Journal officiel
de l'Union européenne

FR
Série C

C/2026/6013

17.11.2026

COMMUNICATION DE LA COMMISSION

Orientations de la Commission relatives à l'application du règlement (EU) 2024/2847 (règlement sur la cyberrésilience)

(C/2026/6013)

Table des matières

Page

1. INTRODUCTION 3
   - 1.1. Le règlement sur la cyberrésilience 3
   - 1.2. Objectif des orientations 3
2. CHAMP D'APPLICATION 4
   - 2.1. Mise sur le marché 4
   - 2.2. Les logiciels en tant que produits comportant des éléments numériques 5
   - 2.3. Code informatique 6
   - 2.4. Combinaison de produits matériels et logiciels formant un produit comportant des éléments numériques 7
   - 2.5. Connexion de données 8
   - 2.6. Systèmes complexes 8
   - 2.7. Produits comportant des éléments numériques conçus avant l'entrée en application du règlement sur la cyberrésilience 9
3. LOGICIELS LIBRES ET OUVERTS 11
   - 3.1. Conditions dans lesquelles un logiciel libre et ouvert relève de la responsabilité d'une personne physique ou morale 12
   - 3.2. Conditions dans lesquelles un logiciel libre et ouvert est mis sur le marché de l'Union 13
     - 3.2.1. Facturation d'un prix 13
     - 3.2.2. Monétisation d'autres services ou nécessitant le traitement de données à caractère personnel 13
     - 3.2.3. Services d'assistance 14
     - 3.2.4. Dons 15
     - 3.2.5. Financement des logiciels libres et ouverts 15
     - 3.2.6. Entités à but non lucratif constituées pour atteindre des objectifs non lucratifs 16
     - 3.2.7. Intégration par d'autres fabricants 16
   - 3.3. Intendants de logiciels ouverts 16
     - 3.3.1. Soutien continu et garantie de la viabilité du logiciel libre et ouvert 17
   - 3.4. Contributeurs et utilisations en aval 18
   - 3.5. Scénarios illustratifs 19
4. MODIFICATIONS SUBSTANTIELLES ET PIÈCES DE RECHANGE 21
   - 4.1. Réparations physiques 22
   - 4.2. Pièces de rechange 23
   - 4.3. Les mises à jour logicielles en tant que modifications substantielles 24

4.4. Conséquences d'une modification substantielle 27
4.4.1. Modifications substantielles effectuées par une personne autre que le fabricant d'origine 28
4.4.2. Modifications substantielles effectuées par le fabricant d'origine 29
5. PÉRIODE D'ASSISTANCE 29
5.1. Modifications substantielles et période d'assistance 31
6. PRODUITS IMPORTANTS OU CRITIQUES COMPORTANT DES ÉLÉMENTS NUMÉRIQUES 32
6.1. Fonctionnalité de base 33
6.2. Évaluation de la conformité pour les produits importants ou critiques comportant des éléments numériques 36
6.3. Implications pour la présomption de conformité 38
7. ÉVALUATION DES RISQUES DE CYBERSÉCURITÉ ET INTÉGRATION DE PRODUITS COMPORTANT DES ÉLÉMENTS NUMÉRIQUES ET DE COMPOSANTS 41
7.1. Évaluation et traitement des risques de cybersécurité 41
7.2. Obligation de concevoir, développer et fabriquer les produits comportant des éléments numériques de manière à garantir un niveau de cybersécurité approprié en fonction des risques 42
7.3. Évaluation des risques et devoir de diligence raisonnable en ce qui concerne les dépendances externes et les composants intégrés 42
7.4. Réutilisation des évaluations des risques et de la documentation de conformité pour les familles de produits comportant des éléments numériques 44
8. TRAITEMENT DE DONNÉES À DISTANCE 44
8.1. Qu'est-ce qui est considéré comme constituant une solution de traitement de données à distance pour un produit comportant des éléments numériques? 45
8.1.1. L'expression «à distance» 46
8.1.2. L'absence du traitement de données empêcherait-elle le produit comportant des éléments numériques d'exécuter une de ses fonctions? 46
8.1.3. Le logiciel a-t-il été conçu et développé par le fabricant ou sous la responsabilité de ce dernier? 47
8.2. Implications pratiques et techniques des solutions de traitement de données à distance et du recours à des solutions tierces 49
8.3. Cas d'utilisation des solutions de traitement de données à distance 50
8.3.1. Application bancaire mobile 51
8.3.2. Thermostat intelligent 52
8.3.3. Liseuse numérique 53
8.3.4. Robot industriel 53
8.3.5. Réseau cellulaire 53
9. ÉLÉMENTS SUPPLÉMENTAIRES 54
9.1. Obligations en matière de communication d'informations 54
9.2. Gestion des vulnérabilités 56
9.2.1. Signalement en amont et partage des correctifs de sécurité 56
9.2.2. Vulnérabilités exploitables connues 57
9.2.3. Obligation de réaliser régulièrement des tests et examens efficaces 58
9.3. Interaction avec d'autres actes législatifs 59
9.3.1. Le règlement (UE) 2019/2144 et le règlement (UE) nº 168/2013 59
9.3.2. Validité des attestations d'examen UE de type (article 69, paragraphe 1) 59

1. **INTRODUCTION**

1.1. **Le règlement sur la cyberrésilience**

1. Le règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) nº 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience) ([1]) est entré en vigueur le 10 décembre 2024. Ce règlement a pour but de renforcer l'approche de l'Union en matière de cybersécurité, d'aborder la cyberrésilience au niveau de l'Union et d'améliorer le fonctionnement du marché intérieur en établissant un cadre juridique uniforme concernant les exigences essentielles de cybersécurité aux fins de la mise sur le marché de l'Union de produits comportant des éléments numériques, et couvrant également le cycle de vie d'un produit comportant des éléments numériques.

2. Le règlement sur la cyberrésilience repose sur le nouveau cadre législatif de l'Union établi par le règlement (CE) nº 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) nº 339/93 du Conseil, ainsi que par la décision nº 768/2008/CE du Parlement européen et du Conseil du 9 juillet 2008 relative à un cadre commun pour la commercialisation des produits et abrogeant la décision 93/465/CEE du Conseil ([2]).

3. La surveillance du marché et le contrôle de l'application de la législation sont assurés par les autorités nationales de surveillance du marché. Les produits comportant des éléments numériques qui relèvent du champ d'application du règlement sur la cyberrésilience sont couverts par le règlement (UE) 2019/1020 du Parlement européen et du Conseil du 20 juin 2019 sur la surveillance du marché et la conformité des produits, et modifiant la directive 2004/42/CE et les règlements (CE) nº 765/2008 et (UE) nº 305/2011. La Commission et l'Agence de l'Union européenne pour la cybersécurité (ENISA) assistent les opérateurs économiques et les États membres dans l'application du règlement sur la cyberrésilience.

1.2. **Objectif des orientations**

4. L'article 26, paragraphe 1, du règlement sur la cyberrésilience impose à la Commission de publier des orientations pour aider les opérateurs économiques à appliquer le règlement, en mettant tout particulièrement l'accent sur la nécessité de favoriser la conformité par les microentreprises et les petites et moyennes entreprises (PME). L'article 26, paragraphe 2, précise les aspects minimaux que les orientations devraient aborder, à savoir: i) le champ d'application du règlement sur la cyberrésilience (en particulier les solutions de traitement de données à distance et les logiciels libres et ouverts); ii) la notion de «périodes d'assistance»; iii) l'interaction entre le règlement sur la cyberrésilience et d'autres actes législatifs de l'Union; et iv) la notion de «modification substantielle».

5. Le 3 décembre 2025, la Commission a publié une foire aux questions (FAQ) destinée à aider les opérateurs économiques à se préparer à la mise en œuvre du règlement sur la cyberrésilience ([3]).

6. Les présentes orientations ont pour but d'aider les opérateurs économiques à se conformer au règlement sur la cyberrésilience et de soutenir les activités des autorités de surveillance du marché, des autorités notifiantes et des organismes notifiés, afin que le règlement sur la cyberrésilience soit appliqué de manière harmonisée dans l'ensemble de l'Union. Elles n'ont pas vocation à couvrir le règlement sur la cyberrésilience dans son ensemble, mais visent à clarifier la raison d'être de certaines dispositions clés et la manière dont elles pourraient être mises en œuvre dans la pratique. Elles concernent le règlement sur la cyberrésilience et ne sont pas applicables à d'autres actes législatifs de l'Union.

([1]) JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Le programme de travail de la Commission pour 2026 prévoit la présentation d'un «acte législatif européen sur les produits» mettant à jour le nouveau cadre législatif, les règles relatives à la surveillance du marché et les règles en matière de normalisation: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:52025DC0870.

([3]) La FAQ peut être téléchargée sur le site internet de la Commission consacré à la mise en œuvre du règlement sur la cyberrésilience, depuis la page internet consacrée à la FAQ.

7. Les parties intéressées ont été largement consultées lors de l'élaboration des présentes orientations, la Commission ayant notamment consulté le groupe d'experts sur la cybersécurité des produits comportant des éléments numériques ([4]) et organisé une consultation publique entre le 3 mars et le 13 avril 2026 ([5]).

8. Les présentes orientations ne sont pas contraignantes pour les opérateurs économiques ou d'autres acteurs soumis au règlement sur la cyberrésilience. Seule la Cour de justice de l'Union européenne peut donner une interprétation faisant autorité du règlement sur la cyberrésilience. Néanmoins, dans les présentes orientations, la Commission expose son interprétation de ce règlement, en vue de faciliter le respect de celui-ci et de contribuer à sa mise en œuvre effective. Par ailleurs, les orientations contiennent un certain nombre d'exemples pour illustrer l'application de dispositions spécifiques. Toutefois, ces exemples ne sauraient se substituer à une évaluation au cas par cas, laquelle sera toujours nécessaire pour tenir compte des spécificités de chaque cas particulier.

9. Conformément à l'article 26 du règlement sur la cyberrésilience, la Commission peut envisager de publier des orientations supplémentaires, telles que des orientations destinées aux fabricants soumis au règlement sur la cyberrésilience et à une autre législation d'harmonisation de l'Union ou à d'autres actes juridiques connexes de l'Union. Ces orientations pourraient, par exemple, couvrir des questions liées à l'interaction entre le règlement sur la cyberrésilience et le règlement (UE) 2024/1689 établissant des règles harmonisées concernant l'intelligence artificielle (règlement sur l'intelligence artificielle), ou le règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier.

2. **CHAMP D'APPLICATION**

2.1. **Mise sur le marché**

10. Le règlement sur la cyberrésilience s'applique aux produits comportant des éléments numériques qui sont mis à disposition sur le marché de l'Union. La notion de «mise à disposition sur le marché» est définie à l'article 3, point 22), du règlement sur la cyberrésilience comme étant «la fourniture d'un produit comportant des éléments numériques destiné à être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale, à titre onéreux ou gratuit». Conformément à l'article 3, point 21), un produit comportant des éléments numériques est mis sur le marché de l'Union lors de sa première mise à disposition.

11. La dernière édition, publiée en 2022, du guide bleu relatif à la mise en œuvre de la réglementation de l'UE sur les produits (ci-après le «guide bleu») ([6]) comporte des orientations visant à faciliter la compréhension de la réglementation de l'UE relative aux produits et son application uniforme dans les différents cadres juridiques sectoriels alignés sur le nouveau cadre législatif, tels que le règlement sur la cyberrésilience. Le guide bleu indique que les concepts de «mise sur le marché» et de «mise à disposition» doivent être compris comme s'appliquant «à chaque produit individuellement et non à un type de produit, qu'il ait été fabriqué comme une unité individuelle ou en séries» (point 2.3).

12. Pour les produits plus «traditionnels» comportant des éléments numériques qui sont couverts par le nouveau cadre législatif, tels que les produits matériels revêtant la forme de machines ou d'équipements radioélectriques comportant des éléments numériques, la notion de «mise sur le marché» est bien établie et le guide bleu contient des orientations supplémentaires clarifiant quand ces produits sont considérés comme mis sur le marché. Les «exemples pour résumer» énumérés au point 2.12 du guide bleu constituent d'autres exemples illustrant la notion de «mise sur le marché».

13. Toutefois, compte tenu de la nature des produits immatériels comportant des éléments numériques (logiciels autonomes, par exemple), il convient de fournir des orientations supplémentaires pour permettre de déterminer quand ces produits comportant des éléments numériques sont considérés comme mis sur le marché. Une fois que la phase de fabrication du logiciel est achevée et que le produit comportant des éléments numériques est proposé aux utilisateurs potentiels sur le marché de l'Union, son fabricant peut être considéré comme ayant fabriqué plusieurs copies du même logiciel comportant des éléments numériques et les ayant fournies en vue de leur distribution ou de leur utilisation. En fait, contrairement aux produits matériels comportant des éléments numériques, les logiciels autonomes ne sont soumis à aucune restriction en matière de production physique ni à aucune limite d'inventaire: chaque acte de mise à disposition du logiciel en vue de son téléchargement ou de sa

([4]) Page du groupe d'experts sur la cybersécurité des produits comportant des éléments numériques dans le registre des groupes d'experts de la Commission et autres entités similaires.
([5]) Consultation publique sur le projet d'orientations de la Commission relatives au règlement sur la cyberrésilience.
([6]) Communication de la Commission – Le «Guide bleu» relatif à la mise en œuvre de la réglementation de l'UE sur les produits 2022 2022/C 247/01 (JO C 247 du 29.6.2022, p. 1).

distribution entraîne la création d'une nouvelle copie identique pour l'utilisateur. Tant que cette version du logiciel n'est pas modifiée d'une manière qui a une incidence sur la conformité avec le règlement sur la cyberrésilience, la mise sur le marché de l'Union doit être considérée comme ayant lieu au moment de la première présentation pour distribution ou utilisation. La possibilité de télécharger ou de distribuer ultérieurement cette version du logiciel comportant des éléments numériques doit donc être considérée comme une mise à disposition de ce logiciel comportant des éléments numériques ([7]).

14. Par conséquent, un logiciel autonome comportant des éléments numériques devrait être considéré comme mis sur le marché une fois que sa phase de fabrication est achevée et que ce logiciel est fourni pour la première fois en vue d'être distribué ou utilisé sur le marché de l'Union dans le cadre d'une activité commerciale. Le fabricant devrait être considéré comme ayant mis sur le marché simultanément plusieurs copies du même logiciel comportant des éléments numériques. Dès lors, bien que toutes ces copies du même logiciel demeurent des produits individuels comportant des éléments numériques, elles sont considérées comme mises sur le marché en même temps, indépendamment du moment auquel la possession de chaque copie individuelle ou le droit de l'utiliser est transféré à une autre personne physique ou morale. Dans le même temps, si le fabricant met à disposition un logiciel en différentes variantes qui diffèrent au niveau de leurs composants inclus, de leurs configurations ou de leurs fonctionnalités activées (par exemple, des versions conçues pour différents systèmes d'exploitation ou des offres groupées incluant différentes séries de fonctionnalités), ces variantes ne peuvent pas être considérées comme constituant plusieurs copies du même logiciel comportant des éléments numériques. Par conséquent, aux fins de leur mise sur le marché, il convient de les traiter comme des produits distincts comportant des éléments numériques.

Exemple 1: le 1er janvier 2028, la société A propose pour la première fois la version 1.0.0 de son logiciel X pour distribution sur son site internet. Le même jour, un client 1 achète une copie de la version 1.0.0 du logiciel X. Le 15 janvier 2028, un client 2 achète une copie de la version 1.0.0 du logiciel X. Pour ces deux copies de la version 1.0.0 du logiciel X, la date de mise sur le marché sera le 1er janvier 2028.

15. Compte tenu de la nature itérative du développement de logiciels, il convient de préciser également que les itérations ultérieures d'un logiciel comportant des éléments numériques sont considérées comme nouvellement mises sur le marché lorsque ces itérations constituent une «modification substantielle» d'un logiciel comportant des éléments numériques déjà mis sur le marché, comme indiqué au considérant 41 du règlement sur la cyberrésilience. Les itérations qui ne constituent pas des modifications substantielles n'imposent pas au fabricant d'effectuer une nouvelle procédure d'évaluation de la conformité et ne modifient donc pas la date de mise sur le marché de ce logiciel. Pour de plus amples orientations sur la notion de «modification substantielle», voir la section *4 Modifications substantielles*.

Exemple 2: le 1er janvier 2028, la société A propose pour la première fois la version 1.0.0 du logiciel X pour distribution sur son site internet. Le même jour, un client 1 achète une copie de la version 1.0.0 du logiciel X. Le 15 janvier 2028, la société A publie la version 1.0.1 du logiciel X dans le cadre d'une mise à jour qui ne constitue pas une modification substantielle. Le 30 janvier 2028, un client 2 achète une copie de la version 1.0.1 du logiciel X. Pour ces deux copies de la version 1.0.0 et de la version 1.0.1 du logiciel X, la date de mise sur le marché sera considérée comme étant le 1er janvier 2028.

16. Les orientations énoncées aux points 13, 14 et 15 s'appliquent exclusivement lorsque le produit comportant des éléments numériques est un logiciel autonome. Tel n'est pas le cas, par exemple, lorsque le logiciel accompagne un produit matériel, comme expliqué à la section *2.4. Combinaison de produits matériels et logiciels formant un produit comportant des éléments numériques*.

2.2. **Les logiciels en tant que produits comportant des éléments numériques**

17. L'article 3, point 1), du règlement sur la cyberrésilience définit un «produit comportant des éléments numériques» comme étant «un produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels mis sur le marché séparément». Les produits comportant des éléments numériques relèvent du champ d'application du règlement sur la cyberrésilience lorsque leur utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau.

([7]) En vertu de l'article 13, paragraphe 11, les fabricants peuvent conserver des archives logicielles publiques améliorant l'accès des utilisateurs aux versions antérieures. Dans ces cas, les utilisateurs sont informés clairement et d'une manière aisément accessible des risques associés à l'utilisation de logiciels non pris en charge.

18. Le règlement sur la cyberrésilience peut donc couvrir un large éventail de produits comportant des éléments numériques, notamment: i) des logiciels autonomes, tels que des applications et des programmes informatiques, qu'ils soient distribués par voie numérique ou sur un support physique; ii) des produits matériels équipés de logiciels intégrés (dispositifs de l'internet des objets, ordinateurs portables ou tablettes, par exemple); iii) des produits matériels autonomes (circuits intégrés ou cartes mères, par exemple); et iv) toute combinaison de produits matériels et logiciels fournis séparément mais destinés à être utilisés ensemble.

19. Les logiciels autonomes relèvent donc du champ d'application du règlement sur la cyberrésilience s'ils sont mis sur le marché en tant que produits comportant des éléments numériques. Il est utile d'opérer une distinction entre les logiciels comportant des éléments numériques qui sont soumis au règlement sur la cyberrésilience et la fourniture à distance de services qui ne relèvent pas du champ d'application de ce règlement.

20. Pour relever du champ d'application du règlement sur la cyberrésilience, un logiciel comportant des éléments numériques doit être fourni à un utilisateur, obtenu par cet utilisateur et exécuté sur un système d'information électronique ou dans le cadre d'un tel système par l'utilisateur. Les logiciels qui sont téléchargés, installés ou fournis d'une autre manière à l'utilisateur et qui s'exécutent sur le système d'information électronique de l'utilisateur remplissent ces critères y compris, par exemple, lorsqu'ils prennent la forme d'une extension de navigateur ou d'une application développée à l'aide de technologies du web mais fournie pour une exécution locale.

21. En revanche, un logiciel qui s'exécute à distance et auquel l'utilisateur a simplement accès ne constitue pas, pour cette seule raison, un produit comportant des éléments numériques. En fait, cette distinction est établie aux considérants 11 et 12 du règlement sur la cyberrésilience, qui expliquent que le traitement ou le stockage des données à distance ne relèvent du champ d'application du règlement que s'ils sont nécessaires à l'exécution des fonctions d'un produit comportant des éléments numériques [c'est-à-dire via la notion de «traitement de données à distance» telle que définie à l'article 3, point 2)], et qu'ils ne constituent pas en soi des produits comportant des éléments numériques. C'est généralement le cas des applications web, y compris des applications web progressives, auxquelles on accède exclusivement au moyen d'un navigateur internet. Il en va de même pour les sites internet: si un site internet peut techniquement, dans une mesure limitée, s'exécuter sur l'appareil de l'utilisateur, il ressort du considérant 12 du règlement sur la cyberrésilience que les sites internet ne doivent pas eux-mêmes être considérés comme des produits comportant des éléments numériques et ne relèvent du champ d'application de ce règlement que s'ils supportent la fonctionnalité d'un produit comportant des éléments numériques, c'est-à-dire s'ils peuvent être considérés comme un traitement de données à distance (comme expliqué plus en détail à la section *8*, et notamment au point *8.1.2* L'absence du traitement de données empêcherait-elle le produit comportant des éléments numériques d'exécuter une de ses fonctions?).

Exemple 3: une application mobile qu'un utilisateur télécharge à partir d'une boutique d'applications et installe sur son téléphone intelligent est fournie à l'utilisateur et s'exécute sur son appareil; il s'agit donc d'un produit comportant des éléments numériques. Si elle est mise sur le marché dans le cadre d'une activité commerciale, cette application peut relever du champ d'application du règlement sur la cyberrésilience.

Exemple 4: une application de bureau développée à l'aide de technologies du web mais destinée à une installation locale est fournie à l'utilisateur et s'exécute sur son appareil; il s'agit donc d'un produit comportant des éléments numériques. Si elle est mise sur le marché dans le cadre d'une activité commerciale, cette application peut relever du champ d'application du règlement sur la cyberrésilience.

Exemple 5: une application web à laquelle l'utilisateur accède exclusivement au moyen d'un navigateur internet ne constitue pas un produit comportant des éléments numériques. Tant qu'elle ne supporte pas la fonctionnalité d'un produit comportant des éléments numériques, cette application ne relève pas du champ d'application du règlement sur la cyberrésilience. En revanche, une application fournie à l'utilisateur sous la forme d'un client installé localement qui s'exécute sur son appareil constitue un produit comportant des éléments numériques. Si elle est mise sur le marché dans le cadre d'une activité commerciale, cette application peut relever du champ d'application du règlement sur la cyberrésilience.

Si ce client s'appuie, pour exécuter une ou plusieurs de ses fonctions, sur un traitement de données à distance répondant à la définition du traitement de données à distance, ce traitement de données à distance fait également partie du produit comportant des éléments numériques.

Exemple 6: un site internet qui ne fait que présenter des informations à ses visiteurs et ne supporte pas la fonctionnalité d'un produit comportant des éléments numériques ne constitue pas lui-même un produit comportant des éléments numériques. Il ne relève donc pas du champ d'application du règlement sur la cyberrésilience.

2.3. **Code informatique**

22. Il est également utile de préciser quand le code source peut constituer un logiciel comportant des éléments numériques. Le règlement sur la cyberrésilience définit un «logiciel» comme étant «la partie d'un système d'information électronique qui consiste en un code informatique» [article 3, point 4)]. Le code informatique peut prendre la forme i) d'un code machine, qui est l'ensemble des instructions directement exécutées par le processeur d'un ordinateur, rédigées au format binaire; ou ii) d'un code source, c'est-à-dire un jeu d'instructions et de déclarations, rédigées dans un langage de programmation, qui doivent être compilées ou interprétées pour être exécutées par un ordinateur. La notion de «logiciel» telle que définie dans le règlement sur la cyberrésilience couvre ces deux types de code.

23. Un autre enjeu consiste à déterminer si une fourniture donnée d'un code informatique équivaut à la mise sur le marché de l'Union d'un produit comportant des éléments numériques, pour laquelle la fourniture dans le cadre d'une activité commerciale est une condition à remplir. Souvent, tel n'est pas le cas pour le code source. Par exemple, une personne physique ou morale qui partage un code informatique libre et ouvert sur des dépôts accessibles au public ne sera généralement pas considérée comme mettant ce code sur le marché de l'Union aux fins du règlement sur la cyberrésilience (comme expliqué plus en détail à la section *3 Logiciels libres et ouverts)*. Un code inachevé qui est partagé durant la phase de conception et de développement d'un produit comportant des éléments numériques (par exemple, à des fins d'essai ou d'examen) ne sera pas non plus considéré comme mis sur le marché aux fins du règlement sur la cyberrésilience, étant donné que la phase de fabrication n'est pas achevée. De même, un code fourni sous la forme d'un échantillon ou à des fins de démonstration dans le cadre de tutoriels ou de ressources de formation ne sera pas non plus considéré comme mis sur le marché aux fins du règlement sur la cyberrésilience ([8]).

24. En revanche, lorsqu'un fabricant fournit à ses clients un code informatique en tant que produit comportant des éléments numériques, ce code sera considéré comme mis sur le marché, qu'il s'agisse d'un code machine ou d'un code source ([9]).

Exemple 7: la société A octroie à la société B une licence pour l'utilisation de son code source en vue de la conception d'une plate-forme interne personnalisable et fournit ce code source sous la forme d'un fichier texte. Même si ce code source doit encore être adapté et compilé par la société B avant d'être utilisé, la société A met ce code source sur le marché et est donc soumise au règlement sur la cyberrésilience. La société A n'est pas responsable de la conformité avec le règlement sur la cyberrésilience de l'adaptation et de la compilation ultérieures de ce code par la société B.

2.4. **Combinaison de produits matériels et logiciels formant un produit comportant des éléments numériques**

25. Pour répondre à la question de savoir si un logiciel fait partie d'un produit comportant des éléments numériques, il ne faut pas se fonder sur les modalités ou le moment de la livraison de ce logiciel à l'utilisateur, mais il y a lieu de déterminer si, compte tenu de l'utilisation prévue ou raisonnablement prévisible du produit, le logiciel est nécessaire pour que le produit comportant des éléments numériques exécute ses fonctions prévues. Lorsqu'un produit matériel comportant des éléments numériques est conçu pour exécuter ses fonctions en étant utilisé avec un logiciel spécifique fourni par le même fabricant, ce produit matériel et ce logiciel constituent ensemble le produit comportant des éléments numériques. Le logiciel qui est nécessaire pour exécuter, configurer, contrôler ou utiliser un produit comportant des éléments numériques conformément à son utilisation prévue fait donc partie du produit comportant des éléments numériques, même s'il est obtenu par un canal distinct (par exemple, via une boutique d'applications, un lien de téléchargement ou un autre canal numérique après la mise sur le marché du produit matériel comportant des éléments numériques). Sa mise sur le marché a donc lieu au même moment que la mise sur le marché des unités des produits matériels comportant des éléments numériques.

Exemple 8: une imprimante en réseau est mise sur le marché en tant que produit matériel comportant des éléments numériques, tandis que les pilotes de logiciel nécessaires pour envoyer des tâches d'impression, configurer l'appareil et gérer son fonctionnement sont mis à disposition pour téléchargement sur le site internet du fabricant. Bien que l'imprimante et les pilotes soient fournis au moyen de canaux différents, ils constituent ensemble un seul et même produit comportant des éléments numériques, car l'imprimante ne peut assurer son utilisation prévue sans les pilotes.

Exemple 9: un dispositif de fitness portable est mis sur le marché pour mesurer la fréquence cardiaque et l'activité d'un utilisateur, tandis qu'une application pour téléphone intelligent fournie par le fabricant est nécessaire pour visualiser les chiffres mesurés, consulter l'historique et configurer le dispositif. Bien que l'application soit téléchargée séparément par l'intermédiaire d'une boutique d'applications, le dispositif portable et l'application constituent ensemble un seul et même produit comportant des éléments numériques, car ils sont conçus et prévus pour être utilisés ensemble pour assurer la fonctionnalité du produit comportant des éléments numériques.

([8]) Il convient également de rappeler que l'article 4, paragraphe 3, permet aux fabricants de mettre à disposition sur le marché des logiciels inachevés qui ne sont pas conformes au règlement, tels que des versions alpha, des versions beta ou des versions candidates à la diffusion, à condition que le logiciel inachevé ne soit mis à disposition que pendant le temps nécessaire pour le tester et recueillir des commentaires.

([9]) Par ailleurs, il convient de signaler qu'aux fins de la législation relative à la responsabilité du fait des produits, le code informatique lui-même ne constitue pas un produit et que, par conséquent, les fabricants qui mettent un tel code sur le marché ne peuvent être tenus pour responsables en vertu de la directive (UE) 2024/2853 (directive sur la responsabilité du fait des produits). En vertu du considérant 13 de cette directive, «[t]outefois, les informations ne doivent pas être considérées comme un produit, et les règles en matière de responsabilité du fait des produits ne devraient donc pas s'appliquer au contenu des fichiers numériques, tels que les fichiers médias, les livres électroniques ou le simple code source des logiciels». Les fabricants peuvent néanmoins être tenus pour responsables en vertu des législations nationales en matière de responsabilité civile.

2.5. **Connexion de données**

26. Aux termes de l'article 2, paragraphe 1, le règlement sur la cyberrésilience «s'applique aux produits comportant des éléments numériques mis à disposition sur le marché dont l'utilisation prévue ou raisonnablement prévisible comprend une connexion directe ou indirecte, logique ou physique, à un dispositif ou à un réseau». Le champ d'application du règlement sur la cyberrésilience est donc ancré non dans la simple présence d'éléments électroniques, mais dans la capacité d'un produit comportant des éléments numériques à échanger des informations numériques.

27. Si les termes «connexion logique» et «connexion physique» sont définis à l'article 3, le règlement sur la cyberrésilience ne définit ni la «connexion de données», ni les «données numériques». Afin de clarifier les limites du champ d'application du règlement sur la cyberrésilience, il est donc utile d'interpréter la notion de «connexion de données». Ces limites sont particulièrement importantes au moment de différencier les produits comportant des éléments numériques qui utilisent simplement des signaux électriques de ceux qui participent à des communications numériques et sont donc exposés à des risques de cybersécurité.

28. Au niveau le plus élémentaire, une connexion de données suppose la transmission d'informations au format binaire, c'est-à-dire sous la forme d'une séquence de 0 et 1. Le simple fait d'ouvrir et de fermer une sortie (c'est-à-dire les états 0 ou 1) ne constitue pas en soi une connexion de données si l'état ouvert/fermé n'est pas destiné à représenter des données ou n'est pas lu par une entrée numérique. Pour qu'il existe une connexion de données, les états binaires doivent être délibérément encodés en tant qu'informations par une source et doivent pouvoir être décodés en tant qu'informations à destination. Autrement dit, il doit exister un émetteur qui génère délibérément des symboles numériques selon un schéma défini, et un récepteur capable d'interpréter ces symboles comme des données. Lorsque des signaux électriques ou électroniques sont utilisés uniquement pour déclencher ou exécuter une fonction, sans transmettre d'informations codées numériquement, il n'existe aucune connexion de données aux fins du règlement sur la cyberrésilience et, par conséquent, le produit comportant des éléments numériques ne relève pas du champ d'application de l'article 2, paragraphe 1.

2.6. **Systèmes complexes**

29. Les produits comportant des éléments numériques qui relèvent du champ d'application du règlement sur la cyberrésilience peuvent consister non seulement en des dispositifs ou des composants logiciels individuels, mais aussi en des systèmes complexes, y compris des systèmes composés de multiples éléments matériels et logiciels qui interopèrent pour exécuter une certaine fonction. Lorsqu'un tel système est mis sur le marché en tant que seul et même produit comportant des éléments numériques, il constitue un produit comportant des éléments numériques au sens du règlement sur la cyberrésilience.

30. Ces systèmes complexes se caractérisent souvent par de longs cycles de conception et de développement – dont les contrats peuvent avoir été signés avant que le règlement sur la cyberrésilience ne s'applique –, par une longue durée de vie opérationnelle et par un degré élevé de complexité technique et organisationnelle. Les systèmes complexes dont la mise sur le marché aura lieu après l'entrée en application du règlement sur la cyberrésilience peuvent s'appuyer sur des composants mis sur le marché avant l'entrée en application de ce règlement, sur des architectures établies ou sur des normes d'interopérabilité largement utilisées, y compris des normes visées par d'autres actes législatifs ou cadres sectoriels de l'Union. Par conséquent, modifier certaines caractéristiques techniques de ces systèmes sans altérer leur utilisation prévue, leur sécurité, leur fiabilité ou leur interopérabilité avec les infrastructures existantes peut être difficile ou exiger des efforts disproportionnés.

31. L'existence de ces caractéristiques n'exclut pas en soi les systèmes complexes du champ d'application du règlement sur la cyberrésilience, mais illustre l'application de l'approche fondée sur les risques du règlement sur la cyberrésilience, qui permet de démontrer la conformité de différentes manières en fonction des caractéristiques et des contraintes du produit comportant des éléments numériques, conformément à l'article 13, paragraphe 3, du règlement. Ces caractéristiques font partie de l'utilisation prévue de ce produit et de son contexte opérationnel et sont donc pertinentes lors de l'évaluation de la conformité avec les exigences essentielles de cybersécurité (ci-après les «exigences essentielles»). En particulier, le considérant 55 reconnaît explicitement que certaines exigences essentielles peuvent ne pas être pleinement compatibles avec la nature d'un produit comportant des éléments numériques. Tel peut être le cas, par exemple, lorsque la conformité compromettrait les exigences contraignantes en matière d'interopérabilité ou le bon fonctionnement du système.

32. En conséquence, les fabricants sont tenus de traiter les risques de cybersécurité sur la base de l'évaluation des risques de cybersécurité visée à l'article 13, paragraphe 2. Comme également expliqué au considérant 55, dans certains cas, des exigences essentielles spécifiques ne sont pas applicables ou ne peuvent pas être respectées moyennant la mise

en œuvre de mesures de sécurité à la pointe de la technologie en raison, par exemple, de l'utilisation prévue du système, qui exige que le produit comportant des éléments numériques interagisse avec des dépendances existantes ou respecte certaines exigences en matière d'interopérabilité. Dans de tels cas, les fabricants devraient recenser et documenter ces contraintes spécifiques, évaluer les risques y afférents et mettre en œuvre des mesures alternatives ou compensatoires appropriées d'atténuation des risques, afin de ne pas compromettre la sécurité du produit comportant des éléments numériques. À ces fins, tant la documentation technique visée à l'article 31 que les informations et instructions destinées à l'utilisateur visées à l'annexe II jouent un rôle essentiel dans la description transparente des contraintes détectées, des risques de cybersécurité y afférents et des mesures d'atténuation des risques mises en œuvre. Conformément à l'obligation de tenir à jour l'évaluation des risques pendant la période d'assistance, les fabricants devraient également réévaluer périodiquement si les contraintes détectées subsistent. Lorsque ces contraintes peuvent être levées ou réduites au fil du temps, les fabricants devraient mettre à jour en conséquence le produit comportant des éléments numériques afin qu'il puisse évoluer vers un niveau de cybersécurité approprié ([10]).

Exemple 10: un fabricant met sur le marché un produit comportant des éléments numériques qui communique avec des systèmes externes au moyen d'un protocole de réseau. Dans le cadre de l'application des exigences essentielles, le fabricant détermine, sur la base de l'évaluation des risques de cybersécurité, que l'utilisation d'un protocole de communication sécurisé est nécessaire pour garantir la confidentialité et l'intégrité des données échangées par le produit comportant des éléments numériques.

