La sécurité dans le marché unique numérique européen

Knockaert, Manon

Published in:
Les obligations légales de cybersécurité et de notifications d'incidents

Publication date:
2019

Document Version
le PDF de l'éditeur

La sécurité dans le marché unique numérique européen : le Règlement 2019/881 (« Cybersecurity Act »)

Manon Knockaert[1]

I. Introduction

Le 13 septembre 2017, le président de la Commission européenne, Jean-Claude Juncker, relève les faiblesses de l'Union européenne face aux cyberattaques alors que les technologies numériques sont au cœur de la vie des individus. Les chiffres sont impressionnants : l'Union rapporte qu'en 2016, plus de 4000 attaques par jour ont été détectées et que 80% des entreprises européennes ont connu au minimum un incident[2].

Consciente des enjeux et bien décidée à y remédier, l'Union européenne adopte, le 12 mars 2019, le Règlement 2019/881[3]. Un nouveau pas est franchi dans le renforcement de la protection des réseaux de communications électroniques. En effet, après avoir adopté une nouvelle réglementation relative aux télécommunications, à savoir la directive « Mieux légiférer »[4], la directive « Droits des citoyens »[5] et le règlement instituant l'Organe des régulateurs européens des communications électroniques[6] ainsi qu'une directive sur la sécurité des réseaux et des systèmes d'information[7], l'Union européenne s'arme d'une réglementation propre à la cybersécurité afin d'accroitre la sécurité et la résilience des services en ligne et dispositifs destinés au public.

L'objet de la présente contribution est de présenter le nouveau règlement relatif à la cybersécurité. La première partie de cette contribution permet une contextualisation de la matière et l'exposition des objectifs poursuivis par le législateur européen. La deuxième partie se concentre sur le schéma européen de certification, premier instrument juridique ayant

[1] Chercheuse au CRIDS-NaDI UNamur. This work has been done with the financial support from the European Union's Horizon 2020 research and innovation program under Grant Agreements no 830892 (SPARTA).
[2] Voyez le Communiqué de presse – État de l'Union 2017 – Cybersécurité : La Commission renforce sa capacité de réaction face aux cyberattaques. Disponible sur : https://europa.eu/rapid/press-release_IP-17-3193_fr.htm.
[3] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), *J.O.*, L 151, 7 juin 2019, p. 15 (ci-après « Règlement »).
[4] Directive (CE) 2009/140 du Parlement européen et du Conseil du 25 novembre 2009 modifiant les directives 2002/21/CE relative à un cadre règlementaire commun pour les réseaux et services de communications électroniques, 2002/19/CE relative à l'accès aux réseaux de communications électroniques et aux ressources associées, ainsi qu'à leur interconnexion, et 2002/20/CE relative à l'autorisation des réseaux et services de communications électroniques, *J.O.*, L 337, 18 décembre 2009, p. 37.
[5] Directive (CE) 2009/136 du Parlement européen et du Conseil du 25 novembre 2009 concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n° 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, *J.O.*, L 337, 18 décembre 2009, p. 11.
[6] Règlement (CE) 1211/2009 du Parlement européen et du Conseil du 25 novembre 2009 instituant l'Organe des régulateurs européens des communications électroniques (ORECE) ainsi que l'Office, *J.O.*, L 337, 18 décembre 2009, p. 1.
[7] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.*, L 194, 19 juillet 2016, p. 1.

vocation à renforcer la sécurité des appareils, des produits et des infrastructures. La troisième partie expose les nouvelles dispositions applicables à un acteur clé de la cybersécurité : l'Agence de l'Union européenne pour la cybersécurité (« ENISA »).

II. Objectifs

L'article 1 dispose que : « *En vue d'assurer le bon fonctionnement du marché intérieur tout en cherchant à atteindre un niveau élevé de cybersécurité, de cyber-résilience et de confiance au sein de l'Union, le présent règlement fixe a) les objectifs, les tâches et les questions organisationnelles concernant l'Agence de l'Union européenne pour la cybersécurité et b) un cadre pour la mise en place de schémas européens de certification de cybersécurité dans le but de garantir un niveau adéquat de cybersécurité des produits TIC, services TIC et processus TIC dans l'Union, ainsi que dans le but d'éviter la fragmentation du marché intérieur pour ce qui est des schémas de certification dans l'Union* »[8].

