Propositions de l'Alliance Française des Industries du Numérique (AFNUM) pour le Cyber Resilience Act

Le 15 septembre 2022 la Commission européenne a publié sa proposition de règlement sur la Cyber Resilience en Europe (Cyber Resilience Act ou CRA).

S'inscrivant dans la stratégie européenne de cybersécurité présentée en 2020 le CRA vise à instaurer un cadre commun de cybersécurité à l'ensemble des produits numériques, qu'ils soient physiques ou immatériels.

En effet, avec le développement de « *l'Internet of Things* » les objets connectés occupent aujourd'hui une place centrale dans notre vie de tous les jours. Des montres connectées aux capteurs industriels ces appareils représentent aussi bien des opportunités économiques et sociales qu'un défi pour les données de leurs utilisateurs. L'interconnexion de ces objets et la présence généralisée des logiciels sont autant de failles potentiellement exploitables pour des cyberattaquants.

Ainsi, dans son étude accompagnant sa proposition de règlement, la Commission européenne note que les cyberattaques visant les produits et les logiciels sont en forte augmentation depuis plusieurs années avec un coût global estimé à 5.5 trillions pour la seule année 2021.

En tant que représentant des industriels du numérique l'AFNUM soutient la proposition de la Commission européenne et promeut le développement de solutions sécurisées pour les utilisateurs. Dans cette optique, nous tenons à formuler certaines remarques et recommandations visant à renforcer l'effectivité et la mise en application de ce projet de règlement.

Sommaire

Synthèse

- Le Cyber Resilience Act devrait opérer **une nette distinction entre les obligations portant sur les développeurs de logiciels et celles propres aux fabricants de produits.**

- Il conviendrait de maintenir les mécanismes actuels régissant les relations entre le Cyber Resilience Act et les autres textes relatifs à la cybersécurité (NIS 2, acte délégué de la directive RED, AI Act).

- La Commission européenne devrait consulter les acteurs de l'industrie dans le cadre de la rédaction des « spécifications communes » venant en appuie des standards européens et internationaux.

- **La liste des produits ciblés par une mise en conformité « lourde » devrait être allégée** afin de permettre de cibler les produits véritablement à risque. En effet, la liste actuelle comporte trop de produit tant en quantité qu'en diversité, ceci risque de provoquer des effets de « goulots » pour les fabricants qui ne pourront pas procéder à la mise en conformité de leurs produits, **le nombre de prestataires pouvant réaliser ces contrôles étant limité.**

- L'obligation faite aux fabricants de fournir des mises à jour pour une durée de 5 ans devrait être repensée afin de **l'aligner avec celle présente dans les différentes garanties légales de conformité** (2 ans de fourniture de mise à jour après la délivrance du bien).

- Enfin, **l'annexe I établissant les critères à prendre en compte dans l'évaluation des risques devrait être alignée avec les méthodes d'évaluation déjà mise en œuvre par les entreprises et appliquées depuis de nombreuses années** (méthode CVSS principalement).

1 CHAMP D'APPLICATION ET DEFINITIONS

En souhaitant faire du CRA le nouveau socle de la cybersécurité la Commission a nécessairement dû opter pour un champ d'application large.

Ainsi, le CRA vise les produits physiques (téléphones, ordinateurs, capteurs etc…), les logiciels (systèmes d'exploitation, de gestion etc…) et leurs composants (semiconducteurs …).

Les considérants 6 et 7 précisent notamment que sont concernés par ce règlement l'ensemble des produits interconnectés ou interconnectables.

Cette notion d'interconnexion doit être entendue au sens large puisqu'elle vise aussi bien les connections physiques (au moyen de ports) que les connections logiques (via des réseaux de communication ou des interfaces de programmation). Le considérant 7 indique également que les fabricants devront prendre en considération les produits permettant des connexions *« indirectes »* puisque les failles de sécurité peuvent provenir de l'ensemble des produits reliés, directement ou indirectement, à un système d'information.

L'AFNUM soutient ce large champ d'application en ce qu'il permet une protection complète du marché européen. Le renforcement de la cybersécurité des produits et des logiciels a toujours été une priorité de nos entreprises adhérentes qui s'efforcent depuis de nombreuses années à proposer des produits sûrs, fiables pour les utilisateurs.

