Position ACN :
Position ACN sur la proposition de Règlement
« Cyber Resilience Act »
23 janvier 2023

Le projet de règlement CRA (*Cyber Resilience Act*), fondé sur la Stratégie de cybersécurité de l'Union européenne (2020), vient utilement compléter le corpus législatif existant (NIS, NIS 2, CSA - *Cybersecurity Act* et ses schémas de certification, eIDAS, RED, …), tout en imposant des exigences horizontales de cybersécurité aux fabricants et aux vendeurs de produits numériques (matériels, immatériels et produits accessoires) offrant ainsi une plus grande sécurité et résilience tout au long de la chaine d'approvisionnement par la reconnaissance d'obligations en matière de sécurité sur l'ensemble du cycle de la vie des produits.

L'ACN (Alliance pour la Confiance Numérique) appelle, depuis de nombreuses années, l'attention des pouvoirs publics sur l'importance de la confiance numérique dans un monde toujours plus connecté. Aujourd'hui, l'ensemble des processus économiques, administratifs et sociaux qui régissent notre quotidien sont numérisés, ce qui offre un potentiel majeur de développement et ouvre de grandes perspectives de progrès. Pour autant, cela impose une vigilance particulière quant à la mise en sécurité de notre cyberespace et de ses applications.

En effet, la multiplication de produits à composants numériques, couplée à l'absence d'une législation dédiée, cohérente et uniforme au sein de l'Union européenne visant à définir des exigences minimales en matière de cybersécurité, crée un risque réel en termes d'autonomie stratégique et de souveraineté numérique, en laissant à la merci d'attaquants toujours plus nombreux, une grande partie de notre espace numérique et de nos activités.

Au-delà, la confiance que chacun peut accorder dans tous les usages numériques est une condition sine qua non du déploiement de ces usages.

C'est pourquoi, l'ACN (Alliance pour la Confiance Numérique) salue la volonté de la Commission européenne de définir, à travers la proposition de règlement « *Cyber Resilience Act* » – CRA, des exigences de cybersécurité communes européennes pour les produits comportant des éléments numériques qui seront mis sur le marché intérieur. Toutefois, les entreprises de la filière de la confiance numérique appellent l'attention du législateur sur la nécessité d'assurer une bonne articulation de ce nouveau texte avec l'ensemble de l'édifice législatif et réglementaire européen existant dans ce domaine, ainsi que la clarification de certaines de ses dispositions afin d'assurer l'application effective de ce texte.

Sur l'élévation générale du niveau de cybersécurité en Europe

L'ACN considère que la double approche retenue par ce projet, à savoir l'intégration dès la conception des notions et obligations de cybersécurité (« *cybersecurity by design* ») tout au long du cycle de vie, et le renforcement du niveau d'information des consommateurs et des entreprises, est de nature à apporter un surcroit important de sécurité et de confiance numérique.

Plus particulièrement, l'accent mis par le projet de règlement sur la gestion des vulnérabilités en cours de vie du produit porte un message opportun : en effet, la cybersécurité d'un produit et la responsabilité du fournisseur qui en découle, ne sauraient s'apprécier uniquement au moment de la conception, mais tout au long du cycle de vie du produit.

Aussi l'ACN se félicite que ce projet de règlement vienne définir un paradigme légal qui intègre des exigences minimales de cybersécurité à respecter dans une vision holistique du cycle de vie du produit, ainsi que les sanctions qui résultent du non-respect de ces exigences.

Par ailleurs, ce texte ayant vocation à s'appliquer à tous les produits numériques et services auxiliaires quelle que soit la taille de l'entreprise, l'ACN souligne que jusqu'alors, il n'existait, pour la plupart des produits numériques, logiciels et matériels, aucune garantie pour le consommateur que le produit acheté réponde à un ensemble minimal d'exigences en matière de cybersécurité. **Le CRA permet ainsi de pallier ce manque et de garantir aux utilisateurs des produits avec un meilleur niveau de sécurité et d'information ce dont l'ACN se félicite.**

Sur la bonne articulation du CRA avec les textes existants

L'ACN souhaite toutefois rappeler l'importance d'une complémentarité et d'une articulation entre les différents textes juridiques pour établir un socle juridique cohérent et uniforme permettant aux produits mis en circulation sur le marché européen d'être robustes.

