Une cyber-souveraineté pour une cybersécurité de confiance

Pierre-Yves HENTZEN
Président - CEO
Stormshield

La souveraineté numérique s'impose comme un enjeu stratégique majeur pour l'Europe. Et pourtant, les organisations publiques et privées s'appuient bien souvent sur des technologies, des services cloud et des infrastructures développés hors du continent. Or cette dépendance croissante fragilise la maîtrise des données, la sécurité des systèmes critiques et la résilience des chaînes de valeur.

Pour pallier cette problématique, la création d'un nouvel outil d'évaluation, l'Indice de Résilience Numérique (IRN), a été annoncée[1] par un collectif d'acteurs économiques et d'experts. Sa première évaluation, prévue à l'automne 2025, offrira aux organisations un point de référence pour orienter leurs décisions stratégiques.

Et si cette démarche marquait une étape vers une prise en compte plus systématique et sérieuse de la souveraineté numérique ?

La cybersécurité au service de la souveraineté numérique

Au cœur de la souveraineté numérique réside la capacité à maîtriser pleinement ses données et ses infrastructures. Cette maîtrise est essentielle pour garantir l'autonomie décisionnelle et la libre disposition de ses ressources numériques. Et dans un contexte mondial marqué par une prolifération constante d'attaques informatiques, qu'elles soient d'origines étatiques, criminelles, à but lucratif ou liées à l'intelligence économique, faire le choix de solutions de cybersécurité européennes s'impose comme un pilier fondamental de cette souveraineté. Ceci, afin de conserver le contrôle sur les actifs numériques et de protéger les données et les infrastructures contre tout accès non autorisé par des tiers. Ce choix contribue ainsi directement à la construction et à la préservation de l'indépendance stratégique d'une entité.

L'instabilité géopolitique, marquée par un déplacement des conflits sur le terrain cyber, et donc l'intensification des cybermenaces accentuent ces enjeux et appellent à une autonomie stratégique renforcée, fondée sur la confiance et la transparence. Ces tensions peuvent en effet amplifier le risque d'attaques ciblées, soulignant l'urgence de renforcer les capacités de prévention et de réaction des organisations.

Il est donc crucial pour les entreprises européennes de prendre en compte ces tensions, notamment dans le choix de leurs outils. Cela leur permet non seulement de conserver la maîtrise de leurs

[1] https://assets.rte-france.com/prod/public/2025-07/2025-07-04-cp-indice-resilence-numerique.pdf

infrastructures et de leurs données, mais aussi de se prémunir contre l'impact des réglementations extraterritoriales, et, comme cela a été observé récemment, de garantir l'accès à des ressources qui pourraient être coupées à tout moment. Le monde évolue et la dépendance aux solutions de cybersécurité non-européennes représente désormais un facteur de risque majeur.

Garantir autonomie et confiance grâce à des solutions souveraines

Au-delà de la simple évaluation, cette démarche d'indice de dépendance est un grand pas dans la bonne direction. Elle vise en effet à encourager une transition vers des écosystèmes numériques plus fiables, en mettant l'accent sur la maîtrise technologique, la capacité à auditer et à contrôler les codes sources, la proximité des acteurs en cas d'incident, ainsi que la conformité aux réglementations européennes. Une souveraineté numérique solide passe aussi par le développement de solutions conçues pour répondre aux standards locaux dès leur conception, garantissant ainsi une meilleure intégration dans les contextes réglementaires comme la directive NIS2 [2] ou le Cyber Resilience Act[3].

Par ailleurs, l'équation entre souveraineté et performance n'implique pas de compromis. En s'appuyant sur des solutions de cybersécurité évaluées ou, a minima, certifiées par des autorités indépendantes comme l'ANSSI[4], il est possible de bénéficier de technologies à la fois fiables et efficaces, tout en préservant la maîtrise des données et des infrastructures. Ces solutions doivent être simples à déployer, afin de protéger efficacement sans freiner la productivité, tout en contribuant à l'indépendance stratégique.

