LA REVISION DE LA DIRECTIVE « SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION » (NIS 2)

Actualité législative publié le **28/11/2023**, vu **916 fois**, Auteur : Murielle Cahen

L'évolution du paysage des menaces a conduit la Commission à effectuer une révision de la directive « sécurité des réseaux et des systèmes d'information ».

Depuis plusieurs années déjà, la législation adoptée se montre favorable à la dématérialisation des usages dans tous les secteurs de l'économie. Sont notamment mis en avant les gains de productivité ainsi que la célérité que garantit l'usage du numérique. La crise Covid marque un tournant dans l'inclusion du numérique à nos sociétés en permettant d'assurer la continuité de nos économies. Et pourtant la cybercriminalité n'a jamais autant explosé que depuis la crise sanitaire liée à la Covid-19.

La dématérialisation de nos échanges, de nos processus de travail, et l'extension de ces usages à tous les étages, en passant de l'Administration, aux déclarations fiscales en ligne, à la dématérialisation des dossiers patients, et bientôt des factures électroniques pour les entreprises, a fait remonter des vulnérabilités.

La protection du secret des affaires, du secret industriel, des inventions, mais également les données des citoyens deviennent une priorité pour les États membres. Nombreuses sont les conséquences politiques, sociales, économiques liées à la protection des réseaux et des systèmes d'information.

A une échelle plus générale, ce sont toutes les activités auxquelles sont intégrées le numérique qui risquent de voir leur bon fonctionnement être perturbé. La mondialisation a accru le phénomène d'interdépendance des acteurs. Dans le domaine du numérique, cette interdépendance est marquée par une asymétrie de la réglementation en fonction des états.

Afin d'endiguer ce problème, la Commission européenne a donc procédé à la révision de la directive « sécurité des réseaux et des systèmes d'information ». Adoptée par le Parlement européen le 10 novembre 2022, chaque État membre de l'Union Européenne dispose désormais d'un délai de 21 mois afin de transposer en droit national les différentes exigences réglementaires. La directive devrait donc entrée en vigueur en France au deuxième semestre 2024, au plus tard.

Sa révision a non seulement permis d'étendre son champ d'application et d'actualiser les notions qui y figuraient (I) mais aussi de créer de nouveaux objectifs face à l'évolution du paysage des cybermenaces qui pèsent sur les états (II).

I. La (nécessaire) modernisation du cadre juridique de la directive SRI

A. L'extension du champ d'application de la directive à de nouveaux secteurs

La révision de la directive « sécurité des réseaux et des systèmes d'information » a permis de revoir à la hausse la liste des secteurs et des activités soumis à des obligations. La première

version de la directive SRI était applicable à sept secteurs. Sa nouvelle version y ajoute à présent les secteurs qui opèrent dans le domaine spatial, les services postaux, les producteurs de certains produits, de la nourriture, des administrations publiques, des services de communication, des eaux usées et de la gestion des déchets.

Cependant, une application facultative de la directive est possible pour certaines entités. Ainsi, l'article 2 de la directive dispose que les États membres peuvent prévoir que le périmètre de la directive s'applique « aux entités de l'administration publique au niveau local […] » Autrement dit, il appartient à chaque État membre d'apprécier la nécessité d'élargir l'application de la directive à ses collectivités territoriales.

Publié fin janvier, le rapport réalisé par l'ANSSI intitulé « Panorama de la cybermenace 2022 » révèle que les collectivités locales constituent la deuxième catégorie de victime la plus affectée par des attaques par rançongiciel derrière les TPE, PME et ETI. Elles représentent ainsi 23 % des incidents en lien avec des rançongiciels traités par ou rapportés à l'ANSSI en 2022.

Enfin, la directive exclut d'office les entités de « l'administration publique qui exercent leurs activités dans les domaines de la sécurité nationale, de la sécurité publique, de la défense ou de l'application de la loi, y compris la prévention et la détection des infractions pénales, ainsi que les enquêtes et les poursuites en la matière. »

Cette directive permet d'adopter des solutions afin d'améliorer la cyber résilience et de réagir plus efficacement aux cyberattaques, en particulier celles ciblant des activités essentielles pour l'économie et la société, tout en respectant les compétences des États membres, y compris la responsabilité qui est la leur en matière de sécurité nationale.

