Transposition de la directive NIS 2
Approches et opportunités

Une version de travail du projet de loi de transposition de la directive européenne NIS 2[1] a été publiée le 4 avril 2024 par *L'Informé*. La note interne à l'administration qui devait accompagner le texte du projet de loi pour l'expliciter a été publiée par le même media en ligne le 5 avril.

Le projet de projet de loi transpose simultanément trois directives, la directive NIS2, la directive sur la résilience des entités critiques (REC) et la directive sur la résilience opérationnelle numérique du secteur financier qui accompagne le règlement DORA.

Pour la partie cybersécurité, le texte qui devrait, selon *L'Informé*, être examiné en interministériel le 9 avril, donne la mise en œuvre de l'application de la directive à l'ANSSI et crée une autorité indépendante qui prendra les sanctions contre les entreprises et leurs dirigeants en cas de manquements.

Malgré l'affirmation d'une forte concertation dans la note d'accompagnement, les ministères de tutelle ou en responsabilité des 15000 (!) futures entités essentielles et importantes prévues par la directive sont exclus du dispositif. Les effectifs supplémentaires nécessaires à la mise en œuvre de la directive devraient être absorbés par l'ANSSI et 180 M€ sur trois ans financeront les dispositions que devront prendre les 661 collectivités qui seront désignées entités essentielles et les 992 communautés de communes désignées entités importantes.

Les chiffres annoncés dans la note ne sont appuyés par aucune étude d'impact à disposition des ministères.

Enfin, la sécurité du numérique n'est pas une fin en soi. Les crises deviennent hybrides, il importe donc de repositionner la sécurité du numérique au cœur et au service des métiers.

Le 4 avril, le CyberCercle était auditionné par la Commission Supérieure du Numérique et des Postes qui prépare un rapport sur la transposition de la directive NIS 2. Au cours de cette audition, le CyberCercle a présenté les éléments présentés ci-après.

***

La transposition de NIS 2 va se matérialiser par un projet de loi que le Parlement devra examiner, amender et voter. Pour la rédaction du projet de loi, deux approches se présentent et s'opposent : une approche administrative conservatrice, une approche politique dynamique.

L'approche administrative que vont probablement suivre les rédacteurs du projet de loi consiste à considérer NIS 2 comme une évolution de NIS 1 en arguant de « l'augmentation de la menace » et du besoin de résilience de nations de plus en plus innervées par le numérique. Dans cette approche, il s'agit de conserver et de conforter l'organisation administrative existante en matière de cybersécurité et les méthodes utilisées pour la transposition de NIS 1 par un projet de loi qui transpose a minima.

[1] https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32022L2555

Malgré le contexte budgétaire, les effectifs et les budgets des administrations concernées - essentiellement SGDSN et ANSSI - sont substantiellement augmentés afin de mettre en œuvre la directive dans tous ses aspects jusqu'à la proposition de sanctions. La mise en œuvre concrète est renvoyée à de nombreux textes réglementaires pour chacun des secteurs et la décision des sanctions (dont sont exclues administrations et collectivités) est confiée à une nouvelle autorité indépendante créée pour l'occasion.

Or, si la mise en œuvre de la partie cybersécurité de la Loi de programmation militaire de 2013 a vu un réel travail de concertation entre l'ANSSI, les ministères coordinateurs et les entités concernées, la transposition de NIS 1 s'est faite sans consultation effective des administrations connaissant les métiers des secteurs et les entités concernés par la directive.

Au regard de l'extension du champ d'application de la directive, la reconduction de méthodes similaires qui excluent les ministères concernés dans l'application de NIS 2 aurait des conséquences négatives pour l'ANSSI (diversion de ses missions essentielles), les ministères concernés (pertes de connaissances sectorielles) et les entités essentielles ou importantes (analyses de risques incomplètes, mesures inadaptées, etc.).

L'approche politique que pourrait suivre le Parlement prend acte d'une part d'un point de vue stratégique du développement du numérique et de son impact dans tous les aspects de la vie quotidienne des nations et des citoyens, et d'autre part d'une évolution continuelle des risques et donc de la nécessité de renforcer de manière cohérente la cybersécurité des écosystèmes concernés.

La rupture de logique entre NIS 1 et NIS 2 dans le champ d'application de la directive, tant dans le nombre d'entités concernées (un minimum de 15000 opérateurs concernés en France soit 50 fois plus que pour NIS 1 !) que dans les objectifs fixés et les sanctions imposées est également prise en compte comme l'est l'opportunité ouverte avec l'identification précise des entités clefs de 18 secteurs d'activité. La transposition doit par ailleurs éviter les atteintes potentielles à la souveraineté et à la défense nationale portées par le texte et mesurer le coût humain et financier de l'application de la directive d'une part pour les finances publiques et d'autre part pour les hôpitaux, entreprises et les collectivités territoriales concernées.