Si l'utilisation de dispositifs numériques connectés est grandissante au sein de l'Union européenne, la question de la sécurité de ces appareils est plus délicate. En effet, l'Union européenne constate tant leur faible sécurité que leur faible résilience[9]. En outre, face à une la menace internationale, le besoin d'une réponse harmonisée pour tous les États membres s'est fait ressentir[10].

Forte de ces considérations, l'Union adopte le Règlement 2019/881[11]. Elle entend ainsi poursuivre deux objectifs essentiels au développement du marché unique numérique, à savoir le renforcement de la confiance des citoyens dans ses dispositifs numériques et un accroissement harmonisé au sein de tous les États membres de la cybersécurité. À cette fin, le législateur ambitionne un renforcement de la coopération et du partage d'informations au sein des différents États membres. Par ailleurs, il souhaite que la cybersécurité de l'Union soit régulièrement évaluée afin d'anticiper au maximum les défis et les menaces futurs[12].

Notons que l'Union s'est déjà dotée de différents outils relatifs à la cybersécurité. En effet, après avoir établi sa stratégie en matière de cybersécurité en 2013, elle adopte quatre instruments juridiques[13].

III. Schéma européen de certification

a. Objectifs

Dans la perspective d'accroitre l'expérience de l'Union européenne en matière de protection des réseaux et systèmes d'information et des personnes exposées aux menaces,

[8] Article 1 Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), *J.O.*, L 151, 7 juin 2019, p. 15 (ci-après « Règlement »).
[9] Considérants 3 et 4 du Règlement.
[10] Considérant 5 du Règlement.
[11] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications, et abrogeant le règlement (UE) n° 526/2013 (règlement sur la cybersécurité), *J.O.*, L 151, 7 juin 2019, p. 15 (ci-après « Règlement »).
[12] Considérants 5 et 6 du Règlement.
[13] Directive UE 2016/1148 ; Règlement UE 2016/679 ; Directive UE 2002/58/CE et Directive UE 2018/1972

la réglementation élabore un cadre européen harmonisé de certification en matière de cybersécurité. L'article 46 du règlement dispose que « *le cadre européen de certification de cybersécurité est établi afin d'améliorer les conditions de fonctionnement du marché intérieur en renforçant le niveau de cybersécurité au sein de l'Union et en permettant de disposer, au niveau de l'Union, d'une approche harmonisée en ce qui concerne les schémas européens de certification de cybersécurité, en vue de créer un marché unique numérique pour les produits TIC, services TIC et processus TIC* ». L'Union européenne y voit également une opportunité pour renforcer la confiance des utilisateurs[14].

À cet égard, le règlement définit la cybersécurité comme « *les actions nécessaires pour protéger les réseaux et les systèmes d'information, les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces* »[15]. La notion de cybermenace, quant à elle, est définie comme « *toute circonstance, tout évènement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes* »[16].

Afin d'atteindre l'idéal de sécurité, l'Union européenne met en place le mécanisme du schéma européen de certification de cybersécurité. Ce schéma consacre un ensemble de normes et d'exigences techniques commun à tous les États membres pour la certification ou l'auto-évaluation de conformité[17], corrigeant de la sorte une fragmentation du marché intérieur et évitant la pratique du « shopping de certifications »[18].