Toutefois, l'utilisation prévue de ce produit inclut l'interopérabilité avec des systèmes existants qui ne prennent en charge qu'un protocole plus ancien ou moins sécurisé. Dans de tels cas, le fabricant peut mettre en œuvre ce protocole lorsque cela est nécessaire à l'interopérabilité, à condition d'avoir recensé et atténué par d'autres moyens les risques de cybersécurité connexes.

Lorsqu'il est techniquement possible pour le produit comportant des éléments numériques de prendre en charge à la fois le protocole sécurisé et le protocole moins sécurisé, le fabricant est censé mettre en œuvre le protocole sécurisé et activer son utilisation par défaut. Le protocole moins sécurisé ne serait autorisé que si l'interopérabilité l'exige.

Exemple 11: le fabricant d'un système d'automatisation industrielle achète certains microcontrôleurs avant l'entrée en application du règlement sur la cyberrésilience. Il procède à l'évaluation des risques de cybersécurité pour son système d'automatisation industrielle, destiné à être mis sur le marché après l'entrée en application du règlement sur la cyberrésilience. Sur la base de cette évaluation des risques de cybersécurité, le fabricant n'a pas détecté de risques de cybersécurité spécifiques associés à l'utilisation de l'un de ces microcontrôleurs. Le fabricant intègre le microcontrôleur dans son système d'automatisation industrielle et veille à ce que le produit comportant des éléments numériques dans son ensemble (le système d'automatisation industrielle) réponde aux exigences essentielles.

2.7. **Produits comportant des éléments numériques conçus avant l'entrée en application du règlement sur la cyberrésilience**

33. Il peut arriver qu'un fabricant mette sur le marché, après l'entrée en application du règlement sur la cyberrésilience le 11 décembre 2027, des unités d'un produit comportant des éléments numériques fabriquées conformément à un type ou à un modèle conçu et développé avant la date d'application de ce règlement. Dans un tel cas, le respect de ce règlement n'exige pas nécessairement de revoir la conception de ces unités du produit comportant des éléments numériques. Le fabricant est tenu de procéder à une évaluation des risques de cybersécurité conformément à l'article 13, paragraphe 2, du règlement sur la cyberrésilience afin de déterminer, sur la base de l'utilisation prévue ou raisonnablement prévisible du produit comportant des éléments numériques, quelles exigences essentielles énoncées à l'annexe I, partie I, sont applicables à ce produit comportant des éléments numériques et comment ces exigences sont mises en œuvre.

34. Lorsque le résultat de cette évaluation des risques démontre que le produit comportant des éléments numériques intègre déjà des mesures de sécurité appropriées et efficaces pour faire face aux risques pertinents, le fabricant peut s'appuyer sur ces mesures existantes pour démontrer la conformité avec le règlement sur la cyberrésilience. Le règlement sur la cyberrésilience n'impose pas en soi l'obligation d'introduire de nouveaux dispositifs de sécurité ou de revoir la conception du produit comportant des éléments numériques lorsque cela n'est pas nécessaire pour faire face aux risques détectés.

([10]) Il convient de signaler que les considérations énoncées dans ce point peuvent s'appliquer, le cas échéant, à tous les produits comportant des éléments numériques qui relèvent du champ d'application du règlement sur la cyberrésilience, et pas seulement aux «systèmes complexes».

35. Néanmoins, le fabricant reste soumis aux obligations prévues par le règlement sur la cyberrésilience. Il doit notamment s'assurer, avant la mise sur le marché du produit comportant des éléments numériques, que la procédure d'évaluation de la conformité applicable a été suivie, que la déclaration UE de conformité a été établie et que le marquage CE a été apposé. Ces exigences sont à respecter que la conception du produit comportant des éléments numériques ait dû être revue ou non à la suite de l'évaluation des risques. Pour les produits comportant des éléments numériques conçus avant la date d'application du règlement sur la cyberrésilience, mais mis sur le marché après cette date, lorsqu'il n'est pas possible pour le fabricant de démontrer comment l'évaluation des risques a été prise en considération au cours de la phase de conception et de développement du produit comportant des éléments numériques, l'obligation prévue à l'article 13, paragraphe 2, devrait s'entendre comme imposant aux fabricants de procéder à une évaluation des risques de cybersécurité et de démontrer sur cette base que le produit comportant des éléments numériques intègre des mesures de sécurité adéquates en vue de réduire au minimum les risques de cybersécurité, de prévenir les incidents et d'en réduire au minimum leurs répercussions, y compris en ce qui concerne la santé et la sécurité des utilisateurs.

36. Par conséquent, les produits comportant des éléments numériques conçus avant l'entrée en application du règlement sur la cyberrésilience pourraient être mis sur le marché dans le cadre de ce règlement sans que le fabricant doive en revoir la conception, à condition qu'il puisse démontrer, au moyen de l'évaluation des risques de cybersécurité et de la documentation technique, que le produit comportant des éléments numériques atteint un niveau de cybersécurité approprié au regard de son utilisation prévue ou raisonnablement prévisible et qu'il est conforme aux exigences essentielles de cybersécurité.

37. Par ailleurs, il est utile de clarifier l'application des obligations d'évaluation de la conformité pour les fabricants de produits comportant des éléments numériques qui sont mis sur le marché après l'entrée en application du règlement sur la cyberrésilience, mais qui sont fabriqués conformément à un type ou à un modèle conçu et développé avant cette date. En vertu de l'article 13, paragraphe 12, le fabricant est tenu de démontrer, au moyen de la procédure d'évaluation de la conformité pertinente, que son produit comportant des éléments numériques est conforme aux exigences essentielles applicables et d'inclure des preuves à cet effet dans la documentation technique du produit (annexe VII, point 6).

38. Toutefois, l'application de ces exigences doit être interprétée à la lumière de l'évaluation des risques de cybersécurité et du profil de risque de cybersécurité du produit comportant des éléments numériques. En particulier dans le cas des produits comportant des éléments numériques conçus avant la date d'application du règlement sur la cyberrésilience (mais mis sur le marché après cette date) et soumis aux procédures d'évaluation de la conformité prévues à l'article 32, paragraphe 1, lorsque l'évaluation des risques démontre que le produit comportant des éléments numériques intègre déjà des mesures de sécurité appropriées et efficaces pour faire face aux risques associés à ce produit, l'obligation de fournir des preuves dans le cadre de la procédure d'évaluation de la conformité ne devrait pas être interprétée comme exigeant du fabricant qu'il fournisse des résultats d'essais couvrant les phases initiales de conception et de développement du produit comportant des éléments numériques. Une telle exigence ne serait pas nécessaire car elle ne contribuerait pas à renforcer la sécurité du produit comportant des éléments numériques lui-même. Lorsque des essais peuvent néanmoins être nécessaires, les fabricants ne sont pas tenus de fournir des preuves des essais effectués pour toutes les variantes du produit, mais peuvent regrouper ces essais en familles de produits comportant des éléments numériques, comme expliqué plus en détail à la section *7.4 Réutilisation des évaluations des risques et de la documentation de conformité pour les familles de produits comportant des éléments numériques*.

39. Néanmoins, le fabricant devrait démontrer comment il se conforme aux processus de gestion des vulnérabilités énoncés à l'annexe I, partie II, devrait tenir à jour son évaluation des risques conformément à l'article 13, paragraphe 3, et s'acquitter de toutes les autres obligations prévues par le règlement sur la cyberrésilience, y compris en fournissant aux utilisateurs des informations et des instructions conformément à l'article 13, paragraphe 18.

Exemple 12: un fabricant met sur le marché un microcontrôleur qui a été conçu et développé avant la date d'application du règlement sur la cyberrésilience. Ce microcontrôleur est destiné à être intégré dans divers produits électroniques comportant des éléments numériques, y compris des produits comportant des éléments numériques dotés de fonctionnalités de connectivité.

Avant de mettre de nouvelles unités du microcontrôleur sur le marché après l'application du règlement sur la cyberrésilience, le fabricant procède à une évaluation des risques de cybersécurité conformément à l'article 13, paragraphe 2. Sur la base de l'utilisation prévue ou raisonnablement prévisible du microcontrôleur, le fabricant recense les risques de cybersécurité pertinents, tels que des risques d'accès non autorisé, de manipulation de logiciels ou de données et de mauvaise utilisation des interfaces disponibles.

Les résultats de l'évaluation des risques montrent que le microcontrôleur, tel qu'il a été initialement conçu, intègre déjà des mesures de sécurité appropriées et efficaces pour faire face aux risques détectés. Le fabricant conclut donc que le produit comportant des éléments numériques satisfait aux exigences essentielles pertinentes énoncées à l'annexe I, partie I, et qu'il n'est pas nécessaire d'en revoir la conception ou d'introduire des fonctionnalités de sécurité supplémentaires.

S'il n'est pas possible de démontrer comment une évaluation des risques de cybersécurité a été prise en considération au cours de la phase initiale de conception et de développement, le fabricant documente une évaluation des risques de cybersécurité qui est en cours et explique comment la conception et les mesures existantes atténuent les risques détectés. Le fabricant n'est pas tenu de recréer une documentation historique de la conception ou des essais, car cela ne contribuerait pas à renforcer la cybersécurité du produit comportant des éléments numériques. Lorsque plusieurs variantes du microcontrôleur sont fondées sur la même conception et partagent le même profil de risque de cybersécurité, le fabricant peut également s'appuyer sur des preuves représentatives couvrant la famille de produits concernée.

Le fabricant veille également au respect des exigences relatives à la gestion des vulnérabilités énoncées à l'annexe I, partie II, notamment en maintenant des processus visant à s'attaquer et remédier aux vulnérabilités et en soumettant l'évaluation des risques de cybersécurité à un examen conformément à l'article 13, paragraphe 3.

Dans ces circonstances, le microcontrôleur conçu avant la date d'application du règlement sur la cyberrésilience peut être mis sur le marché sans que le fabricant doive en revoir la conception, à condition qu'il puisse démontrer, au moyen de l'évaluation des risques de cybersécurité et de la documentation technique, que le microcontrôleur atteint un niveau de cybersécurité approprié au regard de son utilisation prévue ou raisonnablement prévisible et qu'il est conforme aux exigences essentielles applicables.

3. **LOGICIELS LIBRES ET OUVERTS**

40. Comme rappelé à la section *2.1 Mise sur le marché*, le règlement sur la cyberrésilience s'applique aux produits comportant des éléments numériques qui sont mis à disposition sur le marché de l'Union dans le cadre d'une activité commerciale pour la première fois (c'est-à-dire qui sont «mis sur le marché»), ainsi que lors de tout événement ultérieur qui constitue une mise à disposition sur le marché de ce même produit comportant des éléments numériques. Le guide bleu (point 2.2) précise que l'«activité commerciale» doit s'entendre comme la fourniture de biens, à titre onéreux ou gratuit, dans le cadre d'une activité économique et ne peut s'apprécier qu'au cas par cas en tenant compte de la régularité des fournitures, des caractéristiques du produit, des intentions du fournisseur, etc.

41. La fourniture dans le cadre d'une activité commerciale se caractérise par une variété de circonstances, amplement documentées dans le guide bleu et rappelées au considérant 15 du règlement sur la cyberrésilience. Elle peut ainsi être caractérisée par un prix facturé directement, mais également par «le prix des services d'assistance technique lorsqu'il ne sert pas uniquement à récupérer les coûts réels, par une intention de monétisation, par exemple par la fourniture d'une plate-forme logicielle par l'intermédiaire de laquelle le fabricant monétise d'autres services, par l'exigence, comme condition à l'utilisation, du traitement des données à caractère personnel pour des raisons autres qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel, ou par l'acceptation de dons supérieurs aux coûts associés à la conception, au développement et à la fourniture d'un produit comportant des éléments numériques» (considérant 15) ([11]).

42. Toutefois, le règlement sur la cyberrésilience reconnaît les spécificités des différents modes de développement et de publication des logiciels libres et ouverts et contient certaines orientations permettant de déterminer si un logiciel libre et ouvert constitue un produit comportant des éléments numériques mis sur le marché (c'est-à-dire dans le cadre d'une activité commerciale) au sens de ce règlement. Comme expliqué au considérant 18, «[l]es seules circonstances dans lesquelles le produit comportant des éléments numériques a été développé ou la manière dont le développement a été financé ne devraient […] pas être prises en considération au moment de déterminer si l'activité en question est de nature commerciale ou non». Plus précisément, «afin de garantir la distinction claire entre les phases de développement et de fourniture, la fourniture de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts qui ne sont pas monétisés par leur fabricant ne devrait pas être considérée comme une activité commerciale».

([11]) Il convient également de rappeler que, bien que les produits comportant des éléments numériques soient souvent monétisés (également) par le traitement de données à caractère personnel, la protection des données à caractère personnel est un droit fondamental et que, par conséquent, les données à caractère personnel ne peuvent être considérées comme des marchandises, comme indiqué au considérant 24 de la directive (UE) 2019/770 du Parlement européen et du Conseil du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques (JO L 136 du 22.5.2019, p. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Il est donc utile i) de préciser ce qu'est un logiciel libre et ouvert; ii) d'indiquer dans quelles conditions un logiciel libre et ouvert est considéré comme relevant de la responsabilité d'une personne physique ou morale; et iii) de donner des exemples pour aider les parties intéressées à comprendre quand la distribution d'un logiciel libre et ouvert constitue une mise sur le marché. Lorsque le logiciel libre et ouvert n'est pas mis sur le marché, il ne relève pas du champ d'application du règlement sur la cyberrésilience, à moins que l'entité qui le publie ne soit une personne morale qui répond à la définition d'un «intendant de logiciels ouverts» (ci-après «intendant») figurant à l'article 3, point 14). Dans ce cas, seules les obligations prévues à l'article 24 lui sont applicables.

44. L'article 3, point 48), définit un «logiciel libre et ouvert» comme étant «un logiciel dont le code source est partagé de manière ouverte et qui est mis à disposition sous licence libre et ouverte prévoyant tous les droits pour qu'il soit librement accessible, utilisable, modifiable et redistribuable». Bien que les présentes orientations n'indiquent pas explicitement quelles licences libres et ouvertes sont compatibles avec la définition énoncée à l'article 3, point 48), il ressort du libellé de cette disposition que seuls les logiciels qui remplissent cumulativement deux conditions sont considérés comme répondant aux critères de logiciels libres et ouverts aux fins du règlement sur la cyberrésilience: i) le logiciel doit être mis à disposition sous licence libre et ouverte conférant l'ensemble des droits visés à l'article 3, point 48); et ii) son code source doit être partagé de manière ouverte.

45. L'exigence selon laquelle la licence doit prévoir que le logiciel est «librement accessible, utilisable, modifiable et redistribuable» reflète la compréhension traditionnelle des logiciels libres et ouverts, à savoir que les utilisateurs doivent pouvoir avoir accès au code source, l'utiliser sans restriction indue, le modifier et le redistribuer (dans sa version d'origine ou dans des versions modifiées). L'accès au code source est donc une condition préalable nécessaire à l'exercice des autres droits: sans accès au code source, il est pratiquement impossible de modifier ou de réutiliser utilement le logiciel.

46. Toutefois, l'article 3, point 48), ne fait pas seulement référence aux conditions de licence, puisqu'il exige expressément que le code source soit «partagé de manière ouverte». Pour être «partagé de manière ouverte», le code source doit être mis à la disposition du public («en amont» ou «en aval»), et non simplement être fourni avec des restrictions ou sous certaines conditions. Par conséquent, les logiciels distribués sous licence libre et ouverte mais dont le code source n'est partagé (ou ne peut être partagé) qu'avec des clients payants ou un groupe limité d'utilisateurs ne doivent pas être considérés comme des logiciels libres et ouverts au sens de l'article 3, point 48). Aux fins du règlement sur la cyberrésilience, seuls les logiciels dont le code source est mis à la disposition du public et qui font l'objet d'une licence libre et ouverte conférant l'ensemble des droits visés à l'article 3, point 48), devraient donc être considérés comme répondant aux critères de logiciels libres et ouverts.

3.1. **Conditions dans lesquelles un logiciel libre et ouvert relève de la responsabilité d'une personne physique ou morale**

47. Le règlement sur la cyberrésilience fait peser des responsabilités essentielles sur les opérateurs économiques qui fournissent des produits comportant des éléments numériques sur le marché de l'Union. Il définit un «fabricant» comme étant une personne physique ou morale qui fournit un produit comportant des éléments numériques sous son propre nom ou sa propre marque, et ce dans le cadre d'une activité commerciale (mettant ainsi ledit produit sur le marché). De même, un «importateur» est une personne physique ou morale établie dans l'Union qui fournit le produit comportant des éléments numériques d'une personne établie en dehors de l'Union, et ce dans le cadre d'une activité commerciale (mettant ainsi ledit produit sur le marché). Les obligations imposées aux intendants s'appliquent à la personne morale qui fournit un logiciel libre et ouvert destiné à des activités commerciales ([12]), mais qui ne le met pas sur le marché au sens du règlement sur la cyberrésilience.

48. Par conséquent, afin de déterminer si une personne physique ou morale met un logiciel libre et ouvert sur le marché de l'Union, il convient tout d'abord de déterminer si cette personne physique ou morale fournit effectivement le logiciel libre et ouvert. Pour établir à bon droit quelles obligations s'appliquent en vertu du règlement sur la cyberrésilience, il est essentiel de déterminer si la personne physique ou morale se livre effectivement à une opération de fourniture d'un logiciel libre et ouvert. En fait, comme rappelé au considérant 18, le règlement sur la cyberrésilience ne s'applique pas aux personnes physiques ou morales qui contribuent, sous forme de code source, à des produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ne relevant pas de leur responsabilité.

([12]) Il s'agit d'une condition nécessaire mais non suffisante pour qu'une personne morale puisse être considérée comme un intendant de logiciels ouverts, étant donné que la définition figurant à l'article 3, point 14), prévoit des conditions supplémentaires pour qu'une personne morale puisse être considérée comme un intendant.

49. Compte tenu des spécificités du développement des logiciels libres et ouverts, qui, souvent, fait intervenir une multitude de contributeurs, suit des modèles de collaboration décentralisée et se caractérise par une séparation entre contribution et prise de décision, il est utile de préciser qu'un logiciel libre et ouvert est considéré comme «relevant de la responsabilité» des personnes physiques ou morales qui le publient et qui sont les principaux responsables des décisions en matière de développement, de déploiement et de distribution (souvent appelées les «responsables de l'entretien»). Les personnes qui contribuent au code source mais ne contrôlent pas les déploiements, les feuilles de route ou les décisions de gouvernance sont considérées comme des «contributeurs»; dans ce cas, le logiciel libre et ouvert ne relève pas de leur responsabilité, même si elles ont contribué à son code. La simple existence d'autorisations techniques accordées à un contributeur, telles que l'accès en commit, ne suffit pas à établir que le logiciel libre et ouvert relève de sa responsabilité; la responsabilité incombe aux personnes qui publient et contrôlent le logiciel libre et ouvert.

Exemple 13: un développeur agissant individuellement ou un employé d'une entreprise soumet pour un projet de logiciel libre et ouvert une demande de modification ou de fusion de code contenant un correctif de sécurité ou une nouvelle fonctionnalité. Les responsables de l'entretien du projet examinent sa demande, l'acceptent et procèdent à la fusion du code proposé dans le dépôt principal, avant de l'intégrer dans une nouvelle version. Dans ce scénario, la personne qui a soumis la demande de modification est un «contributeur» et n'est pas soumise au règlement sur la cyberrésilience. Bien qu'elle ait contribué au code source, elle n'est pas responsable au premier chef des décisions en matière de développement, de déploiement et de distribution.

3.2. **Conditions dans lesquelles un logiciel libre et ouvert est mis sur le marché de l'Union**

50. Une fois qu'il a été établi qu'un logiciel libre et ouvert relève de la responsabilité d'une personne physique ou morale, il convient de déterminer si cette personne le fournit dans le cadre d'une activité commerciale, ce qui constituerait une mise sur le marché.

3.2.1. *Facturation d'un prix*

51. Si la personne physique ou morale qui fournit un logiciel libre et ouvert facture un prix pour le logiciel lui-même (par exemple, en facturant un prix pour les binaires précompilés), cette personne met un produit comportant des éléments numériques sur le marché. La personne qui met un logiciel libre et ouvert sur le marché est donc un fabricant au sens du règlement sur la cyberrésilience.

52. Il est courant que les fabricants de logiciels libres et ouverts fournissent des versions gratuites de leurs logiciels (souvent appelées «versions communautaires»), dont la base de code est (presque) identique à celle de la version payante. Il existe cependant des différences entre ces produits comportant des éléments numériques: la version payante est monétisée d'une manière ou d'une autre (par exemple, via un prix facturé ou par d'autres moyens, comme expliqué dans la présente section) et est donc considérée comme mise sur le marché, ce qui déclenche l'applicabilité des obligations imposées aux fabricants. La version gratuite (ou communautaire) n'est pas monétisée et n'est donc pas considérée comme mise sur le marché aux fins du règlement sur la cyberrésilience. Tel est également le cas lorsque la version payante est une version commerciale «améliorée», qui contient une version plus élaborée de la base de code de la version gratuite ou l'intègre dans un plus grand produit comportant des éléments numériques (par exemple, comme dans le cas du modèle «cœur ouvert» – *open core*).

53. Si la personne qui fournit la version communautaire est une personne morale, elle sera également soumise aux obligations imposées aux intendants pour la version qu'elle fournit gratuitement (la version communautaire). Si l'entité est une personne physique, la version gratuite (ou communautaire) ne relève pas du champ d'application du règlement sur la cyberrésilience.

3.2.2. *Monétisation d'autres services ou nécessitant le traitement de données à caractère personnel*

54. Une personne physique ou morale qui publie un logiciel libre et ouvert peut également le mettre sur le marché (c'est-à-dire le fournir dans le cadre d'une activité commerciale) lorsqu'elle fournit le logiciel en monétisant d'autres produits comportant des éléments numériques ou d'autres services, ou lorsqu'elle exige, comme condition à l'utilisation, un traitement des données à caractère personnel pour des raisons autres qu'aux seules fins d'améliorer la sécurité, la compatibilité ou l'interopérabilité du logiciel.

Exemple 14: une personne physique ou morale publie une application de place de marché libre et ouverte. Cette application est disponible gratuitement et permet aux utilisateurs d'acheter des biens ou des services par son intermédiaire. Elle permet à la personne qui l'a publiée de monétiser d'autres produits comportant des éléments numériques ainsi que les services proposés par son intermédiaire (par exemple, au moyen de publicités, de commissions ou de redevances d'abonnement). Par conséquent, l'application est considérée comme mise sur le marché dans le cadre d'une activité commerciale.

Exemple 15: une personne physique ou morale publie un VPN libre et ouvert. Cette application est disponible gratuitement, mais permet aux utilisateurs de payer pour accéder à des serveurs supplémentaires ou à des adresses IP dédiées. Elle permet à la personne qui l'a publiée de monétiser d'autres services proposés par son intermédiaire, de sorte qu'elle est considérée comme mise sur le marché dans le cadre d'une activité commerciale.

Exemple 16: une personne physique ou morale publie une application libre et ouverte de suivi de l'activité physique. Cette application est disponible gratuitement, mais son utilisation est subordonnée au traitement des données à caractère personnel des utilisateurs à des fins telles que des publicités ciblées ou des analyses sans lien avec la sécurité, la compatibilité ou l'interopérabilité du logiciel. Un traitement des données à caractère personnel étant exigé comme condition à l'utilisation, l'application est donc considérée comme mise sur le marché dans le cadre d'une activité commerciale.

3.2.3. *Services d'assistance*

55. Le simple fait qu'une personne physique ou morale publiant un logiciel libre et ouvert propose également des services d'assistance payants liés à ce logiciel ne signifie pas, en soi, que le produit comportant des éléments numériques est fourni dans le cadre d'une activité commerciale. Les services d'assistance peuvent comprendre des activités telles que la fourniture de services de conseil, de services de formation ou de services professionnels liés à l'utilisation, à la documentation, à la configuration et au déploiement du logiciel par un client.

56. Le facteur déterminant est la fourniture contre rémunération d'un accès au logiciel libre et ouvert proprement dit (c'est-à-dire la fourniture du produit comportant des éléments numériques), y compris son entretien, et non la simple prestation de services professionnels accompagnant un produit comportant des éléments numériques librement disponible, comme indiqué au considérant 18 du règlement sur la cyberrésilience («la fourniture de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts qui ne sont pas monétisés par leur fabricant ne devrait pas être considérée comme une activité commerciale»). Si le logiciel libre et ouvert peut être téléchargé et installé librement et si les utilisateurs ont la faculté de choisir de payer séparément pour des services professionnels, ce logiciel libre et ouvert ne sera pas considéré comme mis sur le marché.

57. En revanche, dans certains cas, est subordonné à une rémunération l'accès à une version spécifique du produit comportant des éléments numériques qui donne droit à certains avantages tels que la fourniture d'une assistance technique ou l'optimisation des performances. Dans de tels cas, la fourniture du produit comportant des éléments numériques est monétisée dans le cadre d'une activité commerciale et ce produit sera donc considéré comme mis sur le marché. Cela inclut les cas dans lesquels une édition payante ou une version d'entreprise est mise à disposition en vertu d'un accord commercial, qu'un logiciel fonctionnellement équivalent soit ou non également disponible gratuitement sous licence libre et ouverte.

Exemple 17: une personne physique ou morale publie un système d'exploitation libre et ouvert et en propose une version payante qui donne droit à des services d'assistance, tels que la fourniture d'une assistance technique ou l'optimisation des performances. La version payante du système d'exploitation est considérée comme mise sur le marché dans le cadre d'une activité commerciale.

Exemple 18: une personne physique ou morale publie un outil de ligne de commande libre et ouvert. Cet outil est librement accessible et peut être téléchargé et installé par tout un chacun. La personne physique ou morale propose séparément des services professionnels, tels que des services de conseil facultatifs pour former les utilisateurs et les aider à installer et à utiliser l'outil. Le logiciel libre et ouvert n'est pas considéré comme mis sur le marché au sens du règlement sur la cyberrésilience.

58. En particulier dans le cas des personnes physiques publiant un logiciel libre et ouvert, la fourniture d'une assistance technique accompagnant directement l'accès au produit comportant des éléments numériques ne serait toujours pas considérée comme une activité commerciale si, comme indiqué au considérant 15 du règlement sur la cyberrésilience, le prix facturé servait uniquement à récupérer les coûts réels (ceux-ci pouvant inclure divers coûts liés à la conception, au développement et à l'entretien de ce logiciel, y compris les frais de subsistance raisonnables de la personne qui le publie). Dès lors, une personne physique qui publie un logiciel libre et ouvert et propose la fourniture d'une assistance technique pour récupérer ses coûts et recevoir une rémunération équitable ne doit pas être considérée, pour cette seule raison, comme mettant ce logiciel sur le marché de l'Union.

59. Une personne physique ou morale proposant la fourniture d'une assistance technique liée à un logiciel libre et ouvert qui ne relève pas de sa responsabilité n'est pas considérée comme mettant ce logiciel sur le marché, à moins qu'elle n'apporte une modification substantielle au logiciel libre et ouvert, conformément à l'article 22, dans le cadre de la fourniture de cette assistance.

Exemple 19: un fournisseur de services aide un client à installer sur son serveur local un logiciel libre et ouvert qui n'est pas publié par lui-même, et ce sans apporter de modification substantielle à ce logiciel libre et ouvert. Le fournisseur de services n'est donc pas considéré comme mettant le logiciel libre et ouvert sur le marché.

3.2.4. *Dons*

60. Les personnes physiques ou morales publiant des projets de logiciels libres et ouverts mettent régulièrement à la disposition des utilisateurs de leurs logiciels des solutions pour verser volontairement des dons financiers afin de remercier le ou les éditeurs du projet ainsi que de garantir l'entretien actif et continu du projet.

61. Comme indiqué au considérant 15 du règlement sur la cyberrésilience, «[l]e fait d'accepter des dons sans intention lucrative ne devrait pas être considéré comme constitutif d'une activité commerciale». Le seul fait d'inclure un lien renvoyant vers une plate-forme de dons ou des outils similaires pour recevoir des dons ne devrait pas être considéré comme constitutif d'une intention lucrative, même lorsque le montant collecté grâce aux dons dépasse les simples coûts associés à la conception, au développement et à la fourniture d'un produit comportant des éléments numériques (ceux-ci pouvant inclure une compensation raisonnable pour les contributeurs engagés par une personne morale et/ou les frais de subsistance raisonnables d'une personne physique). Les dons, de par leur nature même, fluctuent dans le temps et, par conséquent, il convient de faire preuve de souplesse au moment de déterminer si un logiciel libre et ouvert monétisé exclusivement au moyen de dons est considéré comme mis sur le marché. Il est donc peu probable qu'un logiciel libre et ouvert financé uniquement par des dons soit considéré comme mis sur le marché au sens du règlement sur la cyberrésilience.

Exemple 20: une personne physique ou morale publie un outil logiciel libre et ouvert dans un dépôt public en ligne et autorise tout un chacun à le télécharger, à l'utiliser, à le modifier et à le redistribuer sous licence libre et ouverte. Elle invite les utilisateurs à verser volontairement des dons par l'intermédiaire d'une plate-forme de dons afin de soutenir le développement et l'entretien continus du projet. L'accès au logiciel, à son code source et à ses mises à jour n'est pas subordonné au versement d'un don. Ce logiciel libre et ouvert n'est pas considéré comme fourni dans le cadre d'une activité commerciale et ne sera pas considéré comme mis sur le marché au sens du règlement sur la cyberrésilience.

62. Néanmoins, dans certains cas, un logiciel libre et ouvert financé par des dons peut être considéré comme mis sur le marché, par exemple lorsque, sur la base d'une évaluation globale des circonstances, les dons équivalent de facto à la facturation d'un prix pour accéder au produit comportant des éléments numériques ou à certaines de ses fonctionnalités. Tel peut être le cas, notamment, lorsque l'accès au logiciel libre et ouvert, aux fonctionnalités essentielles ou aux mises à jour est subordonné dans la pratique au versement d'un don, ou lorsque les dons donnent droit à des avantages contractuels ou exclusifs qui vont au-delà de ceux que reçoivent les non-donateurs.

Exemple 21: une personne physique ou morale publie un logiciel comportant des éléments numériques sous licence libre et ouverte, mais fournit des versions téléchargeables et des mises à jour de sécurité uniquement aux utilisateurs qui versent un don. Les non-donateurs n'ont pas accès à la dernière version du logiciel.

Dans ce cas, les dons constituent de facto une condition d'accès au produit comportant des éléments numériques et équivalent donc à la facturation d'un prix. Ce logiciel libre et ouvert est donc considéré comme mis sur le marché au sens du règlement sur la cyberrésilience.

Exemple 22: une personne physique ou morale met le code source d'un logiciel libre et ouvert à la disposition du public, mais fournit exclusivement aux donateurs les binaires précompilés, les mises à jour régulières et les correctifs de sécurité garantis. Dans ce cas, les dons sont corrélés à l'accès à des aspects essentiels du produit comportant des éléments numériques et constituent une rémunération de la fourniture de ce produit. Ce logiciel libre et ouvert est donc considéré comme mis sur le marché dans le cadre d'une activité commerciale.

3.2.5. *Financement des logiciels libres et ouverts*

63. Le simple fait qu'un tiers a payé, parrainé ou financé d'une autre manière le développement d'un logiciel libre et ouvert n'est pas en soi un facteur déterminant pour établir si ce logiciel libre et ouvert est mis sur le marché. Dans l'écosystème des logiciels libres et ouverts, il arrive fréquemment que des entreprises, des organismes publics ou d'autres parrains apportent un concours financier à des développeurs agissant individuellement, des fondations ou des communautés pour les inciter à travailler sur des fonctionnalités spécifiques, à corriger des bogues ou à assurer l'entretien de composants critiques. Ce concours financier peut revêtir de nombreuses formes: subventions, primes à la correction de bogues, parrainages, contrats de services ou rémunération des activités de développement, par exemple.

64. Comme déjà rappelé, le considérant 18 du règlement sur la cyberrésilience précise que les seules circonstances dans lesquelles le produit comportant des éléments numériques a été développé ou la manière dont le développement a été financé ne devraient pas être prises en considération au moment de déterminer si l'activité en question est de nature commerciale ou non.

65. Par conséquent, lorsqu'un logiciel libre et ouvert est partagé de manière ouverte et mis à disposition librement de sorte que tout un chacun peut y avoir accès, l'utiliser, le modifier et le redistribuer, le fait qu'une entité commerciale a pu financer le développement du projet ne devrait pas entrer en ligne de compte au moment de déterminer si le logiciel est mis sur le marché. En fait, si ce logiciel libre et ouvert n'est pas monétisé d'une autre façon, il ne doit pas être considéré comme mis sur le marché. Lorsque l'entreprise qui a financé le développement du logiciel libre et ouvert (ainsi que toute autre entreprise) l'intègre dans son produit comportant des éléments numériques, cette entreprise doit faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5, du règlement sur la cyberrésilience.

Exemple 23: un développeur agissant individuellement publie un projet de logiciel libre et ouvert et l'entretient activement. Le fabricant A lui demande d'ajouter une fonctionnalité spécifique à ce logiciel libre et ouvert et finance ce développement. Le développeur ajoute la fonctionnalité à la base de code du logiciel libre et ouvert, qu'il partage de manière ouverte et met à disposition librement de sorte que tout un chacun peut y avoir accès, l'utiliser, le modifier et le redistribuer. Le développeur n'est pas considéré comme ayant mis le logiciel libre et ouvert sur le marché. Si le fabricant intègre le logiciel libre et ouvert dans son produit comportant des éléments numériques, il doit faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5.

3.2.6. *Entités à but non lucratif constituées pour atteindre des objectifs non lucratifs*

66. Lorsqu'une personne morale publiant un logiciel libre et ouvert est une organisation à but non lucratif «constituée de telle façon que tous les bénéfices sont utilisés pour atteindre des objectifs non lucratifs» (considérant 18 du règlement sur la cyberrésilience), le logiciel libre et ouvert qu'elle publie n'est pas considéré comme mis sur le marché. Si cette personne morale répond à la définition d'un «intendant», elle est soumise aux obligations correspondantes (article 24 du règlement sur la cyberrésilience).

Exemple 24: une personne morale publie un navigateur libre et ouvert qui est directement monétisé par l'intermédiaire de partenariats conclus avec des moteurs de recherche, mais tous ses bénéfices sont utilisés pour atteindre des objectifs non lucratifs. Le navigateur n'est pas considéré comme mis sur le marché au sens du règlement sur la cyberrésilience. La personne morale qui le publie est soumise aux obligations applicables aux intendants.

3.2.7. *Intégration par d'autres fabricants*

67. Dans certains cas, les logiciels libres et ouverts sont publiés par une personne physique ou morale clairement identifiable, mais ils sont «destinés à être intégrés par d'autres fabricants à leurs propres produits comportant des éléments numériques». Dans de tels cas, le logiciel libre et ouvert n'est pas considéré comme mis sur le marché de l'Union, sauf s'il est également monétisé par la personne qui le publie (c'est-à-dire le fabricant d'origine), conformément aux sections précédentes des présentes orientations.

68. Lorsque ce logiciel libre et ouvert n'est pas mis sur le marché, la personne morale qui le publie serait soumise aux obligations imposées aux intendants si elle fournit un soutien continu, conformément à la définition d'un «intendant».