D'un point de vue tactique, certains textes réglementaires appelés par les prémices de NIS 1 (des articles de la loi de programmation militaire de 2013), n'ont été publiés qu'en 2023, soit dix ans après le vote ! Certains de ces textes réglementaires ne prennent pas en compte la réalité des métiers ou les vulnérabilités embarquées dans certains systèmes vendus sur étagère, voire sont orthogonaux à d'autres dispositions réglementaires, dans le domaine de la santé par exemple.

Devant ces constats, le Parlement pourrait choisir d'orienter la transposition selon cinq axes de travail complémentaires.

Premier axe, **incarner les discours sur la souveraineté** en exploitant le recensement des entités essentielles et importantes des 18 secteurs d'activité visés par la directive pour traiter cette cartographie en « filières stratégiques » et travailler à une déclinaison régionale. L'objectif est d'étendre l'analyse de risques, de soutenir les acteurs économiques et leurs écosystèmes, leur développement, d'éviter leur prédation, etc. en les accompagnant de manière interministérielle, sous le pilotage du ministère de tutelle ou en responsabilité. Le rôle économique des Régions peut également contribuer substantiellement à la dynamique des entités identifiées et à la montée en compétence des prestataires informatiques des collectivités.

Le rapport aux entités n'est plus seulement une démarche de contrôle de leur cybersécurité par l'imposition de règles et le recours obligatoire à des prestations de service ou à des équipements mais également un accompagnement dans leur développement et le soutien à l'élaboration d'une offre technique correspondant aux métiers et aux besoins opérationnels.

Deuxième axe, **exploiter les compétences métiers des acteurs institutionnels**. Il s'agit d'utiliser au mieux la connaissance des écosystèmes par les administrations en charge afin d'accompagner efficacement les entités et d'éviter la création de doublons pour limiter l'impact sur les finances publiques.

Dans cette optique les rôles sont répartis en fonction des compétences, des missions et de la connaissance des écosystèmes :

- le SGDSN, en collaboration avec les ministères, définit les politiques de protection des entités essentielles et importantes (comme il le fait par exemple pour la protection du patrimoine scientifique et technique) ;
- les ministères coordinateurs veillent à ce que les entités dont elles ont la tutelle ou la responsabilité sont bien identifiées (après enregistrement en ligne par exemple), s'assurent de la validité des analyses de risques effectuées (avec validation ou soutien de l'ANSSI pour la partie cybersécurité). Cette méthode permet de traiter la masse des entités concernées et d'intégrer la cybersécurité au cœur des « métiers » ;
- l'ANSSI, point de contact et CSIRT national, assure la mise en œuvre technique de la directive, les relations avec l'ENISA et participe au groupe de coopération ;
- certaines administrations ont un rôle transversal, comme par exemple le Commissariat au Plan (si l'on souhaite être ambitieux), la direction générale des entreprises, la direction générale de la sécurité intérieure, etc. Les Régions apportent leur soutien (par exemple en matière de formation des prestataires informatiques de proximité) ;
- instruites par l'ANSSI, les décisions de sanctions sont portées par les ministères coordinateurs qui prennent en compte l'ensemble des paramètres relatifs à l'entité concernée.

Cette répartition du travail permet également d'assurer la lisibilité du dispositif et de respecter le calendrier imposé (par exemple le 17 avril 2025 pour l'établissement de la liste des entités essentielles et importantes).

Troisième axe, **capitaliser sur l'existant**. Au-delà de ses aspects techniques exigeants (logiciels, matériels, audits), et depuis plus de dix ans, des acteurs de natures diverses travaillent en matière de cybersécurité à la sensibilisation et à la prévention de publics variés : politiques, entreprises, collectivités, administrations, associations, etc. Plus récemment, un partenariat public-privé, le GIP ACYMA, favorise la prévention, permet un diagnostic et facilite la mise en relation de victimes d'actes de cybermalveillance et de prestataires susceptibles d'y remédier. Le « 17 Cyber » voulu par le Président de la République participe de cette logique qui reste à développer.

La directive met en avant ce type de partenariat (Cons. 55) et impose la formation des dirigeants et des personnels des entités essentielles (Art. 20). Il importe de favoriser les acteurs ayant acquis les compétences nécessaires et la connaissance des territoires afin d'assurer prévention et formation de qualité pour les entités essentielles et plus largement pour les entités importantes et l'ensemble des acteurs économiques et institutionnels.

Enfin, comme cela se pratique dans d'autres pays, il est souhaitable de s'appuyer sur les normes, standards et référentiels existants et partagés par les acteurs économiques plutôt que d'en créer de nouveaux, au risque de l'incohérence, du cumul des coûts, de la complexité de la mise en œuvre et du contrôle.