Nous estimons également essentiel de conserver la prise en compte des particularités du Cloud, et plus précisément celle des SaaS, par le Cyber Resilience Act. Dans son considérant 9 le CRA précise bien que les SaaS sont conçus et développés comme des services et non comme des logiciels. Cette particularité impose un traitement différencié et ceci d'autant plus qu'ils sont d'ores et déjà régulés par la récente directive NIS 2. Néanmoins, l'article 3(1) dispose que sont incluses dans le champ d'application du CRA les solutions de traitement à distance des données. L'article 3(2) définit ces solutions de tel sorte à y inclure la plupart des services de SaaS.

Ces deux articles soulèvent un important risque d'insécurité juridique du fait de leur contradiction avec le considérant 9, c'est pourquoi, **nous appelons à une exclusion complètes des services de cloud du champ d'application du CRA.**

L'exception prévue pour les logiciels open-source développés en dehors de toute activité commerciale (considérant 10) est aussi une nécessité pour le développement de l'économie numérique européenne.

Ainsi, si le champ d'application est satisfaisant à bien des égards, de nombreuses interrogations demeurent.

En effet, **la définition des *« produits incorporant des éléments numériques »*** inclue, outre les produits et les logiciels**, les composants qui sont placés sur le marché, définis de façon vague**. **En considérant les composants comme des produits le CRA risque d'imposer aux fabricants de produits finis et à leurs fournisseurs des exigences difficilement réalisables**

voire contradictoires. De plus, l'article 6 du CRA prévoit que les produits incorporant des éléments numériques considérés comme critiques ou très critiques deviennent eux-mêmes des produits critiques.

Cet article soulève des questionnements quant à la mise en œuvre pratique des procédures de mise en conformité. En effet, fabricants et fournisseurs travaillent déjà en collaboration pour les évaluations de conformité relatives aux législations sur la sécurité des produits et le marquage CE. Ainsi, un fabricant d'ordinateur portable, responsable pour le marquage CE, transmet à ses fournisseurs ses exigences en matière de sécurité des produits tout en gardant la responsabilité. **Cette situation risquerait d'être compliquée si des centaines de composants devaient à leur tour être soumis eux-mêmes au marquage CE.**

Prenons l'exemple d'un smartphone, celui-ci est composé de centaines de pièces différentes, de la batterie au microprocesseur en passant par sa surcouche logicielle. Puisque l'on retrouve dans l'annexe III certains de ces composants (système d'exploitation, microprocesseurs généraux, système de gestion etc…) **les smartphones seraient,** du fait de l'article 6, **des produits critiques** incorporant des éléments numériques. Les fabricants de smartphones ainsi que (potentiellement) de certains composants, tels que les microprocesseurs, devraient alors se soumettre aux procédures de conformité prévues par le module H ou par les modules B+C or **ces procédures impliquent des difficultés importantes concernant leur mise en application.**

En effet, les fabricants sous-traitent une partie, ou la totalité, de leur production dans de nombreux pays, ils ne sont pas toujours propriétaires des usines et ne peuvent garantir leur ouverture et leur disponibilité.

- **Ainsi, comment s'assurer que l'obligation de surveillance prévue par le module H puisse être remplie par l'organisme notifié ?**
- **Que signifie l'obligation faite au fabricant de prendre *« toutes les mesures nécessaires »* pour assurer la conformité de sa production (module C) ?**
- **A quel niveau de précision le fabricant est-il soumis quant à ces *« mesures nécessaires »* ?**
- **Doit-il détailler l'ensemble du processus de production de son partenaire commercial ?**

Enfin, cette problématique n'est pas seulement une question de site de production puisqu'elle concerne également les logiciels intégrés dans les smartphones. Les fabricants se fournissent bien souvent via des tiers pour leurs logiciels de gestion, en tant qu'importateur de ces logiciels ils seraient alors les responsables de leur conformité.

