Propos liminaires de l'audition du 23 janvier 2025 au Sénat devant la commission spéciale sur le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité

Monsieur le Président,
Messieurs les rapporteurs,
Mesdames, Messieurs

En régions ou à Paris, le CyberCercle rassemble depuis 2012 acteurs économiques, administrations et élus. Ses règles de fonctionnement favorisent les échanges francs et directs entre participants. Cela a été le cas à de multiples reprises, à propos du projet de loi qui est l'objet d'étude de votre commission spéciale. Nos propos d'aujourd'hui reprennent donc certains de ces échanges tenus au sein du CyberCercle.

Nous souhaitons placer ces propos à la lumière d'une citation du Premier ministre, prononcée lors de la déclaration de politique générale du 14 janvier dernier ; je cite : « *le poids des normes, qui pénalise la croissance, (…) est de près de 4 % en France, soit dix fois plus que chez nos voisins. Cette contrainte constitue un frein insupportable à l'activité de notre pays (…). Le gouvernement s'engagera donc dans un puissant mouvement de débureaucratisation.* »

Le CyberCercle partage évidemment les objectifs de cyber-résilience portés par les directives transposées. Parallèlement son ancrage territorial lui donne une vision claire du niveau relatif de sensibilité aux risques numériques des entreprises — comme des collectivités territoriales, et de leur capacité à les traiter au regard de leurs ressources. Enfin, l'attachement du CyberCercle aux politiques publiques lui confère un œil éclairé quant à l'élaboration et la mise en œuvre de ces politiques.

S'agissant du projet de loi, nous avons compris que les avis du conseil d'État du 6 juin, du conseil national d'évaluation des normes et de la délibération de la CNIL du 23 mai, ainsi que l'avis de la Commission supérieure du numérique et des postes du 3 octobre ont porté sur un texte *différent* de celui présenté en conseil des ministres, déposé au Sénat et donc examiné par votre commission spéciale.

*
* *

Trois parties dans ce propos liminaire : les flous, les loups et enfin quelques suggestions de bon sens.

D'abord les flous.

- **Flous à propos du champ d'application du texte…**

Si les secteurs d'activité visés sont fixés par la directive NIS2, les critères de désignation des entités essentielles ou importantes sont significativement à la discrétion des États-membres. A titre d'exemple, la directive prévoit spécifiquement de cumuler les chiffres de l'entité (personnel, etc.) avec une partie de ceux des sociétés du groupe auquel l'entité appartient pour déterminer sa taille, et donc déterminer à quel degré elle est concernée par NIS 2. Or la directive donne la possibilité aux États membres de prendre en compte uniquement les chiffres de l'entité, si les systèmes d'information utilisés par l'entité dans le périmètre de NIS 2 sont indépendant de ceux du groupe.

Ce qui est évidemment clé pour les entreprises dans ce cas. Cette option n'étant pas intégrée dans le projet de loi français, en l'état, toute entité d'un groupe sera donc vraisemblablement considérée comme une grande entreprise, quelle que soit sa taille réelle » ?

L'article 8 du projet de loi dispose qu'un décret en conseil d'État permettra au Premier ministre de désigner par arrêté les entités publiques — ou non, soumises — ou non à la réglementation, sans plus de précision…

D'ailleurs, le projet de loi renvoie par 29 fois à des décrets en Conseil d'État, ce qui n'apporte pas de sécurité juridique aux entités éventuellement visées.

En fait, nul n'est capable de dire aujourd'hui combien d'entités seront finalement concernées, d'autant qu'il y aura nécessairement une extension de l'application aux sous-traitants par la voie contractuelle. Nous serons donc bien au-delà des 15000 annoncées.

- **Flou à propos des coûts à la charge des entités visées…**

Dans la note du 15 mars 2024 qui accompagnait une version précédente du projet de loi telle que les ministères l'ont alors découvert, « *le coût moyen de mise en conformité pour une entité* » était estimé à 400 000 €. En audition devant votre commission spéciale, le directeur général de l'ANSSI l'estimait pour sa part à 200 000 €.