Exemple 25: une personne morale publie une bibliothèque de logiciels libres et ouverts pour la conception d'interfaces utilisateur. Elle ne monétise pas la fourniture de cette bibliothèque, mais l'intègre dans l'un de ses produits comportant des éléments numériques (qui est ensuite mis sur le marché). La bibliothèque n'est pas considérée comme mise sur le marché au sens du règlement sur la cyberrésilience, mais elle est destinée à être intégrée dans des produits comportant des éléments numériques. La personne morale qui la publie en est l'intendant.

Exemple 26: une personne morale met un système d'exploitation sur le marché et publie également des bibliothèques de logiciels libres et ouverts pour servir de références de mise en œuvre aux utilisateurs de ce système d'exploitation. La personne morale ne monétise pas les bibliothèques de logiciels libres et ouverts, qui sont destinées à être intégrées dans d'autres produits comportant des éléments numériques. La personne morale qui publie ces bibliothèques de logiciels libres et ouverts en est l'intendant.

3.3. **Intendants de logiciels ouverts**

69. Le règlement sur la cyberrésilience crée une nouvelle catégorie juridique, celle de l'«intendant de logiciels ouverts», compte tenu de «l'importance que revêtent, en matière de cybersécurité, de nombreux produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts qui sont publiés mais ne sont pas mis à disposition sur le marché au sens du [règlement sur la cyberrésilience]» (considérant 19 du règlement).

70. Dans certains cas, un logiciel libre et ouvert est publié mais n'est pas mis à disposition sur le marché au sens du règlement sur la cyberrésilience par une personne morale «qui a pour objectif ou finalité de fournir un soutien systématique et continu au développement de [logiciels libres et ouverts] […] destinés à des activités commerciales, et qui assure la viabilité de ces produits» [article 3, point 14), du règlement sur la cyberrésilience]. Dans de tels cas, cette personne morale est soumise aux obligations imposées aux intendants.

71. Un intendant est défini comme étant «une personne morale, autre que le fabricant», parce qu'un fabricant, par définition, est une personne physique ou morale qui met des produits comportant des éléments numériques sur le marché («les commercialise») sous son propre nom ou sa propre marque. Une personne morale ne peut être un intendant que pour des produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts qui sont publiés mais ne sont pas mis à disposition sur le marché au sens du règlement sur la cyberrésilience. La notion d'«intendant» s'applique donc à des cas spécifiques de logiciels libres et ouverts «dont la finalité est commerciale, par exemple ceux qui sont destinés à être intégrés à des services commerciaux ou à des produits comportant des éléments numériques monétisés» (considérant 19 du règlement sur la cyberrésilience ([13])), mais qui ne sont pas mis à disposition sur le marché au sens du règlement sur la cyberrésilience, et pour lesquels la personne morale publiant le logiciel libre et ouvert fournit un soutien systématique.

72. Le fait qu'une personne morale est l'intendant d'un logiciel libre et ouvert spécifique ne signifie pas nécessairement qu'elle est également l'intendant des autres logiciels libres et ouverts qu'elle publie. De même, le fait qu'une personne morale est le fabricant d'un logiciel libre et ouvert spécifique ne signifie pas qu'elle ne peut pas être l'intendant d'autres logiciels libres et ouverts, et ce même si elle fournit des versions «communautaires» de ce même logiciel libre et ouvert, comme expliqué à la section *3.2.1 Facturation d'un prix*.

73. Une personne morale peut donc être simultanément l'intendant d'un logiciel libre et ouvert spécifique (fournissant un soutien systématique et continu et assurant la viabilité du logiciel) et le fabricant d'un autre logiciel libre et ouvert spécifique (qu'elle met sur le marché). Autrement dit, une même entité juridique peut être chargée de rôles différents pour différents projets de logiciels libres et ouverts.

74. Pour chaque logiciel libre et ouvert spécifique qu'elle publie, la personne morale devra vérifier si ce logiciel libre et ouvert est considéré comme mis sur le marché au sens du règlement sur la cyberrésilience. Dans l'affirmative, elle sera le fabricant du logiciel. Si le logiciel libre et ouvert n'est pas considéré comme mis sur le marché, la personne morale peut en être l'intendant, si le logiciel est destiné à des activités commerciales et si la personne morale fournit un soutien conformément à la définition d'un «intendant» ([14]).

3.3.1. *Soutien continu et garantie de la viabilité du logiciel libre et ouvert*

75. Le considérant 19 explique que le fait d'apporter un soutien prolongé au développement d'un produit comportant des éléments numériques peut comprendre (sans s'y limiter): i) l'hébergement et la gestion de plateformes collaboratives de développement de logiciels; ii) l'hébergement de code source ou d'un logiciel; iii) l'administration ou la gestion de produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts; et iv) le pilotage du développement de ces produits comportant des éléments numériques.

76. Tel peut être le cas, par exemple, d'une entité juridique qui développe un logiciel libre et ouvert en vue de l'intégrer dans ses propres produits comportant des éléments numériques et qui le publie ensuite sans le mettre sur le marché. Cette question est également examinée à la section *3.2.7 Intégration par d'autres fabricants*. Dans ce cas, l'entité juridique n'est pas le fabricant du logiciel, mais peut en être l'intendant. En outre, comme expliqué également dans les sections précédentes, une entité juridique qui publie une version gratuite (ou communautaire) et une version monétisée d'un même logiciel libre et ouvert est considérée comme l'intendant de la version gratuite (ou communautaire) et comme le fabricant de la version monétisée.

77. De même, une entité juridique qui monétise un logiciel libre et ouvert mais qui est une entité à but non lucratif dont les bénéfices sont utilisés pour atteindre des objectifs non lucratifs (et, par conséquent, son logiciel libre et ouvert n'est pas mis sur le marché au sens du règlement sur la cyberrésilience, comme expliqué à la section *3.2.6 Entités à but non lucratif*) est l'intendant du logiciel libre et ouvert qu'elle publie.

78. Par ailleurs, certaines fondations proposent des plateformes collaboratives régies par différentes formes de gouvernance qui permettent aux fabricants de contribuer régulièrement au développement de logiciels libres et ouverts et/ou qui sont régulièrement financées par les fabricants. Ces fondations doivent être considérées comme les intendants des logiciels libres et ouverts spécifiques qui sont destinés à des activités commerciales et pour lesquels la fondation fournit un soutien continu. Toutefois, comme expliqué à la section *3.3 Intendants de logiciels ouverts*, une telle fondation peut ne pas être soumise aux obligations prévues par le règlement sur la cyberrésilience dans le cas des autres logiciels libres et ouverts spécifiques qu'elle héberge dès lors qu'elle ne fournit pas de soutien systématique au développement d'un logiciel libre et ouvert spécifique, qu'elle n'assure pas la viabilité d'un tel logiciel et/ou que ce logiciel spécifique n'est pas destiné à des activités commerciales.

([13]) Cette notion est aussi couverte par l'expression «destinés à des activités commerciales» incluse dans la définition d'un «intendant de logiciels ouverts» figurant à l'article 3, point 14), du règlement sur la cyberrésilience.

([14]) De plus, la personne morale peut ne pas être soumise aux obligations prévues par le règlement sur la cyberrésilience dans les cas suivants: i) un logiciel libre et ouvert spécifique n'est pas mis sur le marché au sens du règlement sur la cyberrésilience; et ii) l'entité juridique ne répond pas à la définition d'un «intendant» en ce qui concerne ce logiciel libre et ouvert spécifique.

79. Le type de «soutien continu» que les fondations et organisations similaires fournissent au développement de projets de logiciels libres et ouverts spécifiques peut varier considérablement. Par exemple, certaines entités juridiques ne fournissent qu'un soutien non technique, comme la gestion de l'image de marque des projets, l'établissement des règles de gouvernance, l'organisation d'événements communautaires ou la collecte de dons. D'autres entités fournissent également l'infrastructure informatique sous-jacente nécessaire à la gestion du projet, comme l'hébergement de dépôts de code source, la fourniture de systèmes de contrôle des versions ou la génération de clés de signature. D'autres encore fournissent un soutien plus poussé en allouant activement des moyens d'ingénierie au projet, par exemple en y affectant des développeurs, en coordonnant les travaux de développement, en procédant à des contrôles ou à des fusions de code, en gérant les déploiements ou en traitant les signalements de vulnérabilités et les correctifs de sécurité. Si toutes les entités juridiques qui sont considérées comme des intendants au sens du règlement sur la cyberrésilience sont tenues de se conformer aux obligations énoncées à l'article 24, paragraphes 1 et 2, la mesure dans laquelle les obligations énoncées à l'article 14, paragraphes 1, 3 et 8, s'appliquent à ces entités juridiques varie en fonction du type de soutien qu'elles fournissent, conformément à l'article 24, paragraphe 3.

80. Par exemple, un intendant qui ne fournit qu'un soutien non technique ne participe pas, par définition, au développement du produit comportant des éléments numériques et n'est donc pas tenu de signaler les vulnérabilités activement exploitées. Cet intendant ne fournit pas non plus de réseau ou de systèmes d'information pour le développement de ces produits comportant des éléments numériques et n'est donc pas tenu de signaler les incidents graves à l'ENISA et aux CSIRT ou aux utilisateurs touchés. Néanmoins, lorsque l'intendant prend connaissance d'une vulnérabilité activement exploitée (par exemple, au moyen d'un signalement émanant de sources externes, telles que des auteurs de recherches en matière de sécurité), il devrait partager cette information avec les responsables de l'entretien du produit comportant des éléments numériques, conformément à sa politique de cybersécurité. Les responsables de l'entretien des produits comportant des éléments numériques et/ou les intendants devraient également envisager de signaler la vulnérabilité de manière volontaire, conformément à l'article 15.

81. En revanche, lorsque l'intendant fournit l'infrastructure informatique sous-jacente pour certains produits comportant des éléments numériques, il est tenu, conformément à l'article 14, paragraphe 3, de notifier à l'ENISA et aux CSIRT tout incident grave lié à cette infrastructure qui a des répercussions sur la sécurité des produits comportant des éléments numériques. Il doit également, le cas échéant, informer tous les utilisateurs (par exemple au moyen d'une annonce générale). Comme indiqué au point précédent, bien que l'intendant ne soit pas tenu de signaler les vulnérabilités activement exploitées dont il prend connaissance, il devrait favoriser la bonne gestion des vulnérabilités et envisager un signalement volontaire conformément à l'article 15.

82. Enfin, lorsque l'intendant alloue également des ressources d'ingénierie à des produits spécifiques comportant des éléments numériques, il a pour obligation: i) de notifier, conformément à l'article 14, paragraphe 1, les vulnérabilités activement exploitées dont il prend connaissance; et ii) le cas échéant, d'informer tous les utilisateurs. Dans la mesure où l'intendant a également une relation directe avec les utilisateurs touchés, il est également tenu de les informer directement, conformément à l'article 14, paragraphe 8.

83. Lorsqu'une entité cesse de fournir un soutien systématique et continu au développement d'un logiciel libre et ouvert spécifique, il se peut qu'elle ne réponde plus à la définition d'un «intendant» et ne soit donc plus soumise aux obligations correspondantes. Dans un tel cas, cette entité est encouragée à communiquer clairement son changement de statut pour ce logiciel libre et ouvert spécifique.

84. Dans certaines situations, une entité qui était l'intendant d'un projet spécifique peut décider de monétiser directement ce projet, mettant ainsi le produit comportant des éléments numériques sur le marché et déclenchant l'applicabilité des obligations imposées aux fabricants par le règlement sur la cyberrésilience. Dès lors, cette entité sera considérée comme le fabricant du produit comportant des éléments numériques à compter de la date à laquelle elle le met sur le marché (mais pas en ce qui concerne les versions antérieures pour lesquelles elle a agi en tant qu'intendant).

3.4. **Contributeurs et utilisations en aval**

85. Comme déjà indiqué à la section *3.1 Conditions dans lesquelles un logiciel libre et ouvert relève de la responsabilité d'une personne physique ou morale*, le règlement sur la cyberrésilience précise qu'il ne s'applique pas «aux personnes physiques ou morales qui contribuent, sous forme de code source, à des produits comportant des éléments numériques qui répondent aux critères de logiciels libres et ouverts ne relevant pas de leur responsabilité» (considérant 18).

86. Les fabricants de produits comportant des éléments numériques qui intègrent des composants logiciels libres et ouverts dans leurs propres produits comportant des éléments numériques ne deviennent pas non plus responsables de la conformité individuelle de ces composants avec le règlement sur la cyberrésilience, même lorsqu'ils contribuent sous forme de code source à leur entretien.

87. De même, le simple fait qu'un fabricant intègre des composants logiciels libres et ouverts dans ses propres produits (monétisés) comportant des éléments numériques n'a aucune incidence sur le statut de ces composants logiciels libres et ouverts au titre du règlement sur la cyberrésilience. Les responsables de l'entretien de composants logiciels libres et ouverts qui ne sont pas mis sur le marché n'ont aucune obligation à l'égard des autres entités susceptibles d'intégrer ces composants dans leurs produits comportant des éléments numériques. L'applicabilité du règlement sur la cyberrésilience à un composant logiciel libre et ouvert donné dépend uniquement du point de savoir si la personne physique ou morale qui le publie le met sur le marché.

88. Néanmoins, les fabricants de produits comportant des éléments numériques qui intègrent des composants logiciels libres et ouverts sont tenus de se conformer au règlement sur la cyberrésilience pour leurs propres produits comportant des éléments numériques. Ils ont également une obligation de diligence raisonnable, conformément à l'article 13, paragraphe 5, en ce qui concerne les composants logiciels libres et ouverts qu'ils intègrent. En outre, ils sont tenus de signaler les vulnérabilités des composants intégrés et de partager les correctifs de sécurité, conformément à l'article 13, paragraphe 6. Pour de plus amples orientations à ce sujet, voir section *9.2.1 Signalement en amont et partage des correctifs de sécurité*.

3.5. **Scénarios illustratifs**

89. Les exemples énumérés ci-dessous sont purement hypothétiques et ne visent qu'à illustrer les différents cas de figure exposés ci-dessus.

Exemple 27: le développeur A, agissant individuellement, a développé un logiciel libre et ouvert. Il publie ce logiciel libre et ouvert sous son propre nom ou sa propre marque, mais ne facture pas de prix pour son utilisation. Le logiciel est partagé de manière ouverte et mis à disposition librement de sorte que tout un chacun peut y avoir accès, l'utiliser, le modifier et le redistribuer. Le développeur A inclut également un lien renvoyant vers une plate-forme de collecte de dons volontaires.

Les sociétés B, C et D intègrent ce logiciel libre et ouvert dans leurs propres produits comportant des éléments numériques. Afin de soutenir l'entretien continu, les sociétés B, C et D versent des dons volontaires au développeur A. Ces dons permettent à celui-ci d'œuvrer activement à l'entretien du projet.

Le logiciel libre et ouvert n'est pas mis sur le marché au sens du règlement sur la cyberrésilience. Le développeur A n'est pas soumis aux obligations prévues par le règlement sur la cyberrésilience. Les sociétés B, C et D doivent faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5, lorsqu'elles intègrent ce logiciel libre et ouvert dans leurs propres produits comportant des éléments numériques.

Exemple 28: la fondation à but non lucratif F publie un composant logiciel libre et ouvert destiné à être intégré dans d'autres produits commerciaux comportant des éléments numériques. Elle s'engage à fournir un soutien continu au développement de ce logiciel libre et ouvert, afin d'assurer sa viabilité et son adoption. Les sociétés A, B et C intègrent ce logiciel libre et ouvert dans leurs propres produits comportant des éléments numériques. Les sociétés A et B allouent volontairement une partie du temps de travail de leurs développeurs au développement et à l'entretien de projets de logiciels libres et ouverts au sein de la fondation F, y compris pour ce logiciel libre et ouvert.

Étant donné que la fondation F est une entité à but non lucratif constituée de telle façon que ses bénéfices sont utilisés pour atteindre des objectifs non lucratifs, le logiciel libre et ouvert n'est pas considéré comme mis sur le marché au sens du règlement sur la cyberrésilience. La fondation F est l'intendant du logiciel libre et ouvert et est soumise aux obligations correspondantes énoncées à l'article 24. Les sociétés A, B et C doivent faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5, lorsqu'elles intègrent ce logiciel libre et ouvert dans leurs propres produits comportant des éléments numériques.

Exemple 29: la société A a développé un composant logiciel libre et ouvert destiné à être intégré dans ses propres produits comportant des éléments numériques. Elle publie également ce logiciel libre et ouvert séparément sous son propre nom ou sa propre marque et l'entretient activement. Toutefois, elle ne facture pas son utilisation et ne le monétise d'aucune autre manière. Les sociétés B, C et D intègrent ce logiciel libre et ouvert dans leurs propres produits comportant des éléments numériques et allouent volontairement une partie du temps de travail de leurs développeurs à son entretien.

Le logiciel libre et ouvert n'est pas considéré comme mis sur le marché au sens du règlement sur la cyberrésilience. La société A n'est pas son fabricant, mais son intendant. Les sociétés B, C et D doivent faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5, lorsqu'elles intègrent le logiciel libre et ouvert dans leurs propres produits comportant des éléments numériques.

Exemple 30: la société A publie un logiciel libre et ouvert sous son propre nom ou sa propre marque et en propose une version payante donnant droit à certains avantages, tels que la fourniture d'une assistance technique ou l'optimisation des performances. Des développeurs des sociétés B, C et D contribuent à l'entretien du logiciel libre et ouvert, mais celui-ci reste sous le contrôle de la société A.

La société A est considérée comme le fabricant de ce logiciel libre et ouvert ([15]). Les sociétés B, C et D ne sont pas soumises aux obligations prévues par le règlement sur la cyberrésilience pour ce logiciel libre et ouvert spécifique. Si elles intègrent ce logiciel libre et ouvert dans leurs propres produits comportant des éléments numériques, elles sont tenues de faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5.

Exemple 31: la société A publie un logiciel libre et ouvert sous son propre nom ou sa propre marque et fournit un entretien continu pour assurer sa viabilité à long terme, afin de permettre l'intégration de ce logiciel dans les produits comportant des éléments numériques d'autres entreprises. La société A ne facture pas son utilisation, ne traite pas les données à caractère personnel qu'elle collecte au moyen du produit comportant des éléments numériques et ne vend pas de services d'assistance associés à la publication du logiciel libre et ouvert.

La société B contribue sous forme de code à l'entretien du logiciel libre et ouvert et y alloue une partie du temps de travail de ses développeurs, mais elle ne le distribue pas commercialement. Elle propose des services d'assistance technique indépendamment de la distribution du logiciel libre et ouvert. La société A est considérée comme l'intendant de ce logiciel libre et ouvert, tandis que la société B n'est pas soumise aux obligations prévues par le règlement sur la cyberrésilience pour ce logiciel libre et ouvert.

Exemple 32: un composant logiciel libre et ouvert est publié par une entité à but non lucratif constituée de telle façon que tous les bénéfices sont utilisés pour atteindre des objectifs non lucratifs. Cette entité fournit un soutien continu pour assurer la viabilité à long terme du projet. L'entretien est financé par des fonds publics, tels que des subventions à la recherche. Les autres activités de développement, y compris le développement de nouvelles fonctionnalités, sont financées par des dons et dans le cadre de projets spécifiques menés en partenariat avec des fabricants qui intègrent ce logiciel libre et ouvert dans leurs produits comportant des éléments numériques. Ces fonctionnalités sont intégrées dans la base de code du logiciel libre et ouvert.

L'entité à but non lucratif qui publie le logiciel libre et ouvert est considérée comme l'intendant de ce composant logiciel libre et ouvert. Un fabricant qui a contribué au développement de certaines fonctionnalités ne devient pas le fabricant de ce composant logiciel libre et ouvert. Lorsque le fabricant intègre ce composant logiciel libre et ouvert dans son propre produit comportant des éléments numériques, il doit faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5.

Exemple 33: une entité à but non lucratif constituée de telle façon que tous les bénéfices sont utilisés pour atteindre des objectifs non lucratifs publie un kit de développement logiciel (SDK) libre et ouvert et assure son entretien continu. Le SDK est partagé de manière ouverte et mis à disposition librement de sorte que tout un chacun peut y avoir accès, l'utiliser, le modifier et le redistribuer. Le financement est assuré par des cotisations versées à l'entité à but non lucratif et des développeurs employés par les organisations membres contribuent au développement du SDK sous forme de code et par d'autres moyens. Les fabricants utilisent le SDK comme composant pour concevoir d'autres produits comportant des éléments numériques.

L'entité à but non lucratif qui publie le SDK en est l'intendant. Les membres de la fondation ne sont pas responsables de la conformité du SDK avec le règlement sur la cyberrésilience. Lorsque les fabricants utilisent le SDK pour concevoir leur propre produit comportant des éléments numériques, ils doivent faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5.

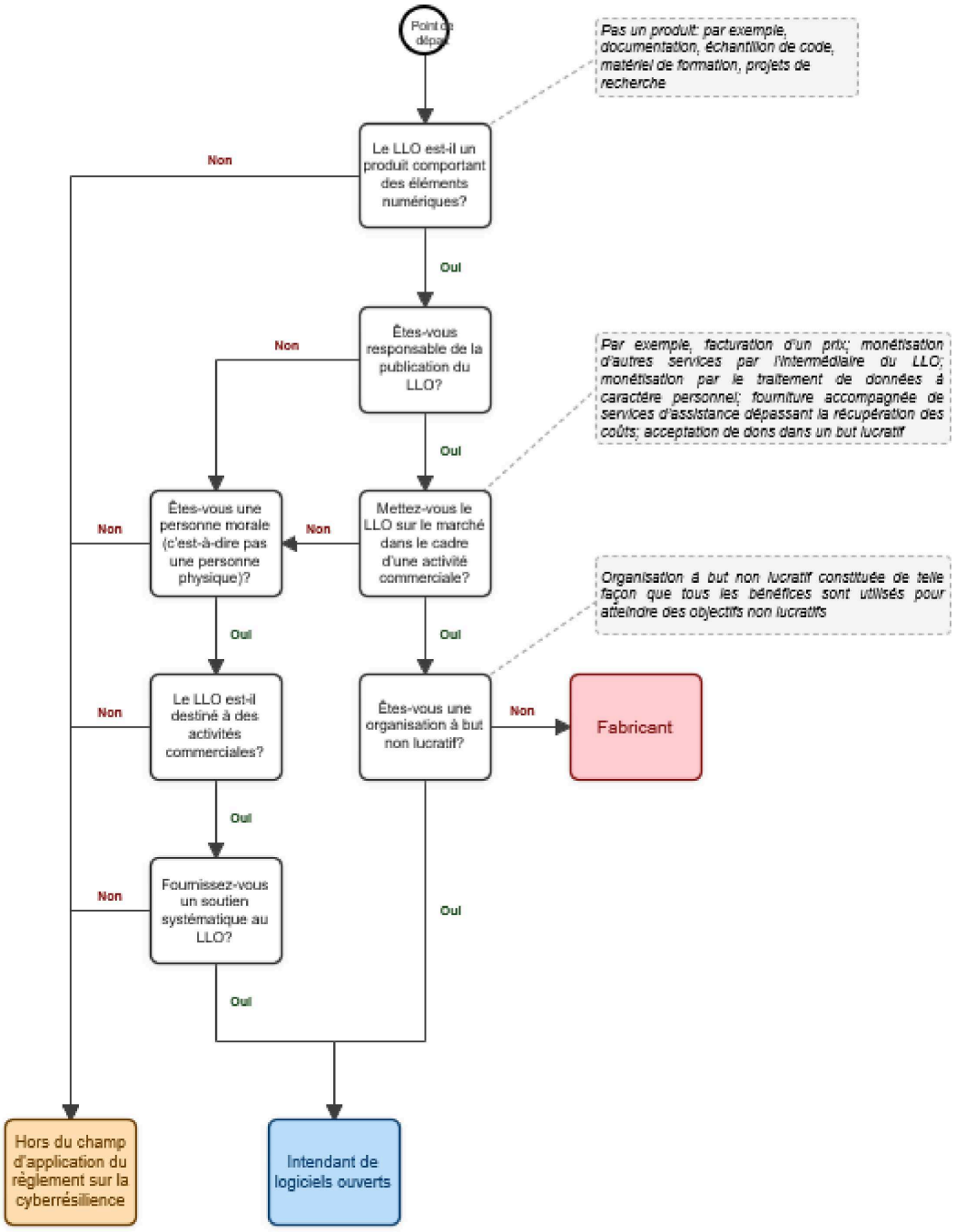
Exemple 34: un développeur agissant individuellement publie une bibliothèque de logiciels libres et ouverts dans un dépôt de paquets public pour un langage de programmation donné et l'entretient activement. Dans la documentation des paquets, le développeur ajoute un lien pour la collecte de dons. Un fabricant télécharge gratuitement cette bibliothèque à partir du dépôt et l'intègre dans son propre produit comportant des éléments numériques.

Le développeur et le dépôt de paquets ne sont pas soumis aux obligations prévues par le règlement sur la cyberrésilience. Le fabricant qui intègre la bibliothèque doit faire preuve de diligence raisonnable conformément à l'article 13, paragraphe 5.

([15]) À moins que la société A ne soit une entité à but non lucratif constituée de telle façon que tous les bénéfices sont utilisés pour atteindre des objectifs non lucratifs, auquel cas elle serait l'intendant de ce logiciel libre et ouvert.

Illustration 1

Diagramme de flux montrant dans quels cas un logiciel libre et ouvert (LLO) est couvert par le règlement sur la cyberrésilience



4. MODIFICATIONS SUBSTANTIELLES ET PIÈCES DE RECHANGE

90. L'article 3, point 30), du règlement sur la cyberrésilience définit une «modification substantielle» comme étant une modification apportée au produit comportant des éléments numériques à la suite de sa mise sur le marché i) qui a une incidence sur la conformité du produit comportant des éléments numériques aux exigences essentielles énoncées à l'annexe I, partie I; ou ii) qui entraîne une modification de l'utilisation prévue pour laquelle le produit comportant des éléments numériques a été évalué.

91. La notion de «modification substantielle» est pertinente pour déterminer si les obligations du règlement sur la cyberrésilience s'appliquent dans certains cas de figure. Ainsi:

a) en vertu de l'article 21, un importateur ou un distributeur qui apporte une modification substantielle à un produit comportant des éléments numériques déjà mis sur le marché est considéré comme étant son fabricant;

b) en vertu de l'article 22, toute personne physique ou morale qui apporte une modification substantielle à un produit comportant des éléments numériques et met ce produit à disposition sur le marché est considérée comme étant son fabricant;

c) en vertu de l'article 69, paragraphe 2, toute personne physique ou morale qui, après le 11 décembre 2027, apporte une modification substantielle à un produit comportant des éléments numériques mis sur le marché avant le 11 décembre 2027 et met ce produit sur le marché est considérée comme étant son fabricant;

d) pour les fabricants de produits comportant des éléments numériques mis sur le marché après le 11 décembre 2027, cette notion est pertinente pour déterminer si un produit comportant des éléments numériques doit faire l'objet d'une nouvelle procédure d'évaluation de la conformité en raison des modifications apportées après cette date, compte tenu notamment de la nature itérative du développement de logiciels.

92. Par conséquent, il importe de fournir des orientations pour aider les opérateurs économiques à comprendre quand des modifications apportées à des produits matériels ou logiciels constituent des modifications substantielles.

4.1. **Réparations physiques**

93. Comme indiqué au considérant 42 du règlement sur la cyberrésilience, «[l]orsqu'un produit comportant des éléments numériques fait l'objet d'une "remise à neuf", d'un "entretien" et d'une "réparation", au sens de l'article 2, points 18), 19) et 20), du règlement (UE) 2024/1781 du Parlement européen et du Conseil, cela n'entraîne pas nécessairement une modification substantielle du produit, par exemple si l'utilisation et les fonctionnalités prévues ne sont pas modifiées et que le niveau de risque demeure inchangé. Toutefois, la mise à niveau d'un produit comportant des éléments numériques par le fabricant pourrait entraîner des modifications dans la conception et le développement de ce produit et donc avoir une incidence sur son utilisation prévue et sa conformité aux exigences énoncées dans le présent règlement». Ces précisions sont conformes au point 2.1 du guide bleu, qui rappelle qu'«[u]n produit ayant fait l'objet de modifications ou de transformations importantes après sa mise en service doit être considéré comme un nouveau produit si: i) sa performance, sa destination ou son type d'origine sont modifiés, sans que cela soit prévu dans l'évaluation initiale des risques; ii) la nature du danger a changé ou le niveau de risque a augmenté par rapport à la législation d'harmonisation de l'Union concernée; iii) le produit est mis à disposition (ou mis en service si la législation applicable inclut également la mise en service dans son champ d'application). Il convient alors de procéder à une évaluation au cas par cas et, plus particulièrement, en fonction de l'objet de la législation et du type de produits couverts par la législation concernée».

94. Les opérations de remise à neuf, d'entretien ou de réparation qui entraînent la modification physique de produits comportant des éléments numériques déjà mis sur le marché ne constituent pas nécessairement des modifications substantielles. Il convient donc de procéder à une évaluation au cas par cas afin de déterminer si la modification physique a une incidence sur la conformité du produit comportant des éléments numériques avec les exigences essentielles énoncées à l'annexe I, partie I, ou entraîne une modification de l'utilisation prévue du produit couverte par l'évaluation des risques de cybersécurité.

95. Le remplacement de pièces défectueuses ou d'éléments usés par des pièces plus performantes (par exemple, en raison du progrès technique ou parce que l'ancienne pièce n'est plus produite) ne constitue pas en soi une modification substantielle du produit comportant des éléments numériques qui est ainsi réparé. Il y a modification substantielle uniquement si les nouvelles performances ou le mode de fonctionnement du produit comportant des éléments numériques une fois réparé i) ont une incidence sur sa conformité avec les exigences essentielles ou ii) entraînent une modification de l'utilisation prévue qui n'était pas couverte par l'évaluation des risques.

Exemple 35: le fabricant d'un serveur informatique effectue une opération de réparation, en remplaçant une mémoire RAM défectueuse par une nouvelle mémoire RAM, plus performante. Ce remplacement n'a pas d'incidence sur la conformité du serveur avec les exigences essentielles. Le serveur est plus performant, mais ses nouvelles performances restent conformes à l'utilisation prévue du serveur telle qu'envisagée dans l'évaluation des risques de cybersécurité. Le serveur informatique n'est pas considéré comme substantiellement modifié.

4.2. **Pièces de rechange**

96. En vertu de l'article 2, paragraphe 6, du règlement sur la cyberrésilience, les pièces de rechange destinées à remplacer des composants identiques et fabriquées conformément aux mêmes spécifications que ces composants ne sont pas soumises au règlement. Le considérant 29 indique en outre que cette dérogation concerne à la fois les pièces de rechange pour les produits comportant des éléments numériques mis à disposition avant l'entrée en application du règlement sur la cyberrésilience et les pièces de rechange qui ont déjà fait l'objet d'une procédure d'évaluation de la conformité en application du règlement.

97. La dérogation prévue à l'article 2, paragraphe 6, du règlement sur la cyberrésilience devrait être interprétée comme s'appliquant uniquement lorsque la pièce de rechange est spécifiquement fournie pour réparer un produit comportant des éléments numériques déjà mis sur le marché (avant ou après le 11 décembre 2027) ou en prolonger la durabilité. Lorsqu'un produit comportant des éléments numériques est fourni en tant que produit autonome, sans aucun lien avec l'entretien ou la réparation d'un produit comportant des éléments numériques préexistant, il est mis sur le marché au sens du règlement sur la cyberrésilience et ne devrait pas être considéré comme une pièce de rechange couverte par l'article 2, paragraphe 6. La finalité de l'opération d'entretien ou de réparation devrait ressortir du contexte de la fourniture, par exemple lorsque le produit comportant des éléments numériques ou la famille de produits est précisé dans le bon de commande ou l'offre commerciale, ou lorsque l'opération est fournie via des canaux de services après-vente ou d'entretien. Les preuves à cet effet devraient également être tenues à la disposition des autorités de surveillance du marché. Le fait qu'un produit comportant des éléments numériques puisse techniquement être utilisé pour remplacer un composant n'est pas, en soi, suffisant pour que ce produit bénéficie de la dérogation en l'absence des preuves concernées.

98. Par conséquent, lorsqu'une pièce de rechange est identique à un composant déjà inclus dans un produit comportant des éléments numériques qui a été mis sur le marché avant la date d'application du règlement sur la cyberrésilience, ou qui a été mis sur le marché en application de ce règlement, cette pièce de rechange n'est pas elle-même soumise au règlement sur la cyberrésilience.

99. Afin de déterminer si une pièce de rechange devrait être considérée comme identique à un composant, il convient de se concentrer sur son rôle fonctionnel dans le produit comportant des éléments numériques et sur les caractéristiques qui peuvent être pertinentes pour la cybersécurité. Bien qu'une évaluation au cas par cas soit toujours nécessaire, les différences qui n'ont pas d'incidence sur les caractéristiques de sécurité ou le profil de risque de cybersécurité du composant n'empêchent pas, en soi, cette pièce de rechange de relever du champ d'application de l'article 2, paragraphe 6, du règlement sur la cyberrésilience.

100. En revanche, les différences ayant trait à des caractéristiques pertinentes pour la cybersécurité du composant, telles que les algorithmes, les protocoles, les mécanismes de chiffrement, les fonctionnalités de contrôle des accès ou d'autres caractéristiques pertinentes pour la sécurité, peuvent signifier que la nouvelle pièce ne peut pas être considérée comme identique au composant qu'elle est destinée à remplacer.

101. Lorsqu'une pièce de rechange n'est pas identique au composant d'origine, elle constitue un produit comportant des éléments numériques à part entière et est donc soumise au règlement sur la cyberrésilience. Dans un tel cas, la conformité avec les exigences essentielles doit être évaluée à la lumière de l'utilisation prévue du composant de remplacement. Ainsi, si le composant de remplacement a pour fonction d'assurer la compatibilité ou l'interopérabilité avec un produit comportant des éléments numériques existant, y compris lorsque ce produit comportant des éléments numériques a été mis sur le marché avant l'entrée en application du règlement sur la cyberrésilience, cela revêt une importance particulière. Lorsque certaines exigences essentielles ne peuvent raisonnablement pas être respectées en raison de cette utilisation prévue ou de contraintes techniques, le fabricant doit en tenir compte dans l'évaluation des risques de cybersécurité et mettre en œuvre des mesures alternatives ou compensatoires appropriées d'atténuation des risques, afin de ne pas compromettre la sécurité du produit comportant des éléments numériques. Comme également expliqué à la section *2.6 Systèmes complexes*, tant la documentation technique que les informations et instructions destinées à l'utilisateur jouent un rôle essentiel dans la description transparente des contraintes détectées, des risques de cybersécurité y afférents et des mesures d'atténuation des risques mises en œuvre. Comme expliqué à la section *4.1 Réparations physiques*, le remplacement de pièces défectueuses ou d'éléments usés par des pièces plus performantes ne constitue pas en soi une modification substantielle du produit comportant des éléments numériques qui est ainsi réparé.

