

Réglementations européennes : vers une finance numérique responsable et souveraine ?

Et si la réglementation devenait un moteur de transformation ? Les services financiers font face à l'inflation réglementaire, un cadre exigeant, parfois contraignant, mais porteur de souveraineté, de responsabilité et de transformation durable.



NICOLAS VETRIAK
associé fondateur,
Novaminds



GEREMY BENKIRANE
Global Head of IT Risk,
BNP Paribas CIB

SUR LES AUTEURS

Ingénieur et titulaire d'un MBA en Finance Internationale, diplômé de l'École nationale des Ponts et Chaussées, **Nicolas Vetriak** dispose de plus de vingt-cinq ans d'expérience dans les services financiers, d'abord dans des fonctions à responsabilités opérationnelles en cyber-sécurité, résilience et risque opérationnel pour de grandes institutions financières puis dans le conseil en stratégie et transformation en data, conformité, risques, résilience et contrôle, pour les banques et assurances.

Ingénieur de formation, avec plus de vingt-cinq ans d'expérience, **Geremy Benkirane** a occupé notamment les fonctions de directeur des contrôles et de la sécurité de l'information, de responsable continuité d'activité et data protection officer du groupe exane. Précédemment, il était responsable sécurité du système d'information chez State Street Bank. Il occupe depuis février 2022 la fonction de Responsable Global des Risques IT pour BNP Paribas CIB.

Réglementations, catalyseurs de transformation numérique

Le paysage réglementaire des services financiers se densifie à un rythme soutenu, avec l'entrée en vigueur de DORA sur la résilience opérationnelle, du Cyber Resilience Act sur la sécurité des produits numériques, ainsi que de l'IA Act et du Data Act, qui renforcent la gouvernance des données et l'encadrement de l'intelligence artificielle. Cyber-Sécurité, résilience, IA et *data privacy* s'imposent comme des priorités pour les régulateurs. Ce cadre réglementaire redéfinit les trajectoires technologiques et les défis auxquels sont confrontées les institutions financières. Les modèles d'organisation évoluent en profondeur pour répondre à cette nouvelle donne. On assiste à une montée en puissance des fonctions de gouvernance réglementaire et technologique, souvent intégrées aux directions des risques, de l'informatique ou de la transformation digitale. Ces fonctions traditionnellement en silo ont pour enjeu désormais de s'articuler au travers d'une gouvernance transversale et agile ; capable d'adresser les évolutions réglementaires en continu.

Une stratégie européenne au service de la souveraineté numérique

L'Union européenne est dans une dynamique réglementaire structurante pour affirmer son autonomie numérique. Cette dynamique s'appuie sur un corpus de textes convergents : résilience opérationnelle (DORA), Cyber-Sécurité (Cyber Resilience Act, Cyber Solidarity Act), gouvernance des données (Data Act), encadrement de l'IA (IA Act), régulation des plateformes (Digital Services Act) et supervision des cryptoactifs (MiCA). Ce cadre vise à renforcer la confiance dans les technologies et à garantir un marché numérique fiable, éthique et souverain. La dynamique s'accompagne d'un effort d'harmonisation entre secteurs et États membres. L'objectif : assurer l'interopérabilité des exigences (DORA, IA Act, CSRD, Data Act), éviter les silos normatifs et faciliter les déploiements transfrontaliers. Les entreprises opérant à l'international doivent composer avec des réglementations le plus souvent hétérogènes, asiatiques, américaines... pouvant avoir une portée extraterritoriale. L'enjeu est de construire des dispositifs de conformité agiles, adaptables et cohérents, capables d'adresser plusieurs référentiels avec

une gouvernance holistique à tous les niveaux de l'organisation en intégrant les contraintes locales.

Gouverner la donnée et les usages : sécurité, intégrité, éthique

Le Data Act, l'IA Act... réaffirment l'importance de la donnée. Ces textes imposent des exigences croissantes de transparence, de qualité, de sécurité et de supervision des traitements. Ils encadrent également les usages de l'intelligence artificielle selon leur niveau de risque.

Ce cadre appelle un pilotage renforcé de la donnée — devenue un actif stratégique — et un effort massif de documentation, d'explicabilité des modèles, de contrôle des usages, mais aussi de reconstitution historique. L'identification et la classification des données représentent un chantier de long terme, qui conditionne la conformité à venir.