Au passage, nous comprenons qu'il s'agit de coûts moyens relatifs à la seule transposition de NIS2. REC et DORA visent chacun des acteurs spécifiques et entraîneront des coûts particuliers.

Il nous semble délicat de demander aux entités régulées une décision de gestion qui engage de tels budgets au seul argument que ce montant serait moins coûteux que les conséquences d'une attaque informatique.

Par ailleurs, en ce qui concerne les futures entités importantes et à propos des mesures à appliquer, prendre comme hypothèse que l'entité concernée serait incapable d'effectuer une analyse de risque va à l'encontre du quotidien des dirigeants d'entreprises ou de collectivités.

Quoi qu'il en soit, selon les chiffres avancés, et pour le seul titre 2 du projet de loi présenté, le coût global de mise en œuvre à la charge des entités visées oscillerait entre 3 et 6 milliards d'euros. Il est facile d'imaginer l'impact de tels montants sur la trésorerie et la capacité financière des entreprises ainsi que la répercussion sur le coût de leurs produits et services. Vous connaissez à l'avance la réaction des collectivités territoriales face à ces charges nouvelles dans un contexte budgétaire qui se contracte.

- **Flou à propos des sanctions**

Dans son avis du 6 juin 2024, le Conseil d'État estime que si l'on exclut les collectivités territoriales des sanctions, il y a rupture d'égalité et obstacle à l'atteinte des objectifs de NIS2. On pourrait sans doute porter une remarque identique à propos des administrations, ce qui est ouvert par le point 16 de l'avis du Conseil d'État.

En audition il a été indiqué à votre commission spéciale — par l'administration, que les sanctions visant les dirigeants d'entreprise seront dans la loi mais qu'elles ne seront pas appliquées… L'interdiction de gestion temporaire pour les dirigeants d'entités essentielles est bien présente dans la directive et c'est la commission des sanctions telle que prévue dans le projet de loi qui prendra la décision à partir de l'instruction faite par l'ANSSI. Affirmer qu'aucune interdiction de gestion ne sera prononcée revient à indiquer que la commission des sanctions ne sera pas indépendante.

Nous nous interrogeons par ailleurs sur la composition de la commission des sanctions telle que présentée dans le projet loi.

- **Flou à propos du rôle de l'ANSSI**

Le même avis du Conseil d'État dans son point 15 suggère de donner au Premier ministre la possibilité de nommer une autre autorité pour la mise en œuvre du contrôle des opérateurs, avant, dans son point 18 d'estimer *« que les quatre premiers chapitres du titre II du projet de loi assurent la transposition fidèle et complète de la directive NIS2* ». Or le texte du projet a été profondément modifié après l'avis rendu par le Conseil d'État. Ainsi les missions de l'ANSSI ne sont plus précisées dans la nouvelle rédaction, ce qui a fermé la porte, de fait, à la nomination éventuelle d'une autre autorité (excepté dans le domaine de la défense).

Il y a un paradoxe à affirmer que l'ANSSI concentrera ses interventions sur les entités essentielles et vouloir y centraliser l'ensemble des procédures relatives aux entités importantes. La cybersécurité étant liée aux métiers, il semble important de donner le rôle qui leur revient aux ministères coordonnateurs des secteurs d'activité visés par la directive et aux tissus institutionnel et économique de proximité des entités concernées.

Nous pensons que charger la seule ANSSI de la mise en œuvre de l'ensemble du dispositif nuirait à son efficacité, surtout dans la perspective de l'évolution prévisible de la réglementation européenne — dans le cas d'une extension du nombre des secteurs d'activité par exemple.