Exemple 36: un fabricant a mis des unités de contrôle connectées sur le marché de l'Union, dans un cas en 2026, avant la date d'application du règlement sur la cyberrésilience, et dans un autre cas en 2028, en application du règlement sur la cyberrésilience. En 2028, un module de communication numérique inclus dans les deux types d'unités de contrôle devient défectueux. Le fabricant fournit comme pièce de rechange un module de remplacement qui est identique au module d'origine et fabriqué conformément aux mêmes spécifications.

Dans les deux cas, le module de remplacement relève de la dérogation prévue à l'article 2, paragraphe 6. La pièce de rechange n'est pas elle-même soumise au règlement sur la cyberrésilience, même s'il s'agit d'un produit comportant des éléments numériques, car elle remplace un composant identique dans un produit comportant des éléments numériques. La réparation ne constitue pas une modification substantielle du produit comportant des éléments numériques.

Exemple 37: un fabricant a mis un système de commande industriel connecté sur le marché de l'Union en 2026, avant la date d'application du règlement sur la cyberrésilience. En 2028, une puce de communication incluse dans ce système de commande devient défectueuse. Étant donné que le fabricant ne fabrique plus cette puce, afin d'assurer la compatibilité et la continuité de fonctionnement, il fournit comme pièce de rechange une puce plus récente à la fonctionnalité équivalente, mais mettant en œuvre une solution de chiffrement différente et dotée d'un mécanisme de démarrage sécurisé mis à jour.

Dans ce cas, la puce de remplacement ne peut pas être considérée comme identique, étant donné que les différences ayant trait à la solution de chiffrement et au mécanisme de démarrage sécurisé ont une incidence sur les propriétés de cybersécurité de la puce. Elle ne bénéficie donc pas de la dérogation prévue à l'article 2, paragraphe 6, et constitue un produit comportant des éléments numériques soumis au règlement sur la cyberrésilience. La conformité de la pièce de remplacement doit être évaluée à la lumière de son utilisation prévue, y compris de son rôle dans la garantie de l'interopérabilité avec le produit comportant des éléments numériques mis sur le marché avant l'entrée en application du règlement sur la cyberrésilience.

Exemple 38: en 2028, un fabricant met sur le marché une unité de contrôle domotique intelligente conformément au règlement sur la cyberrésilience. En 2029, le module sans fil de cette unité de contrôle devient défectueux. Étant donné que le fabricant ne fabrique plus ce module, il fournit comme pièce de rechange un nouveau module qui remplit la même fonction en utilisant les mêmes protocoles de communication et mécanismes de sécurité, mais qui repose sur un jeu de puces différent et intègre un micrologiciel mis à jour, sans que cela ait d'incidence sur des caractéristiques susceptibles d'être pertinentes pour la cybersécurité.

Dans ce cas, le module de remplacement peut être considéré comme identique. Il bénéficie donc de la dérogation prévue à l'article 2, paragraphe 6, et n'est pas soumis au règlement sur la cyberrésilience.

102. La dérogation pour les pièces de rechange s'applique que la pièce de rechange remplace un composant d'un produit comportant des éléments numériques ou remplace un produit comportant des éléments numériques complet qui fait lui-même partie d'un produit plus grand, y compris lorsque ce plus grand produit comportant des éléments numériques est constitué de plusieurs composants intégrés, à condition que la pièce de remplacement soit spécifiquement fournie en tant que pièce de rechange, comme expliqué aux points précédents.

Exemple 39: en 2027, un fabricant met sur le marché un système d'automatisation industrielle dont l'un des composants est une unité de programmation logique. En 2031, l'unité centrale de traitement de l'unité de programmation logique devient défectueuse. Le fabricant propose deux possibilités de réparation: i) la fourniture d'une unité centrale de traitement de remplacement, qui peut être considérée comme identique à l'unité centrale de traitement d'origine; ou ii) la fourniture d'une unité de programmation logique de remplacement complète, qui peut être considérée comme identique à l'unité de programmation logique d'origine. Dans chaque cas, la pièce de remplacement est fournie par le canal de services après-vente du fabricant en tant que pièce de rechange et le système d'automatisation industrielle auquel le remplacement est destiné est indiqué clairement. Dans les deux cas, le remplacement relève de la dérogation prévue à l'article 2, paragraphe 6, qu'il concerne un composant de l'unité de programmation logique ou l'unité de programmation logique dans son ensemble.

4.3. **Les mises à jour logicielles en tant que modifications substantielles**

103. Le développement de logiciels est de nature itérative, les logiciels comportant des éléments numériques déjà mis sur le marché étant mis à jour fréquemment et de manière continue. Dans ce contexte, il est utile de fournir des orientations supplémentaires permettant de déterminer dans quels cas un logiciel doit être considéré comme substantiellement modifié. Ces orientations visent notamment à aider les fabricants de logiciels comportant des éléments numériques qui apportent des modifications à leurs propres produits à déterminer si ces modifications constituent une modification substantielle.

104. Le considérant 39 indique qu'un produit comportant des éléments numériques est substantiellement modifié lorsqu'une modification altère le niveau de risque de cybersécurité et que le niveau de risque ainsi altéré ou le risque supplémentaire n'a pas été envisagé par le fabricant dans son évaluation des risques et, par voie de conséquence, dans sa mise en œuvre des exigences essentielles. Un fabricant devrait donc évaluer, au cas par cas, si une mise à jour logicielle crée de nouveaux risques de cybersécurité ou exacerbe les risques de cybersécurité existants, et si ces risques ont déjà été envisagés dans son évaluation des risques.

105. Lorsqu'un fabricant introduit de nouvelles fonctionnalités dans un produit comportant des éléments numériques qui entraînent une modification de l'utilisation prévue du produit dans son ensemble, cette modification n'aura vraisemblablement pas été envisagée dans son évaluation des risques. Dans un tel cas, la modification serait généralement considérée comme une modification substantielle.

Exemple 40: un fabricant met sur le marché un tableau de bord qui collecte des données provenant de machines et affiche des tendances et des alertes, mais qui ne permet pas de contrôler ces machines. Il développe ensuite une nouvelle version de ce tableau de bord, dans laquelle il introduit des fonctionnalités qui permettent de contrôler les machines, notamment en ajustant les paramètres de fonctionnement et en redémarrant les machines en cas de défaillance. À la suite de cette modification, l'utilisation prévue du tableau de bord a évolué au-delà de ce qui était envisagé dans l'évaluation des risques: il ne s'agit plus simplement d'un outil d'information, mais d'un produit comportant des éléments numériques destiné à exercer un contrôle opérationnel sur d'autres appareils. Le tableau de bord a donc été substantiellement modifié.

Exemple 41: un fabricant met sur le marché une application logicielle grand public destinée à organiser et afficher des données à caractère personnel – telles que des courriers électroniques, des messages ou des documents – et à prendre en charge des fonctions de recherche et de filtrage de base. Il introduit ensuite une mise à jour qui permet à l'application d'analyser automatiquement le contenu de l'utilisateur afin de générer des profils comportementaux et de prendre des décisions automatisées de hiérarchisation, de suppression ou de recommandation de contenu sans intervention de l'utilisateur. À la suite de cette modification, l'utilisation prévue du logiciel a évolué: il ne s'agit plus simplement d'un outil de gestion d'informations contrôlé par l'utilisateur, mais d'un système de prise de décision automatisé, ce qui n'était pas envisagé dans l'évaluation des risques. L'application a donc été substantiellement modifiée.

106. Toutefois, dans le même temps, il est possible qu'un fabricant introduise progressivement de nouvelles fonctionnalités qui étaient déjà prévues dans son évaluation des risques ou qui n'altèrent pas, en soi, le profil de risque de cybersécurité du produit comportant des éléments numériques. Tel peut être le cas, par exemple, lorsque le fabricant a anticipé le développement de ces fonctionnalités, a déjà décrit et évalué les risques y afférents et a mis en œuvre des mesures d'atténuation appropriées pour garantir que son produit reste conforme aux exigences essentielles. Tel peut également être le cas lorsque les nouvelles fonctionnalités n'entraînent pas de modifications créant de nouveaux risques ou exacerbant les risques existants. Les mises à jour de cette nature ne devraient donc pas être considérées comme des modifications substantielles, car elles n'augmentent pas le risque de cybersécurité et, par conséquent, ne modifient pas la mise en œuvre des exigences essentielles.

Exemple 42: une application de messagerie est initialement déployée en incluant une fonctionnalité limitée à la messagerie directe. L'évaluation des risques du fabricant couvre l'introduction ultérieure d'une fonctionnalité de messagerie de groupe et envisage, par exemple, la complexité accrue de l'acheminement des messages. Lors d'une mise à jour ultérieure, le fabricant ajoute une fonctionnalité de discussion de groupe ainsi que des contrôles d'administrateur et des outils de modération qui étaient déjà prévus et évalués dans le cadre de la conception initiale. La mise à jour introduit des fonctionnalités qui relèvent de l'utilisation prévue à l'origine et de l'évaluation des risques initiale. L'application de messagerie n'a donc pas été substantiellement modifiée.

Exemple 43: un système de surveillance de la production est mis sur le marché en incluant des tableaux de bord activés en lecture seule, tandis que des fonctionnalités de contrôle automatisées sont présentes dans l'architecture du système mais restent désactivées. L'évaluation des risques du fabricant couvre explicitement l'activation future de boucles de contrôle automatisées, y compris les risques de cybersécurité associés au contrôle en boucle fermée, ainsi que celle de garde-fous tels que des mécanismes de neutralisation par l'opérateur et des modes de sécurité intégrée. Lors d'une mise à jour ultérieure, le fabricant active les fonctionnalités de contrôle automatisées et les garde-fous tels qu'initialement évalués. Le système de surveillance de la production n'a donc pas été substantiellement modifié.

107. À l'inverse, même de nouvelles fonctionnalités limitées ou apparemment mineures peuvent créer des risques de cybersécurité importants qui ont une incidence sur la conformité avec les exigences essentielles. Pour déterminer s'il y a modification substantielle, il ne faut donc pas se fonder sur l'ampleur ou la complexité de la modification, mais il y a lieu de tenir compte de ses répercussions négatives potentielles sur le profil de risque de cybersécurité du produit comportant des éléments numériques et, par voie de conséquence, sur la mise en œuvre des exigences essentielles.

Exemple 44: un fabricant introduit dans une application logicielle une mise à jour dans le cadre de laquelle il ajoute une fonctionnalité «se souvenir de moi» ou une fonctionnalité de connexion persistante qui stocke localement les jetons d'authentification afin d'améliorer la facilité d'utilisation pour l'utilisateur. Bien que la fonctionnalité introduite ait une portée limitée, elle crée de nouveaux risques (en matière de vol de jeton, d'accès non autorisé et de détournement de session) qui n'ont pas été envisagés dans l'évaluation des risques. La mise à jour a donc une incidence sur la conformité avec les exigences essentielles. L'application logicielle a été substantiellement modifiée.

Exemple 45: un fabricant ajoute à un logiciel comportant des éléments numériques existant une nouvelle fonctionnalité de journalisation et de diagnostic permettant d'exporter des journaux de système détaillés à des fins de dépannage. Bien que cette fonctionnalité semble mineure, elle entraîne la collecte et le stockage de données opérationnelles sensibles dans un format non chiffré, ce qui crée des risques d'exposition des données qui n'ont pas été évalués ou atténués au préalable. La modification peut donc avoir une incidence importante sur le profil de risque de cybersécurité du produit comportant des éléments numériques. Le logiciel comportant des éléments numériques a été substantiellement modifié.

108. Conformément au considérant 39 du règlement sur la cyberrésilience, les mises à jour de sécurité ne doivent généralement pas être considérées comme des modifications substantielles, car leur objectif premier est de réduire le niveau de risque de cybersécurité associé au produit comportant des éléments numériques. Une mise à jour de sécurité qui ne modifie pas l'utilisation prévue de ce produit et ne crée pas de nouveaux risques de cybersécurité ne devrait donc pas être considérée comme une modification substantielle, même lorsque des modifications techniques importantes peuvent en résulter. Cela vaut notamment lorsque certaines fonctionnalités sont modifiées ou limitées dans le seul but d'atténuer les vulnérabilités recensées et de garantir que le produit reste conforme aux exigences essentielles.

Exemple 46: un fabricant déploie une mise à jour de sécurité pour remédier à une vulnérabilité dans la base de code d'un produit comportant des éléments numériques en corrigeant une erreur de validation des entrées qui pourrait entraîner un débordement de tampon ou en corrigeant une faille logique qui permet un contournement d'authentification au moyen de la validation inappropriée d'un jeton de session. La mise à jour modifie la mise en œuvre interne du logiciel sans altérer l'utilisation prévue de ce produit ni créer de nouvelle exposition. Elle est exclusivement destinée à réduire le risque de cybersécurité. La mise à jour de sécurité ne devrait pas être considérée comme une modification substantielle.

Exemple 47: un fabricant introduit une mise à jour de sécurité qui renforce les configurations de sécurité existantes, par exemple en durcissant les règles de pare-feu, en désactivant les ports réseau inutilisés, en modifiant les politiques de mot de passe par défaut des administrateurs ou en rendant obligatoire l'authentification multifactorielle alors que cette fonctionnalité était déjà disponible ou prévue. Bien que la mise à jour puisse avoir une incidence sur la manière dont les utilisateurs configurent le produit comportant des éléments numériques ou y ont accès, elle n'altère pas son utilisation prévue et sert uniquement à améliorer son niveau de sécurité. La mise à jour de sécurité ne devrait pas être considérée comme une modification substantielle.

Exemple 48: un fabricant met sur le marché un logiciel comportant des éléments numériques qui, comme expliqué dans la documentation technique et l'évaluation des risques du produit, sécurise les communications à l'aide d'un cadre de chiffrement configurable prenant en charge plusieurs algorithmes cryptographiques et tailles de clé. L'évaluation des risques couvre toutes les options cryptographiques du produit comportant des éléments numériques et anticipe l'abandon futur de certains algorithmes. Elle inclut également des mesures d'atténuation, telles que l'agilité cryptographique, la gestion interne des clés et la réalisation de tests de compatibilité. Pour tenir compte de nouvelles orientations en matière de chiffrement, le fabricant déploie une mise à jour de sécurité qui désactive un algorithme déconseillé et active une autre solution plus forte et déjà prise en charge, sans introduire de nouvelles dépendances externes ni modifier les flux de données. Étant donné que la mise à jour de sécurité met en œuvre une mesure de sécurité qui a été prévue et évaluée dans le cadre de la conception initiale et ne crée pas de nouveaux risques de cybersécurité, elle ne devrait pas être considérée comme une modification substantielle.

109. En revanche, une mise à jour de sécurité peut constituer une modification substantielle lorsque, nonobstant son objectif de sécurité, elle modifie l'utilisation prévue du produit comportant des éléments numériques au-delà de ce qui était prévu initialement ou lorsqu'elle crée de nouveaux risques de cybersécurité ou exacerbe les risques de cybersécurité existants. Tel peut être le cas, par exemple, lorsqu'une mise à jour modifie sensiblement les limites ou la structure de dépendance de ce produit d'une manière non prévue dans l'évaluation des risques, par exemple en modifiant sensiblement les flux de données ou en ajoutant de nouvelles interfaces accessibles depuis l'extérieur.

Exemple 49: un fabricant met sur le marché un logiciel comportant des éléments numériques qui est destiné au chiffrement local de fichiers pour les données stockées sur l'appareil d'un utilisateur et grâce auquel les utilisateurs peuvent chiffrer et déchiffrer des fichiers à la demande. À la suite de la découverte d'une vulnérabilité dans le flux de chiffrement, le fabricant déploie une mise à jour de sécurité qui supprime la fonctionnalité de chiffrement locale et exige désormais que tous les fichiers soient téléchargés, stockés et traités sur un service de chiffrement à distance exploité par le fabricant. À la suite de cette modification, le produit comportant des éléments numériques n'effectue plus le chiffrement local comme prévu initialement, mais devient un service de chiffrement et de traitement de données à distance. Bien que la mise à jour soit introduite pour des raisons de sécurité, elle modifie fondamentalement l'utilisation prévue de ce produit d'une manière non prévue dans l'évaluation des risques et constitue donc une modification substantielle.

Exemple 50: un fabricant met sur le marché un logiciel comportant des éléments numériques qui repose sur un protocole de chiffrement établi et un cycle de vie des clés géré en interne pour sécuriser les communications entre les composants de ce produit comportant des éléments numériques. Après la détection de nouvelles faiblesses cryptographiques, le fabricant introduit une mise à jour de sécurité qui remplace le mécanisme de chiffrement existant par un autre protocole, nécessitant l'utilisation d'un service externe de gestion des clés exploité par un tiers. À la suite de cette modification, les dépendances et les flux de données du produit comportant des éléments numériques sont sensiblement modifiés. En effet, le fabricant introduit de nouvelles interfaces externes et une dépendance à l'égard de services tiers non envisagées dans l'évaluation des risques. Bien que la mise à jour soit axée sur la sécurité, elle crée de nouveaux risques de cybersécurité et constitue donc une modification substantielle.

110. Comme indiqué au point 104 ci-dessus, une évaluation au cas par cas s'impose pour déterminer si une mise à jour logicielle constitue une modification substantielle. Dans le cadre de cette évaluation, les fabricants peuvent examiner, sans s'y limiter, si la mise à jour logicielle:

a) introduit de nouveaux vecteurs de menace (tels que des interfaces supplémentaires, des canaux de communication, des environnements d'exécution ou des dépendances externes) par le biais desquels des menaces pourraient se concrétiser;

b) ouvre la voie à de nouveaux scénarios d'attaque, notamment de nouvelles conditions dans lesquelles il serait plausible que se produise un accès non autorisé au produit comportant des éléments numériques ou aux données traitées par celui-ci, ou que ce produit ou ces données soient manipulés ou fassent l'objet d'une atteinte ou d'une mauvaise utilisation;

c) modifie la probabilité de la survenance des scénarios d'attaque préalablement recensés, par exemple en réduisant le niveau d'effort ou d'expertise nécessaire pour exploiter les vulnérabilités, en augmentant l'exposition à des acteurs non fiables ou en affaiblissant les garde-fous existants;

d) change les répercussions potentielles des scénarios d'attaque préalablement recensés, au niveau, par exemple, de l'ampleur des données ou fonctions concernées, de la gravité des conséquences opérationnelles, économiques ou en matière de sécurité, ou de la capacité à détecter un incident, à le contenir ou à s'en rétablir.

111. Dans certains cas, une mise à jour logicielle n'introduit pas de nouveaux vecteurs de menace, n'ouvre pas la voie à de nouveaux scénarios d'attaque et est sans effet sensible sur la probabilité ou les répercussions des scénarios d'attaque préalablement recensés. Cela peut indiquer que la mise à jour ne crée pas de nouveaux risques de cybersécurité ou n'exacerbe pas les risques de cybersécurité existants, à condition que les hypothèses et les mesures d'atténuation sur lesquelles repose l'évaluation des risques restent valables et efficaces. Il est donc probable que la mise à jour ne constitue pas une modification substantielle.

112. À l'inverse, une mise à jour logicielle peut introduire de nouveaux vecteurs de menace, ouvrir la voie à de nouveaux scénarios d'attaque ou avoir un effet sensible sur la probabilité ou les répercussions des scénarios d'attaque existants. Dans de tels cas, le fabricant devrait réévaluer les risques de cybersécurité du produit comportant des éléments numériques et déterminer s'il demeure conforme aux exigences essentielles, en établissant ainsi si la mise à jour crée de nouveaux risques ou exacerbe les risques existants au-delà de ce qui était prévu dans l'évaluation des risques.

113. La question de savoir si une mise à jour logicielle constitue une modification substantielle est pertinente pour déterminer si certaines obligations prévues par le règlement sur la cyberrésilience s'appliquent, comme indiqué au point 91. Toutefois, que la modification soit substantielle ou non, les fabricants doivent continuer de veiller à la sécurité des mises à jour logicielles et de leur produit comportant des éléments numériques pendant sa période d'assistance, conformément aux exigences relatives à la gestion des vulnérabilités énoncées à l'annexe I, partie II, du règlement sur la cyberrésilience. En outre, qu'une mise à jour logicielle constitue une modification substantielle ou non, les fabricants sont tenus de veiller à ce que l'évaluation des risques et la documentation technique demeurent exactes, complètes et constamment à jour, conformément à l'article 13, paragraphe 7, et à l'article 31, paragraphe 2.

4.4. **Conséquences d'une modification substantielle**

114. Les conséquences d'une modification substantielle apportée à un produit comportant des éléments numériques déjà mis sur le marché par un acteur autre que son fabricant d'origine sont couvertes par les articles 21 et 22 du règlement sur la cyberrésilience. L'article 21 concerne les importateurs et les distributeurs, tandis que l'article 22 concerne toute personne physique ou morale autre que le fabricant, l'importateur ou le distributeur.

115. Si la modification substantielle est apportée à un produit comportant des éléments numériques par son fabricant d'origine, les conséquences sont celles qui résultent de la notion généralement établie de modification substantielle visée au considérant 41 du règlement sur la cyberrésilience et qui sont précisées davantage au point 2.1 du guide bleu. Ce point du guide bleu précise qu'un produit ayant fait l'objet de modifications ou de transformations importantes après sa mise sur le marché doit être considéré comme un nouveau produit si sa performance, sa destination ou son type d'origine sont modifiés, si la nature du danger a changé ou le niveau de risque a augmenté et si le produit comportant des éléments numériques est mis à disposition sur le marché.

116. La conséquence généralement établie est donc que, lorsqu'une modification d'un produit comportant des éléments numériques constitue une modification substantielle et que le produit comportant des éléments numériques modifié est mis à disposition sur le marché, il doit être traité comme un nouveau produit comportant des éléments numériques aux fins du règlement sur la cyberrésilience. Par conséquent, la mise à disposition sur le marché du produit substantiellement modifié constitue une nouvelle mise sur le marché, et ce que la modification substantielle soit effectuée par le fabricant d'origine ou par une autre personne. Afin de garantir que les différentes catégories d'acteurs susceptibles de procéder à une modification substantielle appliquent le règlement sur la cyberrésilience de manière uniforme et proportionnée, les sous-sections suivantes traitent des obligations qui en découlent pour la personne qui procède à la modification substantielle lorsque le produit comportant des éléments numériques substantiellement modifié est mis sur le marché. Les conséquences pour la période d'assistance du produit comportant des éléments numériques sont examinées à la section *5 Période d'assistance*.

4.4.1. *Modifications substantielles effectuées par une personne autre que le fabricant d'origine*

117. En vertu des articles 21 et 22, lorsqu'une modification substantielle est apportée à un produit comportant des éléments numériques déjà mis sur le marché par une personne physique ou morale autre que le fabricant du produit comportant des éléments numériques, la personne qui effectue la modification substantielle et met le produit comportant des éléments numériques modifié à disposition sur le marché est considérée comme le fabricant du produit comportant des éléments numériques modifié, que cette personne ait ou non participé à la conception initiale ou à la première mise sur le marché de ce produit.

118. L'article 22 précise en outre que la personne qui procède à la modification n'est soumise aux obligations énoncées aux articles 13 et 14 qu'en ce qui concerne la partie du produit comportant des éléments numériques sur laquelle porte la modification substantielle, si cette modification n'a pas de répercussions sur la cybersécurité du produit comportant des éléments numériques dans son ensemble.

119. Lorsqu'une modification substantielle a une incidence sur la conformité avec les exigences essentielles mais n'a pas de répercussions négatives sur la cybersécurité du produit comportant des éléments numériques dans son ensemble, la personne qui procède à la modification est soumise à l'article 13 (y compris l'obligation d'assurer la conformité avec les exigences essentielles et de mener une procédure d'évaluation de la conformité) et à l'article 14 (obligations en matière de communication d'informations) uniquement en ce qui concerne la partie du produit comportant des éléments numériques sur laquelle porte la modification substantielle ([16]). En outre, les obligations incombant au fabricant d'origine en vertu du règlement sur la cyberrésilience continuent de s'appliquer au produit comportant des éléments numériques initialement mis sur le marché, ce qui garantit la continuité de la gestion des vulnérabilités et de la conformité des pièces non modifiées.

120. Il ne faut pas confondre la notion de «modification substantielle» et celle d'«intégration», au sens de laquelle une personne assemble des composants (y compris, le cas échéant, en les modifiant) pour obtenir un nouveau produit comportant des éléments numériques qu'elle met elle-même sur le marché. Dans un tel cas, l'intégrateur ne modifie pas un produit comportant des éléments numériques déjà mis sur le marché par un autre fabricant, mais met sur le marché un nouveau produit comportant des éléments numériques qui lui est propre. L'intégrateur est le fabricant de ce nouveau produit comportant des éléments numériques aux fins du règlement sur la cyberrésilience et est tenu de se conformer à l'intégralité de ce règlement en ce qui concerne le produit comportant des éléments numériques dans son ensemble. Lorsque le fabricant intègre des composants qui sont soumis au règlement sur la cyberrésilience, il peut s'appuyer sur les activités de mise en conformité des fabricants de ces composants pour faciliter sa propre mise en conformité avec le règlement sur la cyberrésilience.

Exemple 51: une entreprise achète des modules de microcontrôleur et des composants de connectivité disponibles dans le commerce auprès de fournisseurs tiers, développe un micrologiciel propriétaire et un ensemble de capteurs, et les assemble en un produit de surveillance agricole connecté comportant des éléments numériques qu'elle met sur le marché sous son propre nom. Bien qu'elle ait modifié les modules de microcontrôleur sous-jacents et les ait combinés avec d'autres composants, cette entreprise n'apporte pas de modification substantielle à un produit comportant des éléments numériques déjà mis sur le marché; au contraire, elle met sur le marché un nouveau produit comportant des éléments numériques. L'entreprise est le fabricant du produit de surveillance agricole aux fins du règlement sur la cyberrésilience et est tenue de se conformer à ce règlement en ce qui concerne le produit de surveillance agricole dans son ensemble.

([16]) Aux termes du point 2.1 du guide bleu, «[i]l n'est pas nécessaire de répéter les essais ou de produire de nouveaux documents pour les aspects non concernés par la modification. Il appartient à la personne physique ou morale modifiant ou faisant modifier le produit de démontrer que tous les éléments de la documentation technique ne doivent pas faire l'objet d'une mise à jour. La personne physique ou morale modifiant ou faisant modifier le produit est responsable de la conformité du produit modifié et établit une déclaration de conformité, même si elle s'appuie sur des essais et une documentation technique existants».

121. Lorsqu'une modification substantielle apportée à un produit comportant des éléments numériques par une personne autre que son fabricant d'origine a des répercussions négatives sur la cybersécurité de ce produit dans son ensemble, par exemple parce que la modification n'est plus ciblée ou limitée à un composant ou sous-système spécifique, le produit comportant des éléments numériques modifié mis à disposition sur le marché devrait être traité comme un nouveau produit comportant des éléments numériques soumis au règlement sur la cyberrésilience dans son intégralité. Dans un tel cas, le profil de risque de cybersécurité global de ce produit a changé et il est impossible d'évaluer la modification sans tenir compte du produit comportant des éléments numériques dans son ensemble. La personne qui procède à la modification est soumise aux obligations applicables aux fabricants en vertu des articles 13 et 14 en ce qui concerne le produit comportant des éléments numériques modifié dans son ensemble.

4.4.2. *Modifications substantielles effectuées par le fabricant d'origine*

122. Lorsque la modification substantielle est effectuée par le fabricant d'origine, y compris dans le cadre du développement itératif de logiciels comportant des éléments numériques, ce fabricant reste le fabricant aux fins du règlement sur la cyberrésilience. Toutefois, le produit comportant des éléments numériques substantiellement modifié doit être considéré comme nouvellement mis sur le marché.

123. Conformément au point 2.1 du guide bleu, le fabricant d'origine qui met sur le marché le produit comportant des éléments numériques substantiellement modifié peut réutiliser la documentation et les essais existants pour les aspects du produit comportant des éléments numériques qui ne sont pas concernés par la modification substantielle. En particulier lorsque le fabricant met sur le marché des versions substantiellement modifiées d'un même produit comportant des éléments numériques, la procédure d'évaluation de la conformité devrait se concentrer sur les pièces substantiellement modifiées du produit comportant des éléments numériques. De même, lorsque l'évaluation de la conformité est effectuée par un tiers, l'organisme qui procède à l'évaluation de la conformité devrait concentrer son évaluation sur les pièces substantiellement modifiées. Pour les pièces du produit comportant des éléments numériques qui ne sont pas modifiées, il peut réutiliser la documentation et les résultats d'essais existants.

124. Les considérations de proportionnalité énoncées dans la sous-section précédente s'appliquent également aux modifications substantielles apportées par le fabricant d'origine d'un produit comportant des éléments numériques mis sur le marché avant le 11 décembre 2027. Une telle modification substantielle effectuée par le fabricant d'origine n'oblige pas, en soi, le fabricant à mettre l'ensemble du produit comportant des éléments numériques mis sur le marché avant cette date en totale conformité avec le règlement sur la cyberrésilience, à moins que la modification n'ait des répercussions négatives sur la cybersécurité du produit comportant des éléments numériques dans son ensemble. Lorsque la modification n'a pas de répercussions sur la cybersécurité du produit comportant des éléments numériques dans son ensemble, les obligations imposées au fabricant d'origine en ce qui concerne la modification devraient être limitées aux pièces substantiellement modifiées.

5. **PÉRIODE D'ASSISTANCE**

125. L'article 13, paragraphe 8, du règlement sur la cyberrésilience impose aux fabricants de déterminer la période d'assistance au cours de laquelle les vulnérabilités du produit comportant des éléments numériques, y compris de ses composants, sont gérées efficacement et conformément aux exigences essentielles énoncées à l'annexe I, partie II. La période d'assistance reflète la période pendant laquelle le produit comportant des éléments numériques est censé pouvoir être utilisé (la durée d'utilisation prévue); elle devrait être déterminée à la lumière des critères énoncés à l'article 13, paragraphe 8, en particulier des attentes raisonnables des utilisateurs, de la nature du produit comportant des éléments numériques, y compris de son utilisation prévue, ainsi que du droit de l'Union applicable déterminant la durée de vie des produits comportant des éléments numériques ([17]). Dans l'ensemble, il convient de tenir compte de ces critères de manière à garantir la proportionnalité lors de la détermination de la période d'assistance.

([17]) L'article 13, paragraphe 8, prévoit des critères supplémentaires dont il est possible de tenir compte, notamment les périodes d'assistance des produits comportant des éléments numériques offrant une fonctionnalité similaire mis sur le marché par d'autres fabricants, la disponibilité de l'environnement opérationnel, les périodes d'assistance des composants intégrés qui assurent des fonctions essentielles et proviennent de tiers, ainsi que les orientations pertinentes fournies par le groupe de coopération administrative (ADCO) institué en vertu du règlement sur la cyberrésilience, et par la Commission.

126. L'article 13, paragraphe 8, exige en outre que la période d'assistance soit d'au moins cinq ans, à moins que le produit comportant des éléments numériques ne soit censé pouvoir être utilisé pendant moins de cinq ans, auquel cas la période d'assistance correspond à la durée d'utilisation prévue. La période d'assistance minimale sert donc uniquement de garantie assurant que les vulnérabilités sont gérées pendant une période suffisamment longue, tout en permettant aux fabricants de tenir compte des produits comportant des éléments numériques dont la durée d'utilisation prévue est réellement plus courte. Le considérant 60 fournit davantage d'orientations à cet égard, en précisant que les produits comportant des éléments numériques dont on peut raisonnablement s'attendre à ce qu'ils soient utilisés pendant plus de cinq ans devraient ainsi être couverts par des périodes d'assistance plus longues. Une période d'assistance de cinq ans ne doit donc pas être considérée comme la période par défaut pour tous les produits comportant des éléments numériques. Au lieu de cela, le fabricant devrait déterminer la durée appropriée de la période d'assistance à la lumière des critères énoncés à l'article 13, paragraphe 8.

127. L'article 13, paragraphe 19, impose aux fabricants d'indiquer au moment de l'achat, d'une manière claire et compréhensible, la date de fin de la période d'assistance (au moins le mois et l'année). Cette disposition impose également aux fabricants de prévoir l'affichage d'une notification aux utilisateurs à l'expiration de la période d'assistance, lorsque cela est techniquement possible compte tenu de la nature du produit comportant des éléments numériques. Cette obligation vise à assurer la transparence pour les utilisateurs en ce qui concerne la durée prévisible de l'assistance en matière de sécurité.

128. Dans le cas des logiciels comportant des éléments numériques, qui sont souvent développés et déployés de manière itérative et pour lesquels des versions substantiellement modifiées peuvent fréquemment être mises sur le marché au fil du temps, la période d'assistance doit être comprise à la lumière de ce modèle de développement. Pour chaque version substantiellement modifiée d'un logiciel comportant des éléments numériques mis sur le marché, la période d'assistance déclarée doit être conforme à l'article 13, paragraphe 8, et la période d'assistance minimale doit ainsi être d'au moins cinq ans, à moins qu'il ne soit prouvé que la durée d'utilisation prévue de cette version est plus courte, comme précisé également au considérant 60. La section *5.1 Modifications substantielles et période d'assistance* précise en outre que, lorsqu'une modification substantielle n'entraîne pas de modification des facteurs qui ont servi à la détermination initiale de la durée d'utilisation prévue du produit comportant des éléments numériques, la période d'assistance initiale demeure inchangée (c'est-à-dire y compris lorsque la période d'assistance restante est inférieure à cinq ans).

129. L'article 13, paragraphe 10, offre une certaine souplesse aux fabricants de logiciels comportant des éléments numériques en leur permettant, sous certaines conditions, de garantir la conformité avec l'exigence relative à la gestion des vulnérabilités énoncée à l'annexe I, partie II, point 2) (gestion et correction des vulnérabilités), uniquement pour la dernière version mise sur le marché du logiciel comportant des éléments numériques, et ce à condition que les utilisateurs des versions précédemment mises sur le marché aient accès gratuitement aux dernières versions mises sur le marché et ne doivent pas supporter des coûts supplémentaires pour adapter l'environnement matériel et logiciel dans lequel ils utilisent la version originale de ce produit.

130. Aux fins de l'article 13, paragraphe 10, la notion de «coûts supplémentaires» devrait être interprétée de manière pratique et proportionnée, en tenant compte des pratiques normales et attendues en matière d'entretien et d'exploitation des logiciels. Elle ne recouvre pas les efforts opérationnels raisonnables qui sont inhérents à l'application de mises à jour logicielles ou à l'entretien d'un environnement opérationnel sécurisé, tels que le temps consacré par le personnel, les essais de routine, les ajustements de configuration ou les mises à niveau des dépendances logicielles sous-jacentes qui sont nécessaires pour gérer les composants en fin de vie ou traiter les vulnérabilités connues en matière de sécurité. En revanche, les «coûts supplémentaires» correspondent aux frais qui vont au-delà de ce qui peut normalement être escompté dans le cadre des mises à jour logicielles, tels que l'achat obligatoire de nouveau matériel, le remplacement de l'infrastructure ou les modifications fondamentales de l'environnement opérationnel.