Cette cohérence est importante tant pour assurer une bonne diffusion des pratiques de cybersécurité dans les secteurs visés, que pour assurer une lecture de cet édifice pour les utilisateurs et les consommateurs, renforçant ainsi leur confiance dans les produits numériques. Enfin, cette cohérence est aussi primordiale pour les entreprises du secteur de la confiance numérique afin d'éviter toute distorsion de concurrence éventuelle qui résulterait d'interprétations divergentes des textes et/ou de leur articulation dans les différents pays européens, mais aussi pour leur assurer un cadre règlementaire lisible sans surcharge administrative excessive. Ainsi il est capital de mutualiser, autant que faire se peut, les exigences administratives résultant de tous ces textes, dès lors qu'elles portent sur les mêmes aspects.

Aussi l'ACN appelle la Commission à porter une attention particulière pour que les exigences posées par le CRA soient parfaitement alignées avec celles issues des autres textes européens applicables dans le domaine, tels que le *Cybersecurity Act (CSA)*, la

directive NIS2, DORA, le RGPD, la directive vie privée et communications électroniques, le projet de règlement sur l'Intelligence Artificielle, la révision du règlement eIDAS sur l'identité numérique, RED, etc., mais aussi les critères d'exigence issus des normes et certifications aujourd'hui existantes.

Cette nécessité d'harmonisation est particulièrement importante concernant certains points :

- Les délais de notification concernant la survenue d'une attaque devraient être identiques à ceux mentionnés dans la directive NIS et le RGPD (pour la fuite de données personnelles). Concernant les produits soumis à de multiples déclarations d'incident, un guichet unique de déclaration d'incidents pourrait être mis en place, afin d'éviter de multiples saisies liées à diverses obligations dans un moment où l'entreprise est en train de faire face à une crise… Une entreprise du secteur financier ou de l'énergie par exemple serait alors théoriquement soumise à l'obligation d'effectuer une déclaration auprès de l'ENISA (au titre du CRA), de ses autorités nationales (au titre de NIS2) et de son superviseur sectoriel (DORA).

- Chaque texte définit ses propres mécanismes de supervision. Or les exigences essentielles décrites dans l'annexe 1 de la proposition de règlement CRA portent sur des aspects déjà couvert par de nombreux autres textes :
    - Protection de la confidentialité des données stockées ou transmises (eIDAS, RGPD, directive vie privée et communications électroniques) ;
    - Incident de sécurité sur un QSCD (eIDAS) ;
    - Incident de sécurité sur un service de confiance (NIS2, eIDAS).

Ces supervisions multiples sont un facteur accru de complexité et de coût pour les entreprises tombant sous le coup de ces différentes réglementations. Ainsi l'ACN appelle à une supervision rationalisée entre tous ces textes.

- Les exigences de cybersécurité demandées et la manière de les évaluer/certifier/attester devront également faire l'objet d'une réflexion approfondie. Il apparaît utile que l'ENISA soit chargée de l'élaboration des référentiels et des schémas de certification nécessaires à la mise en œuvre du CRA (mais aussi des autres textes ayant une composante de cybersécurité) conformément à sa mission définie par le *European Cybersecurity Act*. Cela permettrait de limiter les risques de voir des entreprises et des produits et/ou services soumis à des exigences issues de multiples référentiels liés à des normes ou des standards non-coordonnés voire contradictoires et la distorsion de concurrence que cela pourrait engendrer. En particulier :
    - Pour les produits couverts par la catégorie de classe I, il demeure peu clair à ce stade quels seront les standards harmonisés applicables.

