Numérisation, Réglementation

La cybersécurité, ***débarrassée des illusions réglementaires***

21.01.2026

D'un coup d'oeil

- Après des années de densification réglementaire, l'UE a décidé de simplifier et d'harmoniser les réglementations et d'assurer la sécurité des investissements, au lieu d'élaborer de nouvelles règles détaillées
- Pour la résilience, mieux vaut des mesures fondées sur le marché, des standards internationaux et l'expertise technologique que des prescriptions étatiques de plus en plus détaillées
- En ce qui concerne le cyberespace, la Suisse a jusqu'ici fait preuve de modération. Il est décisif de poursuivre ainsi et d'éviter de reprendre des réglementations que l'UE elle-même commence à rectifier

L'Union européenne ouvre un nouveau chapitre dans sa politique numérique: après des années de densification réglementaire, les signes annonçant un changement de cap se multiplient. Avec l'omnibus numérique, le Digital Networks Act annoncé, la révision du Cyber Security Act ainsi que le bilan de qualité numérique en cours, la tendance est claire: simplifier, harmoniser, inciter à investir et mettre en œuvre au lieu de multiplier les règles détaillées.

Ce que l'UE constate aujourd'hui et les leçons que la Suisse peut en tirer

De nombreux débats sont encore influencés aujourd'hui par l'idée erronée voulant que la cybersécurité ne verrait le jour que lorsque l'État obligerait des entreprises à agir. Des mesures facultatives et des mécanismes de marché ne seraient pas suffisants. La pratique montre toutefois une autre réalité.

La cybersécurité n'est pas un atout pour les entreprises, elle est un facteur existentiel. Des pertes de données, des arrêts de production ou des dommages réputationnels ont des conséquences économiques directes. L'importance et la précocité des investissements dans la cybersécurité varient considérablement en fonction de la taille de l'entreprise.

Les PME en particulier subissent déjà une pression considérable en lien avec les coûts et les charges administratives. Elles ont souvent une marge de manœuvre financière insuffisante pour mettre en œuvre à un stade précoce des prescriptions réglementaires complexes dans le domaine de cybersécurité. De nouvelles réglementations détaillées n'y changeraient donc rien. Il est bien plus efficace de sensibiliser les entreprises, de les conseiller et de leur fournir des informations leur permettant de faire face aux risques de manière proportionnée et progressive. Pour ce qui est des standards et des certifications internationaux, comme la norme ISO 27001 ou le cadre du NIST, ils vont souvent bien au-delà des exigences légales minimales.

En ce qui concerne les prestataires de technologies en nuage et de sécurité modernes, ils disposent déjà de centres d'opérations de sécurité à l'échelle mondiale et investissent des milliards dans la détection d'attaques, la redondance et l'automatisation. Leur niveau de sécurité découle de la proximité avec la technique et d'une adaptabilité rapide – et non de prescriptions administratives annuelles.

Cela ne signifie pas pour autant que l'État n'ait aucun rôle à jouer. Son intervention est souhaitée là où les mécanismes du marché touchent à leurs limites: pour élaborer des standards minimums destinés à des infrastructures critiques, clarifier les responsabilités et créer la transparence. Il n'est toutefois pas le bon acteur pour assurer la cybersécurité au quotidien. Les menaces évoluent en effet plus vite que la réglementation.

C'est précisément là que l'Union européenne opère un changement de cap. Le Cyber Resilience Act illustre bien le virage qui est désormais pris par l'UE. L'économie a vivement critiqué cette loi, considérant qu'il s'agit d'une intervention complexe et bureaucratique dans le cycle de vie des produits. En décidant de tenir compte des réserves exprimées, l'UE admet surtout que des réglementations excessives sont devenues un désavantage concurrentiel majeur.

Un vrai changement de paradigme

L'objectif n'est pas de déréglementer, mais de prendre soin de la place économique. La sécurité découle de la fiabilité et non d'une multiplication des obligations. Les entreprises investissent dans la cybersécurité là où elles ont la sécurité juridique.

Le changement de cap de l'UE en ce qui concerne les réglementations relatives à l'espace numérique est un signal d'alarme – non pas en raison d'un cavalier seul actuel de la Suisse, mais pour rappeler l'importance de ne pas abandonner la ligne suivie jusqu'ici. En ce qui concerne le cyberespace, la Suisse a bien fait de ne pas se précipiter et de mettre en œuvre les prescriptions européennes en faisant preuve de retenue. Il est désormais décisif d'éviter de reprendre les réglementations que l'UE elle-même juge trop complexes et qu'elle a commencé à corriger.

Une cybersécurité durable voit le jour là où des entreprises assument leurs responsabilités – des jalons étatiques clairs et simples apportent un soutien, mais ne font pas tout. L'UE commence à aller dans cette direction. La Suisse doit donc agir avec prudence.

Angela Anthamatten

Responsable suppleante du Département Concurrence et Réglementation

David Stauffacher

Responsable de project infrastructures et numérisation

Basile Dacorogna

Suppléant de la direction romande, Responsable de projet Concurrence et régulation