131. Pour les logiciels comportant des éléments numériques, qui sont en constante évolution, les fabricants peuvent mettre sur le marché des versions successives substantiellement modifiées à des intervalles relativement courts et s'attendre à ce que les utilisateurs les mettent à jour régulièrement. Dans ce cas, la période d'assistance déclarée pour chaque version substantiellement modifiée doit être conforme à l'article 13, paragraphe 8, au moment de sa mise sur le marché. Autrement dit, le fabricant doit déclarer une nouvelle période d'assistance pour cette version substantiellement modifiée. Toutefois, il peut se prévaloir de l'article 13, paragraphe 10, pour mettre fin à la gestion et à la correction des vulnérabilités des versions antérieures une fois que les utilisateurs sont en mesure de

passer à une version ultérieure gratuitement et sans supporter de coûts supplémentaires, comme indiqué ci-dessus, même s'il en résulte une période d'assistance effective plus courte pour ces versions antérieures ([18]). Le fabricant reste soumis aux autres exigences relatives à la gestion des vulnérabilités énoncées à l'annexe I, partie II, ainsi qu'aux obligations en matière de communication d'informations prévues à l'article 14. Comme expliqué également au considérant 40, ces exigences imposent notamment, pour toutes les versions ultérieures substantiellement modifiées du logiciel comportant des éléments numériques mis sur le marché: i) de maintenir une politique de divulgation coordonnée des vulnérabilités; et ii) d'appliquer des mesures visant à faciliter le partage d'informations relatives à de possibles vulnérabilités ([19]).

Exemple 52: un fabricant met un modèle de téléphone intelligent sur le marché de l'Union et déclare une période d'assistance de X ans à compter de la date de mise sur le marché, au cours de laquelle il fournira des mises à jour de sécurité pour remédier aux vulnérabilités. Au cours de cette période, le fabricant publie régulièrement des mises à jour logicielles et des versions substantiellement modifiées du système d'exploitation, que les utilisateurs peuvent installer gratuitement sans devoir acquérir de nouveau matériel.

Le fabricant peut, conformément à l'article 13, paragraphe 10, gérer et corriger les vulnérabilités de la dernière version du système d'exploitation mise à disposition pour ce modèle de téléphone intelligent, à condition que les versions antérieures puissent être mises à niveau gratuitement et sans coûts supplémentaires. Pendant la durée de la période d'assistance, le fabricant reste soumis aux autres exigences relatives à la gestion des vulnérabilités, telles que la divulgation coordonnée des vulnérabilités et les mesures de partage d'informations.

Exemple 53: un fabricant met sur le marché un logiciel d'entreprise comportant des éléments numériques et publie des versions substantiellement modifiées tous les deux ou trois mois, afin d'intégrer des améliorations en matière de sécurité et de nouvelles fonctionnalités et d'assurer la compatibilité avec les systèmes d'exploitation et les plateformes mis à jour. Chaque version est mise sur le marché avec une période d'assistance déclarée conformément à l'article 13, paragraphe 8. Le fabricant s'attend à ce que les utilisateurs procèdent régulièrement à des mises à jour dans le cadre d'un fonctionnement normal et donne gratuitement accès à la dernière version. L'application des mises à niveau peut nécessiter des efforts opérationnels raisonnables, tels que des essais ou des ajustements de configuration, mais n'exige pas de coûts supplémentaires, tels que l'achat de nouveau matériel ou des modifications fondamentales de l'infrastructure. Dans ce contexte, le fabricant peut se prévaloir de l'article 13, paragraphe 10, pour mettre fin à la gestion et à la correction des vulnérabilités des versions antérieures une fois que les utilisateurs sont en mesure de passer à la dernière version, tout en continuant à se conformer aux autres exigences relatives à la gestion des vulnérabilités pour toutes les versions ultérieures substantiellement modifiées.

5.1. **Modifications substantielles et période d'assistance**

132. Comme expliqué à la section 4.4 *Conséquences d'une modification substantielle*, lorsqu'une modification d'un produit comportant des éléments numériques constitue une modification substantielle et que le produit comportant des éléments numériques modifié est mis à disposition sur le marché, il doit être traité comme un nouveau produit aux fins du règlement sur la cyberrésilience et la mise à disposition sur le marché du produit comportant des éléments numériques substantiellement modifié constitue une nouvelle mise sur le marché. Il est donc utile de préciser l'effet que cette nouvelle mise sur le marché a sur la période d'assistance du produit comportant des éléments numériques substantiellement modifié.

133. La période d'assistance d'un produit comportant des éléments numériques substantiellement modifié devrait être déterminée en fonction de la durée d'utilisation prévue de ce produit, à la lumière des critères énoncés à l'article 13, paragraphe 8, du règlement sur la cyberrésilience. Une modification substantielle devrait donc nécessiter une réévaluation à l'aune de ces critères, mais n'entraîne pas automatiquement une réinitialisation, ni même une prolongation, de la période d'assistance. La question à se poser est de savoir si la modification substantielle a une incidence sur les facteurs qui ont servi à la détermination initiale de la durée d'utilisation prévue de ce produit et, par voie de conséquence, sur la période d'assistance initiale.

([18]) Il convient de rappeler que l'article 13, paragraphe 19, impose aux fabricants, lorsque cela est techniquement possible compte tenu de la nature du produit comportant des éléments numériques, de prévoir l'affichage d'une notification aux utilisateurs les informant que leur produit comportant des éléments numériques a atteint la fin de sa période d'assistance. Par conséquent, lorsqu'il est mis fin à la gestion et à la correction des vulnérabilités des versions antérieures, les utilisateurs qui ne sont pas passés à la version la plus récente devraient en être informés, si cela est techniquement possible.

([19]) Il convient de signaler que, lorsque les utilisateurs peuvent passer à la dernière version du logiciel sans coûts supplémentaires, les fabricants peuvent néanmoins choisir de maintenir la gestion et la correction des vulnérabilités des versions antérieures de ce logiciel, y compris à titre onéreux ou dans le cadre d'autres accords commerciaux. Le règlement sur la cyberrésilience n'exige pas des fabricants qu'ils fournissent gratuitement des mises à jour de sécurité pour ces versions antérieures.

134. Si la modification substantielle n'a pas d'incidence sur ces facteurs, la durée d'utilisation prévue qui a été déterminée initialement en application des critères énoncés à l'article 13, paragraphe 8, demeure inchangée et la période d'assistance du produit comportant des éléments numériques modifié devrait correspondre au reste de la durée d'utilisation prévue du produit tel qu'il a été initialement mis sur le marché. Tel sera généralement le cas lorsque la modification n'a aucune incidence sur des facteurs qui ont été déterminants pour la durée d'utilisation prévue, tels que la durabilité physique des composants matériels, ou lorsque la modification substantielle ne concerne que des fonctionnalités logicielles ou des services d'arrière-plan.

Exemple 54*: un fabricant met sur le marché un aspirateur robot dont la durée d'utilisation prévue est de X ans, qu'il a déterminée en fonction de la nature du produit comportant des éléments numériques, y compris de la durabilité physique et des caractéristiques d'usure des composants matériels, et en tenant compte des attentes raisonnables des utilisateurs quant à la durée de vie de ce produit. Le fabricant déclare une période d'assistance de X ans. Après Y ans, le fabricant publie une mise à jour logicielle qui ajoute de nouveaux modes de nettoyage et de nouvelles fonctionnalités de navigation; cette mise à jour constitue une modification substantielle. La mise à jour logicielle n'a pas d'incidence sur la durabilité physique du produit matériel et ne modifie pas les attentes raisonnables des utilisateurs quant à la durée de vie de ce produit. La durée d'utilisation prévue en application des critères énoncés à l'article 13, paragraphe 8, demeure donc inchangée. La période d'assistance du produit comportant des éléments numériques modifié correspond au reste de la durée d'utilisation prévue qui a été déterminée initialement.*

Exemple 55: un fabricant met sur le marché une machine industrielle complexe comportant des éléments numériques, qui inclut en arrière-plan des services en nuage constituant une solution de traitement de données à distance. À la lumière des attentes raisonnables des utilisateurs et de la nature du produit comportant des éléments numériques, notamment la durabilité physique de la machine et l'usure escomptée, la durée d'utilisation prévue est de X ans. La période d'assistance est fixée à X ans pour correspondre à cette durée d'utilisation prévue. Après Y ans, le fabricant revoit l'architecture des services en nuage d'arrière-plan (la solution de traitement de données à distance), en introduisant de nouvelles interfaces de programmation d'application et de nouveaux flux de données dans le cadre d'une modification qui constitue une modification substantielle du produit comportant des éléments numériques, mais qui ne modifie pas la nature de ce produit et n'a pas d'incidence sur les attentes des utilisateurs. La durée d'utilisation prévue en application des critères énoncés à l'article 13, paragraphe 8, demeure donc inchangée. La période d'assistance du produit comportant des éléments numériques modifié correspond au reste de la durée d'utilisation prévue qui a été déterminée initialement.

135. Lorsque la modification substantielle a une incidence sur les facteurs qui ont servi à la détermination initiale de la durée d'utilisation prévue du produit comportant des éléments numériques, le fabricant devrait recalculer la période d'assistance afin de tenir compte de la nouvelle durée d'utilisation prévue, en appliquant en conséquence les critères de l'article 13, paragraphe 8. Tel peut être le cas, par exemple, lorsque le fabricant apporte des modifications matérielles qui revitalisent ce produit et en prolongent la durée de vie opérationnelle ou lorsqu'il revoit de manière substantielle la programmation ou le code du logiciel de base de ce produit de façon à modifier sensiblement sa durée d'utilisation prévue ([20]).

Exemple 56: un fabricant met sur le marché une unité de programmation logique d'une durée d'utilisation prévue de X ans, déterminée principalement en fonction de la nature du produit comportant des éléments numériques et de la durabilité du matériel sous-jacent. La période d'assistance est fixée en conséquence. Plusieurs années après la première mise sur le marché, le fabricant procède à une modification substantielle qui consiste à remplacer la plate-forme informatique intégrée de l'unité de programmation logique, y compris le processeur, la mémoire et l'environnement d'exécution, par une nouvelle génération de composants conçus pour une durée de vie opérationnelle nettement plus longue. À la suite de la modification, les attentes raisonnables des utilisateurs et la nature du produit comportant des éléments numériques ont changé: l'utilisateur de l'unité de programmation logique peut désormais raisonnablement s'attendre à ce que, grâce à la nouvelle plate-forme informatique, l'unité de programmation logique puisse encore être utilisée de manière productive au-delà de la durée d'utilisation prévue initialement déclarée. La durée d'utilisation prévue en application des critères énoncés à l'article 13, paragraphe 8, est donc plus longue et le fabricant recalcule en conséquence la période d'assistance pour cette unité de programmation logique spécifique.

6. **PRODUITS IMPORTANTS OU CRITIQUES COMPORTANT DES ÉLÉMENTS NUMÉRIQUES**

136. En vertu de l'article 7, paragraphe 1, du règlement sur la cyberrésilience, les produits comportant des éléments numériques dont la fonctionnalité de base est celle d'une catégorie de produit énoncée à l'annexe III de ce règlement sont considérés comme des «produits importants comportant des éléments numériques». L'annexe III répartit en outre les produits importants comportant des éléments numériques en une classe I et une classe II. De même, l'article 8, paragraphe 1, prévoit que les produits comportant des éléments numériques dont la fonctionnalité de base est celle d'une catégorie de produits qui figure à l'annexe IV du règlement sur la cyberrésilience sont considérés comme des «produits critiques comportant des éléments numériques» ([21]).

([20]) Il convient de rappeler que, comme indiqué à la section 4.1 *Réparations physiques*, les opérations de remise à neuf, d'entretien ou de réparation ne sont généralement pas considérées comme constituant des modifications substantielles.

([21]) Le règlement d'exécution (UE) 2025/2392 de la Commission établit la description technique des catégories de produits importants et critiques.

137. La classification d'un produit comportant des éléments numériques en tant que produit important ou critique ou, à l'inverse, en tant que produit de la catégorie «par défaut» ([22]) est pertinente pour déterminer quelle procédure d'évaluation de la conformité le fabricant doit suivre, conformément à l'article 32, avant de pouvoir mettre ce produit comportant des éléments numériques sur le marché. Notamment, dans le cas des produits comportant des éléments numériques qui appartiennent à la catégorie par défaut, le fabricant peut toujours recourir à la procédure de contrôle interne fondée sur le module A («autoévaluation») ([23]). Les produits importants comportant des éléments numériques qui relèvent de la classe I ou de la classe II et les produits critiques comportant des éléments numériques sont soumis à des procédures d'évaluation de la conformité plus strictes, mais cette obligation ne s'applique pas aux produits importants comportant des éléments numériques qui relèvent de la classe I ou de la classe II et qui répondent aux critères de logiciels libres et ouverts qui sont mis sur le marché, pour lesquels, conformément à l'article 32, paragraphe 5, les fabricants sont autorisés à suivre les procédures de la catégorie par défaut.

138. La notion de «fonctionnalité de base» est dès lors essentielle pour permettre au fabricant de déterminer quel régime d'évaluation de la conformité lui est applicable. Toutefois, cette notion n'est pas explicitement définie dans le règlement sur la cyberrésilience. Les produits comportant des éléments numériques peuvent exécuter une série de fonctions, dont certaines peuvent être auxiliaires par rapport à la fonctionnalité de base de ce produit et ne devraient pas avoir d'incidence sur sa classification en tant que produit par défaut/produit important de classe I/ produit important de classe II/produit critique. Il est donc utile de fournir des orientations supplémentaires afin d'aider les fabricants à exécuter correctement les procédures d'évaluation de la conformité pertinentes et d'aider les autorités de surveillance du marché à garantir l'application harmonisée du règlement sur la cyberrésilience dans l'ensemble de l'Union.

6.1. **Fonctionnalité de base**

139. On entend par «fonctionnalité de base» d'un produit comportant des éléments numériques les principales fonctions et capacités techniques de ce produit, sans lesquelles son utilisation prévue ne serait pas possible. Elle peut s'apprécier à la lumière du contexte et des conditions spécifiques d'utilisation de ce produit, compte étant tenu, entre autres, des informations communiquées par le fabricant dans la notice d'utilisation, dans les indications publicitaires ou de vente, ainsi que dans la documentation technique.

Exemple 57: un logiciel comportant des éléments numériques inclut une couche d'abstraction avec le matériel sous-jacent et gère l'exécution des composants logiciels. Ses principales fonctions sont l'initialisation du matériel et des périphériques, la gestion des processus et de la mémoire, le contrôle entrée-sortie, la programmation, l'allocation des ressources et l'exposition des services de système et des interfaces de programmation d'application par l'intermédiaire desquels les applications interagissent avec les ressources matérielles et logicielles de l'appareil. La documentation technique indique que le produit comportant des éléments numériques orchestre les ressources informatiques, met en œuvre les configurations du système et fournit des interfaces normalisées pour les modules logiciels et les périphériques connectés. Le fabricant souligne que ces capacités permettent à la plate-forme de servir d'environnement logiciel central sur lequel les applications peuvent s'exécuter de manière fiable. Le produit comportant des éléments numériques a la fonctionnalité de base d'un système d'exploitation, telle que décrite à l'annexe I, point 11, du règlement d'exécution (UE) 2025/2392.

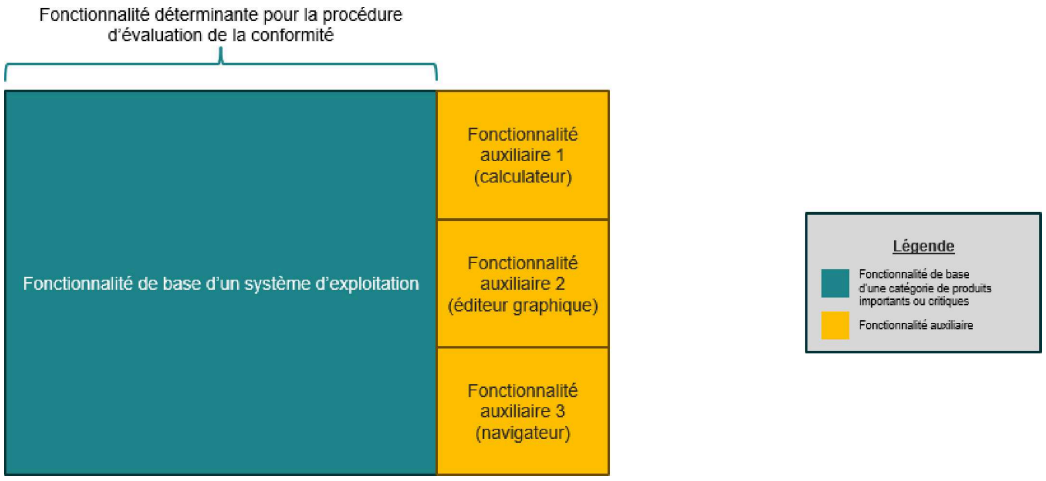
140. La fonctionnalité d'un produit comportant des éléments numériques est rarement limitée exclusivement à sa fonctionnalité de base, étant donné que les produits comportant des éléments numériques exécutent souvent, voire toujours, des fonctions supplémentaires qui ne contribuent pas à la fonctionnalité de base du produit. Le produit peut également intégrer des composants qui ont eux-mêmes la fonctionnalité d'un autre produit important ou critique comportant des éléments numériques. Toutefois, le fait qu'un produit comportant des éléments numérique s remplisse des fonctions autres que celles détaillées dans les descriptions techniques des produits importants ou critiques comportant des éléments numériques ou en complément de celles-ci n'empêche pas en soi ce produit d'avoir la fonctionnalité de base d'un tel produit important ou critique.

([22]) La notion de «catégorie par défaut» n'est pas définie dans le règlement sur la cyberrésilience. Cette expression telle qu'utilisée dans le présent document désigne les produits comportant des éléments numériques dont la fonctionnalité de base n'est pas celle d'une catégorie de produits énoncée à l'annexe III ou IV du règlement sur la cyberrésilience et qui, par conséquent, sont soumis au régime d'évaluation de la conformité prévu à l'article 32, paragraphe 1.

([23]) Le fabricant peut néanmoins toujours choisir d'appliquer une procédure d'évaluation de la conformité plus stricte prévue à l'article 32, paragraphe 1.

Illustration 2

Diagramme montrant que c'est la fonctionnalité de base, et non les fonctionnalités auxiliaires, qui détermine la procédure d'évaluation de la conformité applicable



141. Un produit comportant des éléments numériques peut avoir la capacité d'exécuter les fonctions d'une catégorie de produits importants ou critiques, mais sa fonctionnalité de base peut néanmoins être différente de celle de cette catégorie de produits. Dans ce cas, le produit comportant des éléments numériques ne serait pas considéré comme un produit important ou critique comportant des éléments numériques. Comme indiqué explicitement à l'article 7, paragraphe 1, du règlement sur la cyberrésilience pour les produits importants comportant des éléments numérique s (et la même logique vaut pour les produits critiques comportant des éléments numériques), la simple intégration d'un produit important ou critique comportant des éléments numériques dans un produit comportant des éléments numériques n'amène pas en tant que telle ce dernier produit à être un produit important ou critique comportant des éléments numériques.

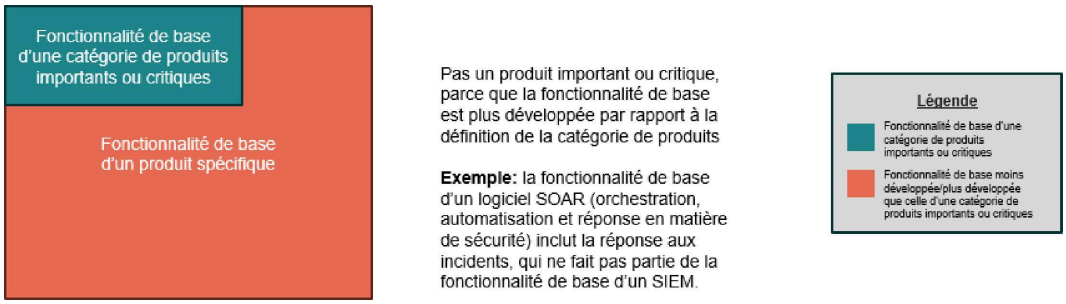
Exemple 58: un téléphone intelligent intègre un système d'exploitation qui fournit les fonctionnalités décrites à l'annexe I, point 11, du règlement d'exécution (UE) 2025/2392. Tandis que le système d'exploitation permet la gestion des ressources matérielles et l'exécution d'applications logicielles, le téléphone intelligent dans son ensemble a une fonctionnalité de base différente (par exemple, permettre aux utilisateurs de communiquer et d'accéder à des informations et à des services). La simple intégration d'un système d'exploitation ne signifie pas que le téléphone intelligent possède la fonctionnalité de base d'un système d'exploitation.

142. Certains produits comportant des éléments numériques peuvent être semblables à une catégorie de produits importants ou critiques, ou appartenir à la même famille générale de produits, mais leur fonctionnalité de base peut être largement plus développée/moins développée que celle de cette catégorie. Tel n'est pas le cas lorsqu'un produit comportant des éléments numériques inclut des fonctionnalités supplémentaires qui ne font que compléter ou renforcer la fonctionnalité de base, qui correspond elle-même à celle d'une catégorie de produits importants ou critiques; dans un tel cas, le produit comportant des éléments numériques conserve la fonctionnalité de base de cette catégorie et est classé en conséquence. Aux fins de cette évaluation, il y a lieu de se fonder sur les principales fonctions et capacités techniques de ce produit, considérées objectivement à la lumière de son utilisation prévue, et non sur la manière dont le produit comportant des éléments numériques est décrit ou commercialisé, lorsque cette description ne reflète pas les caractéristiques techniques réelles du produit.

Exemple 59: un logiciel SOAR (orchestration, automatisation et réponse en matière de sécurité) a souvent la capacité d'exécuter les fonctions de produits comportant des éléments numériques dans la catégorie des «systèmes de gestion des informations et des événements de sécurité (SIEM)», c'est-à-dire de recueillir des données provenant de sources multiples, de les analyser, de les mettre en corrélation et de les présenter comme des informations exploitables à des fins de sécurité. Toutefois, la fonctionnalité de base de ce logiciel, dont les capacités techniques incluent comme éléments de base des services tels que la réponse aux incidents, est largement plus développée que celle d'un SIEM. Par conséquent, le logiciel SOAR n'est généralement pas considéré comme ayant la fonctionnalité de base d'un SIEM.

Illustration 3

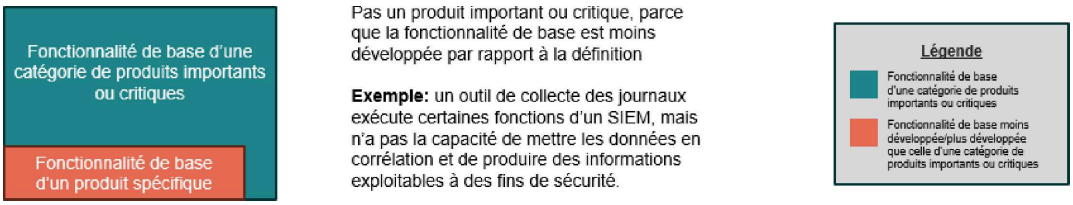
Diagramme illustrant la fonctionnalité de base d'un produit comportant des éléments numériques qui est largement plus développée par rapport à la définition d'une catégorie de produits importants ou critiques



Exemple 60: certains outils de collecte et de visualisation des journaux ont la capacité de digérer les données de ces journaux et de présenter des tableaux de bord rudimentaires affichant les événements du système. Bien que ces outils puissent supporter des activités de surveillance de la sécurité, leur fonctionnalité de base est moins développée que celle d'un SIEM, car ils ne mettent pas les données en corrélation et ne produisent pas des informations exploitables à des fins de sécurité. Par conséquent, ces outils ne doivent généralement pas être considérés comme ayant la fonctionnalité de base d'un SIEM.

Illustration 4

Diagramme illustrant la fonctionnalité de base d'un produit comportant des éléments numériques qui est largement moins développée par rapport à la définition d'une catégorie de produits importants ou critiques

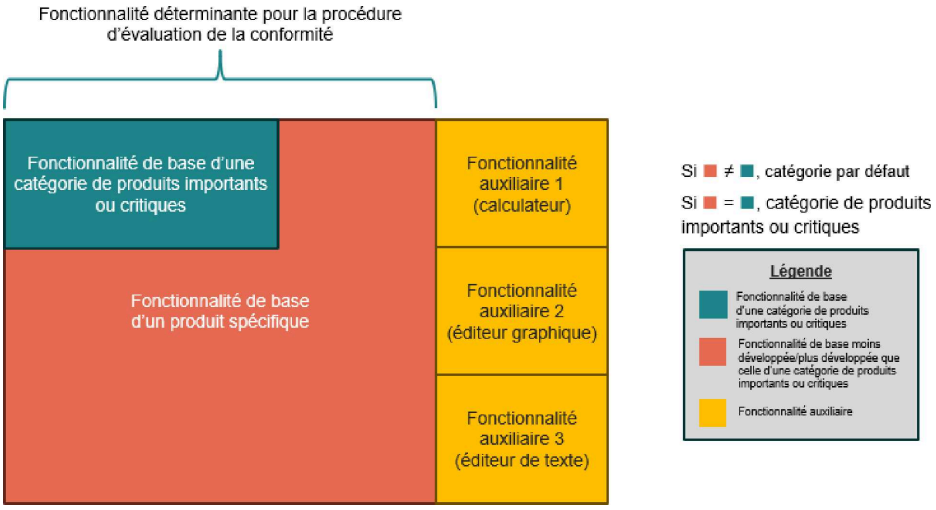


143. Un fabricant ne peut pas dénaturer la fonctionnalité de base de son produit comportant des éléments numériques de manière à se soustraire au régime d'évaluation de la conformité applicable aux produits importants ou critiques comportant des éléments numériques, par exemple en mettant en avant ou en minimisant de manière excessive le rôle de certaines fonctionnalités, de façon à faire accroire que la fonctionnalité de base du produit est largement plus développée/moins développée qu'une fonctionnalité de base donnée. Tel serait le cas, par exemple, lorsqu'il existe des incohérences manifestes entre les indications publicitaires, la notice d'utilisation et la documentation technique.

144. Un produit comportant des éléments numériques ne peut avoir plus d'une fonctionnalité de base aux fins de la détermination du régime d'évaluation de la conformité applicable. En vertu de l'annexe VII du règlement sur la cyberrésilience, dans le cadre de la documentation technique d'un produit, les fabricants sont tenus de décrire l'utilisation prévue de leur produit comportant des éléments numériques ainsi que la procédure d'évaluation de la conformité qu'ils ont suivie. La fonctionnalité de base du produit devrait donc être indiquée clairement, et ce afin que le régime d'évaluation de la conformité applicable soit déterminé à bon droit et afin que les autorités de surveillance du marché puissent superviser l'application du règlement et vérifier qu'il a été appliqué correctement.

Illustration 5

Diagramme montrant que c'est la fonctionnalité de base d'un produit comportant des éléments numérique s spécifique qui détermine la classification de ce produit et, par voie de conséquence, la procédure d'évaluation de la conformité applicable



145. Certains produits comportant des éléments numériques sont mis sur le marché en tant que produits individuels comportant des éléments numériques, mais sont composés de modules distincts ayant chacun ses propres fonctionnalités. Si un fabricant met également ces modules à disposition sur le marché séparément, par exemple lorsqu'il les propose individuellement à la vente, sous licence ou contre un abonnement, ces modules constituent des produits autonomes comportant des éléments numériques à part entière. Dès lors, ils doivent être classés sur la base de leurs fonctionnalités de base respectives (et donc être soumis au régime d'évaluation de la conformité approprié sur la base de la fonctionnalité de base de chaque module). Cela est sans préjudice des modules fournis uniquement en tant que composants d'un produit intégré comportant des éléments numériques et qui ne sont pas mis à disposition séparément; dans ce cas, la fonctionnalité de base est déterminée au niveau du produit intégré comportant des éléments numériques.

Exemple 61: un fabricant met sur le marché une suite de sécurité unifiée intégrant plusieurs modules, dont un SIEM, un système de détection des intrusions et un module d'analyse. Il permet également de souscrire des abonnements pour chacun de ces modules. Dans ce scénario, chaque module constitue un produit distinct comportant des éléments numériques et est classé sur la base de sa propre fonctionnalité de base. Le module SIEM est soumis au régime d'évaluation de la conformité applicable aux produits importants comportant des éléments numériques relevant de la classe I, étant donné que sa fonctionnalité de base est celle des «systèmes de gestion des informations et des événements de sécurité (SIEM)». Le système de détection des intrusions est soumis au régime d'évaluation de la conformité applicable aux produits importants comportant des éléments numériques relevant de la classe II, étant donné que sa fonctionnalité de base est celle des «pare-feu, systèmes de détection et de prévention des intrusions». Le module d'analyse est soumis au régime d'évaluation de la conformité applicable aux produits comportant des éléments numériques relevant de la catégorie «par défaut», étant donné que sa fonctionnalité de base n'est pas celle d'une catégorie de produits importants ou critiques.

146. Le non-respect des obligations énoncées à l'article 32 du règlement sur la cyberrésilience peut faire l'objet d'une amende administrative, conformément à l'article 64, paragraphe 3.

6.2. Évaluation de la conformité pour les produits importants ou critiques comportant des éléments numériques

147. Une fois que le fabricant a déterminé la fonctionnalité de base de son produit comportant des éléments numériques, il doit exécuter l'une des procédures d'évaluation de la conformité applicables. Il doit veiller à ce que le produit comportant des éléments numériques dans son ensemble satisfasse aux exigences essentielles, en tenant compte, le cas échéant, de la sécurité des composants ou des fonctionnalités qui y sont intégrés.

148. Une procédure d'évaluation de la conformité plus stricte, nécessitant l'intervention d'un tiers (sur la base des modules B + C, du module H ou des schémas de certification de cybersécurité), est obligatoire pour les produits importants comportant des éléments numériques qui relèvent de la classe II (à l'exception de ceux qui répondent aux critères de logiciels libres et ouverts, conformément à l'article 32, paragraphe 5) et pour les produits critiques comportant des éléments numériques ([24]). En revanche, les produits importants comportant des éléments numériques qui relèvent de la classe I (à l'exception de ceux qui répondent aux critères de logiciels libres et ouverts, conformément à l'article 32, paragraphe 5) ne sont soumis à une procédure d'évaluation de la conformité nécessitant l'intervention d'un tiers que si le fabricant n'a pas appliqué ou n'a appliqué qu'en partie des normes harmonisées pertinentes dont les références ont été publiées au *Journal officiel de l'Union européenne* (ci-après les «normes harmonisées»), des spécifications communes ou des schémas européens de certification de cybersécurité ayant débouché sur un niveau d'assurance au moins «substantiel» ([25]).

149. Par conséquent, pour qu'un produit important comportant des éléments numériques qui relève de la classe I puisse bénéficier de la procédure de contrôle interne, i) toutes les exigences applicables d'une norme harmonisée pertinente doivent être appliquées; et ii) cette norme doit couvrir au moins tous les risques de cybersécurité associés à la fonctionnalité de base de ce produit.

150. Le champ d'application du produit comportant des éléments numériques peut être plus large que ce qui est couvert par la norme harmonisée pertinente, et ces fonctions supplémentaires peuvent présenter des risques de cybersécurité différents ou supplémentaires. Le fabricant est toujours tenu de procéder à une évaluation des risques conformément à l'article 13, paragraphe 2, et devrait par conséquent vérifier si la mise en œuvre d'une norme harmonisée couvre tous les risques associés au produit comportant des éléments numériques. Lorsque la mise en œuvre de la norme ne couvre pas tous les risques, le fabricant devrait s'assurer par d'autres moyens que son produit comportant des éléments numériques est conforme aux exigences essentielles.

151. Par conséquent, si le fabricant d'un produit important comportant des éléments numériques qui relève de la classe I a appliqué une norme harmonisée pertinente qui couvre les risques associés à la fonctionnalité de base de ce produit, il peut décider de recourir à la procédure de contrôle interne pour démontrer la conformité de son produit. Dans le cadre de ses activités d'évaluation de la conformité, il sera toujours tenu de démontrer qu'il a traité tous les risques applicables à son produit comportant des éléments numériques. Dès lors, en cas de divergence entre ce qui est couvert par la norme harmonisée et le champ d'application du produit comportant des éléments numériques dans son ensemble, le fabricant devra toujours documenter les mesures supplémentaires qu'il a mises en place pour traiter ces risques.

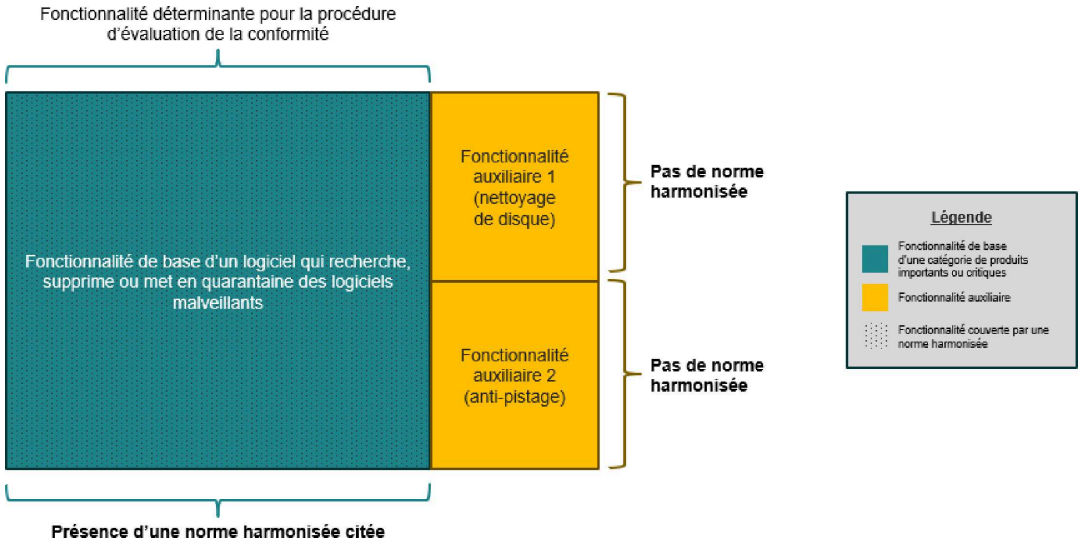
Exemple 62: un logiciel antivirus a la fonctionnalité de base d'un logiciel qui recherche, supprime ou met en quarantaine des logiciels malveillants, telle que décrite à l'annexe I, point 4, du règlement d'exécution (UE) 2025/2392. Ce produit comportant des éléments numériques inclut également des fonctions supplémentaires, à savoir une fonction de nettoyage de disque et une fonction anti-pistage protégeant l'utilisateur lorsqu'il navigue sur l'internet. Le fabricant procède à une évaluation des risques couvrant le produit comportant des éléments numériques dans son ensemble, y compris la fonctionnalité de base de l'antivirus, la fonction de nettoyage de disque et la fonction anti-pistage. Il applique une norme harmonisée couvrant les risques associés à la fonctionnalité de base de l'antivirus, ainsi que des mesures supplémentaires pour faire face aux risques découlant des fonctions supplémentaires. Il est autorisé à recourir à la procédure de contrôle interne pour son évaluation de la conformité couvrant le produit comportant des éléments numériques dans son ensemble, y compris la fonction de nettoyage de disque et la fonction anti-pistage.

([24]) Tel est également le cas lors du recours à un schéma européen de certification de cybersécurité ayant débouché sur un niveau d'assurance au moins «substantiel», étant donné que l'intervention d'un organisme de certification tiers est requise.