- L'articulation avec la législation sur l'IA (*AI Act*) en ce qui concerne les systèmes d'intelligence artificielle à haut risque soulève un certain nombre de questions :
  - Selon l'article 8.2, la vérification de conformité avec les exigences essentielles définies dans l'annexe 1 pour les produits non critiques doit être réalisée conformément aux procédures prévues dans la législation sur l'IA (AI Act - article 43). Or il n'est pas du tout évident que ces procédures apportent un niveau de confiance comparable à ceux prévus dans le CRA (article 24). L'ACN souhaiterait donc que ce point soit clarifié.
  - La disposition dérogatoire précisée dans l'article 8.3 pour les produits critiques (classe I et classe II) prévoyant une vérification de conformité en accord avec le CRA (selon l'article 24) n'est pas applicable en l'état aux produits hautement critiques. Ainsi, il semblerait que les produits hautement critiques ne soient astreints qu'à une vérification de conformité avec les exigences essentielles définies dans l'annexe 1 conformément aux procédures prévues dans la législation sur l'IA (*AI Act* - article 43), lesquelles ne permettant pas d'atteindre le niveau de confiance prévu par le CRA pour de tels produits dans l'article 6.5 (certificat de cybersécurité conforme à un schéma de certification de cybersécurité conformément au règlement 2019/881). L'ACN souhaiterait donc que ce point soit clarifié.
  - La disposition dérogatoire précisée dans l'article 8.3 pour les produits critiques (classe I et classe II) semble exclure la possibilité d'utiliser un certificat de cybersécurité conforme à un schéma de certification de cybersécurité conformément au règlement 2019/881 comme moyen de vérification de conformité aux exigences essentielles de l'annexe 1, alors qu'elle est explicitement permise pour les produits qui ne sont pas des systèmes d'intelligence artificielle à haut risque selon l'article 18. L'ACN souhaiterait donc que ce point soit clarifié.

L'ACN appelle la Commission Européenne à clarifier l'articulation entre le CRA et la législation sur l'IA (*AI Act*) et assurer une cohérence du niveau de cybersécurité.

Au-delà de ces aspects, il importe de construire un cadre juridique sécurisé pour les entreprises soumises au CRA et à d'autres règlementations en garantissant que la démonstration de conformité à une ou des exigences essentielles du CRA (décrites dans l'annexe 1), lorsqu'elles sont aussi requises par une autre règlementation, soit admise et reconnue par celle-ci et emporte donc présomption de conformité à cette dernière. En particulier, mais de manière non limitative :

- La démonstration de conformité aux exigences essentielles 1.3.c (protection de la confidentialité des données), 1.3.d (protection de l'intégrité des données) et 1.3.e (traitement uniquement de données adéquates, pertinentes et limitées au besoin) devrait être admise et reconnue par le

RGPD et emporter présomption de conformité aux exigences correspondantes de l'article 5.1(c) et de l'article 32 ;
- La démonstration de conformité à l'exigence essentielle 1.3.c (protection de la confidentialité des données) devrait être admise et reconnue par la directive vie privée et communications électroniques et emporter présomption de conformité à l'article 5 ;

- Cet aspect est essentiel pour sécuriser les entreprises soumises à de multiples réglementations mais aussi pour alléger leurs charges de conformité.

Ainsi l'ACN recommande d'introduire dans le texte du CRA le principe de présomption de conformité aux exigences d'un autre texte – quel qu'il soit, dès lors qu'elles sont couvertes par une ou plusieurs des exigences essentielles de l'annexe 1. En particulier, l'ACN recommande d'introduire les principes de présomption de conformité suivant :

- **À l'article 5 de la directive vie privée et communications électroniques dès lors que l'exigence essentielle 1.3.c est vérifiée ;**
- **Aux exigences correspondantes de l'article 5.1(c) et de l'article 32 du RGPD dès lors que les exigences essentielles 1.3.c, 1.3.d et 1.3.e sont vérifiées ;**

Sur la nécessaire clarification de certaines dispositions clés pour une effective application du texte

- Le concept de « niveau de protection » est employé dans le CRA à de nombreuses reprises sans être jamais clairement défini. L'ACN recommande d'apporter une définition précise de ce terme dans l'article 3.