Pour ce faire, le législateur européen matérialise, à l'article 51, les différents objectifs de sécurité nécessaires à la réalisation de ce schéma européen de certification de cybersécurité. En substance, les produits TIC[19], services TIC[20] et les processus TIC[21] seront ainsi évalués afin de vérifier leur conformité, dès la conception, aux exigences de sécurité spécifiées, à savoir la

[14] En témoigne plusieurs considérants. Voyez notamment le considérant 7 pour la nécessaire confiance en la sécurité : « *Un renforcement de la confiance peut être facilité par une certification mise en œuvre à l'échelle de l'Union prévoyant des exigences et des critères d'évaluation communs en matière de cybersécurité dans l'ensemble des marchés nationaux et des secteurs* ». Voyez également le considérant 65 visant spécifiquement le mécanisme de la certification : « *La certification de cybersécurité joue un rôle important dans l'amélioration de la sécurité des produits TIC, services TIC et processus TIC et le renforcement de la confiance qui leur est accordée. Le marché unique numérique, et en particulier l'économie des données et l'IdO, ne peuvent prospérer que si le grand public est convaincu que ces produits, services et processus offrent un certain niveau de cybersécurité* ».

[15] Article 2, 1) du Règlement.

[16] Article 2, 8) du Règlement.

[17] Article 2, 9) du Règlement.

[18] Considérants 66 et 70 du Règlement. Le « shopping de certifications » traduit la pratique consistante, pour un fabricant ou un vendeur, à choisir le pays dans lequel obtenir la certification en fonction d'exigences de sécurité plus ou moins souples.

[19] L'article 2, 12) définit un « produit tic » comme étant « *un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information* ».

[20] Le service TIC est entendu comme « *un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information* » (article 2, 13) du Règlement).

[21] L'article 2, 14) définit le « processus TIC » comme « *un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance* ».

garantie de la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, qu'ils s'agissent de données à caractère personnel ou non[22].

Il convient de relever que le certificat de conformité, une fois délivré, est reconnu par tous les États membres[23]. L'objectif est d'éviter la démarche de certifications multiples dans plusieurs États membres aux fabricants et vendeurs de produits, de services ou de processus[24]. En effet, l'Union dénonce l'urgence d'adopter « *une approche commune et d'établir un cadre européen de certification de cybersécurité établissant les principales exigences horizontales pour les schémas de certification de cybersécurité à développer, et permettant la reconnaissance et l'utilisation dans tous les États membres des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne pour les produits TIC, services TIC ou processus TIC* »[25].

Soulignons que le mécanisme de certification ne peut se suffire à lui-même et doit s'accompagner d'une réelle sensibilisation des acteurs et un développement d'une culture commune de la sécurité. L'Union européenne appelle ainsi tous les fabricants et vendeurs de produits et services à développer une « *hygiène informatique* »[26]. À titre d'illustration, il est important que les fabricants soient vigilants lors de l'utilisation de technologies, composants ou interfaces de programmation de tiers, étants liés à leur vulnérabilité[27].

b. La certification

i. Le programme de travail glissant de l'Union pour la certification

Véritable outil stratégique, la Commission doit évaluer les produits, services et processus TIC devant en priorité entrer dans le champ d'application d'un schéma européen de certification. Cette évaluation doit reposer sur i) la disponibilité et le développement des schémas nationaux de certification afin de corriger une fragmentation au sein de l'Union ; ii) le droit ou la politique applicable de l'Union ou d'un État membre ; iii) la demande du marché ; iv) l'évolution de la situation en ce qui concerne les cybermenaces et enfin v) une demande de préparation d'un schéma candidat spécifique par le Groupe européen de certification de cybersécurité (« GECC »)[28].

Lorsque l'urgence le justifie, le groupe des parties prenantes pour la certification de la cybersécurité[29], organe représentatif des parties concernées par la certification comme les entreprises actives dans le secteur des nouvelles technologies, les autorités de contrôle de la protection des données, les universitaires, et., peut exprimer le souhait à la Commission et au GECC d'ajouter des schémas de certification au programme de travail[30].

---

[22] Article 51 du Règlement ; F. DUMORTIER, « Chapter VI – Security and incident reporting requirements », *in* GARZANTI, O'REGAN, DE STREEL and VALCKE (eds), *Electronic communications, audiovisual services and the internet: Competition Law and Regulation*, Sweet & Maxwell, 2019 (à paraître).
[23] Article 56.10 du Règlement.
[24] Considérant 67 du Règlement.
[25] Considérant 69 du Règlement.
[26] Considérant 8 du Règlement.
[27] Considérant 11 du Règlement.
[28] Sur le schéma candidat, *infra*.
[29] Sur les missions et le fonctionnement du groupe des parties prenantes, *infra*.
[30] Article 22.3, e) du Règlement.

