décembre 2024

Projet de loi « Résilience »
Contribution de Numeum

Dans un contexte d'aggravation de la menace cyber, la directive NIS 2 constitue un gage de résilience accrue de l'Europe et va permettre une élévation de notre niveau global de protection en matière cyber. Avec un nombre d'entités couvertes par la directive qui augmente très fortement en France (estimé entre 11.000 et 15.000 entités), notre objectif collectif est de faire de cette transposition une réussite sur le plan opérationnel. Outre les entités directement assujetties à la directive, un effet de « ruissellement » est à anticiper et il est probable que le niveau d'exigence prescrit par la directive se diffuse progressivement dans le reste de l'économie. Dans ce cadre, il est nécessaire qu'acteurs publics et écosystèmes agissent ensemble pour sensibiliser et accompagner le plus grand nombre d'entités à la mise en œuvre de ce texte. Le rôle des membres de Numeum est double à cet égard : d'une part, un certain nombre de nos entreprises seront assujetties aux obligations visées par la directive et sa transposition ; d'autre part, de nombreux membres joueront pleinement leur rôle d'acteurs de la conformité.

Le projet de loi « Résilience », qui transpose les directives NIS 2 et REC et adapte le droit français au nouveau règlement DORA, est par conséquent une étape importante dans ce mouvement de mise à niveau de notre protection. Numeum formule plusieurs recommandations présentées ci-dessous pour renforcer le caractère opérationnel de ce projet de loi et s'assurer que la transposition de la directive en France soit suffisamment harmonisée avec les autres Etats-membres de l'Union européenne.

Le projet de loi prévoit qu'un certain nombre de dispositions de la directive NIS2 feront l'objet d'une transposition par voie réglementaire, majoritairement par des décrets en Conseil d'Etat. Si ce choix est compréhensible pour conserver un certain degré de lisibilité dans le texte, Numeum insiste sur la nécessité, une fois que le projet de loi sera adopté, de consulter aussi largement que possible les écosystèmes dans l'élaboration des textes d'application. Cela sera clé pour accompagner la bonne mise en œuvre de la directive.

1. Des incertitudes qui demeurent sur la directive

Sur le champ d'application

Si la directive prévoit explicitement qu'un certain nombre d'acteurs du numérique sont assujettis aux dispositions du texte, des interrogations demeurent quant à l'application du texte à certaines catégories d'acteurs (certains acteurs du numérique, certaines professions libérales type expert-comptable, notaire, etc.). S'agissant des acteurs du numérique :

- L'annexe de la directive ne mentionne pas explicitement les éditeurs de logiciels comme entités assujetties aux dispositions du texte. Néanmoins, une incertitude demeure s'agissant des **éditeurs de logiciels en SaaS** (*Software as a Service*). En effet, le considérant 33 de la directive, relatif aux services d'informatique en nuage, prévoit que « *les modèles de services liés à l'informatique en nuage comprennent, entre autres, les*

infrastructures services (IaaS), les plateformes services (PaaS), les logiciels services (SaaS) et les réseaux services (NaaS) ». Les éditeurs proposant leurs services en SaaS représentant une part importante des éditeurs de logiciels en France, ce point doit être clarifié.

- Conformément aux articles 2 et 3 de la directive, l'article 10 du projet de loi prévoit que le Premier ministre peut désigner une entité, quelle que soit sa taille, comme entité essentielle ou importante dans plusieurs cas de figure, notamment lorsque la perturbation du service fourni par l'entité *« pourrait avoir un impact important sur [...] la santé publique* ». Ce point peut être déterminant sur **l'application de la directive aux TPE/PME du numérique en santé**, nombreuses chez Numeum. Il est dès lors nécessaire de clarifier la notion « *d'impact important sur la santé publique* » en élaborant par exemple, en concertation avec les opérateurs intéressés, une liste de critères objectifs permettant aux acteurs de déterminer s'ils sont assujettis, ou non, à la directive et sa transposition.