B. **La restructuration des opérateurs de services essentiels**

La révision de la directive SRI a pour objectif de surmonter les lacunes de la différenciation entre les opérateurs de services essentiels et les fournisseurs de services numériques, qui s'est avérée obsolète puisqu'elle ne reflète pas l'importance des secteurs ou des services pour les activités économiques et sociétales dans le marché intérieur.

Le périmètre de ces opérateurs régulés sera divisé en deux typologies d'acteurs prévus à l'article 3 de la directive. D'une part, les entités essentielles (EE) et d'autres part, les entités importantes (EI), dont la différenciation se fera par la criticité des secteurs associés. Elle comprend désormais toutes les entités de taille moyenne et grande dont les activités entrent dans le champ de la directive. Les entités essentielles et importantes sont confrontées aux mêmes obligations, mais celles qui relèvent de la deuxième catégorie sont soumises à un régime d'application plus léger.

Ces entités essentielles et importantes devront « prendre des mesures techniques, opérationnelles et organisationnelles appropriées pour gérer les risques liés à la sécurité des réseaux et des systèmes d'information. » Cette stratégie devra également prendre en compte les sous-traitants, qui représentent encore le maillon le plus faible dans la chaîne de valeur, notamment en raison des attaques par rebond engagées par les cyberattaquants afin de remonter vers un prestataire plus important.

Les États membres et leurs autorités nationales compétentes devront s'assurer de la mise en œuvre de la stratégie initiée par la directive. Elle permet d'une part d'éveiller les entités visées par la directive à l'importance de la mise en œuvre de mesures appropriées pour garantir la sécurité de leurs réseaux et de leurs systèmes d'information. D'autre part, elle tend à responsabiliser la direction des entités concernées par la directive qui pourra voir sa responsabilité engagée en cas de non-conformité.

Enfin, bien qu'ils ne soient plus responsables dans la détermination des opérateurs de services essentiels, les États membres devront établir une liste des entités essentielles et importantes ainsi que des entités fournissant des services d'enregistrement de noms de domaine. Les États membres devront dresser cette liste au plus tard pour le 17 avril 2025 et procéder à sa mise à jour régulièrement, puis au moins tous les deux ans par la suite. Le contenu de cette liste est fixé par son article 3.4)

Afin de faciliter le travail des États membres, la directive prévoit qu'ils devraient pouvoir considérer comme des entités essentielles, les entités déjà identifiées comme opérateurs de services essentiels conformément à la directive (UE) 2016/1148.

Les États membres devront également communiquer à la Commission des informations relatives aux entités essentielles et importantes. La communication de ces informations permettra un suivi en temps réel de la situation au niveau européen ainsi qu'une meilleure coordination en vue d'adopter une stratégie commune.

II. L'harmonisation du cadre européen comme rempart face à la cybercriminalité

A. La consolidation de la coopération transfrontalière (dans la gestion des cyber incidents)

La cybersécurité est un facteur essentiel permettant à de nombreux secteurs critiques d'embrasser la transformation numérique et de saisir pleinement les avantages économiques, sociaux et durables de la numérisation.

En vertu de l'article 7, chaque État membre devra adopter une stratégie nationale en matière de cybersécurité. Cet article instaure un certain nombre de points dans lesquels chaque état devra œuvrer. Parmi ces différents points, il est possible de retenir que chacun devra élaborer « un plan comprenant les mesures nécessaires en vue d'améliorer le niveau général de sensibilisation des citoyens à la cybersécurité. »

La cybersécurité doit s'immiscer dans les plus petites structures et auprès des citoyens afin de rendre effective la stratégie européenne et pour cela, la sensibilisation devra en être un des piliers. L'erreur humaine reste en effet une des principales sources des cyber incidents qui surviennent en entreprise

La révision de la directive a permis de prendre des mesures afin remédier à la fragmentation du marché intérieur. En effet, face au degré de résilience variable des États membres, l'adoption d'une réponse conjointe à la crise semblait nécessaire. Sa mise à jour reprend les objectifs déjà mis en place par son ancienne version tout en y ajoutant un cadre de coopération.

Pour ce faire, chaque État membre devra en vertu de l'article 8, désigner quelle(s) autorité(s) compétentes seront chargées d'une part de la cybersécurité et, d'autre part, de la gestion des incidents de cybersécurité majeurs et des crises. Cette coopération sera assurée par la collaboration entre trois autorités.