- **Flou enfin dans la partie de l'étude d'impact relative à la transposition de NIS2**

Nous avons noté que le Conseil national d'évaluation des normes a systématiquement donné un avis négatif sur les articles pour lesquels il était consulté. L'étude d'impact, pourtant verbeuse, n'en donne pas les raisons.

L'étude d'impact annonce certains éléments dans le tableau de transposition mais ne les communique pas. On peut citer par exemple la fiche d'impact intitulée « *Périmètre de compétence de l'ANSSI et exigences de sécurité* » à laquelle il est renvoyé dans le tableau à dix reprises, ou celle relative à la « *Notification d'incidents et partage d'informations* » ou encore à la fiche d'impact « *Supervision et procédures de contrôles et de sanction* » à laquelle il est renvoyé sept fois.

*

* *

Les loups ensuite.

Toutes les parties prenantes sont attentives à la sur-transposition des directives. Nous sommes en revanche souvent moins attentifs à la sous-transposition pourtant ici significative et portant sur des enjeux majeurs.

Sur les 4 objectifs fixés par l'article 2 de la directive NIS2, le projet de loi ne répond qu'à 2 d'entre eux.

La directive NIS 2 demande dans son article 7 l'adoption et la mise à jour — au moins tous les cinq ans, d'une stratégie nationale de cybersécurité et souligne dix-huit points auxquels devrait répondre cette stratégie.

Or, dans le projet de loi de transposition, on ne trouve nulle trace de réponse à l'objectif de clarté stratégique fixé par la directive. Le mot stratégie ne se trouve d'ailleurs pas dans le texte.

Au cours d'une audition devant la commission de la Défense et des Affaires étrangères du Sénat, il a été fait allusion au fait qu'une stratégie nationale de cybersécurité avait été élaborée mais que les aléas politiques n'avaient pas permis de la rendre publique.

Nous avons pu consulter ce projet de stratégie. Un travail de qualité qui ne répond pas toutefois à l'ensemble des points demandés par la directive.

Le deuxième loup concerne les règles et obligations pour le partage d'informations en matière de cybersécurité. L'article 29 de la directive demande aux États-membres la mise en place entre les entités visées d'accords de partage d'informations en matière de cybersécurité et notamment d'informations sur la menace, tout en reconnaissant ce partage conforme au RGPD. Or le projet de loi ne reprend pas cette disposition pourtant attendue par nombre d'acteurs de l'écosystème et cruciale pour permettre une lutte opérationnelle contre les attaques informatiques.

Enfin, et contrairement à la première version du projet de loi, la définition d'un « incident » donnée dans l'article 6 de la directive NIS2 n'est pas transposée et l'étude d'impact est muette sur cette notion pourtant capitale dans les articles traitant de notification des incidents.

En 2002, le choix avait été fait de ne pas transposer en droit français la définition de l'expression « support durable » inclus dans une directive. Pendant plusieurs années, la compréhension de la DGCCRF de « support durable » qui n'était pas alignée avec la définition européenne a notablement compliqué la situation et l'activité des opérateurs économiques souhaitant proposer des documents à valeur légale sous formes numérisées.

Nous notons que la Belgique a fait le choix de transposer intégralement l'article 6 de la directive NIS 2 et d'y ajouter des définitions annexes.

*

* *

Quelques suggestions de bon sens pour terminer.

En raison du retard pris pour la transposition des directives, le CyberCercle a conscience que le temps de travail du Parlement est contraint malgré l'importance d'un sujet aussi transversal.

Les suggestions que nous vous présentons ici seront détaillées et complétées dans une note qui vous sera remise ultérieurement.

Première suggestion : transposer certains articles des directives absents dans la rédaction actuelle du projet de loi.

- Ainsi les articles 4 de la directive REC et 7 de la directive NIS2 relatifs respectivement à la stratégie pour la résilience des entités critiques et la stratégie nationale en matière de cybersécurité ;
- l'article 29 de NIS2 relatif aux accords de partage d'informations en matière de cybersécurité — en s'appuyant sur les considérants 120 et 121 de la directive.