Sur la notion d'incident

La notion « d'incident important », centrale dans la directive, devra faire l'objet de précisions. Si l'article 23 de la directive fournit quelques éléments sur cette qualification, il est nécessaire d'**établir des critères objectifs** pour guider les futurs assujettis dans leur mise en conformité. L'article 17 du projet de loi prévoit qu'un décret en Conseil d'Etat fixera les critères d'appréciation des caractères importants et critiques des incidents et des vulnérabilités.

L'acte d'exécution du 17 octobre 2024 de la Commission européenne fixe ces critères pour les acteurs du numérique. Il est important que les critères fixés en France par décret pour toutes les autres catégories d'acteurs s'inscrivent **en cohérence avec la grille de lecture retenue par la Commission européenne**.

Par ailleurs, il sera important d'informer au plus tôt les écosystèmes sur les catégories de critères qui seront retenues, et si ces derniers reposeront ou non sur une ou plusieurs normes existantes et reconnues par le marché.

Sur l'application de la directive dans un groupe de sociétés

L'application de la directive aux entités intégrées à un groupe de sociétés devrait être explicitée : en effet, un même groupe peut détenir des filiales assujetties à la directive situées dans plusieurs Etats-membres de l'Union. Par ailleurs, **dans un même groupe, des filiales peuvent répondre à la qualification d'entité essentielle ou importante** : une qualification doit-elle s'imposer aux autres à l'ensemble du groupe ? Cette interrogation s'applique également pour les groupes dont les filiales proposent des services à vocation civile et militaire.

Sur l'application de la directive en cas de pluralité d'activités

Une **même entreprise** peut avoir **différentes activités**, **certaines correspondant à des secteurs identifiés comme critiques ou hautement critiques dans la directive, d'autres non**. Dans cette hypothèse, comment apprécier les critères d'application de la directive ? L'entreprise doit-elle prendre en compte uniquement la part de son chiffre d'affaires/bilan ou de ses effectifs qui correspond à l'activité identifiée comme critique pour déterminer si elle est assujettie ou non à la directive ?

Sur les voies de recours

Conformément à l'article 10 du projet de loi, le Premier ministre peut désigner des entités comme essentielles ou importantes dans plusieurs cas de figure. Dans l'hypothèse où **l'entité concernées serait en désaccord avec l'application à son égard de cette qualification, quelle(s) voie(s) de recours** lui seraient ouvertes pour contester le cas échéant cette désignation ?

Recommandation : **ces cinq points devraient faire l'objet d'une clarification**, que ce soit par la voie législative ou réglementaire, pour s'assurer du caractère opérationnel de texte. En tout état de cause, ces précisions devraient être fournies **suffisamment en amont pour permettre aux acteurs de se mettre en conformité dans les délais impartis par la directive**.

2. Sur le titre II « Cybersécurité » du projet de loi

Sur les seuils d'application

L'article 2 de la directive NIS2 vise une application du texte aux entités :

- qui constituent des entreprises moyennes en vertu de l'annexe 2 de l'annexe de la recommandation 2003/361/CE, soit celles dont l'effectif est d'au moins 50 personnes **et** dont le CA ou le bilan excède 10 millions d'euros.
- qui dépassent les plafonds prévus au paragraphe 1 du même article, soit celles dont l'effectif est d'au moins 250 personnes **et** dont le CA excède 50 millions d'euros ou dont le total du bilan excède 43 millions d'euros.

Il ressort ainsi de la lecture de la recommandation 2003/361/CE que **le critère relatif à la taille de l'effectif et celui relatif au CA/au bilan sont cumulatifs et non alternatifs**. Pourtant, si le projet de loi prévoit que la transposition de ces seuils interviendra par voie réglementaire**, la rédaction des articles 8 et 9 du projet de loi laisse entendre qu'il s'agit de critères alternatifs** (« *les entreprises appartenant à un des secteurs d'activité hautement qui critiques qui emploient au moins 250 personnes* ***ou*** *dont le chiffre d'affaires annuel excède 50 millions d'euros et dont le total du bilan excède 43 millions*» et « *les entreprises appartenant à un des secteurs d'activité hautement critiques ou critiques qui ne sont pas des entités essentielles et qui emploient au moins 50 personnes* ***ou*** *dont le chiffre d'affaires et le total du bilan annuel excèdent chacun 10 millions d'euros* »).