Choisir une solution souveraine renforce la résilience face aux cybermenaces et garantit l'intégrité des données, la confiance et l'autonomie décisionnelle. Pour répondre à ces exigences, les produits doivent non seulement être certifiés, c'est-à-dire évalués selon des critères de sécurité techniques définis par des normes, mais aussi qualifiés par les agences de cybersécurité européennes. La qualification va au-delà de la certification car elle atteste que le produit répond à des besoins opérationnels identifiés par les autorités, qu'il est fiable sur le long terme et qu'il peut être utilisé dans des environnements sensibles. Si leur code source est également soumis à des audits indépendants, cela permettra de détecter toute vulnérabilité, qu'elle soit involontaire (erreurs de programmation) ou volontaire (backdoors introduites pour des accès non autorisés). Cette démarque renforce la confiance et contribue directement aux objectifs de souveraineté numérique.

Construire ensemble un écosystème de cybersécurité souverain

La souveraineté numérique est l'affaire de tous.

Des institutions publiques aux entreprises privées de toutes tailles, tous sont concernés par ces enjeux, que ce soit pour protéger les données des citoyens, des collaborateurs ou les informations sensibles à leurs activités. Cette exigence requiert un engagement collectif vers des solutions de cybersécurité dignes de confiance qui contribueront à garantir un écosystème numérique solide et souverain. Il faut également trouver des consensus entre des pays dont les intérêts peuvent parfois diverger, avec des systèmes politiques et des visions qui diffèrent des objectifs de l'Union Européenne.

C'est dans ce cadre que se pose la question des

[2] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
[3] https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[4] https://cyber.gouv.fr/

leviers de souveraineté numérique. Il s'agit des moyens et instruments que l'on peut mobiliser pour renforcer l'autonomie technologique et la sécurité des acteurs européens. Identifier et activer ces leviers revient à aborder un sujet vaste et complexe, qui nécessite une coordination étroite entre acteurs publics et privés. Ils concernent à la fois la capacité d'innovation technologique, le développement d'infrastructures sécurisées, le soutien à un tissu industriel local compétitif et la mise en place de normes communes au niveau européen. La première étape consiste à réduire la dépendance vis-à-vis des outils numériques, des infrastructures et des solutions de cybersécurité non européennes.

Dans un marché largement dominé par des acteurs extra-européens, privilégier des alternatives locales permet non seulement de reprendre la maîtrise des technologies et des données, mais aussi d'affirmer une véritable autonomie stratégique en matière de sécurité et de numérique.

Ce choix technologique ne se limite pas à une logique de sécurité : il participe également au dynamisme économique. Développer et adopter des solutions européennes revient à soutenir l'industrie numérique et la cybersécurité à l'échelle continentale et à stimuler la création d'emplois qualifiés. A l'inverse, continuer à importer massivement des technologies américaines revient à financer indirectement l'économie numérique des États-Unis, au détriment des capacités locales.

Pour atteindre ces objectifs économiques et renforcer la souveraineté numérique, plusieurs outils sont déjà à la disposition des organisations : le financement de projets de recherche, la coopération et le partage d'informations entre acteurs, l'élaboration et l'adoption de normes communes, ainsi qu'un cadre réglementaire robuste (RGPD [5], NIS2, DORA [6], etc.). Ce sont autant d'initiatives qui visent à consolider un écosystème numérique européen résilient, capable de répondre au défi de la souveraineté, tout en favorisant l'innovation collective.

Réduire cette dépendance signifie aussi limiter l'exposition aux législations extraterritoriales. Le Cloud Act[7] américain, par exemple, autorise l'accès aux données, qu'elles soient privées ou publiques, y compris lorsqu'elles sont stockées hors du territoire américain. Cette réalité juridique illustre le risque d'un manque de souveraineté : laisser une puissance étrangère disposer d'un droit d'accès sur des données sensibles, à l'insu même de leur propriétaire.

Alors, l'objectif ultime consiste à susciter un véritable élan collectif, capable de fédérer l'ensemble des acteurs publics et privés autour d'un objectif partagé, celui de bâtir un numérique européen autonome, sûr et durable. La souveraineté ne saurait reposer sur la seule volonté de quelques parties prenantes de l'écosystème. Elle exige une mobilisation d'ensemble, cohérente et ambitieuse. La dynamique est néanmoins en marche : les pouvoirs publics multiplient les initiatives en ce sens et, sur le terrain, les entreprises comme leurs clients expriment de plus en plus clairement cette exigence d'indépendance technologique.

C'est dans cette convergence d'actions et de volontés que réside la possibilité de transformer la souveraineté numérique en réalité tangible, au service de la sécurité, de l'économie et de l'avenir du continent.

[5] https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[6] https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en
[7] https://www.justice.gov/criminal/cloud-act-resources