Le paragraphe 4 de l'article 10 impose quant à lui au fabricant de faire preuve de diligence lors de l'intégration d'un composant tier à produit. Nous ne parvenons à identifier qui serait le responsable de la mise en conformité des composants. Si l'article 6 laisse à supposer que le fabricant serait responsable de cette mise en conformité l'article 10 ne semble pas aussi catégorique.

- **Le fabricant doit-il assurer la mise en conformité de ces composants ?**

Une telle situation va nécessairement impacter les entreprises de nombreux secteurs (smartphone, ordinateurs ou encore montres connectés) sans pour autant permettre, dans les faits, une meilleure cybersécurité que celle déjà conférée par les fabricants, soumis eux-mêmes aux exigences (dans le cas du smartphone) de la Directive sur les équipements radio qui comprend des exigences en matière de sécurité. **Les premières entreprises impactées seront les TPE/PME et les ETI européennes qui ne pourront ni internaliser leur production ni se mettre en conformité avec les exigences du module H.**

Recommandations de l'AFNUM :

- Instaurer une nette distinction entre les produits physiques (hardware) et les produits immatériels (software) ;
- Clarifier concrètement les produits soumis aux exigences de l'annexe VI ainsi que les moyens techniques à mettre en œuvre pour s'assurer que ces exigences soient applicables ;
- Clarifier le fait que les produits avec des éléments numériques (tels que définis à l'article 3.1) sont des produits conçus et fabriqués avec comme finalité unique d'être placés séparément sur le marché ;

2 RELATION AVEC LES AUTRES LEGISLATIONS

La régulation de la cybersécurité des produits n'est ni une question nouvelle ni une politique publique délaissée par les pouvoirs publics.

Néanmoins, il demeure vrai que la plupart des exigences relatives à la cybersécurité étaient éparpillées dans des textes très divers. Avec le Cyber Resilience Act la Commission souhaite uniformiser les obligations dédiées à la cybersécurité pour les produits incorporant des éléments numériques.

C'est pourquoi, **la question de la relation entre le CRA et les autres réglementations est primordiale puisqu'elle va guider sa mise en application et conditionner son effectivité pour les fabricants/développeurs.**

Ainsi, le considérant 15 fixe la possibilité pour la Commission européenne d'amender ou d'annuler l'acte délégué adopté sur la base de la directive 2004/53/CE (directive « RED ») prévoyant des exigences de cybersécurité pour les équipements radioélectriques. **C'est sur la base de cet acte délégué, adopté en 2022, qu'ont commencé des travaux de standardisation au sein du CEN-CENELEC.**

Si la Commission venait à amender ou annuler cet acté délégué au moment de l'entrée en application du CRA les travaux de standardisation effectués jusqu'alors devraient être pris en considération pour l'élaboration de nouveaux standards, par exemple via une présomption de conformité couplée à une période de transition suffisamment longue pour éviter des vides juridiques.

Cette transition entre le CRA et l'acté délégué de la RED est bien accueillie par l'AFNUM qui estime nécessaire de prendre en considération les travaux déjà menés par les instances de standardisation. Néanmoins, le considérant 15 reste flou quant à la possibilité concrète de voir l'acte délégué annulé ou amendé. Une clarification de cette situation serait bienvenue afin que les constructeurs puissent anticiper plus facilement le calendrier des travaux de standardisation, dont on sait qu'ils ont tendance à durer plus longtemps que prévu.

De la même manière, les dispositions de l'article 8 prévoient une complémentarité entre les obligations de conformité du CRA et l'obligation de cybersécurité instituée à l'article 15 de l'AI Act pour les systèmes d'IA à haut risque.

Ainsi, un système d'IA à haut risque qui serait conforme aux exigences du CRA bénéficierait d'une présomption de conformité par rapport aux exigences de l'article 15 de l'AI Act.

Enfin, l'article 18 dispose que les produits déjà en conformité avec des standards européens doivent être présumés conformes avec les exigences du CRA. Cette disposition est complétée par l'article 19 qui prévoit qu'en cas d'absence de tels standards, ou si ces standards sont insuffisants, la Commission est habilitée à adopter des *« spécifications communes »* au moyen d'actes délégués. Ces spécifications auront la même force que les standards européens et permettront de bénéficier d'une présomption de conformité.