Recommandation : **aligner la rédaction des articles 8 et 9 avec la recommandation 2003/361/CE et clarifier que les critères de l'effectif d'une part, et du chiffre d'affaires ou du bilan d'autre part, sont bien cumulatifs et non alternatifs.**

Sur la notification à l'ANSSI en cas d'incident

L'article 17 du projet de loi prévoit une notification « *sans retard injustifié* » auprès de l'ANSSI en cas d'incident important, un décret pris en Conseil d'Etat devant fixer les modalités de cette notification. Or, l'article 23 de la directive prévoit un double-délai de notification de **24/72h**. **Ce double-délai est le fruit d'un compromis longuement débattu entre les colégislateurs européens** lors de l'adoption de la directive.

S'il semble légitime de recourir à la voie réglementaire pour prévoir les modalités pratiques de cette obligation, il est indispensable que **le projet de loi respecte la lettre de la directive NIS2**. Dans ce cadre, l'absence de référence au délai de 24/72h n'apparait pas conforme au double-délai expressément prévu par la directive. **Des législations hétérogènes entre Etats-membres sur la procédure de notification complexifierait considérablement l'application du texte** pour les entreprises qui sont présentes dans plusieurs Etats. A titre de comparaison, le législateur belge a transposé cette disposition dans les termes exacts de la directive, en mentionnant explicitement dans la loi le double-délai de notification de 24/72h[1].

En outre, il sera important que le texte réglementaire pris en application de l'article 17 **sanctuarise le temps nécessaire à l'entité pour analyser et qualifier l'incident**, cette phase intervenant avec l'aide des équipes opérationnelles et généralement durant une phase de crise. **La loi ne devrait faire débuter le début du délai qu'à l'issue de cette phase de qualification**. Cette logique a notamment été retenue par le décret pris pour l'application de l'article 66 de la loi de programmation militaire 2024-2030 (relatif à la déclaration de vulnérabilité pour les éditeurs de logiciels).

Enfin, il serait utile que la loi prévoie les moyens et les mesures qui seront mis en œuvre par l'ANSSI pour permettre que les notifications servent à la résilience de l'ensemble des acteurs concernés, tout en préservant le caractère confidentiel des informations notifiées.

Recommandation : assurer, que ce soit par la voie législative ou la voie réglementaire, que le délai de notification retenu en droit français en cas d'incident important soit **conforme au double-délai (24/72h) de notification tel que prévu par les colégislateurs européens lors de l'adoption de la directive NIS2.** A défaut, les entreprises risquent d'être assujetties à des procédures de notification hétérogènes entre les Etats-membres.

Sur la notification aux destinataires de service

L'article 17 prévoit que les entités notifient « sans délai » aux destinataires de leurs services « *les vulnérabilités critiques affectant leurs services ou les affectant potentiellement, ainsi que les mesures ou corrections, dès qu'elles ont connaissance, que ces destinataires peuvent appliquer en réponse à cette vulnérabilité ou à cette menace* ».

Cette rédaction appelle plusieurs observations :

- La mention d'une notification **« sans délai »** semble trop restrictive par rapport à la rédaction de l'article 23 de la directive, qui comprend la mention « sans retard injustifié ».
- La directive prévoit une notification pour les seules vulnérabilités remédiées là où le projet de loi est plus large et **semble inclure les vulnérabilités non-remédiées**. La notification à un volume potentiellement large de destinataires (celles « *potentiellement* » affectées par la vulnérabilité) de vulnérabilités non-remédiées apparait contre-productif et pourrait accroitre le risque d'exploitation par des acteurs malveillants de la vulnérabilité ainsi notifiée. Une rédaction plus conforme à la directive serait ainsi opportune.

