Le numérique - La stratégie de cybersécurité de l'UE

Pourquoi est-ce important pour les intermédiaires ?

La **stratégie de cybersécurité de l'UE** est une initiative visant à renforcer la résilience face aux cybermenaces au sein de l'Union et à faire en sorte que les citoyens et les entreprises bénéficient de technologies numériques dignes de confiance. Afin de mettre en œuvre cette stratégie, les législateurs européens travaillent sur plusieurs propositions législatives. La **loi sur la cyberrésilience** vise à établir des règles communes de cybersécurité pour les produits numériques et les services associés qui sont mis sur le marché dans l'UE. La loi sur la cyberrésilience complétera la **Directive relative à des mesures visant à assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union (SRI2).** La **loi sur la cybersolidarité** vise à renforcer les capacités de l'UE à détecter les menaces et les attaques en matière de cybersécurité, à s'y préparer et à y réagir.

Etat des lieux

La loi sur la cyberrésilience

Le 15 septembre 2022, la Commission européenne a adopté une proposition de Règlement concernant les exigences horizontales en matière de cybersécurité applicables aux produits comportant des éléments numériques (loi sur la cyberrésilience). Selon la Commission, le matériel informatique et les logiciels font de plus en plus souvent l'objet de cyberattaques réussies, ce qui se traduit par des coûts annuels élevés de la cybercriminalité à l'échelle mondiale. Dans un environnement connecté, un incident de cybersécurité touchant un produit peut affecter toute une organisation ou toute une chaîne d'approvisionnement.

La loi sur la cyberrésilience vise donc à créer les conditions nécessaires au développement de produits sécurisés comportant des éléments numériques et à créer les conditions permettant aux utilisateurs de prendre en compte la cybersécurité lors de la sélection et de l'utilisation de produits comportant des éléments numériques. La proposition comprend :

- des règles pour la mise sur le marché de produits comportant des éléments numériques, afin de garantir leur cybersécurité ;
- des exigences essentielles pour la conception, le développement et la production de produits comportant des éléments numériques, et des obligations pour les opérateurs économiques concernant ces produits en matière de cybersécurité ;
- des procédures spécifiques d'évaluation de la conformité pour les "produits critiques" comportant des éléments numériques ;
- des exigences essentielles pour les processus de traitement de la vulnérabilité mis en place par les fabricants afin de garantir la cybersécurité des produits comportant des éléments numériques tout au long de leur cycle de vie et des obligations pour les opérateurs économiques en ce qui concerne ces processus ;
- des règles relatives à la surveillance du marché et à l'application des règles et exigences susmentionnées.

Le 31 mars 2023, le rapporteur de la commission ITRE du PE a présenté son projet de rapport sur la proposition. Le projet de rapport du rapporteur :

- met sur pied un groupe d'experts sur la cyberrésilience pour soutenir la Commission et les autorités ;
- retarde quelque peu la manière dont les produits critiques devront se conformer aux schémas de certification de la cybersécurité prévus dans la proposition ;
- exige que l'argent des amendes perçues en cas de non-respect du Règlement soit affecté au programme numérique de l'UE.

Un certain nombre d'amendements supplémentaires ont été présentés par d'autres députés et ITRE doit encore adopter une version finale de son projet de rapport. Entre-temps, le Conseil doit également adopter sa position finale sur la proposition avant que les négociations en trilogue ne puissent commencer.

La loi sur la cybersolidarité

Le 18 avril 2023, la Commission a adopté sa proposition de Règlement établissant des mesures destinées à renforcer la solidarité et les capacités de l'Union en matière de détection des menaces et incidents liés à la cybersécurité, de préparation et de réaction à ces menaces et incidents (loi sur la cybersolidarité). Selon la Commission, l'objectif de la loi sur la cybersolidarité est de soutenir la détection et la sensibilisation aux menaces et incidents de cybersécurité, de soutenir la préparation des entités critiques et de renforcer la solidarité, la gestion concertée des crises et les capacités de réaction dans les Etats membres.

La proposition comprend les mesures suivantes :

- **la création d'un "bouclier cybernétique européen"** comprenant des centres d'opérations de sécurité nationaux et transfrontaliers. L'objectif du bouclier cybernétique est de détecter les cybermenaces et d'agir en temps utile grâce à l'utilisation de l'IA et de l'analyse avancée des données ;
- **la création d'un "mécanisme d'urgence cybernétique"** visant à accroître la préparation et à améliorer les capacités de réponse aux incidents. Ce mécanisme sera notamment chargé de tester les entités des secteurs

hautement critiques. Il créera également une nouvelle "réserve de cybersécurité de l'UE" qui consistera en des services de réponse aux incidents fournis par des prestataires de services de confiance ayant fait l'objet d'un contrat préalable ;
- **la création d'un "mécanisme d'examen des incidents de cybersécurité"** visant à renforcer la résilience de l'Union par l'examen et l'évaluation des incidents de cybersécurité importants.

La proposition va désormais être examinée par le Parlement européen et le Conseil.

La Directive relative à des mesures visant à assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union (Directive SRI2)

La Directive SRI2 a été adoptée le 14 décembre 2022 et est entrée en vigueur le 16 janvier 2023. Elle a remplacé la Directive relative à la sécurité des réseaux et des systèmes d'information (Directive SRI) et améliore la résilience et les capacités de réponse aux incidents des secteurs public et privé et de l'UE dans leur ensemble.

La Directive SRI2 est un cadre contenant des mesures générales visant à renforcer la cybersécurité dans l'UE. Elle s'applique aux entités essentielles et importantes, tant publiques que privées, qui fournissent leurs services ou exercent leurs activités au sein de l'Union. Les secteurs auxquels s'applique la Directive SRI2 sont énumérés à l'annexe de la Directive et comprennent le secteur bancaire (et notamment les établissements de crédit) et le secteur des infrastructures des marchés financiers (et en particulier les opérateurs de plateformes de négociation en vertu de la MiFID II et les contreparties centrales en vertu du Règlement EMIR). Les intermédiaires d'assurance et les conseillers financiers ne sont pas mentionnés dans les annexes (mais il s'agit d'une Directive d'harmonisation minimale, ce qui signifie que les Etats membres peuvent choisir d'étendre son champ d'application).

Les Etats membres devront adopter et publier les mesures nécessaires pour se conformer à la Directive SRI2 avant le 17 octobre 2024, et devront appliquer ces mesures à partir du 18 octobre 2024.

Position / messages clés du BIPAR

Le BIPAR soutient l'initiative visant à renforcer la cyberrésilience et la coopération dans l'ensemble de l'Union. Il a souligné la nécessité pour les cadres émergents de prendre en compte les règles sectorielles préexistantes (par exemple la loi sur la résilience opérationnelle numérique pour le secteur financier) afin d'éviter la duplication des obligations ou la fragmentation du cadre.

Prochaines étapes

Le BIPAR continuera à suivre les procédures relatives à l'adoption de la loi sur la cyberrésilience et de la loi sur la cybersolidarité au fur et à mesure de leur examen par le Parlement européen et le Conseil, et à évaluer l'impact que ces propositions pourraient avoir sur notre secteur.

Liens

- La stratégie de cybersécurité
- Loi sur la cyberrésilience
- Directive SRI2
- Loi sur la cybersolidarité
- Projet de rapport du rapporteur de la commission parlementaire ITRE
- Site web du BIPAR : dossier sur le numérique