Ce programme doit voir le jour au plus tard le 28 juin 2020. Ensuite, il devra faire l'objet d'une révision autant de fois que nécessaire et, en tous les cas, tous les trois ans au minimum[31].

ii. Contenu

À l'inverse du mécanisme d'auto-évaluation[32], la certification est un document nécessairement délivré par un organisme compétent[33] assurant que la conformité aux exigences de sécurité d'un produit, service ou processus TIC a été contrôlée[34]. Notons que le recours à la certification s'effectue sur une base volontaire – sauf disposition contraire du droit de l'Union[35] ou du droit national – du fabricant ou du fournisseur du produit, service ou processus TIC, qui doit alors communiquer toutes les informations nécessaires à l'évaluation à l'organisme compétent[36].

Par ailleurs, un certificat est délivré pour le temps défini par le schéma européen de certification. Il est renouvelable sous réserve du maintien de l'ensemble des exigences techniques[37].

L'article 54 du règlement énumère les éléments que doit au moins comprendre un schéma européen de certification : i) leur objet et leur portée, en ce compris le type ou les catégories de processus, produits et services TIC couverts ; ii) une description claire de la finalité du système et de la manière dont les normes, les méthodes d'évaluation sélectionnées et le niveau s'assurance correspondent aux besoins des utilisateurs ; iii) les références aux normes internationales, européennes ou nationales appliquées dans l'évaluation ou, lorsque ces normes n'existent pas ou sont inappropriées, aux spécifications techniques qui satisfont aux exigences du règlement figurant à l'annexe II, si ces spécifications ne sont pas disponibles, aux spécifications techniques ou aux autres exigences en matière de cybersécurité définies le schéma européen de certification ; iv) la mention indiquant si l'auto-évaluation de la conformité[38] est autorisée ; v) les exigences spécifiques ou supplémentaires éventuelles auxquelles sont soumis les organismes d'évaluation de conformité ; vi) les critères et méthodes d'évaluation spécifiques devant être utilisées ; vii) les informations nécessaires à la certification qu'un demandeur doit fournir aux organismes d'évaluation de conformité ; viii) les règles de contrôle du respect des exigences des certificats ou de la déclaration de conformité de l'UE, y compris les mécanismes visant à démontrer le respect continu des exigences spécifiées en matière de cybersécurité ; xi) les conditions éventuelles permettant de délivrer, de maintenir, de prolonger et de renouveler les certificats européens de cybersécurité ainsi que les conditions auxquelles il est possible d'étendre ou de réduire leur champ d'application ; x) les règles concernant les conséquences de la non-conformité des produits, services et processus TIC certifiés ; xi) les règles relatives aux modalités de signalement et de traitement des vulnérabilités de cybersécurité non détectées précédemment ; xii) l'identification des schémas nationaux ou internationaux de certification pour des produits, services ou processus TIC similaires TIC ;

[31] Article 47 du Règlement.
[32] Sur le mécanisme d'auto-évaluation, *infra*.
[33] Pour la détermination de l'organisme compétant pour la certification, *infra*.
[34] Article 2, 11) du Règlement.
[35] À cet égard, la Commission européenne est tenue à une réévaluation régulière de l'efficacité des schémas de certification afin de déterminer si un schéma de certification doit être obligatoire afin d'assurer et de maintenir un niveau de sécurité adéquat au sein de l'Union et permettre le bon fonctionnement du marché intérieur.
[36] Articles 56.2 et 56.7 du Règlement. Voyez également F. DUMORTIER, *op.cit.*
[37] Article 56.9 du Règlement.
[38] Sur ce point, *infra*

xiii) le contenu et le format des certificats de cybersécurité européens et des déclarations de conformité de l'Union européenne à délivrer ; xiv) la période de disponibilité de la déclaration de conformité, de la documentation technique et de toutes autres informations pertinentes dont disposent le fabricant ou le fournisseur ; xv) la durée maximale de validité des certificats de cybersécurité européens délivrées dans le cadre du schéma ainsi que ; xvi) les conditions de reconnaissance mutuelle des schémas de certification avec les pays tiers.