[1] Loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, article 35.

Par ailleurs, le projet de loi prévoit que l'obligation de notification ne s'étend pas « *aux informations dont la divulgation porterait atteinte aux intérêts de la défense et de la sécurité nationale* ». Il serait pertinent de préciser que la **protection du secret des affaires et des informations commerciales confidentielles** puisse entrer également dans ce cadre.

Sur le recueil d'information par les autorités

Type d'informations collectées

L'article 32 de la directive ouvre la possibilité pour les autorités nationales d'accéder auprès des entités assujetties à « *des données, à des documents et à toutes informations nécessaires à l'accomplissement de leurs tâches de supervision* ».

Dans ce cadre, l'article 27 du projet de loi liste **les informations auxquelles les agents de l'ANSSI peuvent accéder en cas de contrôle d'une entité, sans que le secret professionnel ne puisse être opposé : les systèmes d'informations, les logiciels, les programmes informatiques et les données stockées**. Cette disposition, particulièrement large et portant sur des informations stratégiques et hautement confidentielles pour les entités régulées, apparait **disproportionnée** et devrait être davantage encadrée. Un critère limitant la collecte et l'exploitation des données aux seules données **directement utiles** à la réalisation de la mission de contrôle semble nécessaire. La **destruction** des données qui ne sont pas directement utiles au contrôle semble également nécessaire. Plus largement, il serait pertinent d'expliciter en amont en quoi le recueil de ce type d'information particulièrement sensible contribue directement au renforcement de notre résilience collective : cela sera clé pour garantir la confiance de tous les acteurs.

Echange d'informations entre autorités

La directive tout comme le projet de loi prévoient la mise en place d'une coopération entre les autorités chargées de la sécurité des systèmes d'information et d'autres autorités, en particulier celles chargées de la protection des données à caractère personnel. Cette coopération entre autorités est positive et constitue un gage d'efficacité dans l'élévation de notre résilience collective.

Plus précisément, l'article 2 de la directive NIS2 prévoit les conditions qui régissent les échanges de données confidentielles entre autorités : « *les informations considérées comme confidentielles en application de la réglementation de l'Union ou nationale, telle que les règles applicables au* ***secret des affaires****, ne peuvent faire l'objet d'un échange avec la Commission et d'autres autorités concernées conformément à la présente directive* ***que si cet échange est nécessaire à l'application de la présente directive****. Les informations échangées* ***se limitent au minimum nécessaire et sont proportionnées à l'objectif*** *de cet échange. Cet échange d'informations* ***préserve la confidentialité des informations concernées et protège la sécurité et les intérêts commerciaux des entités concernées****.* »

Le projet de loi comporte quant à lui les dispositions suivantes :

- L'article 17 prévoit que **l'ANSSI informe la CNIL de tout incident susceptible d'entraîner une violation de données à caractère personnel**.

- L'article 23 prévoit que **l'échange d'informations entre autorités peut intervenir simplement « *aux fins de l'accomplissement de leurs missions respectives* »**, sans que les dispositions de l'article 11 du code de procédure pénale ou celles relatives aux autres secrets protégés par la loi ne puissent y faire obstacle.

Ces deux dispositions appellent les observations suivantes :