Si ces dispositions nous semblent essentielles nous considérons qu'elles ne prennent pas en considération la réalité concrète de l'industrie. **En effet, de nombreux industriels et développeurs utilisent déjà des standards internationaux (principalement des normes ISO) reconnus par l'ensemble du secteur comme fiables et sûrs.** Or, ces standards n'étant pas publiés au Journal Officiel de l'Union Européenne ils ne rentrent pas dans le champ d'application de l'article 18. Ainsi, et quand bien même ces standards répondent à l'ensemble des exigences du CRA, les entreprises les utilisant ne peuvent prétendre à une présomption de conformité sans avoir à repasser par un organisme notifié, via un processus parfois long.

L'article 18 souffre d'une autre limite importante à savoir l'absence complète de standards européens propres aux logiciels. Les standards actuellement en développement découlent de l'acte délégué de la directive RED qui ne cible que les produits matériels. Ainsi, **cette complémentarité entre les standards européens et les exigences du CRA n'est que partielle et ne permettra aux fabricants de la mettre en œuvre dans le cadre de l'équivalence prévue par l'annexe VI.** En tout état de cause, le CRA devrait clarifier le fait que les spécifications communes doivent rester une procédure de dernier ressort uniquement.

L'article 19 quant à lui n'offre pas les garanties nécessaires en matière de transparence pour assurer que ces « spécifications communes » soient en phase avec les attentes des fabricants mais aussi des utilisateurs.

Dans le cadre des processus de standardisation les entreprises sont des acteurs centraux au même titre que les institutions or lors de l'élaboration des « spécifications communes » la Commission européenne travaille seule et sans consulter les acteurs économiques.

C'est pourquoi l'AFNUM invite les législateurs européens à élargir les catégories de standards pouvant justifier une présomption de conformité tout en imposant à la Commission à, a minima, consulter les représentants de l'industrie lors de l'élaboration des « spécifications communes ».

Recommandations de l'AFNUM :

- Maintenir les mécanismes actuels assurant les relations entre le CRA et les autres textes propres à la cybersécurité ;
- Préciser si, et dans quel délai, l'acte délégué de la directive RED sera abrogé ;
- Fonder les nouveaux travaux de standardisation sur ceux déjà menés sous l'empire de l'acte délégué de la directive RED ;
- Elargir les catégories de standard permettant de justifier d'une présomption de conformité ;
- Imposer à la Commission européenne de consulter les acteurs de l'industrie lors de la rédaction des « spécifications communes » ;

3 PROCEDURES DE MISE EN CONFORMITE

S'inscrivant dans le cadre du New Legislative Framework (NLF) le CRA prévoit une obligation de mise en conformité des produits avant leur placement sur le marché.
Cette procédure de mise en conformité est semblable à celle déjà présente dans la directive RED de 2014.

Ainsi, l'annexe 6 prévoit 4 procédures pour assurer la conformité des produits au travers de 4 modules (A, B, C et H).

Comme pour les autres réglementations découlant du NLF ces différents modules correspondent à des procédures de plus en plus contraignantes (Module A → Module H). Ainsi, le module A prévoit un mécanisme d'auto-évaluation de la part du fabricant qui atteste que ses produits sont conformes aux exigences listés dans l'annexe 1.

Le module B impose que la procédure de mise en conformité soit réalisée par un organisme notifié qui se chargera d'évaluer le design, le développement et les procédures de gestion des incidents de conformité.

La procédure établie par le module C doit être réalisée en complément de celle du module B et est réalisée par le fabricant. Celui-ci est chargé d'évaluer sa production interne et d'établir sa déclaration de conformité. Le fabricant peut également choisir d'utiliser un standard européen et ainsi bénéficier d'une présomption de conformité quant aux exigences de l'annexe I.

Enfin, le dernier module, le H, correspond au degré le plus élevé de contrôle et est également réservé aux produits critiques. Le processus d'évaluation de la conformité est réalisé par un organisme agréé qui sera chargé de vérifier que le design technique, le développement, la production du produit correspondent aux exigences de l'annexe 1. De plus, ce même organisme évaluera les procédures mises en œuvre par le fabricant pour gérer les failles de sécurité.