L'ESG, levier de maturité réglementaire

Désormais, la conformité dépasse le champ technique. L'empreinte environnementale des systèmes, la transparence des algorithmes et l'accessibilité numérique deviennent des critères de conformité à part entière, avec des obligations accrues en matière de *reporting* extra-financier.

LES POINTS CLÉS

- L'UE renforce sa souveraineté technologique grâce à un encadrement ambitieux et harmonisé des services financiers.
- DORA, IA Act, Cyber Resilience Act... Des textes structurants qui redéfinissent les priorités des établissements financiers.
- Des exigences croissantes en matière de gouvernance, de contrôle et de responsabilité.
- L'ESG est au cœur des obligations numériques du secteur financier.
- Une opportunité de transformation durable des modèles IT, data et risques.

Plus largement, l'empreinte numérique — dans ses dimensions écologiques, sociales et techniques — devient un indicateur de maturité réglementaire. L'attente ne vient pas seulement des régulateurs, mais aussi des investisseurs et de la société civile : la réglementation structure la responsabilité, limite les risques et renforce la robustesse des stratégies d'investissement.

Anticiper pour transformer durablement

Intégrer les exigences réglementaires dès la conception des dispositifs est devenu un impératif. Cette anticipation permet de gagner en robustesse, en fluidité et en efficacité opérationnelle. L'auditabilité et la traçabilité doivent être intégrées dans l'exploitation quotidienne, les chaînes de décisions identifiées, les responsabilités portées jusqu'au plus haut niveau (l'organe de direction).

Cette posture proactive est un levier : elle permet de structurer les processus métiers et de sécuriser la transformation ; cela renforce, par ailleurs, l'efficacité opérationnelle et *in fine* la compétitivité des établissements.

Renforcer la maîtrise des risques technologiques

Les évolutions réglementaires exigent une maîtrise des risques technologiques avec la mise en place de dispositifs de contrôle adaptés et intégrés opérationnellement. Cela suppose une gestion globale des risques numériques selon une approche métier, notamment : classification des actifs, maîtrise des dépendances technologiques, contrôle des prestataires, gestion des menaces ou encore réponse aux incidents...

Souveraineté, résilience, responsabilité au plus haut niveau : la réglementation devient un moteur de transformation de la finance

La maîtrise des risques technologiques est aujourd'hui au cœur des attendus des superviseurs en matière de conformité, de résilience et de responsabilité numérique. Les fonctions Risques, Cyber-Sécurité et Contrôle doivent collaborer étroitement pour un pilotage, du design à l'exploitation, de la

maîtrise de l'ensemble des chaînes de valeur de l'établissement. Cela suppose de renforcer les référentiels de contrôle selon une approche par les risques, la supervision continue et les capacités de test et remédiation. Ces exigences appellent une refonte des cartographies de risques technologiques, une gouvernance des changements plus rigoureuse et un dialogue renforcé entre les métiers, l'informatique, la conformité, et plus largement l'ensemble des fonctions idoines de l'établissement. L'enjeu est de piloter les dispositifs selon les seuils de tolérance définis (Risk Appetite Framework), tout en assurant la traçabilité des décisions et des mesures correctrices.

Enfin, l'outilage devient un levier structurant : les solutions GRC centralisent la gestion des risques et des contrôles ; des outils (SIEM, SOC...) renforcent les capacités de détection, de réaction et de coordination face aux incidents. Une approche intégrée est essentielle pour répondre aux attentes des régulateurs et sécuriser les opérations, et plus largement la continuité d'exploitation de l'entreprise.

Vers une finance numérique maîtrisée, durable et interopérable

Les autorités de supervision renforcent leur niveau d'exigence. Elles multiplient les inspections, demandent des preuves concrètes de conformité des dispositifs, peuvent exiger la mise en place de mesures correctrices et de prononcer des sanctions. Face à l'émergence des nouvelles technologies et des nouveaux défis (objets connectés, technologies quantiques, IA autonome ou finance décentralisée), la régulation continue d'évoluer. Cela implique d'investir dans la veille, les compétences, l'acculturation des équipes et l'outilage. La réglementation n'est plus un simple cadre de conformité. Elle est le socle d'une transformation durable, maîtrisée et responsable. ♦