- La définition de la durée de vie prévue du produit (Article 10.6.) : Alors que le CRA fixe l'obligation de maintenir en condition de sécurité un produit pendant sa durée de vie prévue ou cinq ans, ce dernier néglige la forte dépendance entre les différents produits couverts par le CRA, certains étant composants de produits et donc intégré dans un autre. La durée de vie prévue n'étant pas définie dans le texte, des produits reposant sur des composants dont la durée de vie prévue serait différente de la leur seraient rendus non conformes par effet domino. L'ACN demande aux co-législateurs de préciser la mise en œuvre de ce principe de durée de vie prévue, notamment dans ce contexte d'interdépendance entre produits.

- **Une vulnérabilité exploitable n'est en aucun cas un concept absolu ou binaire et sa définition doit être clarifiée.**
  Toute vulnérabilité peut devenir exploitable dès lors qu'un attaquant y met suffisamment de moyens (temps, financier, humain et technique). La véritable question est de parvenir à (1) quantifier les moyens nécessaires pour rendre une

vulnérabilité exploitable et (2) l'intérêt pour l'attaquant de mettre en œuvre de tels moyens pour exploiter cette vulnérabilité. Par ailleurs :

- un produit comportant des éléments numériques peut contenir une vulnérabilité exploitable mais sur des fonctionnalités non exploitables (la fonctionnalité présentant la vulnérabilité n'est pas accessible à l'utilisateur). Dans ce cas la vulnérabilité exploitable est sans impact ;

- un produit contient une vulnérabilité exploitable affectant des fonctionnalités qui n'altèrent en rien la finalité et l'usage du produit, et qui ne sont pas mises en œuvre lorsque les informations et les instructions à l'utilisateur sont correctement suivies. Dans ce cas la vulnérabilité exploitable est sans impact.

La définition de « vulnérabilité exploitable connue » (annexe 1.1.2) doit être clarifiée, car le CRA interdit la mise sur le marché des produits comportant des vulnérabilités exploitables connues alors qu'en pratique cette notion est relative en fonction (1) du risque, (2) la complexité/coût pour l'attaquant, les (3) usages considérés, (4) la nature du produit en question.

L'exploitabilité doit donc s'évaluer dans le contexte du produit, et en s'appuyant sur des méthodologies éprouvées, celles de la certification. Les schémas de certification de sécurité conformes au règlement 2019/881 (*Cybersecurity Act*) prennent très bien en compte ces aspects liés à l'exploitabilité des vulnérabilités. En revanche, la prise en compte de ces aspects dans les méthodes d'évaluation de conformité décrites dans l'article 24 (module A, modules B+C ou module H) semble absente et reste à préciser. L'évaluation de conformité selon ces modules semble reposer sur l'idée fausse selon laquelle une vulnérabilité est soit exploitable, soit non exploitable.

L'ACN recommande une vision homogène entre le CSA et le CRA dans la manière dont l'exploitabilité des vulnérabilités est appréciée. En cela nous appelons à réutiliser dans l'article 24 sur l'évaluation de conformité, tout ce qui a été mis en place via le CSA portant sur l'identification et la caractérisation des vulnérabilités exploitables. Ainsi, l'ENISA grâce aux schémas de certification de sécurité, conformément au CSA qu'elle met en œuvre, dispose d'une forte expérience. L'ACN recommande donc de lui confier la gestion et le maintien d'une liste officielle de vulnérabilités exploitables qui servirait de référentiel aux acteurs couverts par le CRA.

Classification des produits

La liste des produits tombant dans les classe I et classe II décrite dans l'annexe III devrait être explicitée plus avant de sorte à éviter toute ambiguïté quant à la classification des produits comportant des éléments numériques.