Soulevons que l'Union appelle à des solutions flexibles et des schémas de certification se préservant d'une obsolescence rapide[39].

iii. Trois niveaux d'assurance

L'article 2, 21) définit le niveau d'assurance comme « *le fondement permettant de garantir qu'un produit TIC, service TIC ou processus TIC satisfait aux exigences de sécurité d'un schéma européen de certification de cybersécurité spécifique, indique le niveau auquel un produit TIC, service TIC ou processus TIC a été évalué* ». Prudent, le législateur européen précise toutefois que l'indication du niveau d'assurance ne mesure pas, en tant que tel, la sécurité du produit, service ou processus évalué[40].

Un schéma européen de certification de cybersécurité peut garantir trois niveaux d'assurance en fonction des exigences de sécurité et de la méthodologie du contrôle. Précisons qu'un même schéma européen de certification peut préciser plusieurs niveaux d'assurance[41]. En effet, trois niveaux sont mis en place[42].

Premièrement, le règlement prévoit le niveau d'assurance élémentaire. Afin d'assurer la minimisation des risques élementaires connus d'incidents et de cyberattaques, l'examen doit *a minima* porter sur la documentation technique qui accompagne le produit, service ou processus TIC concerné. En outre, lorsque la certification inclut des processus TIC, le processus de conception, de développement et de maintenance d'un produit ou d'un service devrait également être évalué. Une fois l'examen effectué, ce niveau assure que les produits, services ou processus TIC satisfont aux exigences élémentaires identifiées[43].

Deuxièmement, le règlement prévoit le niveau d'assurance substantiel. Afin de se voir reconnaitre cette qualité, le produit, service ou processus TIC doit assurer la minimisation des risques et des cyberattaques provenant d'acteurs aux aptitudes et aux ressources limitées. À cette fin, l'examen d'évaluation porte sur la démonstration de l'absence de vulnérabilités connues du public et des vérifications démontrant la correcte mise en œuvre des fonctionnalités de sécurité nécessaires[44].

[39] Considérant 72 du Règlement.
[40] Article 2. 21) du Règlement.
[41] En effet, l'article 52.1 dispose que : « *Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants pour les produits TIC, services TIC et processus TIC : 'élémentaire', 'substantiel', 'élevé'. Le niveau d'assurance correspond au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC ou processus TIC, en termes de probabilité et répercussions d'un incident* ».
[42] Considérant 86 du Règlement.
[43] Considérant 88 et article 52.5 du Règlement.
[44] Considérant 89 et article 52.6 du Règlement.

Troisièmement, le règlement prévoit également le niveau d'assurance élevé. À nouveau, le produit, service ou processus TIC évalué devra passer les deux premiers tests, à savoir l'assurance élémentaire et substantielle. En outre, la qualité « élevée » ne pourra être accordée après un test d'efficacité évaluant la résistance des fonctionnalités de sécurité. Le considérant 90 du règlement explique, avec imprécision, que ce test d'efficacité sera soumis à des « *cyberattaques élaborées lancées par des personnes au aptitudes solides et aux ressources importantes* ».[45] L'examen porte sur l'absence de vulnérabilités connues du public, la démonstration d'une mise en œuvre correcte des fonctionnalités de sécurité, la résistance du produit, service ou processus TIC face à des attaques émanant d'acteurs compétents au moyen de tests de pénétration[46].

En tous les cas, la personne physique ou morale ayant soumis le produit, service ou processus TIC à l'évaluation et qui est titulaire d'un certificat de cybersécurité européen doit informer l'organisme compétent lui ayant délivré le certificat de toute vulnérabilité ou irrégularité détectée par la suite susceptibles d'impacter le respect des exigences liées à la certification. Dans un second temps, l'autorité nationale de certification ou l'organisme d'évaluation doit informer sans retard l'autorité nationale de certification de cybersécurité concernée[47].

iv. Organisme compétent

a. Niveau d'assurance élémentaire ou substantiel

L'organisme en charge de la délivrance d'une certification d'un niveau de sécurité élémentaire ou substantiel d'un produit, service ou processus TIC est l'organisme d'évaluation de conformité[48]. Institué par le Règlement 765/2008, il a pour mission d'effectuer « *des opérations d'évaluation de la conformité, comme l'étalonnage, les essais, la certification et l'inspection* »[49].

