Fédération des Industries Mécaniques

www.fim.net

NOTE DE POSITION

Position FIM sur le projet de Règlement sur la cybersécurité des produits

Contact: **Roxana Turcanu**
rturcanu@fimeca.org - + 33 (0)1 47 17 64 87

Publication : **04/05/2023**

Contexte et défis

La recrudescence des attaques de type rançongiciel (ransomware) et l'hameçonnage (phishing) depuis 2017 poussée par l'essor de l'économie cybercriminelle « as a service » rendent nécessaire une approche économique, géopolitique, réglementaire et pragmatique de la cybersécurité, dans l'objectif de renforcer la capacité industrielle et d'innovation de l'Union Européenne. Alors que le cadre législatif européen couvrait déjà des aspects liés à la cybersécurité sous différents angles (produits, services, gestion des crises et criminalité)[1], la Commission européenne a estimé qu'un règlement à large application sur la cybersécurité des produits avec des éléments numériques était nécessaire pour :

- Créer les conditions pour le développement de produits comportant des éléments numériques sécurisés
- Créer des conditions permettant aux utilisateurs de prendre en considération la cybersécurité lorsqu'ils sélectionnent et utilisent des produits comportant des éléments numériques.

Ainsi, le 15 septembre 2022 la Commission a publié sa proposition de règlement concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020.

La FIM soutient les objectifs énumérés, toutefois nous estimons que pour les atteindre, des dispositions du projet de règlement mériteraient une rédaction plus claire, alignée sur les principes de droit européen existants et des obligations proportionnelles. Ainsi, pour une meilleure applicabilité et efficacité du règlement, la FIM souhaite proposer des amendements concernant les points suivants :

- La classification des produits et les critères pour déterminer le niveau de risque de cybersécurité,
- La modification substantielle,
- L'applicabilité des exigences produit au moment de la livraison,
- La clarté et les conséquences de certaines obligations dans le cadre de la gestion des vulnérabilités,
- La mise à jour de l'évaluation de la conformité et de la déclaration de conformité,
- La présomption de conformité par l'application des schémas de certification,
- L'articulation du règlement avec le Règlement machines,
- L'étendue des sanctions,
- La date d'application.

Comme remarque générale, nous attirons l'attention sur la mauvaise qualité de la traduction en français et encourageons l'utilisation d'une terminologie appropriée en français, qui ne change pas le sens ou l'étendue des exigences et des obligations par rapport à la version en anglais.

[1] La Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information
La Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union remplacée bientôt par NIS2
Le Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications

Classification des produits

Le projet de règlement classe les produits en trois catégories (article 6) :

- Produits sans criticité
- Les produits critiques de classe I (Annexe III) qui peuvent faire l'objet d'une démarché d'autocertification si des normes harmonisées sont disponibles (article 24.2)
- Les produits critiques de classe II qui feront impérativement l'objet d'une évaluation de la conformité et certification par un tiers (article 24.3). Un produit dont une fonctionnalité clef est citée dans l'annexe III, tombe dans la catégorie respective de sa fonctionnalité clé.

Ces dispositions soulèvent plusieurs questions.

D'abord, l'article 6 stipule que « Les produits comportant des éléments numériques relevant d'une catégorie qui figure à l'annexe III sont considérés comme des produits critiques comportant des éléments numériques. Les produits dont la fonctionnalité de base est celle d'une catégorie énumérée à l'annexe III du présent règlement sont considérés comme relevant de cette catégorie ». Faisant exception de la rédaction qui prête à confusion (par exemple : de quelle classe est un produit avec un élément numérique de l'annexe III qui n'assure pas une fonctionnalité clé ?), ces dispositions sur les produits critiques avec des éléments numérique ne suivent pas la définition donnée par l'article 3 (3) « un produit comportant des éléments numériques, qui présente un risque de cybersécurité selon les critères énoncés à l'article 6, paragraphe 2, et dont la fonctionnalité de base est définie à l'annexe III; ».

En second lieu, les différences entre les produits critiques de classe I et classe II de l'annexe III ne sont pas évidentes alors que connaître la classe exacte d'un produit influence le choix du module de conformité appliqué. Ainsi, des critères clairs devraient être appliqués pour aboutir à cette classification.