- Le signalement « automatique » par l'ANSSI à la CNIL de toute incident susceptible d'entrainer une violation de données à caractère personnel tel que prévu à l'article 17 soulève des **interrogations en matière de sécurité juridique** : dans quelle mesure cet échange d'information est nécessaire au regard des objectifs poursuivis par la directive ? Ne porte-t-il pas atteinte à la procédure de déclaration auprès de la CNIL qui est justement prévue par le règlement général de protection des données (RGPD) en cas de violation de données ? Cette disposition pourrait en effet placer les responsables de traitement dans une situation de contrôle de conformité « a priori » par l'autorité de protection des données.
- Bien que le projet de loi prévoie un décret en Conseil d'Etat pour en fixer les modalités d'application, la rédaction de l'article 23 apparait **bien moins protectrice de la confidentialité et du secret des affaires que la directive**. Le projet de loi devrait adopter une rédaction plus conforme à l'esprit de cette dernière en n'autorisant les échanges d'informations entre autorités **que s'ils sont (i) nécessaires à l'application du texte, (ii) limités au minimum nécessaire et proportionnés à l'objectif et (iii) préservant la confidentialité, la sécurité, et les intérêts commerciaux des entités concernés**.
- Parmi les destinataires du partage d'informations mentionnés par l'article 23 du projet de loi figurent les **« *organismes internationaux concourant aux missions de sécurité ou de défense des systèmes d'informations* »**. Cette notion, définie ni par la directive ni par le projet de loi, soulève des interrogations : quelles organisations seraient éligibles à cette qualification (organisations supranationales, autorités étrangères, associations, etc.) ? Cette incertitude peut faire peser des risques sur les entités assujetties, que ce soit en termes de sécurité juridique, de préservation de la confidentialité et des intérêts commerciaux, ou encore de protection des données à caractère personnel.

Sanctions

L'article 28 du projet de loi prévoit des sanctions pouvant aller jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial lorsqu'une entité fait obstacles aux demandes d'informations de l'ANSSI, ou **en cas de fourniture de renseignements incomplets**. Ce dernier point semble disproportionné : l'urgence inhérente à une crise cyber ne permet pas toujours à une entité de fournir l'ensemble des informations requises dans les délais impartis, sans pour autant que sa bonne foi ne puisse être remise en cause. Un tel régime sanction apparait ainsi particulièrement répressif et n'est pas de nature à installer un cadre de confiance entre les entités et les autorités. Pour remédier à cette difficulté, la notion d'intention pourrait être intégrée dans la rédaction de l'article 20 pour exclure de la sanction les entités agissant de bonne foi.

Recommandation : **exclure les entités agissant de bonne foi du régime de sanction applicable en cas de transmission d'informations incomplètes.**

Proposition de rédaction de l'article 28, paragraphe 2 :

« *Le fait, pour la personne contrôlée, de faire obstacle aux demandes de l'autorité nationale de sécurité des systèmes d'information nécessaires à la recherche des manquements et à la mise en œuvre des pouvoirs prévus par la présente sous-section, notamment en fournissant* ***[sciemment]*** *des renseignements incomplets ou inexacts, ou en communiquant des pièces incomplètes ou dénaturées, est puni d'une amende administrative prononcée par la commission des sanctions mentionnée à l'article L. 1332-16 du code de la défense dont le montant, proportionné à la gravité du manquement, ne peut excéder dix millions d'euros ou 2 % du chiffre d'affaires annuel mondial, hors taxes, de l'exercice précédent, le montant le plus élevé étant retenu.* »

Sur les pouvoirs de l'ANSSI

A titre liminaire, le **cadre procédural entourant le contrôle d'une entité par l'ANSSI** pourrait faire l'objet de clarifications, à l'image des procédures de contrôle menées par d'autres régulateurs (ex. Arcep). En effet, la notion de « procédure » n'est elle-même évoquée qu'à l'article 31 du projet de loi et ne semble concerner que la phase postérieure au contrôle d'une entité par l'ANSSI.

L'article 29 décrit les formes que peut prendre un contrôle de l'ANSSI, notamment des audits ou des scans de sécurité. Il est précisé que **le coût de ces mesures est à la charge des entités contrôlées**, sauf décision contraire et exceptionnelle de l'ANSSI. Cette disposition est **disproportionnée** et peut, compte-tenu du coût potentiel de ces mesures, placer les entités contrôlées en difficultés financières.