En ce qui concerne les produits hautement critiques, l'article 6.5 contient une ambigüité majeure qu'il importe de clarifier. En effet plusieurs interprétations de cette disposition sont possibles à savoir :

- La Commission Européenne précisera les catégories de produits tombant dans la classification « hautement critique » **et tout** produit hautement critique devra obtenir un certificat de cybersécurité selon un schéma de certification de cybersécurité conformément au règlement 2019/881 ;
- La Commission Européenne précisera **seulement** les catégories de produits tombant dans la classification « hautement critique » pour lesquels un certificat de cybersécurité selon un schéma de certification de cybersécurité conforme au règlement 2019/881 est requis ;

L'ACN souhaiterait que ces points essentiels soient clarifiés.

Mise en application du texte

Comme précisé dans l'article 10, un fabricant de produit comportant des éléments numériques doit obligatoirement préparer l'évaluation des risques de cybersécurité correspondants. Cette évaluation est la pierre angulaire du suivi des risques dans le temps. Pourtant, la méthodologie, le format et la structure de cette évaluation des risques de cybersécurité ne sont pas précisés et sont renvoyés à un acte délégué ultérieur (article 23). Par conséquent, le délai pour la mise en application de ce texte doit être décompté à partir de la publication de cet acte délégué car sans lui il ne sera pas possible de mettre en application ce règlement. **Ainsi, l'ACN recommande que la méthodologie, le format et la structure de cette évaluation des risques de cybersécurité soient publiés dès que possible et que le délai de mise en application du texte soit décompté à partir de la publication de l'acte délégué correspondant**.

Plus généralement le texte, tel que proposé, donne à la Commission Européenne la faculté de modifier de manière substantielle de nombreux aspects du règlement via des actes délégués. Si une telle approche est légitime, elle doit néanmoins prendre en compte les contraintes des entreprises qui ne pourront pas mettre en œuvre instantanément ces modifications et auront besoin de temps pour s'y conformer. **Ainsi, le texte devrait prévoir d'ores et déjà une période minimale avant toute mise en application de toute modification introduite via un acte délégué. A cette fin, l'ACN recommande un délai minimal de 2 ans (24 mois) qui correspond aux contraintes industrielles.**

Enfin, la situation des produits comportant des éléments numériques mis sur le marché avant la date de mise en application de l'entièreté du texte (24 mois après publication du texte tel que proposé dans l'article 57) et donc non soumis au respect des exigences essentielles définies dans l'annexe 1, mais intégrés dans un autre produit mis sur le marché après la date de mise en application de l'entièreté du texte et donc soumis au respect des exigences essentielles définies dans l'annexe 1 doit être clarifiée. **En particulier, dans le cas des produits classifiés comme critiques (classe I et classe II) ou hautement critiques, les produits les intégrant qui sont mis sur le marché après la date de mise en**

application de l'entièreté du texte seront-il aussi exemptés du respect des exigences essentielles définies dans l'annexe 1 ? Ou bien à contrario les produits les intégrant mis sur le marché après la date de mise en application de l'entièreté du texte devront ils prendre à leur charge la vérification de conformité avec les exigences essentielles définies dans l'annexe 1 ?

L'ACN recommande de clarifier cet aspect qui est essentiel aux yeux de l'industrie.

Spécifications communes et capitalisation sur les référentiels techniques et les schémas de conformité sectoriels existants

D'après l'article 19, les spécifications communes pouvant servir de base pour la démonstration de conformité aux exigences essentielles d'un produit comportant des éléments numériques sont vues uniquement comme une solution de repli dans le cas où des standards harmonisés seraient inexistants, ne seraient pas disponibles dans les temps ou insuffisants. Cette approche semble trop restrictive car au contraire, les spécifications communes peuvent être dans certains cas plus adaptées que des standards harmonisés, en particulier pour permettre de capitaliser sur des référentiels techniques et des schémas de conformité sectoriels existants dont il aura été démontré qu'ils permettent d'assurer le respect - en partie ou en totalité - des exigences essentielles de l'annexe 1. En cela, les spécifications techniques sont donc un outil très intéressant et très puissant permettant de réutiliser des référentiels techniques et des schémas de conformité sectoriels existants, ce qui procure deux bénéfices notables :

- Permettre une mise en application rapide de ce texte ;
- Limiter voire supprimer la duplication des travaux de conformité pour les entreprises et donc en réduire les coûts ;

Cette approche est par exemple tout à fait pertinente pour le secteur des cartes de paiement qui disposent de solides référentiels techniques et schémas de conformité assurant le respect de la plupart des exigences essentielles de l'annexe 1.