Quatrième axe, **élaborer une stratégie nationale de cybersécurité globale.** La directive prévoit l'élaboration de stratégies nationales de cybersécurité et en propose un contenu. Le travail interministériel en cours devrait intégrer les aspects proposés par la Commission afin de renouer avec une certaine visibilité de la politique et de l'action publique et de favoriser la mobilisation des énergies nationales. Le travail d'évaluation du Parlement en serait par ailleurs facilité.

Cinquième axe, **impliquer le Parlement.** Le Parlement a publié de nombreux rapports sur des questions liés au numérique et à la cybersécurité. L'impact de ces rapports dans la décision publique a été limité malgré la qualité de certains travaux. Des parlementaires portent par ailleurs des sujets qui méritent une part plus importante dans le débat public.

Afin d'avoir une meilleure visibilité sur la mise en œuvre de la directive, de mieux contrôler et évaluer l'action du Gouvernement, le texte de transposition pourrait prévoir que les rapports prévus dans le texte (Art. 14, 16, 18, 23, 40) lui soient transmis.

Le texte du projet de loi qui sera présenté au Parlement mettra en évidence le choix du Gouvernement. S'il choisit une approche administrative conservatrice, il pourrait l'imposer avant l'été par une procédure accélérée (une seule lecture par Chambre).

Il appartiendrait alors au Parlement d'amender voire de réécrire un texte qui exploiterait au mieux l'opportunité portée par la transposition de NIS 2 de dynamiser 18 secteurs d'activité et d'assurer le développement de 15000 entités essentielles et importantes tout en augmentant de manière significative la résilience de la France.

ANNEXE

Quelques points d'attention

Si la directive suscite des réserves quant aux documents qui ont contribué à son élaboration[2], elle constitue surtout une rupture de logique avec celle qui a prévalue lors l'élaboration de la LPM 2013 et de NIS 1 et confirme l'envahissement du domaine de la cybersécurité par la bureaucratie et par le droit, de forme anglo-saxonne qui plus est[3].

A la lecture de ses 144 considérants, de ses 46 articles et 3 annexes, cette directive présente des risques pour la souveraineté et la sécurité nationale, le fonctionnement et l'équilibre des entités appartenant aux secteurs d'activité visés par la directive.

Le changement de logique entre les mesures de la LPM 2013 destinées aux opérateurs d'importance vitale (OIV), NIS 1 et NIS 2 :

- NIS 2 entraîne un élargissement considérable du champ d'application de la directive (Cons. 83, 85. Art. 21) : de 7 à 18 secteurs d'activité ; en France, de 300 entités suivies actuellement à bien plus de 15000 puisqu'est évoquée l'applicabilité de la directive aux fournisseurs de fournisseurs des entités ! Applicable jusqu'au petites entreprises ou au micro entreprises (Cons. 7) selon certaines conditions si les Etats-membres le souhaitent.
- Contrairement à la LPM 2013 ou à NIS 1 dans lesquelles seuls les systèmes d'information critiques des entités font l'objet de mesures de protection, dans NIS 2, l'ensemble des systèmes d'information est soumis à mesures.
- Au prétexte d'harmonisation du marché intérieur, le principe de subsidiarité qui prévalait dans NIS 1 devient l'exception au profit de la Commission, notamment dans la gestion de crise (Cons 71).

Les risques relatifs à la sécurité et à la souveraineté nationale :

- La directive donne à la Commission la capacité d'imposer par des « actes délégués » et par des « actes d'exécution » de mesures ou d'utilisation de produits devant s'appliquer aux entités essentielles ou importantes (Cons.22, Art.23, 24, 38) sans qu'un Etat-membre puisse déroger.
- Bien que les administrations des domaines de la défense, de la sécurité publique et de l'application de la loi soient exclues du champ de la directive (Cons. 8, 9. Art. 2) et qu'il soit précisé qu'un Etat-membre n'est pas tenu de transmettre une information susceptible de nuire à sa sécurité ou à sa défense nationale (cons. 9), la vigilance s'impose quant à la nature des informations transmises. Ainsi les informations d'identification (noms, coordonnées…) ou techniques (plages IP…) que les Etats-membres doivent transférer à la Commission ou à l'ENISA relatifs à l'identité des entités essentielles, importantes ou à propos des incidents sont potentiellement de nature à favoriser l'espionnage ou l'intelligence économique contre des

[2] Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union | Shaping Europe's digital future (europa.eu)
https://op.europa.eu/en/publication-detail/-/publication/3b6ad641-d23c-11eb-ac72-01aa75ed71a1/language-en/format-PDF/source-309992224

[3] Ce qui entraîne un texte souvent verbeux.
Exemple du considérant 102 : « *Les Etats membres devraient veiller à ce que l'obligation de soumettre cette alerte précoce, ou la notification d'incident ultérieure, ne détourne pas les ressources de l'entité effectuant la notification des activités liées à la gestion des incidents qui devraient avoir la priorité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents importants ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard.* »

intérêts nationaux. (Cons. 19, Art. 3, 9, 27). La question du gain réel, en termes de sécurité du numérique, de transmettre ces éléments peut être posée.