Par la suite, les critères pour déterminer le niveau de risque de cybersécurité utilisés par la Commission (article 6.2) sont répétitifs et trop étendus. Le point a) et ses sous-points sont similaires au point c). La rédaction du point (e) pose la question de la « la mesure dans laquelle l'utilisation de produits comportant des éléments numériques a déjà causé une perte ou une perturbation matérielle ou immatérielle » et du seuil applicable. Qui décide de ce seuil et sur la base de quels critères ? Enfin, la terminologie « préoccupations importantes » est très large et semble faire appel à un jugement d'ordre subjectif et émotionnel. Le point (d) est assuré par l'articulation avec la directive NIS2.

Amendements FIM

Dans un souci de cohérence avec l'article 3 (3), la FIM suggère d'amender l'article 6 comme il suit :

> « Les produits comportant des éléments numériques relevant d'une catégorie qui figure à l'annexe III et **assurant une fonctionnalité clé,** sont considérés comme des produits critiques comportant des éléments numériques. ~~Les~~ **Ces** produits ~~dont la fonctionnalité de base est celle d'une catégorie énumérée à l'annexe III du présent règlement sont considérés comme relevant de cette catégorie~~ relèvent de la ~~catégorie~~ classe des éléments numériques qu'ils comportent ».

Concernant l'article 6.2 nous suggérons de :

- Supprimer le point (a) vu son doublonnage avec le point (c).
- Supprimer le point (d) vu que son application est prise en compte par les exigences applicables aux entités importantes et essentielles de la directive NIS2.
- Supprimer le point (e) qui ne permet pas une caractérisation objective du niveau de risque de cybersécurité.
- Rendre les critères (b) et (c) cumulatifs.

En conséquence l'article 6.2 devrait être rédigé comme il suit :

> « 2. La Commission est habilitée à adopter des actes délégués conformément à l'article 50 pour modifier l'annexe III en ajoutant une nouvelle catégorie à la liste des catégories de produits critiques comportant des éléments numériques ou en retirant une catégorie existante de cette liste. Lorsqu'elle évalue la nécessité de modifier la liste figurant à l'annexe III, la Commission tient compte du niveau de risque de cybersécurité lié à la catégorie de produits comportant des éléments numériques. Pour déterminer le niveau de risque de cybersécurité, ~~un ou plusieurs des~~ **les** critères suivants sont pris en compte: ».

Modification substantielle

L'article 3 (31) définit la « modification substantielle » comme « une modification apportée au produit comportant des éléments numériques à la suite de sa mise sur le marché, qui a une incidence sur la conformité du produit comportant des éléments numériques aux exigences essentielles énoncées à l'annexe I, section 1, ou entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué ».

Vu les objectifs du présent règlement, son application horizontale, nous questionnons la pertinence de cette définition dans ce cadre. La réglementation sectorielle et le cadre NLF définissent les situations où un produit doit être considéré comme neuf. Cela permet une articulation logique avec les règlements horizontaux et d'éviter l'instabilité juridique et la confusion provoquées par le doublonnage des concepts et définitions.

Amendement FIM

Etant donné le traitement de ce concept par d'autres textes sectoriels et son manque d'intérêt en l'espèce, nous demandons la suppression de la définition de la modification substantielle.

Exigences de cybersécurité applicables aux produits

Les exigences de cybersécurité applicables aux produits doivent être satisfaites au moment de la mise sur le marché du produit et non lors de la livraison du produit comme indiqué par le projet de règlement (annexe I, section 1.2). Cela permettrait de rester aligné sur le nouveau cadre législatif et proportionner cette obligation par rapport aux moyens à déployer par le fabricant pour assurer la cybersécurité de son produit. Dans le même temps, vu la portée de l'obligation de la gestion des vulnérabilités, « effective » tout au long de la vie du produit ou pour une durée de 5 ans (l'annexe I, section 2), le fabricant devra de toute façon assurer des mises à jour et agir sur les vulnérabilités identifiées après la mise en service.

L'obligation de justifier pourquoi certaines exigences essentielles ne sont pas applicables au produit (article 10.3) est remplie de facto grâce à l'analyse de risque en vertu de laquelle le fabricant appliquera les exigences de l'annexe I, section 1.3. Une justification en plus de l'analyse de risque nous semble disproportionnée.

Amendements FIM

Pour une meilleure applicabilité du texte nous suggérons la modification suivante à l'annexe I, section 1, point 2 :

> « (2) Les produits comportant des éléments numériques doivent être **mis sur le marché** ~~livrés~~ sans aucune vulnérabilité exploitable connue. »

Cette modification devrait être également apportée au point 3.a de l'annexe I.