L'article 32 du projet de loi vise à confier à l'ANSSI la capacité de mobiliser un éventail de « *mesures consécutives aux contrôles* », par exemple le prononcé d'une « *mise en garde* », l'adoption d'instructions contraignantes, ou encore la capacité « d'*enjoindre* [les assujettis] *de se mettre en conformité avec les obligations* », etc. Ce dispositif appelle plusieurs remarques :

- Tout d'abord, **la « *notion de mise en garde* » apparaît très peu précise et semble devoir être clairement définie**.
- Par ailleurs, **le quantum journalier projeté de l'astreinte prévu dans cet article (5.000€) semble très important pour les acteurs**, a fortiori s'agissant des entités importantes. **Un quantum différent** pour les entités importantes serait justifié.

Sur les mesures de gestion des risques

L'article 14 du projet de loi prévoit, conformément à la directive, que les entités assujetties doivent prendre certaines mesures techniques, opérationnelles et organisationnelles pour gérer les risques auxquels elles font face. L'article prévoit en outre qu'un décret en Conseil d'Etat « *fixe les objectifs* » auxquels doivent se conformer les entités afin que les mesures de gestion de risque à mettre en œuvre garantissent un niveau de sécurité adapté. Cette rédaction interroge : en vertu de l'article 21 de la directive, **les Etats-membres doivent-ils fixer les « mesures » à mettre en œuvre ou des « objectifs » à atteindre ?**

En tout état de cause, il conviendra d'assurer que ces mesures s'articulent correctement avec l'acte d'exécution de la Commission européenne du 17 octobre 2024 sur les mesures propres aux acteurs du numérique, et qu'elles soient fondées uniquement sur des critères techniques, objectifs, vérifiables et non-discriminatoires.

Sur l'application de la directive aux collectivités territoriales

L'article 8 du projet de loi prévoit l'application des exigences de la directive à plusieurs catégories de collectivités territoriales, en particulier les communes de 30.000 habitants. Ce seuil, qui ne concerne certes pas les entreprises en tant que telles, entraîne des conséquences pour les nombreux membres de Numeum qui compte des collectivités parmi leurs clients.

Si le chiffre de trente mille habitants n'appelle pas en lui-même de commentaire particulier, **le nombre d'habitants ne semble pas être un critère totalement pertinent pour déterminer l'application ou non de la directive**, car ne tenant pas compte des spécificités de chaque territoire (présence d'activités sensibles sur le territoire, variation de population selon les saisons, etc.). L'**évaluation de la criticité de chaque territoire et de chaque système d'information ou service public effectivement rendu par la collectivité**, semble être une piste davantage pertinente pour déterminer l'application de la directive aux collectivités.

Sur la mise en place d'un label de conformité

Il pourrait être pertinent de mettre en place un label dédié à la conformité aux exigences de la directive NIS2. Cela permettrait de guider les acteurs assujettis dans leur mise en conformité en en mettant à leur disposition des indicateurs fiables et objectifs sur le niveau d'exigence attendu. Un tel label pourrait reposer sur des critères de conformité préexistants et reconnus sur le marché (ex. certification ISO).

A propos de Numeum

Numeum est le syndicat patronal et la première organisation des professionnels du numérique en France. Membre de la fédération Syntec qui constitue la deuxième branche représentative du MEDEF, il représente les entreprises de services du numérique (ESN), les éditeurs de logiciels, les plateformes et les sociétés d'Ingénierie et de Conseil en Technologies (ICT). Numeum rassemble plus de 2 500 entreprises adhérentes qui réalisent 85% du chiffre d'affaires total du secteur qui lui-même représente 70 milliards d'euros de chiffre d'affaires et 670 000 collaborateurs en France. Présidé par Véronique Torner depuis juin 2023, Numeum met en œuvre un projet d'impact pour faire rayonner la filière et fédérer les écosystèmes des professionnels du Numérique en France et en Europe. La présidence se fixe trois grandes priorités : les régions, pour accompagner les adhérents partout en France, les compétences, pour répondre aux défis de l'attractivité et de la mixité, et le numérique responsable pour accompagner et soutenir le développement d'un écosystème numérique dans une trajectoire d'impact positif sur le plan économique, social, sociétal et environnemental. Pour en savoir plus : www.numeum.fr