- En instaurant une gouvernance européenne de la cybersécurité (Art. 18, 19, 22, 24), cette directive représente vraisemblablement les prémices d'un futur règlement qui transférerait à la Commission et à ses agences les compétences souveraines des Etats-membres.

Les risques susceptibles de mettre en danger l'activité des entités essentielles et importantes :

- L'ensemble du système d'information des entités essentielles et importantes est concerné par la mise en œuvre de la directive ce qui représente un coût qui pour beaucoup d'entités est insupportable (hôpitaux, établissements publics de recherche, collectivités territoriales, PME-PMI, etc.).
- Intervient dans la vie des entreprises Art 20, intrusive, Art 21, Art 29, Art 32 et (Cons. 133, Art. 33) dirigeants.
- Les sanctions prévues par la directive sont de nature à pénaliser gravement les entreprises et dirigeants qui seraient exposés. Les décisions relatives aux sanctions doivent rester à la main des administrations et ne doivent pas relever d'une entité indépendante qui n'aurait pas la capacité d'en mesurer toutes les conséquences (Art.31).
- La directive introduit la notion « d'incidents évités » (Cons. 139, Art. 6, 13, 14, 15, 23, 29, 30) et soumet ces incidents à notification. La définition proposée par la directive impliquerait potentiellement de signaler chaque jour des centaines d'incidents, ce qui est évidemment irréaliste, nonobstant la multiplication des entités qu'il faut notifier (ANSSI, CNIL, Archives, CERT Sectoriels…).
- NIS 1 a mis en évidence les risques de distorsions économiques liés aux diverses transpositions et le coût des mesures de cybersécurité pour les OSE. NIS 2, certes plus précise dans les exigences, ne règle toujours pas ce phénomène de distorsions que ce soit dans les mesures, notamment techniques, imposées ou dans le régime de sanction.
- Difficulté à identifier de quelles réglementations les entités dépendent les régulations, s'empilent ou non… selon la nature des mesures imposées RGPD (Cons. 14, 23).

Les risques institutionnels et d'applicabilité :

Une transposition de la directive qui confierait sa mise en œuvre aux seules administrations en charge de la sécurité ou de la cybersécurité entraînerait mécaniquement :

- Une perte de la connaissance par les ministères des entités essentielles et importantes qui dépendent de leur champ : d'une part les agents recrutés au SGDSN ou à l'ANSSI pour travailler les analyses de risques, coupés des ministères au quotidien, n'auront pas la connaissance fine des écosystèmes ; d'autre part il ne peut être demandé aux entreprises de consacrer un temps de travail pour leur ministère de tutelle et un temps de travail pour le même sujet à une administration qui ne connaît pas leur métier.
- Des coûts non maîtrisés pour les finances publiques et la duplication de fonctions : les agents recrutés à l'ANSSI pour la connaissance des 18 secteurs d'activités visés par la directive feront doublon avec ceux des ministères dont ces secteurs relèvent, qui plus est dans un contexte de pénurie de ressources en matière de cybersécurité. De son côté, la création d'une entité indépendante dédiée aux sanctions, outre le fait qu'il s'agit d'une dépossession de l'Etat, nécessiterait la création de postes de catégorie A, le recrutement d'experts techniques, des locaux, etc. dans un contexte de réduction souhaitée du budget de fonctionnement de l'Etat.
- Le métier de l'ANSSI évoluerait de la performance technique à la performance bureaucratique, la part significative de ses effectifs existante ou recrutée alors consacrée au suivi des secteurs

d’activités venant de plus solliciter les effectifs chargés de l’analyse de la menace et de sa remédiation technique. Il y a un risque d’entrave à l’activité de l’agence alors même que la directive ouvre ou élargit certaines opportunités techniques (Cons. 43, 44).

- Le Premier ministre devrait gérer une entité qui s’éloignerait plus encore de ses missions d’anticipation et frôlerait « l’obésité », avec déjà plus de 1200 agents (SGDSN + IHEDN + OSIIC + VIGINUM + ANSSI + Haut-Commissaire à l’énergie atomique), qui plus est dans une gestion dérogatoire par rapport aux autres services du Premier ministre.