L'AFNUM est sceptique sur le fait qu'il y aura assez d'organismes notifiés qui seront

autorisés à opérer pour le CRA au moment de son entrée en vigueur. Il y a 71 organismes notifiés pour la directive RED, dont 20 sont des organismes de pays tiers, notifiés uniquement en vertu d'accords internationaux ne couvrant, par définition, pas le CRA[1]. **Même en partant du principe que tous les organismes notifiés de la RED souhaiteraient et arriveraient à être notifiés pour le CRA, cela reste trop peu au regard du nombre de produits et logiciels couverts par le champ d'application extrêmement large du CRA.**

Un recours obligatoire aux modules B + C ou H aurait pour conséquence de créer des goulots d'étranglement sur le marché au moment de l'entrée en vigueur du texte et de retarder le placement sur le marché de produits et composants, et ce alors que l'Union Européenne fait actuellement face à de sérieux défis d'approvisionnement en matériaux critiques tels que les semi-conducteurs.

Il est compréhensible qu'une approche fondée sur les risques, en cohérence avec la NLF, impose de passer par un organisme notifié pour une évaluation de la conformité pour une minorité de produits à haut-risque. **Néanmoins, l'annexe III, partie 2, telle que formulée dans la proposition actuelle ne représente pas loin s'en faut une minorité de produits mais un volume trop important pour être absorbé par les organisme notifiés actuels.**

C'est pourquoi, nous estimons également nécessaire de repousser l'entrée en application du texte afin de permettre aux fabricants et développeurs de s'adapter à ces nouvelles obligations, d'augmenter le nombre d'organismes notifiés capables de répondre aux attentes européennes et de favoriser l'émergence de standards européens.

Recommandations de l'AFNUM :

- Modifier l'annexe III, partie 2, afin de réduire le nombre de produits ciblés par les modules B+C et H ;
- Différer l'entrée en application du règlement en la faisant passer de 24 à 48 mois ;

4 OBLIGATIONS POUR LES OPERATEURS ECONOMIQUES

Les procédures de mise en conformité s'accompagnent logiquement de diverses obligations pour les opérateurs économiques proposant des produits numériques. Ces obligations sont présentes au sein du chapitre 2 et elles se divisent entre les obligations des fabricants, des importateurs et des distributeurs.

Les fabricants doivent notamment s'assurer que leurs produits soient conformes aux exigences de l'annexe I au moyen d'évaluation de conformité et de fourniture de mises à jour de sécurité.

Si l'AFNUM défend le besoin d'une législation uniformisée nous estimons nécessaire

[1] https://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=directive.notifiedbody&dir_id=154428

d'apporter des précisions aux exigences mentionnées à l'annexe 1.

En effet, cette annexe impose aux entreprises de délivrer leurs produits numériques sans vulnérabilités connues exploitables. Cette obligation, bien que louable, **est en réalité inadaptée à tous les acteurs de l'industrie et rendrait très difficile, voire impossible, de délivrer les biens sans ralentir fortement tout le processus de production des systèmes complexes.** Cette difficulté est notamment prégnante pour les industriels des réseaux de télécommunication.

C'est pourquoi, **l'AFNUM propose de repenser cette obligation en utilisant le concept de « Common Vulnerability Scoring System » (CVSS) déjà adopté par les industriels** et les autorités de contrôles en charge de la cybersécurité (CERT-FR par exemple pour la France). Cet indice permet d'établir le risque induit par chaque vulnérabilité et ainsi de leur attribuer un score traduisant leur impact (faible – moyen – élevé – critique).

Ainsi, pour permettre aux industriels de maintenir leurs niveaux de production tout en assurant un haut niveau de cybersécurité **l'AFNUM plaide pour que seules les vulnérabilités classées « critiques » et « élevés » soient considérées comme exploitables et donc absentes des produits au moment de leur délivrance.**

En outre, **l'obligation faite aux fabricants de livrer le produit avec « une configuration sécurisée par défaut » ne correspond pas non plus à la réalité de toute l'industrie**. En effet, certains secteurs d'activité, notamment en B2B, proposent de nombreuses configurations possibles pour leurs appareils suivant les besoins de leurs clients. Par exemple, dans le cadre de systèmes complexes comme celui des réseaux de télécommunication les fabricants ne sont pas en mesure de contrôler les décisions prises par les acheteurs en matière de sécurité. La configuration de ces systèmes est établie en fonction des besoins de l'acheteur et de l'architecture dans laquelle le système sera intégré.

