée et bien gouvernée, un levier de souveraineté opérationnelle — celui qui permet à la vision de la convergence normative de passer du document stratégique à la réalité du terrain.

Le mot de la fin

La France a toutes les cartes en main pour réussir cette transformation. Elle dispose d'une tradition juridique qui valorise la cohérence et la systématicité. Elle dispose d'un écosystème de cybersécurité parmi les plus compétents d'Europe. Elle dispose d'une administration publique qui, lorsqu'elle se coordonne, est capable de portages institutionnels ambitieux. Elle dispose, surtout, d'une position centrale dans la construction du droit numérique européen qui lui donne une influence considérable sur la manière dont les règles communes seront conçues et articulées.

Ce qu'elle doit choisir, c'est d'exercer cette influence non pas pour ajouter des couches supplémentaires à une architecture déjà surchargée, mais pour en être **l'architecte de la cohérence**. Pour être le pays qui a compris, avant les autres, que la régulation intelligente est une forme de puissance — et que la simplicité bien conçue est plus souveraine que la complexité mal maîtrisée. Le millefeuille a été construit couche par couche, sans plan d'ensemble, sous la pression des urgences et des agendas sectoriels. Le défaire ne peut pas se faire de la même manière. Cela requiert une vision, une architecture et une volonté.

Cette tribune stratégique est une invitation à formuler cette vision, à dessiner cette architecture, et à trouver cette volonté.

> **La convergence n'est pas une utopie. C'est un choix.**

Liste des réglementations

AI Act Artificial Intelligence Act, règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle. https://eur-lex.europa.eu/eli/reg/2024/1689/oj. 3, 5, 10, 11, 14, 17, 18, 22, 24, 27

CRA Cyber Resilience Act, règlement (UE) 2024/2847 du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques. https://eur-lex.europa.eu/eli/reg/2024/2847/oj. 3, 9, 16, 22

DORA Digital Operationnal Resilience Act, règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier. https://eur-lex.europa.eu/eli/reg/2022/2554/oj. 3, 4, 7, 9–11, 16–18, 22

DSA Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques. https://eur-lex.europa.eu/eli/reg/2022/2065/oj. 3

DSP2 Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les Services de Paiement dans le marché intérieur. http://data.europa.eu/eli/dir/2015/2366/oj. 3

FIDA Financial Data Access, Proposition de RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL relatif à un cadre pour l'accès aux données financières. https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52023PC0360. 3, 16, 24

NIS2 Network and Information Security, directive (UE) 2022/2555 du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. http://data.europa.eu/eli/dir/2022/2555/oj. 3–6, 9, 10, 15, 16, 19, 22

RGPD Règlement Général sur la Protection des Données, règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. https://eur-lex.europa.eu/eli/reg/2016/679/oj. 3, 4, 6, 7, 9–12, 14, 16–19, 22, 24

Solvabilité II Directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (solvabilité II). http://data.europa.eu/eli/dir/2009/138/oj. 3