([25]) Par souci de concision, le reste de la présente section ne fait référence qu'aux normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne*. Toutefois, les mêmes orientations s'appliquent également aux spécifications communes adoptées conformément à l'article 27, paragraphe 2, et aux schémas européens de certification de cybersécurité précisés par la Commission au moyen d'actes délégués conformément à l'article 27, paragraphe 9.

Illustration 6

Diagramme montrant que c'est l'application d'une norme harmonisée citée couvrant uniquement la fonctionnalité de base qui détermine la procédure d'évaluation de la conformité applicable



152. Tel est également le cas lorsque le produit comportant des éléments numériques intègre une fonction supplémentaire qui est elle-même celle d'un autre produit important ou critique comportant des éléments numériques. En fait, c'est la fonctionnalité de base du produit comportant des éléments numériques dans son ensemble, et non la fonctionnalité des composants intégrés pris isolément, qui détermine si le produit comportant des éléments numériques appartient à la catégorie de produits importants ou critiques (et qui détermine donc le régime d'évaluation de la conformité applicable). Par exemple, si un produit comportant des éléments numériques a la fonctionnalité de base d'un produit important comportant des éléments numériques qui relève de la classe I, ce produit dans son ensemble est soumis au régime d'évaluation de la conformité applicable aux produits importants comportant des éléments numériques qui relèvent de la classe I, même s'il intègre un composant qui est lui-même un produit critique comportant des éléments numériques. Dans ce cas, lorsque le fabricant applique une norme harmonisée couvrant les risques associés à la fonctionnalité de base de ce produit, il est autorisé à recourir à la procédure de contrôle interne.

Exemple 63: un produit matériel comportant des éléments numériques a la fonctionnalité de base d'un routeur, telle que décrite à l'annexe I, point 12, du règlement d'exécution (UE) 2025/2392. Ce produit comportant des éléments numériques inclut également des fonctionnalités supplémentaires, dont des capacités de pare-feu, étant donné qu'il intègre un composant de pare-feu. Le fabricant procède à une évaluation des risques couvrant le produit comportant des éléments numériques dans son ensemble, y compris la fonctionnalité de base du routeur et la fonctionnalité de pare-feu. Il applique une norme harmonisée couvrant les risques associés à la fonctionnalité de base du routeur, ainsi que des mesures supplémentaires pour faire face aux risques découlant des fonctions supplémentaires. Par exemple, il peut appliquer la norme harmonisée relative aux pare-feu afin de couvrir les risques associés à la fonctionnalité de pare-feu. Il est autorisé à recourir à la procédure de contrôle interne pour son évaluation de la conformité couvrant le produit comportant des éléments numériques dans son ensemble, y compris la fonctionnalité de pare-feu.

6.3. Implications pour la présomption de conformité

153. En vertu de l'article 27, paragraphe 1, du règlement sur la cyberrésilience, les produits comportant des éléments numériques et les processus mis en place par le fabricant qui sont conformes à des normes harmonisées ou à des parties de normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne* sont présumés conformes aux exigences essentielles de ce règlement qui sont couvertes par ces normes ou parties de ces normes ([26]). L'article 27, paragraphe 5, étend cette même présomption de conformité aux produits comportant des éléments numériques et aux processus mis en place par le fabricant qui sont conformes aux spécifications

([26]) Comme indiqué clairement au point 4.1.2.2 du guide bleu, «[d]ans la législation d'harmonisation afférente aux risques, […] un fabricant, même lorsqu'il applique des normes harmonisées dont les références sont publiées au *Journal officiel de l'Union européenne*, est pleinement tenu d'évaluer l'ensemble des risques de son produit afin de déterminer les exigences essentielles (ou autres exigences) concernées. Au terme de cette évaluation, un fabricant peut alors choisir d'appliquer les spécifications techniques contenues dans les normes harmonisées dont les références sont publiées au *Journal officiel de l'Union européenne*, afin de mettre en place les "mesures de réduction des risques" fixées par les normes harmonisées».

communes adoptées par la Commission au moyen d'actes d'exécution, et l'article 27, paragraphe 8, établit la présomption de conformité pour les produits comportant des éléments numériques et les processus mis en place par le fabricant pour lesquels une déclaration de conformité de l'Union ou un certificat ont été délivrés dans le cadre d'un schéma européen de certification de cybersécurité adopté conformément au règlement (UE) 2019/881, si cela a été précisé au moyen d'actes délégués conformément à l'article 27, paragraphe 9 ([27]).

154. Par conséquent, lorsque le fabricant a appliqué une norme harmonisée dont les références ont été publiées au *Journal officiel de l'Union européenne*, il bénéficie d'une présomption de conformité pour les risques couverts par cette norme. Tel pourrait être le cas, par exemple, lorsque la norme harmonisée citée couvre tous les risques associés à la fonctionnalité de base d'un produit comportant des éléments numériques et qu'il n'existe pas de fonctionnalités supplémentaires présentant des risques de cybersécurité. Par exemple, il est présumé que la norme harmonisée relative aux routeurs couvre au moins les risques associés à la fonctionnalité de base de ces produits comportant des éléments numériques. Si un tel produit n'inclut pas de fonctionnalités supplémentaires ou s'il inclut des fonctionnalités supplémentaires ne présentant pas de risques non couverts par la norme, le produit comportant des éléments numériques peut bénéficier de la présomption de conformité.

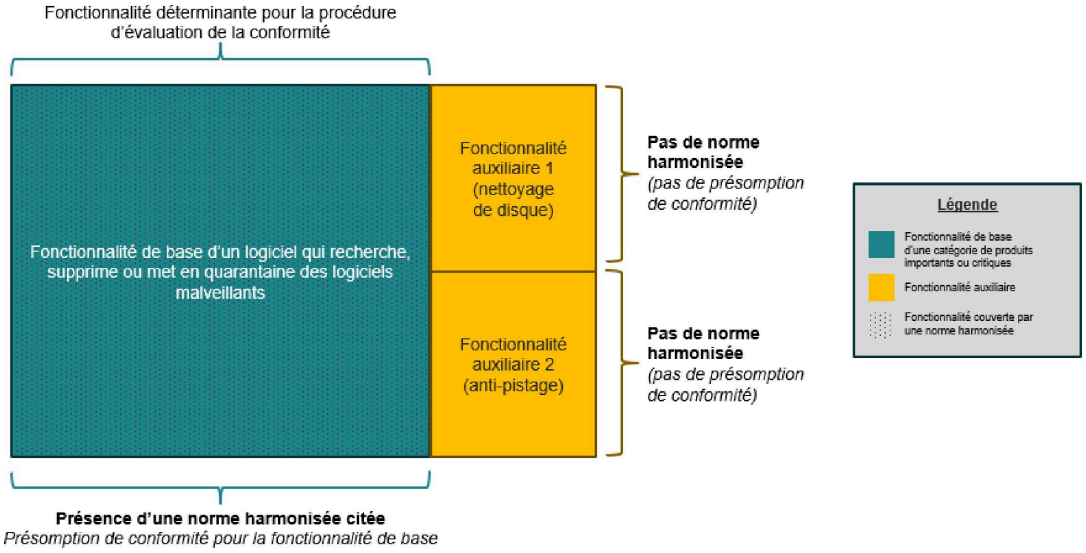
155. Dans les cas examinés aux points 151 et 152, le fabricant est autorisé à recourir à la procédure de contrôle interne parce que la norme harmonisée couvre les risques associés à la fonctionnalité de base du produit comportant des éléments numériques. Toutefois, le champ d'application des produits comportant des éléments numériques décrits dans ces exemples peut être plus large que ce qui est couvert par les normes harmonisées, et il peut exister des fonctionnalités supplémentaires susceptibles de présenter des risques de cybersécurité qui ne sont pas couverts par ces normes harmonisées. Ces produits comportant des éléments numériques ne peuvent donc pas bénéficier de la présomption de conformité pour ces fonctionnalités supplémentaires.

Exemple 64: un logiciel antivirus a la fonctionnalité de base d'un logiciel qui recherche, supprime ou met en quarantaine des logiciels malveillants et les risques associés à cette fonctionnalité de base sont couverts par la norme harmonisée. Ce produit comportant des éléments numériques inclut également des fonctionnalités supplémentaires, à savoir une fonction de nettoyage de disque et une fonctionnalité anti-pistage protégeant l'utilisateur lorsqu'il navigue sur l'internet, et les risques de ces fonctionnalités supplémentaires ne sont pas couverts par la norme harmonisée. S'il applique la norme harmonisée, le fabricant est autorisé à recourir à la procédure de contrôle interne pour son évaluation de la conformité. Il bénéficiera de la présomption de conformité pour les risques associés à la fonctionnalité de base de ce produit, mais pas pour les risques associés aux fonctionnalités supplémentaires.

([27]) Comme indiqué ci-dessus, par souci de concision, le reste de la présente section ne fait référence qu'aux normes harmonisées dont les références ont été publiées au *Journal officiel de l'Union européenne*. Toutefois, les mêmes orientations s'appliquent également aux spécifications communes et aux schémas européens de certification de cybersécurité.

Illustration 7

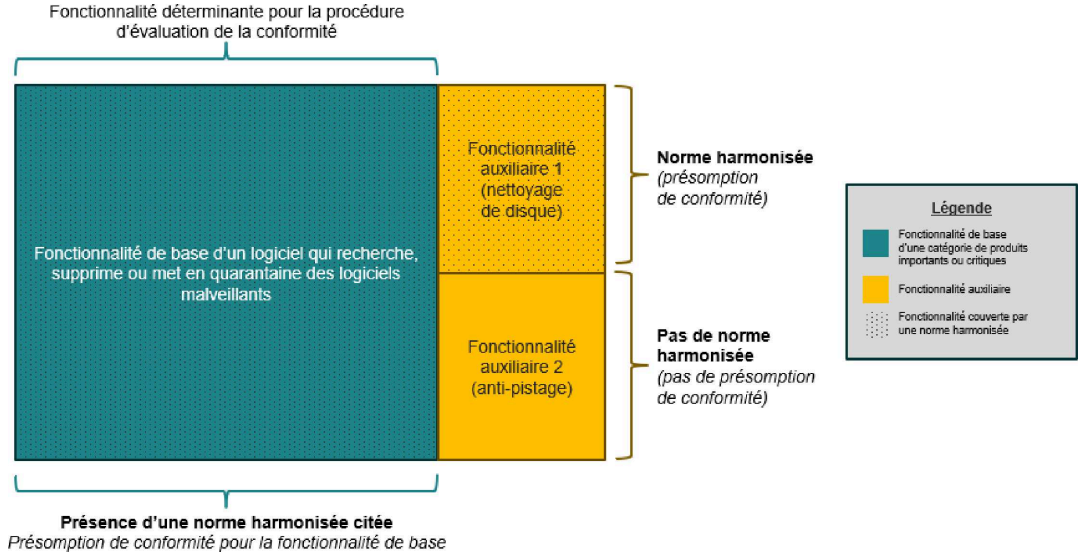
Diagramme montrant que l'application d'une norme harmonisée confère une présomption de conformité pour la fonctionnalité de base (puisque tous les risques associés à la fonctionnalité de base sont couverts par la norme), mais pas pour les fonctionnalités auxiliaires



Exemple 65: dans le même scénario que celui de l'exemple précédent, la norme harmonisée a désormais été mise à jour afin de couvrir également les risques associés à l'une des fonctionnalités supplémentaires, à savoir la fonction de nettoyage de disque, mais pas à l'autre (c'est-à-dire la fonction anti-pistage). S'il applique la norme harmonisée, le fabricant est autorisé à recourir à la procédure de contrôle interne pour son évaluation de la conformité. Il bénéficiera de la présomption de conformité pour les risques associés à la fonctionnalité de base de ce produit et à la fonctionnalité de nettoyage de disque, mais pas pour les risques liés à la fonctionnalité anti-pistage.

Illustration 8

Diagramme montrant que l'application d'une norme harmonisée confère une présomption de conformité pour la fonctionnalité de base et la fonctionnalité auxiliaire 1 (puisque tous les risques associés à ces deux fonctionnalités sont couverts par la norme), mais pas pour la fonctionnalité auxiliaire 2



7. ÉVALUATION DES RISQUES DE CYBERSÉCURITÉ ET INTÉGRATION DE PRODUITS COMPORTANT DES ÉLÉMENTS NUMÉRIQUES ET DE COMPOSANTS

7.1. Évaluation et traitement des risques de cybersécurité

156. L'évaluation des risques de cybersécurité prévue à l'article 13, paragraphe 2, du règlement sur la cyberrésilience impose aux fabricants de recenser les risques pertinents et d'évaluer les répercussions que ceux-ci peuvent avoir sur le produit comportant des éléments numériques. Les fabricants doivent également mettre en œuvre des mesures appropriées pour faire face à ces risques, conformément aux exigences essentielles de l'annexe I.

157. Dans le cadre de la gestion des risques organisationnels, les risques sont généralement évalués à l'aune de critères d'acceptation qui sont fonction des objectifs internes de l'organisation ou de son appétence au risque. En revanche, en vertu du règlement sur la cyberrésilience, il convient d'évaluer le risque de cybersécurité résiduel à la lumière de l'exigence selon laquelle le produit comportant des éléments numériques mis sur le marché doit garantir un niveau de cybersécurité approprié en fonction des risques, compte étant tenu de son utilisation prévue ou raisonnablement prévisible.

158. Par conséquent, la tolérance au risque interne du fabricant, sa stratégie commerciale ou de simples considérations de coût ne sont pas pertinentes au moment de déterminer si les risques ont été traités. Aux fins de l'article 13, paragraphes 2 et 3, les fabricants doivent être en mesure de déterminer si, lorsqu'ils mettent en œuvre les exigences essentielles énoncées à l'annexe I, partie I, ils traitent suffisamment les risques de cybersécurité recensés à la lumière de l'utilisation prévue, de l'utilisation raisonnablement prévisible et des conditions d'utilisation, y compris, le cas échéant, de l'environnement opérationnel (par exemple, les utilisateurs prévus du produit comportant des éléments numériques) et des actifs à protéger, compte tenu de la durée prévue d'utilisation du produit comportant des éléments numériques.

159. L'existence d'un risque de cybersécurité résiduel est une conclusion inévitable du processus d'évaluation et de traitement des risques. Il est en effet admis qu'il est impossible d'éliminer totalement les risques de cybersécurité dans la pratique. Toutefois, l'existence d'un risque résiduel ne signifie pas que tout risque puisse être accepté à la discrétion du fabricant. Un produit comportant des éléments numériques ne peut être mis sur le marché que si le fabricant a pris, dans le cadre de la mise en œuvre des exigences essentielles, des mesures appropriées qui traitent suffisamment les risques résiduels, compte étant tenu de l'utilisation prévue ou raisonnablement prévisible du produit comportant des éléments numériques.

160. En vertu de l'article 13, paragraphe 3, lorsque des risques de cybersécurité sont recensés, les fabricants sont tenus d'y faire face au moyen de mesures appropriées, y compris au niveau du produit. Selon les circonstances, ils peuvent, par exemple, réduire la surface d'attaque, mettre en place des garde-fous techniques, limiter ou adapter la fonctionnalité, ou définir de façon plus précise l'utilisation prévue du produit comportant des éléments numérique s. Ils peuvent également prendre des mesures pour inciter à une utilisation raisonnablement prévisible du produit comportant des éléments numériques, par exemple en communiquant sur les risques, en fournissant des orientations à l'utilisateur ou en concevant l'interface utilisateur de façon à orienter le comportement de l'utilisateur vers des modes d'utilisation sûrs.

161. Le règlement sur la cyberrésilience ne prévoit pas la possibilité de transférer aux utilisateurs ou à des tiers le risque de cybersécurité ou la responsabilité afin de compenser les lacunes de la conception d'un produit ou de justifier le fait qu'aucune mesure n'ait été prise pour faire face aux risques de cybersécurité. L'obligation de mettre sur le marché un produit comportant des éléments numériques sécurisé et de démontrer la conformité avec les exigences essentielles incombe toujours au fabricant.

162. Les informations et instructions destinées à l'utilisateur peuvent être utilisées pour soutenir le déploiement et l'exploitation sécurisés du produit comportant des éléments numériques, y compris lorsque le fabricant a choisi de limiter l'utilisation prévue de ce produit à des environnements de confiance, et pour informer les utilisateurs des risques résiduels d'une manière adaptée à la nature du produit comportant des éléments numériques et aux utilisateurs auxquels il est destiné.

Exemple 66: un fabricant met au point un capteur industriel destiné à être utilisé dans des environnements de confiance. Afin que le capteur puisse exécuter correctement sa fonctionnalité, le fabricant n'intègre pas dans le capteur lui-même des mesures de protection contre les attaques physiques. Pour atténuer les risques associés à l'utilisation du capteur qu'il a recensés dans le cadre de l'évaluation des risques, le fabricant limite l'utilisation prévue du capteur à des environnements de confiance, qui empêchent tout accès physique non autorisé au produit comportant des éléments numériques. Les informations et instructions destinées à l'utilisateur contiennent des informations claires sur ces restrictions imposées à l'utilisation du capteur, et ce d'une manière adaptée à la nature du produit comportant des éléments numériques et aux utilisateurs auxquels il est destiné.

Exemple 67: un fabricant développe une application logicielle à usage professionnel qui est destinée aux ordinateurs de bureau et appareils mobiles gérés par entreprise. Cette application traite des données sensibles et des contenus générés par les utilisateurs, qui sont stockés localement. Au cours de l'évaluation des risques, le fabricant détermine l'existence d'un risque d'accès non autorisé à ces données si celles-ci sont stockées dans un fichier texte sur l'appareil. Plutôt que de concevoir son propre mécanisme de chiffrement et de l'intégrer dans l'application elle-même, le fabricant choisit d'utiliser les fonctions de chiffrement et de gestion des clés fournies nativement par le système d'exploitation sur lequel l'application est destinée à fonctionner, étant donné que les services cryptographiques intégrés du système d'exploitation sont matures et régulièrement entretenus.

163. Lorsque, dans le cadre de l'évaluation des risques de cybersécurité, le fabricant recense des risques qu'il ne peut traiter suffisamment en prenant des mesures appropriées, il peut être amené, pour garantir la conformité avec le règlement sur la cyberrésilience, à devoir revoir la conception, la fonctionnalité ou l'utilisation prévue du produit comportant des éléments numériques. Les considérations liées uniquement au coût ou à la faisabilité commerciale ne constituent pas des motifs suffisants pour que ces risques restent sans réponse si cela empêche le produit comportant des éléments numériques de satisfaire aux exigences essentielles.

7.2. Obligation de concevoir, développer et fabriquer les produits comportant des éléments numériques de manière à garantir un niveau de cybersécurité approprié en fonction des risques

164. L'exigence essentielle de cybersécurité énoncée à l'annexe I, partie I, point 1), du règlement sur la cyberrésilience prévoit que les produits comportant des éléments numériques sont conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques.

165. Cette exigence essentielle vise à couvrir tous les risques de cybersécurité qui ont été détectés dans le cadre de l'évaluation des risques de cybersécurité, et notamment les risques de cybersécurité qui ne sont pas traités de manière appropriée dans le cadre de la mise en œuvre des exigences essentielles de l'annexe I, partie I, autres que celles qui sont énoncées au point 1). Cette exigence essentielle est différente de l'obligation légale de procéder à une évaluation des risques de cybersécurité, qui doit être effectuée en vertu de l'article 13, paragraphe 2.

166. Lorsque tous les risques de cybersécurité pertinents liés à un produit comportant des éléments numériques sont traités par la mise en œuvre de mesures adéquates répondant aux exigences essentielles applicables autres que celles qui sont énoncées au point 1), l'exigence essentielle visée à l'annexe I, partie I, point 1), est réputée remplie. À l'inverse, si l'évaluation des risques de cybersécurité met en évidence des risques supplémentaires qui ne sont pas totalement traités par de telles mesures, les fabricants sont tenus d'intégrer des mesures appropriées dans le produit comportant des éléments numériques pour faire face à ces risques, afin de respecter l'exigence essentielle énoncée à l'annexe I, partie I, point 1). Dans la pratique, dans la plupart des cas, la conformité avec les autres exigences essentielles entraînera vraisemblablement le respect de cette exigence.

7.3. Évaluation des risques et devoir de diligence raisonnable en ce qui concerne les dépendances externes et les composants intégrés

167. Le règlement sur la cyberrésilience fait peser sur les fabricants deux obligations distinctes, mais complémentaires, en ce qui concerne la gestion des risques de cybersécurité. Premièrement, l'article 13, paragraphe 2, impose aux fabricants de procéder à une évaluation des risques de cybersécurité pour le produit comportant des éléments numériques proprement dit. Deuxièmement, l'article 13, paragraphe 5, impose un devoir de diligence raisonnable en ce qui concerne les composants intégrés. Ensemble, ces deux obligations sont conçues pour garantir que le produit comportant des éléments numériques reste sécurisé, y compris lorsqu'il repose sur des solutions de traitement de données à distance, des services à distance ou des composants logiciels ou matériels fournis par des tiers.

168. L'évaluation des risques de cybersécurité suppose la détection et la gestion des risques pertinents susceptibles de se répercuter sur le produit comportant des éléments numériques, y compris les risques qui ne proviennent pas du produit lui-même, tels que les risques associés à des réseaux externes, à des facteurs environnementaux ou à d'autres aspects externes dont le produit comportant des éléments numériques dépend ou qui pourraient se répercuter sur celui-ci. Pour ces risques externes, le règlement sur la cyberrésilience n'impose pas aux fabricants de contrôler ou d'administrer l'environnement externe, mais il exige qu'ils recensent ces risques et les atténuent lors de la conception et du développement du produit comportant des éléments numériques lui-même. Les fabricants doivent à cette fin mettre en œuvre les exigences essentielles appropriées énoncées à l'annexe I, partie I, et, le cas échéant, fournir aux utilisateurs des informations et des instructions sur les risques associés à l'intégration ou au déploiement.

169. Par exemple, un fabricant peut détecter l'existence, pendant l'utilisation d'un produit comportant des éléments numériques, d'un risque d'accès non autorisé à des systèmes d'arrière-plan qui ne font pas partie de ce produit lui-même, qu'il est possible d'exploiter pour tenter d'envoyer des commandes malveillantes au produit comportant des éléments numériques. Ces systèmes d'arrière-plan, lorsqu'ils ne sont pas conçus et développés par le fabricant ou sous la responsabilité de ce dernier ou lorsqu'ils ne supportent pas l'une des fonctions du produit comportant des éléments numériques, ne constituent pas des solutions de traitement de données à distance et ne font donc pas partie du produit comportant des éléments numériques aux fins du règlement sur la cyberrésilience. Néanmoins, le règlement sur la cyberrésilience exige du fabricant qu'il traite les risques qui peuvent en résulter en prenant des mesures au niveau du produit, par exemple en exigeant une authentification cryptographique des commandes à distance, en vérifiant l'intégrité des modifications apportées à la configuration ou en générant des journaux ou des alertes pertinents pour la sécurité lorsque des comportements anormaux sont détectés. De même, lorsqu'un fabricant constate qu'un risque existe en cas d'indisponibilité du service externe, par exemple dans le scénario d'une panne d'électricité ou d'une défaillance de l'infrastructure, le règlement sur la cyberrésilience peut exiger que des mesures d'atténuation de ces risques de cybersécurité soient prises au niveau du produit, le fabricant devant par exemple veiller à ce que l'indisponibilité du service concerné ne se traduise pas par un mode de fonctionnement non sécurisé du produit comportant des éléments numériques. Le règlement sur la cyberrésilience réglemente la manière dont le produit comportant des éléments numériques doit répondre aux risques externes dans ces cas de figure, mais il n'impose aucune obligation en ce qui concerne l'organisation de l'infrastructure d'arrière-plan, son exploitation ou l'affectation de personnel, et ne considère pas non plus cette infrastructure comme faisant partie du produit comportant des éléments numériques.

170. Le devoir de diligence raisonnable s'applique en ce qui concerne les éléments qui font partie du produit comportant des éléments numériques lui-même, en particulier les composants logiciels ou matériels intégrés fournis par des tiers. Les fabricants sont tenus de prendre des mesures appropriées pour veiller à ce que ces composants ne compromettent pas la conformité du produit comportant des éléments numériques avec les exigences essentielles. Il est indispensable, à cet effet, qu'ils déterminent ce qui est exigé des composants du produit comportant des éléments numériques pour que les objectifs en matière de cybersécurité soient respectés et qu'ils vérifient, eu égard aux risques, que ces composants répondent aux besoins du produit, comme également indiqué au considérant 34.

171. Conformément à son évaluation des risques de cybersécurité, le fabricant doit déterminer les exigences auxquelles le composant intégré devrait satisfaire. Par exemple, si le produit comportant des éléments numériques repose sur des fonctions cryptographiques, des communications sécurisées ou des mécanismes de mise à jour fournis par un composant, le fabricant devra, dans le cadre de son devoir de diligence raisonnable, recenser ces besoins et vérifier que le composant y satisfait. Il pourra se fonder sur des documents obtenus auprès du fabricant du composant, tels que les spécifications techniques, la documentation de sécurité ou la documentation pertinente en matière de conformité ou d'assurance. Le cas échéant, le fabricant peut également effectuer des essais pour vérifier que les composants concernés exécutent correctement les fonctions dont il a besoin. Bien que le devoir de diligence raisonnable constitue une obligation légale distincte, il soutient et sous-tend la capacité du fabricant à démontrer la conformité avec les exigences essentielles pour le produit comportant des éléments numériques dans son ensemble.

172. Aux fins de l'évaluation des risques pour le produit comportant des éléments numériques dans son ensemble, le fabricant doit tenir compte des éléments extérieurs au produit, tels que les éléments environnementaux, l'infrastructure externe ou les autres systèmes ou réseaux potentiels, dans le cadre de son évaluation des risques de cybersécurité et, le cas échéant, traiter ces risques en prenant des mesures au niveau du produit afin de garantir la conformité du produit comportant des éléments numériques avec les exigences essentielles. Les composants qui sont intégrés physiquement ou logiquement dans le produit comportant des éléments numériques mais qui proviennent d'un tiers doivent également être examinés dans le cadre de l'évaluation des risques. Toutefois, aux fins de sa mise en conformité, le fabricant devrait traiter ces composants comme des composants obtenus à l'extérieur dont les propriétés sont à vérifier dans le cadre du devoir de diligence raisonnable qui s'applique au moment de l'intégration, puisqu'il est possible que le fabricant intègre ces composants sans revoir leur conception ou leur développement.

173. La même logique vaut pour le développement et l'intégration de composants. Lorsque le fabricant développe lui-même des fonctionnalités, il doit directement mettre en œuvre les exigences essentielles. S'il intègre des composants développés par des tiers, il doit veiller, dans le cadre de son devoir de diligence raisonnable, à ce que ces composants puissent être utilisés de manière à garantir la conformité du produit comportant des éléments numériques dans son ensemble. Dans les deux cas, l'objectif reste le même: le produit comportant des éléments numériques tel qu'il est mis sur le marché doit atteindre un niveau de cybersécurité approprié conformément aux exigences du règlement sur la cyberrésilience, compte tenu des risques recensés lors de l'évaluation des risques de cybersécurité.

7.4. **Réutilisation des évaluations des risques et de la documentation de conformité pour les familles de produits comportant des éléments numériques**

174. Les fabricants peuvent mettre sur le marché des produits comportant des éléments numériques qui se ressemblent, par exemple en déclinant en des variantes, configurations ou modèles différents une même famille de produits. Lorsque ces produits comportant des éléments numériques partagent la même architecture, la même conception pertinente pour la sécurité et la même utilisation prévue et sont exposés aux mêmes risques de cybersécurité, le règlement sur la cyberrésilience n'exige pas des fabricants qu'ils traitent chaque variante comme un produit comportant des éléments numériques entièrement distinct aux fins de l'évaluation des risques et de l'évaluation de la conformité.

175. Dans de tels cas, pour autant que toutes les variantes concernées soient couvertes de manière adéquate au niveau des risques pertinents et des exigences essentielles applicables, les fabricants peuvent s'appuyer sur: i) une seule et même évaluation des risques de cybersécurité effectuée conformément à l'article 13, paragraphe 2, du règlement sur la cyberrésilience; ii) une seule et même documentation technique; et iii) une seule et même procédure d'évaluation de la conformité. Ils peuvent également se prévaloir d'une seule et même déclaration UE de conformité pour le groupe de produits comportant des éléments numériques, pour autant que cette déclaration désigne clairement les variantes de produit auxquelles elle s'applique.

176. Ce qui est déterminant, c'est de savoir si les différences entre les variantes sont importantes du point de vue de la cybersécurité. Les variations qui n'ont pas d'incidence sur les propriétés du produit comportant des éléments numériques en matière de cybersécurité, telles que les différences de couleur, de facteur de forme ou de taille de mémoire ou les différences ayant trait à d'autres caractéristiques non liées à la sécurité, ne nécessitent pas d'évaluations distinctes des risques ou de la conformité. À l'inverse, dans certains cas, les variantes peuvent présenter des différences qui influent sur la mise en œuvre des exigences essentielles; tel est le cas, par exemple, lorsque les différences portent sur les interfaces de communication, les piles technologiques, les mécanismes de mise à jour ou les solutions de connectivité à distance. Il convient, dans ce cas, de tenir compte de ces différences dans l'évaluation des risques et, le cas échéant, dans l'évaluation de la conformité et dans la documentation technique.

177. Il incombe toujours aux fabricants de veiller à ce que l'évaluation des risques et la documentation y afférente reflètent fidèlement les produits comportant des éléments numériques mis sur le marché. Lorsqu'une nouvelle variante crée de nouveaux risques de cybersécurité ou se répercute sur la mise en œuvre des exigences essentielles, l'évaluation des risques et la documentation de conformité existantes doivent être mises à jour en conséquence. Le recours à une seule et même évaluation de la conformité n'est possible que si les produits comportant des éléments numériques ne présentent pas de différences en ce qui concerne leurs propriétés en matière de cybersécurité.

8. **TRAITEMENT DE DONNÉES À DISTANCE**

178. L'article 3, point 1), du règlement sur la cyberrésilience définit un «produit comportant des éléments numériques» comme étant «un produit logiciel ou matériel et ses solutions de traitement de données à distance, y compris les composants logiciels ou matériels mis sur le marché séparément». Dans ce contexte, le fabricant doit considérer le produit comportant des éléments numériques dans son ensemble, y compris ses solutions de traitement de données à distance. Par exemple, lorsqu'il démontre que son produit comportant des éléments numériques est conforme aux exigences essentielles énoncées à l'annexe I, le fabricant doit tenir compte des solutions de traitement de données à distance, et ce dès l'évaluation des risques (article 13, paragraphe 2). Il en va de même dans le contexte des obligations applicables tout au long du cycle de vie, telles que l'obligation de signaler les vulnérabilités activement exploitées et les incidents graves (article 14).

179. L'objectif des présentes orientations est de donner aux fabricants des explications supplémentaires afin de leur permettre d'établir si leur produit comportant des éléments numériques contient des solutions de traitement de données à distance, telles que définies dans le règlement sur la cyberrésilience, et de déterminer comment remplir leurs obligations de conformité à cet égard. Après une analyse initiale des définitions et des considérants énoncés dans le règlement sur la cyberrésilience, ces orientations présenteront des questions que les fabricants pourront se poser en vue de déterminer si leur produit comportant des éléments numériques contient des solutions de traitement de données à distance (voir section *8.1 Qu'est-ce qui est considéré comme constituant une solution de traitement de données à distance* pour un produit comportant des éléments numériques?). Elles développeront ensuite les implications techniques des solutions de traitement de données à distance et la manière d'évaluer la conformité avec le règlement sur la cyberrésilience (voir section *8.2 Implications pratiques et techniques des solutions de traitement de données à distance et du recours à des solutions tierces*).

180. En fait, à l'article 3, point 2), la notion de «traitement de données à distance» est définie comme étant «tout traitement de données à distance pour lequel le logiciel est conçu et développé par le fabricant ou sous la responsabilité de ce dernier, et dont l'absence empêcherait le produit comportant des éléments numériques d'exécuter une de ses fonctions». Les solutions de traitement de données à distance sont donc définies comme étant les éléments logiciels [«la partie d'un système d'information électronique qui consiste en un code informatique», aux termes de l'article 3, point 4)] du traitement de données à distance. Cette définition n'a pas vocation à couvrir les éléments matériels d'un produit comportant des éléments numériques qui sont susceptibles d'être utilisés pour le traitement de données à distance.

181. Les considérants 11 et 12 contiennent de plus amples explications sur la manière d'interpréter cette notion. Le considérant 11 précise que l'objectif de l'inclusion des solutions de traitement de données à distance est de garantir que «les produits concernés sont sécurisés dans leur intégralité et de façon adéquate par leur fabricant, que les données soient traitées ou stockées localement, sur l'appareil de l'utilisateur, ou à distance, par le fabricant». Il précise également que, «[p]ar conséquent, les exigences relatives aux solutions de traitement de données à distance qui relèvent du champ d'application du présent règlement ne comportent pas de mesures techniques, opérationnelles ou organisationnelles visant à gérer les risques qui pèsent sur la sécurité des réseaux et systèmes d'information d'un fabricant dans leur ensemble».

182. Dès lors, il ressort du considérant 11 que les exigences du règlement sur la cyberrésilience ne visent pas à couvrir l'ensemble de l'infrastructure informatique d'une organisation, mais uniquement les composants logiciels qui permettent l'exécution de la solution de traitement de données. Par exemple, ne devraient pas être considérés comme constituant des solutions de traitement de données à distance les systèmes internes concernant la gestion des ressources humaines du fabricant, des fiches de paie et des relations avec la clientèle, les chaînes d'intégration continue/de déploiement continu ou la distribution des mises à jour de sécurité aux emplacements périphériques. De même, les systèmes liés aux activités d'audit et d'essai, tels que les tests d'intrusion, la chasse aux menaces et les simulations par équipes rouges, ne font pas partie d'un produit comportant des éléments numériques tel que couvert par le règlement sur la cyberrésilience. Il importe de signaler que, si l'obligation de soumettre régulièrement les produits comportant des éléments numériques à des tests et examens de sécurité efficaces est une exigence essentielle énoncée à l'annexe I, partie II, point 3), du règlement sur la cyberrésilience, cela ne signifie pas que ces activités doivent être considérées comme constituant des solutions de traitement de données à distance pour le produit comportant des éléments numériques.

183. Le considérant 12 est axé sur les services en nuage et détaille les circonstances dans lesquelles ces services pourraient être considérés comme constituant des solutions de traitement de données à distance. Il s'achève en rappelant que les services d'informatique en nuage et les modèles de services en nuage relèvent du champ d'application de la directive (UE) 2022/2555 (SRI 2) ([28]), qui établit des exigences en matière de gestion des risques de cybersécurité pour les fournisseurs de services d'informatique en nuage. Ces exigences sont précisées davantage dans le règlement d'exécution (UE) 2024/2690 de la Commission ([29]).

8.1. Qu'est-ce qui est considéré comme constituant une solution de traitement de données à distance pour un produit comportant des éléments numériques?