Nous attirons l'attention sur les termes « vulnérabilité exploitable connue » qui ne sont pas définis. Ce type de vulnérabilité supposerait l'existence préalable d'une base de données publique avant l'entrée en application du CRA. Nous estimons qu'une clarification de ces termes est nécessaire à l'application de cette exigence.

Au sujet de l'article 10 (3) nous estimons nécessaire la suppression de la dernière phrase :

> « Lorsqu'il met sur le marché un produit comportant des éléments numériques, (…) l'évaluation des risques de cybersécurité peut faire partie de l'évaluation des risques prévue par ces actes de l'Union. ~~Lorsque certaines exigences essentielles ne sont pas applicables au produit comportant des éléments numériques commercialisé, le fabricant fait figurer une justification claire dans cette documentation. »~~

Exigences de gestion des vulnérabilités des produits

Certaines obligations énumérées par l'annexe I, section 2 semblent disproportionnées et imprécises. L'obligation d'effectuer « des tests et les examens efficaces et réguliers de la sécurité du produit avec éléments numériques » (annexe I, section 2.3) nous semble inapplicable car elle nécessiterait de superviser l'ensemble des produits.

Par la suite, nous comprenons l'intérêt pour le fabricant de tenir une nomenclature logicielle. Toutefois l'obligation de permettre à l'utilisateur de consulter la nomenclature logicielle (annexe II, point 6), alors que celle-ci dans la définition donnée par l'article 3.37 est une véritable cartographie des relations commerciales du fabricant parait difficilement justifiable. L'utilité de cette information pour l'utilisateur est nulle, étant donné les obligations de gestion de vulnérabilité par le fabricant. En revanche, la publication de telles informations peut être préjudiciable

pour le fabricant et contraire au secret d'affaires. Toute éventuelle demande de la part de l'utilisateur concernant des éléments de la nomenclature logicielle devrait être traitée par voie contractuelle.

Liée à la bonne gestion des vulnérabilités du produits, l'obligation d'informer les utilisateurs du produit comportant des éléments numériques d'un incident et, le cas échéant, des mesures correctives que l'utilisateur peut mettre en place pour en atténuer l'impact (article 11.4) et les obligations prévues par les points (4), (8) de la partie 2 de l'annexe I, peuvent être difficilement mises en œuvre lorsque le produit connait plusieurs utilisateurs successifs.

Amendements FIM

Nous suggérons de supprimer le point 3 de la section 2 de l'annexe I.

Concernant l'obligation de permettre à l'utilisateur de consulter la nomenclature logicielle, nous recommandons la suppression du point 6 de l'annexe II.

Enfin, pour palier le problème concernant la traçabilité de l'utilisateur, nous suggérons d'amender l'article 11.4 de la façon suivante :

> « Dans les meilleurs délais après avoir pris connaissance de l'incident **significatif**, le fabricant informe **le premier utilisateur** ~~les utilisateurs~~ du produit comportant des éléments numériques de cet incident **significatif** et, le cas échéant, des mesures correctives que l'utilisateur peut mettre en place pour en atténuer l'impact. »

Une conception dynamique de l'évaluation des risques et de la conformité

La conformité telle qu'envisagée par le texte n'est pas conforme à l'approche NLF. Le texte laisse entendre que la conformité n'est jamais acquise et que la déclaration de conformité du produit doit évoluer (articles 10.2, 10.3, 10.5 et 20.2). La présence du caractère évolutif de la cybermenace n'est pas une raison de sortir du nouveau cadre législatif, étant donné la mise en œuvre du procès de gestion des vulnérabilités (annexe I, partie 2), similaire à la mise en place d'une maintenance. Des conséquences lourdes sont prévisibles pour les produits avec des éléments numériques soumis à l'évaluation par un tiers. Par exemple, l'urgence de mettre à jour le système n'est pas compatible avec l'intervention d'un tiers.

Amendement FIM

Nous proposons l'amendement suivant à l'article 20.2 :

> « La déclaration UE de conformité est établie selon le modèle figurant à l'annexe IV et contient les éléments précisés dans les procédures d'évaluation de la conformité applicables prévues à l'annexe VI. ~~Cette déclaration est constamment mise à jour~~. Elle est disponible dans la ou les langues requises par l'État membre dans lequel le produit comportant des éléments numériques est mis sur le marché ou mis à disposition. »

La conformité par des schémas de certification

Alors que l'application d'un schéma européen de certification de cybersécurité (article 18.3) permet une présomption de conformité au même titre que les normes harmonisées, il nous semble important de bâtir ces futurs schémas à partir de procès et savoir-faire déjà utilisés à l'échelle industrielle, en utilisant le cadre de la série des normes IEC 62443 *Réseaux de communication industriels - Sécurité informatique des réseaux et des systèmes*.