L'ACN recommande donc de :

- **considérer l'utilisation des spécifications techniques comme un outil permettant de capitaliser sur des référentiels techniques et des schémas de conformité sectoriels existants dont il aura été démontré qu'ils permettent d'assurer le respect - en partie ou en totalité - des exigences essentielles de l'annexe 1, et donc de revoir l'article 19 à cette aune.**
- **capitaliser autant que possible sur les solides référentiels techniques et schémas de conformité disponibles dans le secteur des cartes de paiements pour la démonstration de conformité aux exigences essentielles de l'annexe 1.**

Au-delà, il est absolument essentiel de capitaliser sur des référentiels techniques et des schémas de conformité sectoriels existants dont il aura été démontré qu'ils permettent d'assurer le respect - en partie ou en totalité - des exigences essentielles de l'annexe 1. Toutefois l'utilisation des spécifications techniques comme décrit ci-dessus ne permettra

peut-être pas dans tous les cas d'organiser cette capitalisation. Ainsi, le CRA devrait être amendé pour permettre de manière alternative l'utilisation directe de schémas de conformité sectoriels existants comme démonstration de conformité, dès lors qu'il aura été démontré que ces schémas permettent d'assurer le respect - en partie ou en totalité - des exigences essentielles de l'annexe 1.

C'est pourquoi l'ACN recommande d'ajouter une troisième possibilité de démonstration de conformité aux exigences essentielles de l'annexe 1 (en plus de celles prévues dans l'article 18 et de l'article 24) dans le CRA, reposant sur l'utilisation directe de schémas de conformité sectoriels existants, dès lors qu'il aura été démontré que ces schémas permettent d'assurer le respect - en partie ou en totalité - des exigences essentielles de l'annexe 1.

Exigences essentielles (annexe 1)

Exigence 1.2.8

Alors que la disposition portant sur la gratuité des mises à jour de sécurité parait à première vue censée, des *business model* vertueux reposent sur des systèmes d'abonnement payant de support en sécurité. A titre d'exemple, OpenSSL, l'un des composants open source majeur en sécurité, est maintenu au travers d'un modèle d'abonnement payant, les dernières versions étant gratuites tandis que les correctifs pour les versions précédentes ne le sont pas. Ainsi, le support étendu finance le développement des nouvelles versions et encourage les vendeurs à adopter les versions les plus récentes. Alors que l'obligation de maintenir le niveau de sécurité du produit est nécessaire, rendre celle-ci gratuite pourrait détruire des modèles vertueux de support de sécurité.

L'ACN recommande de ne pas exclure ces modèles d'affaires.

Exigence 1.3.k

La seconde moitié de l'exigence (« […] le cas échéant, par des mises à jour automatiques et la notification des mises à jour disponibles aux utilisateurs ») ne dépend pas uniquement du produit mais aussi de sa connectivité qui n'est pas sous le contrôle du produit, mais essentiellement de l'utilisateur.

Ainsi l'ACN recommande de supprimer la seconde moitié de cette exigence.

Exigence 2.2

La seconde moitié de l'exigence (« […] gérer et corriger sans délai les vulnérabilités […] ») est bien trop contraignante. En effet, un temps minimal est nécessaire pour gérer et corriger une vulnérabilité (analyse, correction, distribution du correctif...), ce qui peut prendre plusieurs jours, voire plusieurs semaines.

Par conséquent, l'ACN recommande de formuler l'exigence comme suit : « […] faire de son mieux pour gérer et corriger sans délai les vulnérabilités […] »

Exigence 2.3

La signification de « […] tests et examens de sécurité efficaces » devrait être précisée. **Par ailleurs, l'ACN considère que la notion d'efficacité des tests et examens de sécurité devrait être rapprochée de celle de vulnérabilité exploitable discutée plus haut**. En effet, ces tests et examens de sécurité ont pour objectifs de déterminer si une vulnérabilité est exploitable.