184. La définition du traitement de données à distance énoncée à l'article 3, point 2), repose donc sur trois éléments: i) le traitement de données est effectué «à distance»; ii) l'absence du traitement de données empêcherait le produit comportant des éléments numériques d'exécuter une de ses fonctions; et iii) le logiciel est conçu et développé par le fabricant ou sous la responsabilité de ce dernier. Les trois sous-sections suivantes donnent plus de détails sur chacun de ces éléments.

([28]) Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) (JO L 333 du 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Règlement d'exécution (UE) 2024/2690 de la Commission du 17 octobre 2024 établissant des règles relatives à l'application de la directive (UE) 2022/2555 pour ce qui est des exigences techniques et méthodologiques liées aux mesures de gestion des risques en matière de cybersécurité et précisant plus en détail les cas dans lesquels un incident est considéré comme important, en ce qui concerne les fournisseurs de services DNS, les registres des noms de domaine de premier niveau, les fournisseurs de services d'informatique en nuage, les fournisseurs de services de centres de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, ainsi que les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne et de plateformes de services de réseaux sociaux, et les prestataires de services de confiance (JO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *L'expression «à distance»*

185. La présence d'un traitement de données effectué «à distance» [aux termes de l'article 3, point 2)] est pertinente, mais pas suffisante, pour déterminer si un produit comportant des éléments numériques contient des solutions de traitement de données à distance. Au demeurant, compte tenu de la diversité des solutions susceptibles de relever de cette notion, il n'est pas possible de définir de façon exhaustive l'expression «à distance». Le fabricant doit procéder à une évaluation au cas par cas.

186. Le considérant 11 du règlement sur la cyberrésilience mentionne les données traitées ou stockées «à distance, par le fabricant» par opposition aux données traitées ou stockées «localement, sur l'appareil de l'utilisateur». Généralement, le traitement de données à distance est effectué en dehors de l'environnement utilisateur d'un produit comportant des éléments numériques ou de l'environnement opérationnel d'une organisation (pour un utilisateur professionnel). Néanmoins, le traitement peut également avoir lieu à proximité de l'appareil («en périphérie»). La transmission des données peut se faire via une connexion filaire (câble Ethernet, par exemple) ou une connexion sans fil (Wi-Fi ou Bluetooth, par exemple). L'informatique en nuage, y compris l'informatique en périphérie, est un exemple typique de traitement de données effectué «à distance». Par exemple, dans le cas d'une fonction en nuage à laquelle l'utilisateur accède à partir d'une application mobile, une partie du traitement des données a lieu dans le nuage, en dehors de l'environnement de l'utilisateur.

187. Il importe de signaler que les solutions de traitement de données à distance ne sont pas nécessairement exploitées sur des infrastructures en nuage tierces. Un traitement de données à distance effectué sur des serveurs locaux installés sur le site du fabricant peut également constituer une solution de traitement de données à distance. Autrement dit, une solution exploitée sur site et dans un nuage privé est tout aussi susceptible de constituer une solution de traitement de données à distance qu'une solution exploitée dans un nuage public et hors site.

188. Les deux questions déterminantes et cumulatives pour établir qu'un traitement de données constitue une solution de traitement de données à distance couverte par le règlement sur la cyberrésilience sont exposées ci-après, aux sections *8.1.2* et *8.2*. En cas de réponse affirmative à ces deux questions, le traitement de données à distance constitue une solution de traitement de données à distance.

8.1.2. *L'absence du traitement de données empêcherait-elle le produit comportant des éléments numériques d'exécuter une de ses fonctions?*

189. Comme indiqué dans la définition du «traitement de données à distance» figurant à l'article 3, point 2), pour qu'un traitement de données à distance constitue une solution de traitement de données à distance, son absence devrait empêcher le produit comportant des éléments numériques d'exécuter une de ses fonctions. La notion de «fonctions» présente dans cette définition ne se limite pas à la «fonctionnalité de base» ou à l'«utilisation prévue» du produit comportant des éléments numériques, étant donné que le règlement sur la cyberrésilience ne prévoit pas de telle restriction. Les fonctions qui relèvent du champ d'application du règlement sur la cyberrésilience sont à la fois les fonctions qui jouent un rôle direct dans l'exécution de l'utilisation prévue du produit comportant des éléments numériques telle qu'elle est vécue par les utilisateurs et les fonctions qui supportent la performance globale du produit.

190. Exemples de fonctions pour lesquelles un traitement de données à distance peut avoir lieu et dont l'absence empêcherait un produit comportant des éléments numériques d'exécuter une de ses fonctions: i) l'envoi de commandes à un appareil; ii) la synchronisation des fichiers; iii) l'enrôlement de l'utilisateur; iv) la configuration (personnalisation du produit comportant des éléments numériques); v) la distribution automatisée des mises à jour, y compris la mise à jour des fonctionnalités et les correctifs de sécurité; vi) la gestion des identités et des accès.

191. Dans certains cas, l'utilisateur peut exécuter une fonction aussi bien à distance que manuellement (il peut, par exemple, allumer une ampoule à l'aide d'une application ou manuellement). L'existence de cette possibilité n'exclut pas la qualification en tant que solution de traitement de données à distance du traitement de données associé à l'exécution à distance de la fonction. L'exécution de cette fonction à distance est également considérée comme faisant partie des fonctions proposées par le produit comportant des éléments numériques.

192. En revanche, lorsque l'absence d'un certain traitement de données n'empêche pas le produit comportant des éléments numériques d'exécuter une de ses fonctions, ce traitement n'est pas considéré comme constituant une solution de traitement de données à distance au sens du règlement sur la cyberrésilience. Tel est le cas, par exemple, de l'analyse à distance de données de télémétrie collectées uniquement à des fins statistiques ou pour le futur développement de produits.

193. Néanmoins, même lorsque le traitement de données ne supporte pas une fonction d'un produit comportant des éléments numériques, les fabricants peuvent être amenés, dans le cadre de leur évaluation des risques de cybersécurité, à devoir examiner si ces composants de traitement à distance créent des risques pour le produit comportant des éléments numériques (par exemple, à la lumière de l'environnement opérationnel du produit) et atténuer ces risques en conséquence (par exemple, en prenant des mesures d'atténuation au niveau du produit).

194. Les sites internet représentent un cas particulier qui mérite des précisions supplémentaires, comme expliqué également à la *section 2.1 Mise sur le marché*. Ces sites ne constituent pas des solutions de traitement de données à distance s'ils ne supportent pas une fonction d'un produit comportant des éléments numériques, comme expliqué au considérant 11 du règlement sur la cyberrésilience. Il ne suffit pas qu'un site internet contienne des informations sur un produit comportant des éléments numériques pour qu'il soit considéré comme constituant une solution de traitement de données à distance, même si le produit redirige vers ce site internet. Par exemple, le fait de rediriger les utilisateurs vers une page internet externe qui contient des informations et instructions destinées à l'utilisateur ne constitue pas une solution de traitement de données à distance. En revanche, un site internet peut constituer une solution de traitement de données à distance s'il permet ou supporte une fonction d'un produit comportant des éléments numériques. Par exemple, un portail d'authentification qui délivre des identifiants ou des jetons nécessaires au fonctionnement d'un produit comportant des éléments numériques serait considéré comme constituant une solution de traitement de données à distance (pour autant que les autres critères de la définition soient également remplis).

8.1.3. *Le logiciel a-t-il été conçu et développé par le fabricant ou sous la responsabilité de ce dernier?*

195. La définition du «traitement de données à distance» figurant à l'article 3, point 2), du règlement sur la cyberrésilience précise en outre que le logiciel du traitement de données à distance doit être conçu et développé par le fabricant ou sous la responsabilité de ce dernier. Un logiciel de traitement de données à distance entièrement développé et conçu par le fabricant (en interne) constituerait naturellement une solution de traitement de données à distance. Tel serait également le cas si le fabricant s'appuyait sur un fournisseur de services tiers pour le développement et la conception d'une solution (c'est-à-dire «sous [s]a responsabilité»). L'expression «sous la responsabilité [du fabricant]» fait référence aux solutions de traitement à distance qui sont développées sur mesure pour le fabricant. Dans un tel cas, le fabricant ne se contente pas d'acquérir une licence pour l'utilisation d'un produit existant comportant des éléments numériques, d'un service qu'un fournisseur de services propose à ses clients, ou de versions légèrement modifiées de ceux-ci. L'expression «sous la responsabilité [du fabricant]» signifie que le logiciel est développé uniquement par le fabricant ou en son nom, sur la base de conceptions et de spécifications fournies par celui-ci.

196. Aux fins de l'interprétation de la notion de «solutions de traitement de données à distance», le point de savoir «qui exploite la solution» n'est pas déterminant, étant donné que la définition énoncée dans le règlement sur la cyberrésilience ne fait référence qu'à la conception et au développement des solutions de traitement de données à distance. Cela est conforme à l'approche suivie dans le règlement sur la cyberrésilience, qui impose des exigences et des obligations aux fabricants, mais qui ne régit pas le fonctionnement du produit comportant des éléments numériques. Si un fabricant conçoit et développe des solutions qui sont ensuite exploitées par un tiers, il reste responsable de la conformité du produit comportant des éléments numériques qu'il met sur le marché avec les exigences essentielles du règlement sur la cyberrésilience.

197. Il est nécessaire d'opérer une distinction entre le scénario dans lequel la conception et le développement sont réalisés par les fabricants (ou sous leur responsabilité) et le scénario dans lequel il est fait recours à des solutions tierces qui ne sont pas conçues et développées par les fabricants (ou sous leur responsabilité). À titre d'exemple, il est utile de considérer les modèles de services en nuage les plus courants, également cités au considérant 12 du règlement sur la cyberrésilience – à savoir les logiciels service (SaaS), les plateformes services (PaaS) et les infrastructures services (IaaS) –, qui permettent différents degrés de contrôle de la part des utilisateurs.

198. Dans le cas d'une solution IaaS tierce, le fabricant ne gère ni ne contrôle les ressources physiques et virtuelles sous-jacentes (telles que le matériel sous-jacent et l'hyperviseur du fournisseur de services en nuage), mais est en mesure de déployer et d'exécuter des logiciels arbitraires utilisant ces ressources, tels que des systèmes d'exploitation et des applications. Ces logiciels sont conçus et développés par le fabricant ou sous la responsabilité de ce dernier, et peuvent donc être considérés comme constituant une solution de traitement de données à distance (s'ils répondent aux autres éléments de la définition).

199. Dans le cas d'une solution PaaS tierce, le fabricant déploie sa propre application (qu'il a créée ou acquise) à l'aide de langages de programmation et d'environnements d'exécution fournis par le fournisseur de services en nuage et intègre l'application dans son produit comportant des éléments numériques. Le fabricant exerce un contrôle sur cette application et, éventuellement, sur les paramètres de configuration de l'environnement d'exécution. L'application est donc conçue et développée par le fabricant ou sous la responsabilité de ce dernier, et peut donc être considérée comme constituant une solution de traitement de données à distance (si elle répond aux autres éléments de la définition).

200. Dans le cas d'une solution SaaS tierce, le fournisseur du SaaS procure au fabricant une application entièrement développée destinée à être intégrée dans le produit comportant des éléments numériques du fabricant. La capacité du fabricant à gérer les paramètres de configuration de l'application propres à l'utilisateur est limitée. L'application n'est donc pas conçue et développée par le fabricant ou sous la responsabilité de ce dernier.

201. Néanmoins, lorsque certains éléments ne constituent pas des solutions de traitement de données à distance (par exemple, l'hyperviseur dans le cas d'une IaaS tierce, le système d'exploitation dans le cas d'une solution PaaS tierce, ou l'application SaaS tierce), mais sont intégrés dans le produit comportant des éléments numériques d'une manière qui a une incidence sur sa sécurité, il convient de considérer ces solutions comme comparables à des composants tiers. Le fabricant est tenu de recenser et d'évaluer les risques liés à l'intégration de ces éléments et d'y remédier lorsqu'il met en œuvre les exigences essentielles pour le produit comportant des éléments numériques lui-même. Il peut, le cas échéant, s'appuyer sur les fonctions de sécurité mises à disposition par le fournisseur de services en nuage dans le cadre de son modèle de responsabilité partagée, qui permet au fabricant d'utiliser ou de configurer ces fonctions pour faire face aux risques recensés. En outre, le fabricant est censé exercer une obligation semblable au devoir de diligence raisonnable prévu à l'article 13, paragraphe 5, en ce qui concerne la sécurité de ces composants, d'une manière proportionnée au risque que représente la solution à distance pour la sécurité du produit comportant des éléments numériques.

202. En résumé:

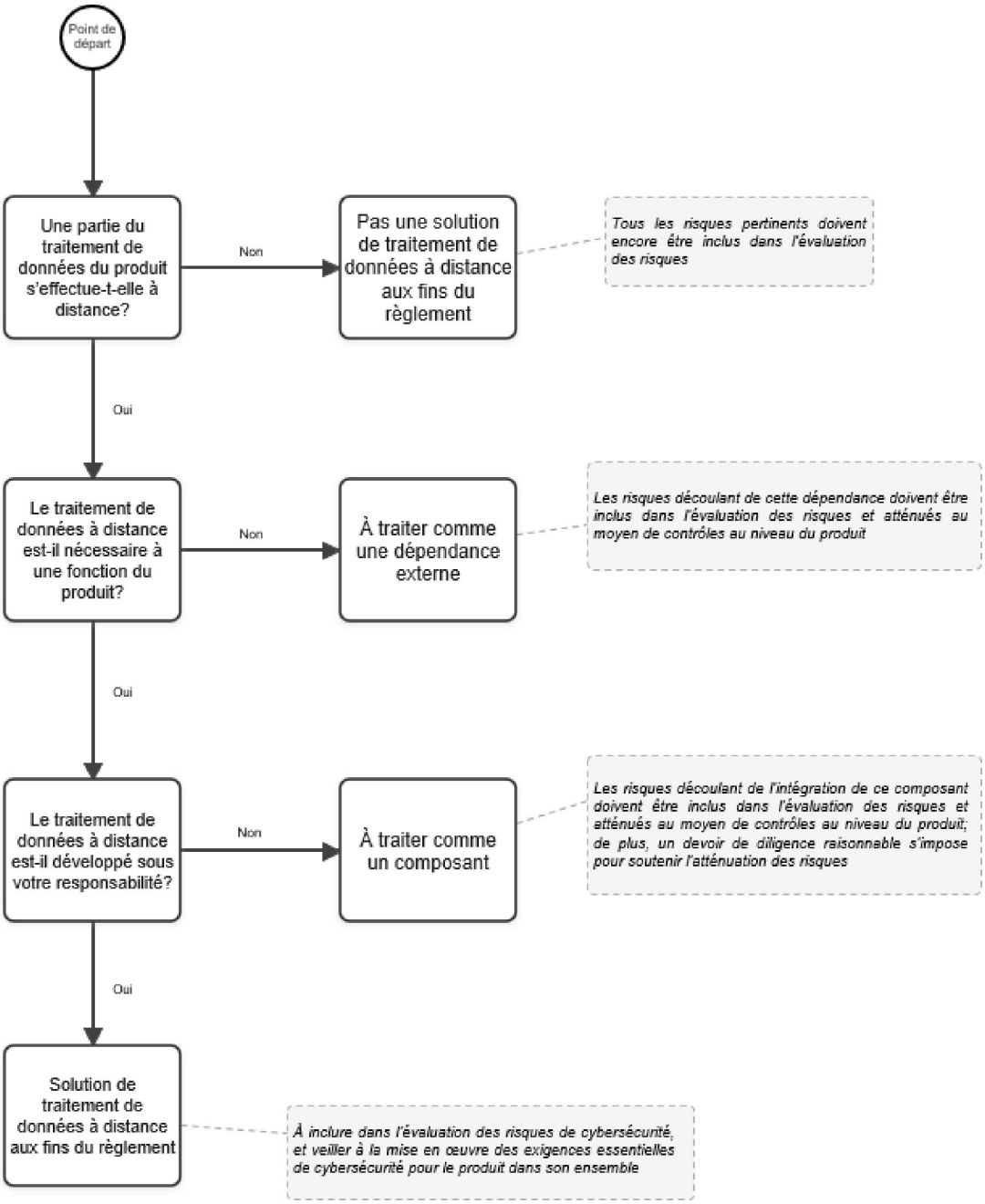
a) pour qu'un traitement de données constitue une solution de traitement de données à distance, la réponse aux deux questions posées aux sections *8.1.2 L'absence du traitement de données empêcherait-elle le produit comportant des éléments numériques d'exécuter une de ses fonctions?* et *8.1.3 Le logiciel a-t-il été conçu et développé par le fabricant ou sous la responsabilité de* ce dernier? doit être affirmative;

b) si la réponse à la question faisant l'objet de la section *8.1.2 L'absence du traitement de données empêcherait-elle le produit comportant des éléments numériques d'exécuter une de ses fonctions?* est négative, les fabricants devraient évaluer les risques découlant de l'existence du traitement de données dans le cadre de leur évaluation des risques;

c) si la réponse à la question faisant l'objet de la section *8.1.2 L'absence du traitement de données empêcherait-elle le produit comportant des éléments numériques d'exécuter une de ses fonctions?* est affirmative mais que la réponse à la question faisant l'objet de la section *8.1.3 Le logiciel a-t-il été conçu et développé par le fabricant ou sous la responsabilité de* ce dernier? est négative, les fabricants devraient traiter la solution tierce comme un composant. Dans le cadre de l'évaluation des risques, les fabricants devraient évaluer les risques découlant de l'intégration de cette solution et les atténuer en conséquence. En outre, les fabricants devraient faire preuve de diligence raisonnable.

Illustration 9

Diagramme de flux permettant de déterminer si un produit comportant des éléments numériques contient des solutions de traitement de données à distance



8.2. Implications pratiques et techniques des solutions de traitement de données à distance et du recours à des solutions tierces

203. Le règlement sur la cyberrésilience suit une approche fondée sur les risques, qu'il consacre à l'article 13, paragraphes 2 et 3, ainsi qu'à la première exigence essentielle de l'annexe I, partie I, selon laquelle «[l]es produits comportant des éléments numériques sont conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques». Par conséquent, une approche fondée sur les risques devrait être envisagée lors de l'application des exigences du règlement sur la cyberrésilience aux solutions de traitement de données à distance et lors du traitement des risques découlant de services tiers intégrés dans le produit comportant des éléments numériques.

204. Tout d'abord, les fabricants devraient i) indiquer dans la documentation technique que leur produit comportant des éléments numériques contient des solutions de traitement de données à distance ou s'appuie sur des solutions à distance tierces et ii) décrire ces solutions. Si une même solution de traitement de données à distance supporte plusieurs produits comportant des éléments numériques, cette solution de traitement de données à distance doit être déclarée dans la documentation technique de chaque produit. La documentation relative à une solution de traitement de données à distance qui supporte plusieurs produits comportant des éléments numériques peut être réutilisée d'une évaluation de la conformité d'un produit à une autre.

205. Comme indiqué au considérant 11, les solutions de traitement de données à distance qui font partie du produit comportant des éléments numériques et qui sont donc soumises à l'évaluation de la conformité de ce produit devraient être limitées aux modules logiciels qui sont responsables de la fonctionnalité du produit comportant des éléments numériques et aux interfaces que ces modules utilisent pour interagir avec des services externes. Les autres systèmes d'arrière-plan qui effectuent un traitement ultérieur et avec lesquels le produit comportant des éléments numériques n'interagit pas directement ne sont pas considérés comme constituant des solutions de traitement de données à distance.

206. Néanmoins, ces systèmes d'arrière-plan demeurent des dépendances externes qu'il y a lieu d'évaluer dans le cadre de l'évaluation des risques de cybersécurité et d'atténuer au moyen de mesures prises au niveau du produit. En fait, dans le cadre de son évaluation des risques, le fabricant devrait tenir compte: i) des risques liés aux solutions de traitement de données à distance; ii) des risques liés à l'utilisation de solutions à distance tierces (comparables à des composants tiers); et iii) des risques liés à l'environnement du produit (par exemple, le matériel sous-jacent). Afin d'atténuer ces risques, les fabricants devraient mettre en œuvre des contrôles de sécurité dans le produit comportant des éléments numériques lui-même.

207. En outre, dans le cadre de l'évaluation de la conformité et/ou du respect du devoir de diligence raisonnable lié aux services à distance tiers, les artefacts d'assurance énumérés ci-après à titre non exhaustif peuvent être réutilisés à l'appui de l'évaluation du fabricant:

a) la preuve du respect des obligations prévues par le règlement d'exécution (UE) 2024/2690 de la Commission;

b) la preuve du respect des obligations prévues par le règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier;

c) une déclaration de conformité ou un certificat délivré dans le cadre d'un schéma européen de certification de cybersécurité [adopté conformément au règlement (UE) 2019/881 (règlement sur la cybersécurité)];

d) la preuve de la conformité avec la norme ISO/IEC 27017:2015 ou ISO/IEC 27001:2022.

208. Enfin, dans leurs interactions avec les fournisseurs de services à distance tiers, les fabricants doivent mettre en œuvre les mesures de sécurité les plus appropriées sur la base de leur évaluation des risques (et, le cas échéant, prises en charge par le modèle de responsabilité partagée du fournisseur). Ces mesures d'atténuation devraient comprendre des contrôles de sécurité pour leurs produits comportant des éléments numériques et une vérification des mesures de sécurité fournies par les fournisseurs tiers eux-mêmes (devoir de diligence raisonnable). Un outil permettant d'atténuer ces risques peut consister à intégrer des garanties de sécurité dans les accords de niveau de service conclus avec les fournisseurs tiers, y compris des garanties que ces fournisseurs gèrent correctement les vulnérabilités. Une modification majeure des solutions fournies par les fournisseurs de services à distance tiers ne devrait pas être considérée comme une modification substantielle du produit comportant des éléments numérique s, étant donné que ces éléments ne relèvent pas de la responsabilité du fabricant. Toutefois, dans le cadre de leur devoir de diligence raisonnable et afin d'atténuer correctement les risques découlant du recours à des fournisseurs tiers, les fabricants sont encouragés à veiller à ce que leurs fournisseurs tiers de services en nuage les tiennent correctement informés des modifications qu'ils apportent à leurs solutions. Sur la base de ces informations, les fabricants devraient éventuellement revoir leur évaluation des risques. Dans le cadre de l'évaluation des risques actualisée, les fabricants devraient examiner si les garanties de cybersécurité des fournisseurs de services tiers sont encore suffisantes et si les contrôles de sécurité au niveau du produit sont toujours appropriés. Dans certains cas, il se peut que les fabricants doivent adapter ces contrôles ou changer de fournisseur de services tiers.

8.3. **Cas d'utilisation des solutions de traitement de données à distance**

Afin que les fabricants puissent disposer d'orientations pratiques supplémentaires, la présente section expose une série de cas d'utilisation fictifs, en décrivant des archétypes de produits comportant des éléments numériques qui reposent sur un traitement de données à distance et en indiquant si ce traitement constitue une solution de traitement de données à distance au sens du règlement sur la cyberrésilience.

8.3.1. *Application bancaire mobile*

Un établissement financier met sur le marché une application bancaire mobile. Les systèmes d'arrière-plan de l'application prennent en charge, entre autres, l'authentification, l'autorisation, la gestion des comptes et les paiements. Pour supporter les fonctionnalités de cette application, l'établissement financier utilise une stratégie hybride, qui se décline en une infrastructure interne et en des solutions à distance tierces, à savoir:

une infrastructure autohébergée développée par l'établissement financier:

— le client ouvre l'application bancaire mobile et est authentifié par l'intermédiaire de l'interface bancaire, une solution autohébergée développée par l'établissement financier qui reçoit les demandes de l'application et renvoie les réponses correspondantes. L'interface bancaire vérifie l'identité du client en interrogeant le système de gestion des comptes et donne accès à l'application;

— le client lance un virement via l'application. L'application transmet l'instruction à l'interface bancaire, qui soumet une demande correspondante au système du registre;

— le système de gestion des comptes et le système du registre, tous deux autohébergés mais séparés logiquement de l'interface bancaire, enregistrent la transaction;

— le système du registre communique le statut de la transaction à l'interface bancaire, qui présente le résultat au client.

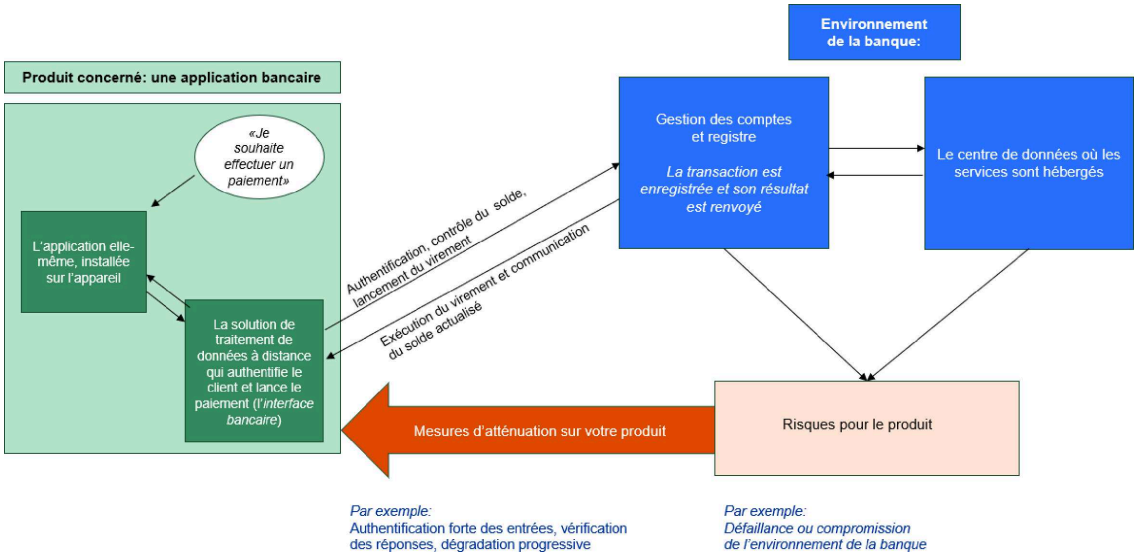
Implications pour la solution de traitement de données à distance:

— l'interface bancaire est nécessaire pour que l'application exécute ses fonctions, à savoir authentifier le client, soumettre les instructions du client, y compris ses instructions de paiement et de virement, et communiquer le statut final. L'interface bancaire est conçue et développée sous la responsabilité du fabricant. Étant donné que la réponse aux deux questions présentées dans les sections précédentes est affirmative, l'interface bancaire doit être considérée comme constituant une solution de traitement de données à distance. Elle doit donc être incluse dans l'évaluation des risques de cybersécurité et dans la mise en œuvre des exigences essentielles pour le produit comportant des éléments numériques dans son ensemble. Une fois qu'une instruction a été soumise, son traitement ultérieur – en particulier l'enregistrement de la transaction dans le système de gestion des comptes et dans le système du registre, son règlement et sa compensation – est effectué par des systèmes avec lesquels l'application n'interagit pas directement et ne constitue pas, pour cette raison, une solution de traitement de données à distance;

— le système de gestion des comptes et le système du registre ne constituent pas des solutions de traitement de données à distance pour l'application bancaire. L'application n'interagit pas directement avec ces systèmes (mais interagit avec l'interface bancaire, laquelle les fait ensuite intervenir). Bien que leur disponibilité puisse être nécessaire à l'exécution d'une fonction, le règlement sur la cyberrésilience ne couvre que les parties du système qui interagissent directement avec le produit comportant des éléments numériques. Ces parties ne relèvent donc pas de la définition des solutions de traitement de données à distance aux fins du règlement sur la cyberrésilience. Toutefois, ils demeurent des dépendances externes susceptibles de créer d'importants risques de cybersécurité pour le produit comportant des éléments numériques. Par exemple, la compromission du système du registre pourrait permettre à un acteur malveillant d'influencer les résultats d'une transaction qui sont ensuite affichés dans l'application. Le fabricant est donc tenu de recenser et d'évaluer ces risques dans le cadre de l'évaluation des risques de cybersécurité et de les atténuer en prenant des mesures au niveau du produit, telles que l'authentification forte des interfaces d'arrière-plan, la protection de l'intégrité des données de transaction, la sécurisation des canaux de communication et la vérification des réponses reçues par l'application;

Illustration 10

Représentation schématique d'une application bancaire reposant sur une solution de traitement de données à distance



un SaaS tiers pour l'assistance à la clientèle:

— l'établissement financier intègre dans son application une solution de discussion en ligne pour l'assistance à la clientèle qui a été développée et est exploitée par un fournisseur tiers, lequel a écrit le code du serveur de discussion, a conçu l'interface utilisateur et exploite l'infrastructure où la discussion s'effectue (il s'agit donc du modèle SaaS);

— lorsque le client introduit une demande d'assistance, l'application le connecte au service tiers pour ouvrir une session de discussion et gérer le flux de messagerie, sans que le tiers ait accès aux systèmes bancaires de base.

Implications pour la solution de traitement de données à distance:

— la solution de discussion en ligne pour l'assistance à la clientèle est nécessaire pour que le produit comportant des éléments numériques exécute une de ses fonctions, mais n'est pas conçue et développée par l'établissement financier ou sous la responsabilité de ce dernier; il ne s'agit donc pas d'une solution de traitement de données à distance. Toutefois, il convient de la traiter comme un composant tiers. Le recours à ce service tiers peut créer des risques de cybersécurité pour l'application bancaire, par exemple si un acteur malveillant décide d'utiliser le canal de discussion pour usurper l'identité de la banque ou envoyer des contenus malveillants aux utilisateurs. L'établissement financier doit tenir compte de ces risques dans son évaluation des risques de cybersécurité et les atténuer en prenant des mesures au niveau du produit, par exemple en isolant la fonction de discussion en ligne des fonctions bancaires de base, en contrôlant les flux de données et en validant les contenus. Il a aussi un devoir de diligence raisonnable en ce qui concerne le SaaS.

8.3.2. *Thermostat intelligent*

Un thermostat intelligent permet aux utilisateurs de contrôler la température de leur logement au moyen d'une application mobile. Cette application mobile et le thermostat intelligent utilisent un traitement de données à distance pour échanger des données (par exemple, les demandes d'augmentation de la température) et stocker des données (par exemple, les préférences de l'utilisateur). Ces fonctions ont été développées et conçues sous la responsabilité du fabricant, mais s'exécutent sur une infrastructure physique et virtuelle sous-jacente fournie par un tiers (IaaS tierce).

Étant donné que le thermostat intelligent ne serait pas en mesure d'exécuter ses fonctionnalités intelligentes sans ce traitement de données à distance, l'absence de celui-ci empêcherait le produit comportant des éléments numériques d'exécuter une ou plusieurs de ses fonctions. En outre, le logiciel a été développé et conçu sous la responsabilité du fabricant du thermostat intelligent. Par conséquent, le traitement de données à distance constitue une solution de traitement de données à distance au sens du règlement sur la cyberrésilience.

Aux fins de la conformité avec le règlement sur la cyberrésilience, le fabricant du thermostat intelligent doit documenter la solution de traitement de données à distance ainsi que la dépendance à l'égard de l'IaaS tierce (y compris les détails du service sous-traité) dans la documentation technique du produit comportant des éléments numériques. Il doit tenir compte de ces éléments dans l'évaluation des risques couvrant l'utilisation prévue ou raisonnablement prévisible du produit comportant des éléments numériques. Le fabricant met en œuvre les exigences essentielles du règlement sur la cyberrésilience en fonction des risques liés à la solution de traitement de données à distance. Pour l'IaaS tierce, le fabricant doit veiller à ce que les mesures de sécurité fournies par le fournisseur tiers soient appropriées et/ou prendre les mesures pertinentes à l'égard de cette infrastructure. Dans le premier cas, le fabricant pourrait, par exemple, demander la preuve que les obligations prévues par la directive SRI 2 ont été respectées.

8.3.3. *Liseuse numérique*

Le fabricant d'un logiciel pour liseuse numérique utilise un service de stockage SaaS tiers pour stocker les livres électroniques achetés par les clients et permettre à ces derniers d'accéder à leurs livres. L'absence de ce service de stockage empêcherait le produit comportant des éléments numériques d'exécuter une de ses fonctions, mais le service de stockage SaaS tiers n'est pas développé par le fabricant ou sous la responsabilité de ce dernier; le fournisseur du SaaS le met à la disposition de sa clientèle pour tout cas d'utilisation.

Le service de stockage SaaS ne répond pas à la définition des solutions de traitement de données à distance. Toutefois, le fabricant de la liseuse numérique s'appuie sur ce service externe pour le fonctionnement de son produit comportant des éléments numériques et doit donc tenir compte des risques y afférents dans son évaluation des risques de cybersécurité. Il devrait traiter le SaaS comme un composant. Le fabricant doit mettre en œuvre des mesures de sécurité appropriées au niveau du produit, telles que l'authentification sécurisée, le chiffrement et la protection de l'intégrité des communications avec le service de stockage. Le devoir de diligence raisonnable qui s'applique au moment de la sélection du fournisseur du SaaS et de l'intégration de son logiciel facilitera également le respect des obligations imposées au fabricant, afin que le produit comportant des éléments numériques dans son ensemble puisse être conforme aux exigences essentielles.

8.3.4. *Robot industriel*

Un robot industriel a pour tâche de collecter des pièces. Ce robot envoie les informations qu'il recueille au moyen de caméras à un service à distance conçu et développé par le fabricant. Ce service s'exécute sur une infrastructure physique et virtuelle sous-jacente fournie par un fournisseur de services tiers (IaaS tierce). Le service en nuage calcule la position d'une pièce sur la base des flux de la caméra et envoie des commandes au robot pour qu'il la saisisse.

L'absence de ce traitement de données empêcherait le robot industriel de collecter les pièces, et donc d'exécuter une de ses fonctions. En outre, le logiciel qui s'exécute sur l'infrastructure a été conçu et développé par le fabricant. Ce logiciel conçu et développé par le fabricant répond à la définition des solutions de traitement de données à distance.

Le fabricant du robot industriel doit documenter la solution de traitement de données à distance ainsi que la dépendance à l'égard de l'IaaS tierce (y compris les détails du service sous-traité) dans la documentation technique du produit comportant des éléments numériques. Il doit également tenir compte de ces éléments dans l'évaluation des risques couvrant l'utilisation prévue ou raisonnablement prévisible du produit comportant des éléments numériques. Le fabricant met en œuvre les exigences essentielles du règlement sur la cyberrésilience pour le produit comportant des éléments numériques, y compris sa solution de traitement de données à distance, en fonction des risques. Le devoir de diligence raisonnable qui s'applique au moment de la sélection du fournisseur de l'IaaS facilitera également le respect des obligations imposées au fabricant. Par exemple, le fabricant pourrait demander la preuve que les obligations prévues par la directive SRI 2 ont été respectées.

8.3.5. *Réseau cellulaire*

Un téléphone intelligent utilise un réseau 5G pour que ses utilisateurs puissent se connecter à l'internet, téléphoner et envoyer des messages (connectivité mobile). Le réseau cellulaire est développé et conçu par des opérateurs de télécommunications. Il se compose de petites cellules et d'antennes-relais, ainsi que d'autres équipements de réseau.