D'une part les « centres de réponse aux incidents de sécurité informatique » auront leur rôle à jouer. Il s'agit d'un centre établi par (et dans) chaque État membre, conformément la directive SRI de 2016, chargée de répondre aux incidents de sécurité. Est également inclus, le Groupe de Coopération NIS, qui rédige les lignes directrices à l'intention des autorités nationales et coordonne leur action.
Enfin, la directive intègre à son article 16 le réseau « CyCLONe ». Créé en 2020, ce réseau a pour objectif de contribuer à la mise en œuvre d'un plan d'action en cas de cyberattaque ou de crise transfrontalière, et de permettre aux entreprises de mieux partager l'information relative aux menaces.

La révision de la directive « sécurité des réseaux et des systèmes d'information » initie ainsi la collaboration entre ces trois intervenants et permet d'envisager une coopération transfrontalière accrue.

B. **La nécessaire intervention de la réglementation dans des domaines annexes**

À peine adoptée, la directive NIS 2 doit être complétée par un nouveau texte relatif à la cybersécurité des objets connectés. Le « Cyber Resilience Act », au stade de la proposition législative, doit renforcer la sécurité informatique des produits numériques en s'attaquant notamment au problème de la vulnérabilité des objets connectés.

À travers l'adoption de cette loi, la Commission entend agir plus fermement sur la sécurité des produits connectés en introduisant la cybersécurité dès la conception et prémunir les consommateurs contre la multiplication des défaillances et des atteintes à la vie privée.

Pour faire respecter ces futures obligations, la Commission européenne table sur des sanctions administratives pouvant aller jusqu'à 15 millions d'euros ou jusqu'à 2,5% du chiffre d'affaires annuel mondial pour le régime de pénalités le plus élevé.

La nouvelle directive a également été alignée sur la législation sectorielle, en particulier sur le règlement sur la résilience opérationnelle numérique du secteur financier (DORA).

Adopté par la Commission européenne le 10 novembre 2022, ce nouveau règlement devrait entrer en vigueur le 17 janvier 2025 au plus tard.

Son principal objectif est d'harmoniser les exigences en matière de risques liés aux technologies de l'information et de la communication à travers l'Europe. Ce règlement permet à l'Union d'exiger des garanties de la part des organisations en les invitant à se plier au respect d'un cadre normatif pour résister notamment aux incidences cyber qui deviennent de plus en plus critiques. Il est possible de citer les fraudes à la carte bancaire, l'usurpation d'identité, ou encore les attaques envers les systèmes d'information. Le règlement DORA devrait ainsi permettre de préserver la stabilité et l'intégrité des marchés financiers mais aussi d'assurer un niveau élevé de protection des investisseurs et des consommateurs.

SOURCES :

La Directive : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555&from=FR

Rapport « Panorama des cybermenaces 2022 » ANSSI : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

Le Département de Seine-Maritime touché par une cyberattaque le 10 octobre 2022 : https://www.paris-normandie.fr/id349866/article/2022-10-10/le-departement-de-seine-maritime-touche-par-une-cyberattaque-les-services

Article concernant les obligations des EI et des EE : https://www.droit-technologie.org/actualites/directive-nis-2-renforcer-la-securite-it-en-europe/

ERIC HAZANE, (In)sécurité numérique et PME : transformer les défis en atouts, CAIRN : https://www.cairn.info/revue-securite-et-strategie-2016-2-page-14.htm

Pour en savoir plus sur le réseau Cyclone : https://www.ssi.gouv.fr/actualite/blue-olex-2020-les-etats-membres-de-lunion-europeenne-lancent-le-reseau-de-coordination-cyclone/

Le cyber résilience Act : https://www.zdnet.fr/actualites/la-commission-europeenne-va-obliger-les-fabricants-d-objets-connectes-a-muscler-leur-cybersecurite-39947278.htm

Le cyber résilience Act : https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act

Proposition Règlement DORA : https://eur-lex.europa.eu/legal-content/FR/ALL/?uri=CELEX:52020PC0595

Clara Saillant, « La directive SRI 2 : élargissement du champ d'application et renforcement de la coopération en matière de cybersécurité », Dalloz Actualités, Revue IP/IT, le 17 janvier 2023 : https://www-dalloz-actualite-fr.gutenberg.univ-lr.fr/flash/directive-sri-2-elargissement-du-champ-d-application-et-renforcement-de-cooperation-en-matiere