Exigence 2.7

Le terme « mécanismes de distribution sécurisée des mises à jour » ne semble pas approprié ici. En effet le fabricant (à qui cette exigence s'applique) ne vend pas nécessairement le produit comportant des éléments numériques à l'utilisateur final mais peut aussi le vendre à un autre fabricant qui l'intègrera dans un de ses produits. Cela peut par exemple être le cas pour des logiciels ou des éléments matériels sécurisés (par exemple *secure element*). Dans un tel cas d'espèce, la distribution sécurisée des mises à jour ne dépendra pas que du fabricant du produit comportant des éléments numériques, mais aussi et surtout du second fabricant l'ayant intégré à son produit, lequel devra accepter de mettre en place les moyens techniques nécessaires à la distribution sécurisée des mises à jour. **Par conséquent l'ACN recommande de parler plutôt ici de « mise à disposition des mises à jour ».**

De plus, « […] soient corrigées ou atténuées rapidement » ne dépend pas uniquement du fabricant, mais aussi de l'utilisateur. En effet la correction ou l'atténuation requiert une connectivité du produit comportant des éléments numériques, laquelle est sous le contrôle de l'utilisateur et pas du produit. Par conséquent, **l'ACN recommande de supprimer le terme « rapidement »**.

Obligations de déclaration d'incidents et communication des vulnérabilités

Selon l'article 11.4, un fabricant doit informer dès qu'il en a connaissance et sans délai les utilisateurs d'un produit comportant des éléments numériques d'un incident et des mesures correctives permettant d'en limiter l'impact. Néanmoins, dans le cas d'incidents sensibles, il n'est pas toujours approprié d'en informer les utilisateurs, en particulier quand tous les produits comportant des éléments numériques ne peuvent être corrigés rapidement, n'ont pu l'être, ou qu'il n'est pas possible de limiter les conséquences de l'incident. **Par conséquent, l'ACN recommande de retirer cette obligation d'information à l'endroit des utilisateurs en cas d'incident et de laisser les autorités de supervision juger de la pertinence d'une telle information.**

De même, l'exigence essentielle 2.4 (annexe 1) impose de communiquer publiquement sur les vulnérabilités corrigées dès lors qu'une mise à jour de sécurité est publiée. **L'ACN considère que cette exigence risque au contraire de nuire à la sécurité des produits comportant des éléments numériques**. En effet, un temps assez long peut s'écouler entre la publication de la mise à jour de sécurité et son application effective dans les produits comportant des éléments numériques, en particulier quand ces derniers ne sont pas

connectés en permanence et/ou la connectivité dépend de l'utilisateur (par exemple carte à puce). Il pourrait même arriver que des produits comportant des éléments numériques ne soient jamais connectés, et donc ne reçoivent jamais de mise à jour de sécurité, mais soient tout de même utilisés. Ainsi lors de la publication de la mise à jour de sécurité d'un produit comportant des éléments numériques, un attaquant aura la connaissance des vulnérabilités corrigées et pourra donc chercher à les exploiter durant le laps de temps – assez long - pendant lequel elle se déploiera, et ce uniquement sur la fraction de produits sur le terrain qui se connecteront. **Ainsi l'obligation de communiquer sur les vulnérabilités corrigées concomitamment à la mise à disposition de la mise à jour de sécurité est hautement questionnable. De plus, dans le cas des vulnérabilités critiques, il peut parfois être plus approprié de ne pas communiquer du tout sur leurs existences et leurs natures. Ainsi l'ACN recommande de supprimer cette exigence ou de laisser les autorités de supervision juger de la pertinence d'une telle information.**

Ambiguïtés concernant l'utilisation des certificats de sécurité conformes au règlement 2019/881 (Cybersecurity Act) à des fins de vérification de conformité

Produits hautement critiques :