Le produit comportant des éléments numériques devrait être capable de se connecter correctement à un réseau; il s'agit là de l'une de ses fonctions. Toutefois, le caractère opérationnel ou non du réseau n'est pas pertinent au moment de déterminer si le produit comportant des éléments numériques fonctionne correctement. Le réseau n'est qu'un canal de communication et n'est pas nécessaire pour que le produit comportant des éléments numériques exécute sa fonction consistant à «se connecter correctement à un réseau». De même, un câble Ethernet, un routeur ou un signal Wi-Fi ne sont pas considérés comme un traitement de données dont l'absence empêcherait le produit comportant des éléments numériques d'exécuter une de ses fonctions; ce sont plutôt des facilitateurs de communication/connectivité.

Par conséquent, le réseau cellulaire ne répond pas à la définition des solutions de traitement de données à distance. Il ne devrait pas être considéré comme un composant tiers, étant donné qu'il n'existe pas de logiciel intégré dans le produit comportant des éléments numériques, ce dernier ne faisant qu'utiliser le réseau. Dès lors, il n'est pas nécessaire que le fabricant exerce son devoir de diligence raisonnable à l'égard du fournisseur de réseau.

9. **ÉLÉMENTS SUPPLÉMENTAIRES**

9.1. **Obligations en matière de communication d'informations**

209. En vertu de l'article 14, paragraphes 1 et 3, du règlement sur la cyberrésilience, un fabricant est tenu de notifier simultanément au CSIRT désigné comme coordinateur et à l'ENISA i) toute vulnérabilité activement exploitée contenue dans son produit comportant des éléments numériques dont il prend connaissance; et ii) tout incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques dont il prend connaissance.

210. En vertu de l'article 69, paragraphe 3, et de l'article 71, paragraphe 2, deuxième phrase, l'obligation de se conformer à l'article 14 s'applique à compter du 11 septembre 2026 à tous les produits comportant des éléments numériques relevant du champ d'application du règlement sur la cyberrésilience, y compris les produits comportant des éléments numériques mis sur le marché avant le 11 décembre 2027. Par ailleurs, contrairement aux obligations en matière de gestion des vulnérabilités, qui ne persistent que pendant la durée de la période d'assistance d'un produit, les obligations en matière de communication d'informations demeurent applicables une fois qu'un produit comportant des éléments numériques n'est plus pris en charge. Lorsqu'un produit comportant des éléments numériques a été mis sur le marché avant le 11 décembre 2027, ou une fois que sa période d'assistance a pris fin, le fabricant n'est pas tenu de se conformer aux obligations en matière de gestion des vulnérabilités énoncées à l'annexe I, partie II.

211. Il convient de rappeler que l'obligation de notifier les événements concernés s'applique dès que le fabricant prend connaissance d'une vulnérabilité activement exploitée ou d'un incident grave qui s'est produit et a compromis la sécurité de son produit comportant des éléments numériques. Par conséquent, des orientations clarifiant quand un fabricant est considéré comme ayant pris connaissance de l'événement concerné devraient aider les fabricants à déterminer à partir de quel moment les délais applicables en matière de communication d'informations commencent à courir.

212. Les fabricants peuvent être soumis à des obligations comparables en matière de communication d'informations en vertu d'autres actes législatifs de l'Union. Afin que la notion de «prise de connaissance» soit interprétée de manière cohérente et que le respect de ces obligations par les fabricants soit facilité, les présentes orientations s'alignent sur le considérant 31 du règlement d'exécution (UE) 2024/2690 de la Commission et sur la section II, point A, des lignes directrices 9/2022 sur la notification de violations de données à caractère personnel en vertu du RGPD.

213. Dans certains cas, un fabricant détectera un événement suspect ou verra son attention portée sur une vulnérabilité ou un incident potentiel par un tiers, tel qu'un particulier, un client, une entité, une autorité, un organisme de médias ou une autre source. Le fabricant devrait dans cette situation évaluer immédiatement l'événement suspect afin de déterminer s'il constitue une vulnérabilité activement exploitée ou un incident grave ayant des répercussions sur la sécurité du produit comportant des éléments numériques. Il convient donc de considérer que le fabricant a pris connaissance de l'événement concerné lorsque, après avoir procédé à cette évaluation initiale, il est raisonnablement certain: i) qu'une vulnérabilité contenue dans son produit comportant des éléments numériques est activement exploitée; ou ii) qu'un incident grave s'est produit et a compromis la sécurité de son produit comportant des éléments numériques.

214. Par conséquent, le moment auquel un fabricant peut être considéré comme ayant pris connaissance de l'événement concerné dépendra des circonstances de la vulnérabilité activement exploitée ou de l'incident grave en cause. Dans certains cas, il sera d'emblée relativement clair qu'une vulnérabilité est activement exploitée ou qu'un incident grave a des répercussions sur la sécurité d'un produit comportant des éléments numériques. Dans d'autres, un certain temps peut s'écouler avant que le fabricant ne soit en mesure de déterminer si un produit comportant des éléments numériques contient une vulnérabilité et si cette vulnérabilité est exploitée par un acteur malveillant, ou si un incident a des répercussions sur la sécurité d'un produit comportant des éléments numériques. Toutefois, il convient de mettre l'accent sur le fait qu'il y a lieu d'agir rapidement pour procéder à l'évaluation initiale visant à déterminer si ces conditions sont effectivement remplies, en particulier lorsque la vulnérabilité peut présenter un risque important, et, si tel est le cas, pour prendre des mesures correctives et notifier l'événement concerné conformément au règlement sur la cyberrésilience.

215. En outre, la structure des obligations en matière de communication d'informations impose aux fabricants de mettre à jour progressivement leurs notifications, à mesure que leurs enquêtes internes progressent et que leur connaissance de la vulnérabilité activement exploitée ou de l'incident devient plus détaillée. En particulier, les fabricants sont tenus de notifier une alerte précoce de vulnérabilité contenant des informations limitées sans retard injustifié et, en tout état de cause, au plus tard 24 heures après en avoir eu connaissance. Des informations supplémentaires sont ensuite requises dans le cadre de la notification que le fabricant doit soumettre sans retard injustifié et, en tout état de cause, au plus tard 72 heures après avoir eu connaissance de la vulnérabilité (ci-après la «notification à soumettre dans les 72 heures»). Le rapport complet doit être soumis dans un délai de 14 jours à compter de la mise à disposition d'une mesure de correction ou d'atténuation pour les vulnérabilités activement exploitées, ou dans un délai d'un mois à compter de la notification à soumettre dans les 72 heures pour les incidents graves.

216. Comme également rappelé à la section *3.3.1 Soutien continu et garantie de la viabilité du logiciel libre et ouvert,* les intendants de logiciels ouverts sont également tenus de signaler les vulnérabilités activement exploitées en vertu de l'article 24, paragraphe 3 ([30]). Cette obligation s'applique lors de la prise de connaissance d'une vulnérabilité activement exploitée, et pas lorsqu'il existe simplement une vulnérabilité dans la base de code d'un logiciel libre et ouvert dont cette entité est l'intendant. Dans la pratique, étant donné que les composants logiciels libres et ouverts sont généralement intégrés en aval dans d'autres produits comportant des éléments numériques, un intendant est susceptible de prendre connaissance d'une vulnérabilité activement exploitée au moyen d'un signalement émanant d'un tiers, qui détectera cette vulnérabilité dans des composants logiciels libres et ouverts intégrés dans d'autres produits comportant des éléments numériques. Tel peut être le cas, par exemple, lorsque le fabricant d'un produit comportant des éléments numériques détecte une vulnérabilité activement exploitée dans un composant logiciel libre et ouvert intégré dans son propre produit et la signale à l'intendant de ce composant; ou lorsqu'un utilisateur ou un auteur de recherches en matière de sécurité trouve des preuves de l'exploitation active d'une vulnérabilité dans un composant logiciel libre et ouvert intégré dans un produit comportant des éléments numériques et en informe l'intendant du composant.

217. Il convient également de préciser que, puisque l'obligation de signaler les vulnérabilités activement exploitées s'applique lorsque le fabricant prend connaissance d'une telle vulnérabilité, celui-ci n'est pas tenu de signaler les vulnérabilités activement exploitées dont il avait déjà connaissance avant le 11 septembre 2026 (date à laquelle l'obligation en matière de communication d'informations commence à s'appliquer). Le règlement sur la cyberrésilience n'exige donc pas le signalement rétroactif de ces vulnérabilités. En revanche, l'obligation s'applique lorsque le fabricant avait connaissance d'une vulnérabilité avant le 11 septembre 2026, mais n'avait pas, à ce moment-là, connaissance d'une exploitation active de celle-ci (soit parce que la vulnérabilité n'avait pas encore été activement exploitée, soit parce que le fabricant n'avait pas encore pris connaissance d'une exploitation active de celle-ci). Si, après le 11 septembre 2026, la vulnérabilité devient activement exploitée ou si le fabricant prend connaissance d'une exploitation active, la vulnérabilité est considérée comme une vulnérabilité activement exploitée soumise à l'obligation en matière de communication d'informations.

218. De même, un fabricant est uniquement tenu de signaler les vulnérabilités activement exploitées contenues dans son produit comportant des éléments numériques. Lorsqu'un produit comportant des éléments numériques contient une vulnérabilité activement exploitée qui provient d'un composant tiers, le fabricant du produit comportant des éléments numériques est tenu de notifier cette vulnérabilité activement exploitée. Toutefois, si un fabricant prend connaissance d'une vulnérabilité contenue dans un composant tiers, mais que cette vulnérabilité i) ne peut pas être exploitée dans son produit comportant des éléments numériques (par exemple, parce que le code vulnérable n'est pas accessible) ou ii) n'a pas été exploitée dans son produit comportant des éléments numériques, cette vulnérabilité ne constitue pas une vulnérabilité activement exploitée contenue dans son produit comportant des éléments numériques et n'est donc pas soumise à l'obligation en matière de communication d'informations pour ce fabricant. Ce fabricant peut toujours notifier cette vulnérabilité de manière volontaire, conformément à l'article 15 du règlement sur la cyberrésilience. Il est également tenu de se conformer aux exigences relatives à la gestion des vulnérabilités énoncées à l'annexe I, partie II, du règlement sur la cyberrésilience, ainsi que de signaler la vulnérabilité à la personne ou à l'entité qui fabrique le composant ou en assure l'entretien, conformément à l'article 13, paragraphe 6, et comme expliqué plus en détail à la section *9.2.1 Signalement en amont et partage des correctifs de sécurité*.

([30]) Dans la mesure où l'intendant participe au développement d'un produit comportant des éléments numériques.

219. Après avoir pris connaissance d'une vulnérabilité activement exploitée ou d'un incident grave, les fabricants sont également tenus, conformément à l'article 14, paragraphe 8, d'informer les utilisateurs touchés et, le cas échéant, tous les utilisateurs. Lorsqu'ils ne le font pas en temps utile, les CSIRT qui ont reçu la notification peuvent fournir ces informations aux utilisateurs lorsqu'ils le jugent proportionné et nécessaire pour prévenir ou atténuer les répercussions de cette vulnérabilité ou de cet incident.

220. Conformément à l'approche fondée sur les risques suivie dans le règlement sur la cyberrésilience, l'obligation d'informer les utilisateurs prévue à l'article 14, paragraphe 8, doit être appliquée de manière proportionnée et en fonction des risques. En particulier, la fourniture d'informations sur une vulnérabilité activement exploitée ou un incident grave ne signifie pas que ces informations doivent être rendues publiques ou divulguées sans discernement. Le cas échéant, et compte tenu de la nature du produit comportant des éléments numériques, des utilisateurs touchés et des répercussions potentielles de la vulnérabilité ou de l'incident, les fabricants peuvent limiter la divulgation d'informations détaillées aux utilisateurs ou clients concernés. Tel est notamment le cas pour les produits comportant des éléments numériques utilisés dans des environnements sensibles ou essentiels, la divulgation publique de détails techniques pouvant elle-même exacerber les risques de cybersécurité ou faciliter la poursuite de l'exploitation de la vulnérabilité.

221. Une fois que la vulnérabilité a été traitée ou atténuée de manière adéquate, une divulgation plus large peut être appropriée. Tel serait le cas, par exemple, si la divulgation est utile à des fins de sensibilisation générale ou permet aux utilisateurs de vérifier que leurs produits comportant des éléments numériques ne sont plus concernés. Le niveau de détail et le calendrier de l'éventuelle divulgation plus large devraient alors rester proportionnés et tenir compte des risques d'exploitation résiduels, de la nature du produit comportant des éléments numériques et des intérêts des utilisateurs concernés. En outre, l'annexe I, partie II, point 4), impose aux fabricants de divulguer publiquement des informations sur les vulnérabilités corrigées dès la publication d'une mise à jour de sécurité.

9.2. **Gestion des vulnérabilités**

9.2.1. *Signalement en amont et partage des correctifs de sécurité*

222. L'article 13, paragraphe 6, du règlement sur la cyberrésilience impose aux fabricants de signaler les vulnérabilités des composants intégrés à la personne ou à l'entité qui fabrique le composant ou en assure l'entretien (ci-après «signalement en amont»).

223. Cette obligation de signalement en amont qui pèse sur les fabricants ne s'applique qu'en ce qui concerne la version du composant qu'ils intègrent. Lorsque la personne ou l'entité qui fabrique le composant ou en assure l'entretien a mis en place des politiques de sécurité, des processus de divulgation coordonnée des vulnérabilités ou des canaux désignés pour signaler les vulnérabilités, les fabricants devraient procéder au signalement en y ayant recours, en particulier lorsque la divulgation prématurée de vulnérabilités non corrigées pourrait exacerber les risques de cybersécurité. Par ailleurs, afin que soit réduite la charge qui pèse sur les responsables de l'entretien en amont, en particulier dans le cadre des projets ouverts, les fabricants ne sont pas liés par l'obligation de signalement en amont lorsqu'ils peuvent confirmer que la personne ou l'entité qui fabrique le composant ou en assure l'entretien a connaissance de l'existence d'une vulnérabilité. Les fabricants sont encouragés à prendre des mesures raisonnables pour éviter les signalements redondants, par exemple en vérifiant les bases de données des vulnérabilités accessibles au public, les avis de sécurité propres à chaque projet ou les systèmes en place de suivi des problèmes avant de signaler les vulnérabilités en amont.

224. Les fabricants ne sont tenus de signaler en amont que les vulnérabilités qui existent dans le composant intégré lui-même, et non les vulnérabilités qui existent à la suite de l'intégration entre le composant et un autre code développé par le fabricant ou de l'intégration d'autres composants. Néanmoins, il se peut que l'intégration d'un composant dans un produit comportant des éléments numériques spécifique révèle des comportements, des interactions ou des caractéristiques pertinentes pour la sécurité de ce composant qui n'étaient pas apparents, ou pas facilement détectables, dans le composant considéré isolément. Dans un tel cas, les fabricants sont encouragés à communiquer cette information à la personne ou à l'entité qui fabrique le composant ou en assure l'entretien, afin de favoriser de bonnes pratiques de gestion des vulnérabilités en vue d'une correction efficace de celles-ci et de l'amélioration de la sécurité globale de l'écosystème du composant.

225. Enfin, les fabricants ne sont pas non plus tenus de signaler la vulnérabilité en amont lorsque plus aucune personne ou entité n'est responsable de l'entretien, ou lorsque le fabricant ne s'appuie plus sur le responsable de l'entretien initial pour les nouvelles versions ou les correctifs de sécurité. Dans ce cas de figure, le fabricant est néanmoins encouragé à informer les utilisateurs de ce composant au moyen d'autres mesures raisonnables, par exemple au moyen de mécanismes communautaires existants (tels que des listes de diffusion ou des tickets de suivi des problèmes) ou au moyen de registres publics des vulnérabilités.

226. En outre, en vertu de l'article 13, paragraphe 6, les fabricants qui ont mis au point une modification logicielle pour remédier à une vulnérabilité d'un composant intégré sont tenus de partager cette modification logicielle («correctif de sécurité») avec la personne ou l'entité qui fabrique le composant ou en assure l'entretien («partage en amont»).

227. Lorsque les fabricants sont tenus de partager un correctif de sécurité en vertu de l'article 13, paragraphe 6, le correctif devrait être fourni dans un format lisible par machine s'il y a lieu, de telle manière qu'il puisse être vérifié aisément et, le cas échéant, être intégré par la personne ou l'entité qui fabrique le composant ou en assure l'entretien. Lorsque le composant est un composant libre et ouvert, le correctif de sécurité devrait être partagé d'une manière compatible avec la licence de ce composant, par exemple en étant partagé sous la même licence ou sous une licence permettant au responsable de l'entretien de distribuer le correctif sous sa propre licence. Si le responsable de l'entretien de ce composant a établi des lignes directrices relatives au partage des correctifs de sécurité, le fabricant devrait s'y conformer.

228. Toutefois, les fabricants ne sont pas tenus par le règlement sur la cyberrésilience de veiller à ce que leurs correctifs de sécurité soient nécessairement acceptés par la personne ou l'entité qui fabrique le composant ou en assure l'entretien. Ils ne sont pas non plus tenus de veiller à ce que ces correctifs soient nécessairement intégrés dans le dépôt de code du composant, le responsable de l'entretien pouvant par exemple préférer une autre option pour corriger le problème. De même, les fabricants ne sont pas tenus d'accepter un correctif proposé par le responsable de l'entretien du composant et peuvent préférer atténuer le problème par d'autres moyens appropriés.

229. Dans certains cas, la personne ou l'entité qui fabrique le composant ou en assure l'entretien peut avoir déjà fourni un correctif de sécurité pour remédier à la vulnérabilité, mais un fabricant met en œuvre une stratégie d'atténuation différente (par exemple en modifiant une configuration différente). Dans de tels cas, le règlement sur la cyberrésilience n'exige pas du fabricant qu'il partage en amont la modification apportée à une autre partie du système. Le fabricant est néanmoins encouragé à le faire lorsque cela peut être utile à la personne ou à l'entité qui assure l'entretien du composant.

9.2.2. *Vulnérabilités exploitables connues*

230. L'une des exigences essentielles de l'annexe I, partie I, du règlement sur la cyberrésilience prévoit que, sur la base de l'évaluation des risques de cybersécurité visée à l'article 13, paragraphe 2, et le cas échéant, les produits comportant des éléments numériques doivent être mis à disposition sur le marché sans vulnérabilité exploitable connue.

231. L'article 3, point 41), définit une «vulnérabilité exploitable» comme étant «une vulnérabilité susceptible d'être utilisée efficacement par un adversaire en conditions de fonctionnement effectives». Les vulnérabilités ne sont pas toutes exploitables en conditions de fonctionnement effectives, et certaines vulnérabilités ne peuvent être exploitées qu'en conditions théoriques (par exemple, dans un laboratoire ou dans une simulation), mais pas dans des conditions qui se produiraient dans l'environnement opérationnel d'un produit comportant des éléments numériques.

232. Le règlement sur la cyberrésilience exige des fabricants qu'ils disposent de politiques et de procédures appropriées pour traiter et corriger les vulnérabilités potentielles signalées par des sources internes ou externes (article 13, paragraphe 8). Toutefois, il ne précise pas explicitement à quel stade une vulnérabilité exploitable devrait être considérée comme connue par le fabricant ni, par voie de conséquence, quand devient applicable l'obligation de se conformer à cette exigence essentielle au moment de la mise sur le marché.

233. Une vulnérabilité devrait être considérée comme connue lorsqu'elle est répertoriée dans les bases de données des vulnérabilités pertinentes et accessibles au public, telles que la base de données européenne des vulnérabilités établie par l'article 12, paragraphe 2, de la directive (UE) 2022/2555 ou d'autres importantes bases de données des vulnérabilités.

234. En outre, une vulnérabilité peut également être connue lorsque le fabricant en prend connaissance grâce à des informations non publiques, par exemple à la suite d'une divulgation coordonnée par un auteur de recherches en matière de sécurité ou du fait de ses propres essais et analyses internes, y compris, par exemple, lorsqu'il a recours à des services fondés sur l'IA. De même, une vulnérabilité peut être connue lorsqu'elle a été signalée publiquement et de manière visible dans des médias fiables, y compris des publications spécialisées en matière de cybersécurité ou des médias de masse généralistes.

235. Néanmoins, le simple fait qu'une vulnérabilité a été signalée ou détectée ne signifie pas, en soi, qu'elle est exploitable dans la pratique ou qu'elle touche le produit comportant des éléments numériques qui est spécifiquement concerné. Le fabricant devra examiner la vulnérabilité et confirmer la véracité des informations et leur applicabilité à son propre produit comportant des éléments numériques. En conséquence, un laps de temps limité peut s'écouler entre le premier signalement de la vulnérabilité et sa confirmation. Comme indiqué à la section *9.1 Obligations en matière de communication d'informations*, il convient de mettre l'accent sur le fait qu'il y a lieu d'agir rapidement pour enquêter et réagir.

236. En outre, l'obligation pour les fabricants de se conformer aux exigences essentielles énoncées à l'annexe I, partie I, s'applique au moment de la mise sur le marché, conformément à l'article 13, paragraphe 1. Dans la pratique, il se peut que de nouvelles vulnérabilités potentiellement exploitables soient découvertes au cours des dernières étapes du cycle de développement du produit comportant des éléments numériques, y compris peu de temps avant qu'il n'entre dans la chaîne de distribution (et ne soit donc mis sur le marché).

237. Étant donné que l'obligation de mettre sur le marché des produits comportant des éléments numériques sans vulnérabilité exploitable connue est fondée sur les risques, il incombe au fabricant de déterminer si, sur la base de l'évaluation des risques de cybersécurité, le produit comportant des éléments numériques peut être mis sur le marché en toute sécurité, conformément au règlement sur la cyberrésilience. Le fabricant peut également décider qu'une nouvelle vulnérabilité qui peut devenir connue doit être corrigée avant que le produit comportant des éléments numériques ne puisse être mis sur le marché. Pour prendre une telle décision, les fabricants devraient tenir compte de la gravité, de l'exploitabilité et des répercussions potentielles de la vulnérabilité, ainsi que des risques qu'elle crée pour le produit comportant des éléments numériques lui-même une fois qu'il est utilisé. Ils peuvent également tenir compte des risques liés à un report du déploiement du produit jusqu'à ce que la vulnérabilité soit corrigée, par exemple parce que la nouvelle version remédie également à d'autres vulnérabilités exploitables ou est nécessaire à la continuité de fonctionnement de systèmes critiques. En tout état de cause, une fois qu'un produit comportant des éléments numériques est mis sur le marché, le fabricant reste soumis à l'obligation de gérer les vulnérabilités efficacement et conformément aux exigences relatives à la gestion des vulnérabilités énoncées à l'annexe I, partie II.

9.2.3. *Obligation de réaliser régulièrement des tests et examens efficaces*

238. L'annexe I, partie II, point 3), impose aux fabricants de soumettre régulièrement les produits comportant des éléments numériques à des tests et examens efficaces, et ce tout au long de la période d'assistance. L'obligation de réaliser régulièrement des tests ne signifie pas qu'il faille répéter mécaniquement, à intervalles fixes, une campagne d'essais inchangée, mais suppose d'examiner régulièrement si de nouvelles données, telles que la détection de nouvelles menaces ou la découverte de nouvelles vulnérabilités, nécessitent de mettre à jour les tests existants et de réaliser de nouveaux essais en conséquence.

239. La fréquence, le niveau de détail et le contenu de l'examen devraient être proportionnés au profil de risque de cybersécurité du produit comportant des éléments numériques, à son évolution dans le temps et à l'état du paysage des menaces. Lorsque l'examen révèle de nouvelles données pertinentes qui ont une incidence sur l'ensemble d'essais, de nouveaux tests ou des tests modifiés devraient être conçus et exécutés sur le produit, et ce afin qu'aucune vulnérabilité ne reste sans réponse. Il peut s'agir de répéter des essais existants lorsqu'une modification apportée au produit comportant des éléments numériques rend ces types d'essais appropriés (essais de régression, par exemple).

240. Si l'examen ne révèle aucune donnée de ce type, il n'est pas nécessaire de concevoir des tests supplémentaires. Les autres obligations en matière de gestion des vulnérabilités, y compris l'obligation de s'attaquer et de remédier aux vulnérabilités en fonction des risques qu'elles posent, continuent de s'appliquer en parallèle.

9.3. **Interaction avec d'autres actes législatifs**

9.3.1. *Le règlement (UE) 2019/2144 et le règlement (UE) nº 168/2013*

241. L'article 2, paragraphe 2, point c), du règlement sur la cyberrésilience dispose que ce règlement ne s'applique pas aux produits comportant des éléments numériques auxquels s'applique le règlement (UE) 2019/2144. Le règlement (UE) 2019/2144 s'applique aux «véhicules des catégories M, N et O, telles que définies à l'article 4 du règlement (UE) 2018/858, ainsi qu'aux systèmes, composants et entités techniques distinctes conçus et construits pour ces véhicules».

242. De même, les produits comportant des éléments numériques qui relèvent du champ d'application du règlement (UE) nº 168/2013 ont été exclus du champ d'application du règlement sur la cyberrésilience par le règlement délégué (UE) 2025/1535 de la Commission. Le règlement (UE) nº 168/2013 s'applique aux véhicules de catégorie L ainsi qu'«aux systèmes, composants et entités techniques, de même qu'aux pièces et équipements, conçus et construits pour être montés sur ces véhicules» (article 2, paragraphe 1).

243. Les véhicules auxquels ces règlements s'appliquent ne sont pas soumis au règlement sur la cyberrésilience. Par ailleurs, des précisions supplémentaires sont nécessaires en ce qui concerne le champ d'application de la dérogation pour les systèmes, composants, entités techniques distinctes, pièces et équipements (ci-après, aux fins de la présente section, les «composants») conçus et construits pour être montés sur les véhicules pertinents qui sont considérés comme des produits comportant des éléments numériques au sens du règlement sur la cyberrésilience.

244. Il est considéré que ces composants ne sont pas soumis au règlement sur la cyberrésilience, à condition qu'ils soient exclusivement conçus et construits pour être intégrés dans des véhicules relevant des règlements (UE) 2019/2144 et (UE) nº 168/2013, et ce que le fabricant de ce composant le vende directement au constructeur automobile ou à un autre opérateur économique de la chaîne d'approvisionnement automobile, pour autant que le composant soit clairement destiné et adapté uniquement à une intégration finale dans ces véhicules.

245. En revanche, un fabricant qui vend des composants génériques qui constituent des produits comportant des éléments numériques pouvant être intégrés dans différents types de produits, et pas exclusivement dans des véhicules couverts par lesdits règlements, est soumis au règlement sur la cyberrésilience.

246. Afin de déterminer si un composant est mis sur le marché au sens du règlement sur la cyberrésilience, il convient de se fonder sur les conditions objectives de sa mise à disposition. Lorsqu'un fabricant propose un composant qui n'est pas exclusivement adapté à une intégration finale dans ces véhicules par l'intermédiaire de canaux de distribution ouverts à des clients extérieurs à la chaîne d'approvisionnement automobile, tels que des points de vente au détail généraux ou des canaux de vente en ligne qui acceptent les commandes du grand public, ce composant relève du champ d'application du règlement sur la cyberrésilience, indépendamment de toute déclaration quant à son utilisation prévue. Dans de telles circonstances, le composant ne peut être considéré comme étant conçu et construit exclusivement pour être intégré dans des véhicules relevant des règlements (UE) 2019/2144 et (UE) nº 168/2013, et le fabricant est tenu de se conformer au règlement sur la cyberrésilience. En revanche, l'utilisation de canaux de distribution réservés aux professionnels et limités à la chaîne d'approvisionnement automobile peut indiquer que le composant est conçu et construit exclusivement pour être intégré dans de tels véhicules.

9.3.2. *Validité des attestations d'examen UE de type (article 69, paragraphe 1)*

247. En vertu de l'article 69, paragraphe 1, du règlement sur la cyberrésilience, «[l]es attestations d'examen UE de type et les décisions d'approbation délivrées en ce qui concerne les exigences de cybersécurité applicables aux produits comportant des éléments numériques qui sont soumis à d'autres législations d'harmonisation de l'Union restent valables jusqu'au 11 juin 2028, à moins qu'elles n'expirent avant cette date, ou sauf disposition contraire dans toute autre législation d'harmonisation de l'Union, auquel cas elles restent valables conformément à cette législation».

248. Le maintien de la validité de ces attestations et décisions d'approbation devrait s'entendre comme étant limité aux risques de cybersécurité et aux exigences correspondantes qui sont couverts par la législation d'harmonisation de l'Union sur la base de laquelle elles ont été respectivement délivrées. En ce qui concerne ces risques, les fabricants ne sont pas tenus de réévaluer ou de démontrer à nouveau la conformité aux seules fins du règlement sur la cyberrésilience au cours de la période de validité visée à l'article 69, paragraphe 1, pour les produits comportant des éléments numériques qu'ils ont l'intention de mettre sur le marché le 11 décembre 2027 ou après cette date et jusqu'au 11 juin 2028 ([31]). Cela vaut pour les attestations et décisions d'approbation délivrées lorsque la législation d'harmonisation de l'Union applicable impose au fabricant d'effectuer la procédure d'évaluation de la conformité par l'intermédiaire d'un organisme notifié, ainsi que lorsque le fabricant a volontairement choisi de le faire.

249. Par conséquent, l'existence d'une attestation ou d'une décision d'approbation valable au titre d'autres législations d'harmonisation de l'Union ne dispense pas les fabricants de l'obligation de procéder à une évaluation complète des risques de cybersécurité en vertu du règlement sur la cyberrésilience (ni des autres obligations imposées par ce règlement), mais leur permet de s'appuyer sur les attestations existantes pour démontrer la conformité de leur procédure d'évaluation de la conformité, si les risques de cybersécurité correspondants sont déjà couverts. Si la validité de l'attestation ou de la décision d'approbation délivrée en vertu d'une autre législation d'harmonisation de l'Union s'étend au-delà du 11 juin 2028, le fabricant peut néanmoins s'appuyer sur cette attestation ou cette décision aux fins du règlement sur la cyberrésilience, mais seulement jusqu'au 11 juin 2028.

250. Lorsque l'évaluation des risques de cybersécurité effectuée conformément à l'article 13, paragraphe 2, révèle l'existence de risques supplémentaires non couverts par les exigences de cybersécurité qui sous-tendent l'attestation ou la décision d'approbation existante, les fabricants restent tenus de gérer ces risques conformément au règlement sur la cyberrésilience. Dans un tel cas, la conformité exige d'évaluer et d'atténuer les lacunes détectées, et ce même si l'attestation ou la décision d'approbation existante reste valable.

251. Prenons le cas, par exemple, d'un produit comportant des éléments numériques qui est soumis aux exigences de cybersécurité énoncées dans le règlement délégué (UE) 2022/30 de la Commission complétant la directive 2014/53/UE (acte délégué relatif à la directive sur les équipements radioélectriques) et qui est couvert par une attestation d'examen UE de type ou une décision d'approbation délivrée sur la base de ces exigences. Dans ce cas, l'attestation ou la décision reste valable, conformément à l'article 69, paragraphe 1, pour les risques de cybersécurité couverts par cette attestation, lesquels se rapportent aux exigences essentielles de cybersécurité de la directive 2014/53/UE (directive sur les équipements radioélectriques).

252. Les fabricants ne sont donc pas tenus, aux fins du règlement sur la cyberrésilience, de réévaluer ou de démontrer à nouveau la conformité en ce qui concerne les risques déjà couverts par ces attestations, tant que l'attestation ou la décision d'approbation concernée reste valable, et, en tout état de cause, jusqu'au 11 juin 2028. Il s'agit, par exemple, des risques de cybersécurité liés à la protection du réseau, à la protection des données à caractère personnel et de la vie privée ou à la prévention de la fraude (dans la mesure où ces risques sont couverts par l'attestation concernée) qui se rapportent aux exigences de cybersécurité de la directive sur les équipements radioélectriques et qui ont été pris en considération dans le cadre de l'évaluation de la conformité.

253. Toutefois, lorsque l'évaluation des risques de cybersécurité effectuée conformément à l'article 13, paragraphe 2, du règlement sur la cyberrésilience révèle l'existence de risques de cybersécurité supplémentaires non couverts par ces attestations, les fabricants restent tenus de gérer ces risques conformément au règlement sur la cyberrésilience. Il peut s'agir, par exemple, de risques liés aux processus de gestion des vulnérabilités, à la minimisation des données et à la réduction de la surface d'attaque, ou d'autres aspects de cybersécurité propres au produit qui ne sont pas couverts par ces attestations ou, en tout état de cause, qui ne sont pas couverts par les exigences essentielles de cybersécurité de la directive sur les équipements radioélectriques.

254. Par conséquent, l'existence d'une attestation d'examen UE de type ou d'une décision d'approbation valable au titre de la directive sur les équipements radioélectriques en ce qui concerne les exigences essentielles de cybersécurité de cette directive ne démontre pas, en soi, une conformité totale avec le règlement sur la cyberrésilience, mais permet aux fabricants de s'appuyer sur l'attestation ou la décision existante afin de démontrer la conformité pour les risques correspondants, tout en veillant à ce que les risques résiduels ou nouvellement recensés soient évalués et atténués conformément au règlement sur la cyberrésilience.

([31]) Les produits comportant des éléments numériques mis sur le marché avant le 11 décembre 2027 sont soumis à la législation de l'Union applicable au moment de leur mise sur le marché et, s'ils sont conformes, peuvent être vendus et mis en service, sauf s'ils font l'objet de modifications substantielles à compter du 11 décembre 2027 inclus. Pour les notions de «mise sur le marché» et de «mise à disposition sur le marché», voir, également, section *2.1 Mise sur le marché* du présent document ainsi que chapitre 2 du guide bleu.

255. De même, lorsqu'un produit comportant des éléments numériques est soumis aux exigences essentielles de santé et de sécurité liées à la cybersécurité énoncées dans le règlement (UE) 2023/1230 (règlement sur les machines), pleinement applicable à compter du 20 janvier 2027, et lorsqu'une attestation d'examen UE de type ou une décision d'approbation a été délivrée sur la base de ces exigences, cette attestation ou cette décision d'approbation reste valable, conformément à l'article 69, paragraphe 1, du règlement sur la cyberrésilience, pour les risques de cybersécurité couverts par ledit règlement.

256. Cela concerne en particulier les aspects de cybersécurité liés à la protection contre la corruption ainsi qu'à la sécurité et à la fiabilité des systèmes de commande, tels qu'énoncés à l'annexe III, sections 1.1.9 et 1.2.1, du règlement sur les machines. En ce qui concerne ces risques, les fabricants ne sont pas tenus, aux fins du règlement sur la cyberrésilience, de réévaluer ou de démontrer à nouveau la conformité tant que l'attestation ou la décision d'approbation concernée reste valable, et, en tout état de cause, jusqu'au 11 juin 2028, et ce dans la mesure où ces risques ont été pris en considération dans le cadre de l'évaluation de la conformité réalisée en vertu du règlement sur les machines.

257. Comme dans le cas des exigences essentielles de cybersécurité susmentionnées de la directive sur les équipements radioélectriques, lorsque l'évaluation des risques de cybersécurité effectuée conformément à l'article 13, paragraphe 2, du règlement sur la cyberrésilience révèle l'existence de risques de cybersécurité supplémentaires qui ne sont pas couverts par l'attestation pertinente délivrée en vertu du règlement sur les machines et qui sont liés aux exigences de cybersécurité dudit règlement, les fabricants restent tenus de gérer ces risques conformément au règlement sur la cyberrésilience.