Du fait de cette particularité il est également difficile, voire impossible, de proposer une réinitialisation du produit à « son état d'origine » puisque que celui-ci est unique en raison de l'héritage des versions logicielles et des différences dans le mix des générations de technologies.

La deuxième section de l'annexe 1 impose aussi aux fabricants de produits numériques de publier les vulnérabilités dont ils ont connaissance dès lors qu'un correctif est disponible. L'AFNUM recommande de modifier cette obligation pour qu'elle corresponde mieux aux pratiques des industriels. Les informations sur ces vulnérabilités doivent être diffusées avec prudence et en suivant les principes de réduction des dommages grâce à une divulgation responsable et centrée sur les acteurs qui peuvent agir pour réduire les risques.

Ainsi, l'AFNUM estime important de recentrer cette obligation d'information sur les clients directement concernés par la vulnérabilité en cause. De plus, nous plaidons également pour un alignement avec la « Recommandation du Conseil sur la gestion des vulnérabilités de sécurité numérique » qui liste les meilleurs pratiques en vigueur.

En outre, le paragraphe 12 de l'article 10 précise que dès le placement sur le marché et

pour la durée de vie attendue du produit, ou 5 ans, les fabricants sont tenus de fournir des mises à jour de sécurité (point 2 (2) de l'annexe 1).

Bien que l'AFNUM soit favorable au renforcement de la cybersécurité des produits, et ceci par tous les moyens, **nous nous interrogeons sur la durée choisie dans ce projet de règlement ainsi que sur la complémentarité de cette obligation avec les différents droits nationaux.**

En effet, les réglementations nationales, en application des directives européennes, prévoient déjà l'obligation de fournir des mises à jour de sécurité dans le cadre des garanties légales de conformité. **Ainsi, en France l'article L217-19 du code de la consommation dispose que le vendeur est tenu de fournir au consommateur des mises à jour pendant une période minimum de 2 ans après la délivrance des biens.**

C'est pourquoi, nous considérons nécessaire d'aligner les exigences du CRA avec celles déjà développées au sein des Etats membres afin d'éviter un allongement *« artificiel »* des différentes garanties légales de conformité.

Il est également important de noter que de très nombreux acteurs interviennent lors du développement d'une mise à jour. En effet, dans le cas d'un smartphone, la plupart des fabricants dépendent d'au moins 2 prestataires (voir plus) pour pouvoir mettre à jour leurs appareils.

Tout d'abord intervient le développeur du système d'exploitation utilisé par le fabricant. Ce développeur propose, sur une base régulière, des mises à jour qu'il met à la disposition des fabricants **dans le cadre d'un contrat négocié pour une période déterminée** (3 ans dans la plupart des situations).

Cette mise à jour doit ensuite être **adaptée par le fournisseur du processeur du smartphone afin qu'elle soit utilisable par le fabricant final**. Là encore, **cette étape est régie par un contrat établit pour une période donnée** (bien souvent celle-ci est adaptée à celle déjà négociée avec le fournisseur du système d'exploitation).

Enfin, le fabricant du smartphone vérifie que la mise à jour soit fonctionnelle sur ses appareils.

Il est donc extrêmement complexe pour les fabricants de prolonger les durées de fourniture de mise à jour sans renégocier l'ensemble de ces contrats et donc d'augmenter les coûts induits par chaque mise à jour.