> L'article 6.5 exige un certificat de sécurité conforme au règlement 2019/881 (« Elémentaire », « Substantiel » ou « Elevé ») tandis que l'article 18.3 portant sur la présomption de conformité indique qu'un certificat de sécurité (« Elémentaire », « Substantiel » ou « Elevé ») ou une déclaration de conformité UE selon le règlement 2019/881 sont suffisants. **L'ACN y voit une contradiction et souhaiterait une clarification concernant l'admissibilité d'une déclaration de conformité UE pour les produits hautement critiques.**

Par ailleurs, si l'ACN recommande, en principe, une certification de sécurité de niveau « Elevé » pour tout produit hautement critique, il subsiste cependant des interrogations majeures quant à la définition de ces produits hautement critiques qui doivent être explicités dans le texte et non par acte délégué.

Produits de classe I :

> L'article 24.2 indique ceci : « […] le fabricant ou le mandataire du fabricant n'a pas appliqué ou n'a appliqué qu'en partie des normes harmonisées, des spécifications communes ou des schémas européens de certification de cybersécurité visés à l'article 18 […] » La signification « d'appliquer des schémas européens de certification de cybersécurité », n'est pas claire et devrait être précisée. **Cela fait-il référence à une certification de sécurité et/ou une déclaration de conformité UE ? L'ACN souhaiterait des clarifications à ce propos.**

Organismes d'évaluation de la conformité

Les critères et exigences applicables aux organismes d'évaluations de la conformité devraient être davantage précisés. En particulier, l'ACN recommande que les organismes d'évaluations de la conformité soient obligatoirement conformes à la norme ISO/IEC 17025.

Les articles 26.2 et 32.2 semblent se contredire concernant l'utilisation d'un organisme d'accréditation national pour l'évaluation et le contrôle des organismes d'évaluation de conformité. Tandis que l'article 26.2 l'autorise au choix des Etats Membres, l'article 32.2 laisse penser au contraire que c'est une procédure obligatoire.

Autres aspects divers

Dans l'article 44.3, l'article 11 du règlement 1025/2012 devrait être référencé au lieu de l'article 10.

Dans l'article 52.2, l'accord du fabricant, de l'importateur ou du distributeur concerné devrait être obligatoire pour la transmission des documents portant sur ses produits comportant des éléments numériques. L'ACN recommande d'ajouter cette précision dans cet article.

Dans l'article 53.3 la non-conformité aux obligations prévues dans l'article 13 (relatif aux importateurs) devrait aussi être considérée comme motif de sanction. En effet, les importateurs sont eux aussi tenus de mettre sur le marché des produits comportant des éléments numériques conformes aux exigences essentielles de l'annexe 1 (article 13.1). L'ACN recommande donc d'inclure dans cet article la non-conformité à l'article 13.

A propos de l'ACN (www.confiance-numerique.fr) :

L'Alliance pour la Confiance Numérique (ACN) représente les entreprises (leaders mondiaux, PME et ETI) du secteur de la confiance numérique notamment celles de la cybersécurité, de l'identité numérique et de l'Intelligence Artificielle de confiance. La France dispose dans ce domaine d'un tissu industriel très performant et d'une excellence internationalement reconnue grâce aux différentes acteurs dynamiques du secteur. D'après l'Observatoire ACN de la confiance numérique 2022 (disponible en téléchargement sur www.confiance-numerique.fr), on dénombre, dans le secteur, plus de 2000 entreprises réalisant près de 24 Milliards d'euros de chiffre d'affaires dans le monde (dont 15 milliards d'euros en France) dans ce secteur en forte croissance (7,5% de croissance moyenne annuelle en France sur la période 2016-2021). Le secteur emploie 110 000 personnes dans le monde de plus de 70 000 en France. L'ACN est membre de la FIEEC (Fédération des Industries Electriques, Electroniques et de Communication), membre associé du Campus Cyber et participe activement aux travaux du Comité Stratégique de Filière – CSF – des industries de sécurité. Par ailleurs, l'ACN est également membre fondateur de l'ECSO (European CyberSecurity Organisation).