Recommandation FIM

Vu l'objectif général de « créer des conditions permettant aux utilisateurs de prendre en considération la cybersécurité lorsqu'ils sélectionnent et utilisent des produits comportant des éléments numériques », nous encourageons l'adoption de la démarche établie par la série de normes IEC 62443.

Concernant les exigences produit, le niveau de sécurité donné par la norme sécurité (1 à 4) peut répondre à une demande d'un client ou à la volonté de mettre sur le marché un produit présentant un niveau de sécurité donné.

Articulation avec d'autres textes

L'articulation entre l'article 9 du projet de règlement sur la cybersécurité et l'article 4 de la Directive machines n'est pas claire. Comme cet article ne cite pas la lex specialis, nous nous demandons si une machine avec des éléments

numérique doit subir une évaluation de la conformité selon le module applicable en vertu de la Directive machine et une évolution de la conformité selon le module applicable en vertu du Règlement cybersécurité. De plus, l'article 9 stipule que la délivrance d'une déclaration de conformité « sur la base du présent règlement » vaut présomption de conformité des machines aux « exigences essentielles de santé et de sécurité énoncées à annexe III, sections 1.1.9 et 1.2.1».

Nous attirons l'attention que les exigences de la section 1.2.1 n'adressent pas exclusivement des EESS en matière de cybersécurité. En conséquence, une telle formulation de l'article 9 pourrait conduire au non-respect des autres exigences de la section 1.2.1.

Amendement FIM

Nous proposons l'amendement suivant à l'article 9 :

> « Les machines et produits connexes relevant du champ d'application du règlement [proposition de règlement sur les machines et produits connexes] qui sont des produits comportant des éléments numériques au sens du présent règlement ~~et pour lesquels une déclaration UE de conformité a été délivrée sur la base du présent règlement sont réputés conformes aux~~ **feront l'objet du principe de *lex specialis* en vertu de l'article [8] du règlement [proposition de règlement sur les machines et produits connexes] concernant** les exigences essentielles de santé et de sécurité **relatives à la cybersécurité** énoncées à l'annexe [annexe III, sections 1.1.9 et 1.2.1] du règlement [proposition de règlement sur les machines et produits connexes], ~~en ce qui concerne la protection contre la corruption ainsi que la sécurité et la fiabilité des systèmes de commande, et dans la mesure où le niveau de protection requis par ces exigences est démontré dans la déclaration UE de conformité délivrée en vertu du présent règlement~~ ».

Sanctions

Vu la taille des entreprises mécaniciennes européennes, les pénalités prévues par l'article 53 semblent disproportionnées.

Amendement FIM

Nous suggérons d'aligner l'article 53 sur le nouveau cadre législatif et supprimer les alinéas (3), (4), (5) de cet article.

Application

L'article 57 du projet de règlement prévoit son entrée en application 24 mois après son entrée en vigueur. Etant donné le temps nécessaire à l'élaboration des normes harmonisées et des schémas de certification, à la notification des organismes, nous trouvons ce délai inopérable.

Amendement FIM

Nous pensons qu'un délai d'application de 48 mois serait plus approprié pour la mise en œuvre effective de ce règlement.

Traduction en français

Lors de la lecture du projet de règlement en français, nous avons aperçu plusieurs traductions erronées.

Amendement FIM

De manière générale, nous suggérons de revoir la traduction et d'utiliser la terminologie française appropriée. En particulier, nous attirons l'attention sur la terminologie utilisée à l'annexe I, point 1 (3)c :

Article	Version anglaise	Version française	Correction proposée
Annexe I, point 1 (3)c	state of the art mechanisms	Mécanismes de pointe	Mécanismes à l'état de l'art

Les industries mécaniques, premier employeur industriel de France, conçoivent des pièces, composants et sous-ensembles et équipements pour tous les secteurs de l'économie :

- Pièces mécaniques issues d'opération de fonderie, forge, usinage, formage, décolletage, traitement de surface, etc.
- Composants et sous-ensembles intégrés dans les produits des clients
- Équipements de production (machines, robots, etc.) et équipements mécaniques (pour la santé, l'agriculture, les TP, le bâtiment, la restauration, la lutte contre l'incendie, l'approvisionnement en eau, la production d'énergie, la mesure, …)
- Produits de grande consommation (arts de la table, outillage, ...