En l'absence de clarification, et dans le cas où l'obligation de fourniture de mise à jour pèserait sur le fabricant, **le CRA risque d'affaiblir considérablement les industriels français et européens qui ne pourront pas s'aligner sur les coûts découlant de cette nouvelle règlementation.**

Pour permettre une meilleure mise en œuvre de cette obligation et un renforcement accru de la cybersécurité, **nous invitons les législateurs à préciser que l'obligation de 5ans de**

mise à disposition de mise à jour concerne la première mise sur le marché de la première unité du modèle. Cette précision permettrait d'assurer une meilleure prévisibilité juridique pour les fabricants, de renforcer la cybersécurité des produits, de faciliter l'alignement des contrats mentionnés ci-dessus et enfin de prolonger la durée de vie des appareils.

Outre cette obligation, le CRA impose également aux fabricants une obligation de signalement (article 11), **dans les 24h**, auprès de l'ENISA de toutes les failles activement exploitées. Si l'intention est louable elle n'en demeure pas moins difficilement applicable tout en pouvant se révéler dangereuse. **Lorsqu'un incident survient, la publicité et la publication de cet incident servent uniquement les intérêts des cybercriminels, la discrétion est absolument nécessaire pour résoudre les situations.**

En effet, la notion de *« failles activement exploitées »* renvoie à un nombre très différents de réalités, il peut s'agir de failles mineures n'impliquant aucunes fuites de données comme de failles très temporaires. **La définition proposée par la Commission est assez large pour nécessiter une remonté d'information quasi constante à l'ENISA.**

De plus, le paragraphe 2 de cet article impose une même obligation pour tous les incidents pouvant avoir un impact sur la cybersécurité de leurs produits.

Ce flux d'informations continu ne permettra pas à l'ENISA de se concentrer sur les failles véritablement susceptibles d'engendrer d'importantes fuites de données tout en imposant un travail administratif très lourd aux entreprises.

C'est pourquoi, **l'AFNUM recommande aux législateurs d'aligner les exigences du CRA sur celles de la directive NIS2 qui prévoient une obligation de signalement, dans les 72h, uniquement dans les situations où la faille perturbe ou risque de perturber de manière significative les activités de l'entreprises (article 13 de la directive NIS 2).**

Recommandations de l'AFNUM :

- Aligner le régime européen sur les régimes nationaux de garantie légale de conformité afin d'éviter un allongement « artificiel » de ces garanties légales ;
- Introduire une notion de « sévérité » dans l'évaluation et la classification des vulnérabilités suivant les méthodes CVSS ;
- Limiter l'obligation « d'absence de vulnérabilités » aux seules vulnérabilités « élevées » et « critiques » ;
- Définir les vulnérabilités en indiquant qu'elles ne découlent pas uniquement des erreurs dans le code mais également d'une mauvaise configuration par l'utilisateur ;
- Compléter « être livré avec une configuration sécurisée par défaut, incluant la possibilité de réinitialiser le produit à son état d'origine » avec « ou selon les modalités contractuelles pour les produits critiques comportant des éléments numériques établis par l'ANNEXE III » ;
- Préciser que l'obligation de 5 ans de mise à disposition de mise à jour concerne la première mise sur le marché de la première unité du modèle ;

- Aligner l'obligation de signalement des failles de cybersécurité sur celle déjà présente dans la directive NIS 2 ;

A propos de l'AFNUM

L'AFNUM (Alliance Française des Industries du Numérique) représente, en France, les industriels du secteur IT, des réseaux, de l'électronique grand public, de l'impression, de la photographie et des objets connectés. Les adhérents de l'AFNUM constituent le « socle numérique » qui permet à toutes les couches supérieures du numérique - logicielles, d'infrastructure ou cloud - d'exister.

Créateurs de richesse et de croissance en France et en Europe**,** les adhérents de l'AFNUM innovent et développent les produits, les applications et les usages du futur. Santé, mobilité, industrie 4.0, environnement, culture, formation : grâce à la numérisation croissante de nombreux secteurs de l'économie, le socle numérique est au cœur des enjeux à venir, fondement d'un futur attractif pour la société, réducteur d'empreinte carbone et durablement porteur de valeur.

Le poids économique des entreprises adhérentes de l'AFNUM est de 100.000 emplois (dont 31.000 emplois directs et plus de 5000 emplois en R&D) pour 28 milliards d'euros de chiffre d'affaires générés en France.

L'AFNUM est membre de la FIEEC, du MEDEF et de Digitaleurope.