Deuxième suggestion : refondre, amender, compléter ou préciser certains articles du projet de loi

- ainsi l'article 5 qui traite de l'autorité nationale de sécurité des systèmes d'information. Nous pensons qu'il faut nommer l'ANSSI et revenir à une version proche du texte initial qui en précisait les missions ;
- l'article 6 en y intégrant la définition d'un incident telle que portée par l'article 6 de la directive NIS2 ;
- les articles 8, 10 ou 11, en s'appuyant sur le considérant 16 de la directive NIS2, afin de clarifier les critères de désignation éventuelle comme entités essentielles d'entreprises exerçant simultanément des activités dans d'autres secteurs que ceux visés par la directive;
- l'article 37 relatif aux sanctions qui peuvent être prises afin d'y définir celles pouvant viser un responsable d'administration, par exemple en renvoyant à un décret en conseil d'État.

Troisième suggestion : faire évoluer l'approche retenue par l'administration dans le dispositif et sa mise en œuvre.

- Les ministères coordonnateurs des secteurs d'activité visés par NIS2 connaissent les métiers, les particularités, les contraintes du secteur et des acteurs économiques relevant de leur compétence. Il nous semble donc nécessaire qu'ils soient en mesure d'amender, compléter et valider la liste des entités essentielles et importantes prévues par NIS2 — article 12 du projet de loi.
- Pour les mêmes raisons, les ministères concernés doivent être intégrés aux processus de définition des référentiels et de contrôle de conformité (articles 14 et 15 du projet de loi).

  Sur ces deux points, la démarche entreprise par le ministère des Armées pour les entreprises relevant de la base industrielle et technologique de défense nous semble à cet égard exemplaire et pourrait être déclinée dans les secteurs d'activités visés par NIS2.

- Dans le même esprit, dans l'article 36 du projet de loi relatif à la composition de la commission des sanctions nous suggérons d'y adjoindre un représentant du ministère coordonnateur du secteur d'activité auquel appartient l'entité mise en cause et d'un représentant de la branche professionnelle de ce secteur afin que les sanctions prises prennent en compte toute considération utile.

Quatrième et dernière suggestion : travailler sur les référentiels et labels de sécurité et de confiance numériques
La directive NIS2 encourage le recours à des normes et des spécifications techniques européennes et internationales et indique que les États membres peuvent prescrire des produits et services certifiés dans le cadre de schémas européens afin de démontrer la conformité à certaines exigences.

Aussi, ce projet de transposition offre l'opportunité d'évaluer le niveau d'efficacité des référentiels existants afin de simplifier et de rendre cohérent le corpus normatif et réglementaire récemment qualifié "d'enfer réglementaire". Les démarches de conformité qui s'imposent aux entreprises en seraient facilitées et allégées.

Le texte pourrait indiquer que lorsqu'il existe des standards sectoriels, les mesures à prendre s'appuieront sur ces standards qui deviendront les textes de références.

Dernier domaine de suggestions qui ne relèvent pas nécessairement de la loi mais pourraient être explicités dans le contenu de la stratégie de cybersécurité :

- la déclinaison territoriale du dispositif national, le rôle des préfets et des collectivités territoriales ;
- le rôle du 17 Cyber ;
- la clarification du rôle et du financement des structures régionales improprement nommées « CSIRT » ;
- l'offre de produits et de services adaptés aux besoins et aux capacités financières et humaines des entités qui devront se mettre en conformité ;
- et enfin la nécessité de politiques d'accompagnement adaptées pour permettre la mise en cybersécurité progressive des entités visées.

*
* *

Voilà Monsieur le Président, Messieurs les rapporteurs, les remarques préliminaires du CyberCercle. Nous sommes évidemment à votre disposition dans le cadre de cette audition ou ultérieurement pour expliciter les différents points évoqués.