Cet organisme d'évaluation de conformité est lui-même accrédité par un organisme d'accréditation[50] mis en place au sein de chaque État membre.

Précisons toutefois que, dans certains cas dûment justifiés, une autorité nationale de certification de cybersécurité ou un organisme public accrédité en tant qu'organisme d'évaluation peut délivrer des certificats de cybersécurité européens[51]. Toutefois, relevons le caractère lacunaire de cette disposition en ce qu'elle n'apporte pas de réelle précision quant aux hypothèses permettant une action d'une autorité nationale ou d'un organisme public.

b. Niveau d'assurance élevé

[45] Considérant 90 du Règlement.
[46] Considérant 90 et article 52.7 du Règlement.
[47] Article 56.8 du Règlement.
[48] Article 56.4 du Règlement
[49] Règlement (CE) 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) n° 339/93 du Conseil, *J.O.*, L 218, 13 août 2008, p. 30.
[50] Selon l'article 2, 11) du Règlement 765/2008, un organisme national d'accréditation est défini comme « *l'unique organisme dans un État membre chargé de l'accréditation, qui tire son autorité de cet État* ».
[51] Article 56.5 du Règlement.

En revanche, seule une autorité nationale de certification de cybersécurité est habilitée à délivrer une certification d'un niveau d'assurance élevé[52].

Toutefois, dans deux hypothèses uniquement, la délivrance peut être effectuée par un organisme d'évaluation de la conformité.

Premièrement, lorsqu'il a obtenu l'approbation préalable de l'autorité nationale de certification.

Deuxièmement, l'organisme d'évaluation de la conformité est compétent moyennant une délégation préalable de cette fonction précise par l'autorité nationale de certification de cybersécurité.

Relevons que, nonobstant le niveau d'assurance, l'Union européenne reste prudente et précisant que l'évaluation de conformité doit être comprise comme une attestation que le produit, le service ou le processus TIC concerné respecte certaines exigences de sécurité mais ne garantit en aucun cas une sécurité totale du point de vue de la cybersécurité[53].

v. Autorités nationales de certification

La réglementation impose à chaque État membre la désignation d'une ou de plusieurs autorités nationales de certification et en informe la Commission européenne[54]. Elles peuvent être une autorité déjà existante ou nouvellement créées[55].

Outre la compétence de délivrer les certificats d'assurance, l'autorité nationale de certification reçoit d'autres missions. Elles consistent principalement en i) la supervision et le respect des règles prévues dans les schémas européens de certification et le respect des exigences des certificats de cybersécurités délivrés sur leur territoire ; ii) le contrôle du respect des obligations par les fabricants ou fournisseurs de produits, services ou processus TIC contenus dans l'auto-évaluation et le schéma européen de certification de cybersécurité correspondant ; iii) l'aide et l'assistance aux organismes nationaux d'accréditation dans le contrôle et la supervision des activités des organismes d'évaluation ; iv) le contrôle et la supervision des organismes publics pour la délivrance de certification d'assurance élémentaire ou substantiel ; v) le traitement et le suivi des réclamations introduites par toute personne physique ou morale et vi) la coopération avec les autres autorités nationales de certification de cybersécurité ou autres autorités publiques, notamment dans le partage d'informations sur d'éventuels manquements dans le respect des exigences de sécurité de la part des fournisseurs ou fabricant de produit, service ou processus TIC[56]. Le législateur européen accorde aux autorités nationales de larges prérogatives pour accomplir leurs missions[57].

---

[52] Article 56.6 du Règlement.

[53] En effet, le considérant 77 déclare que « *L'évaluation de la conformité et la certification ne peuvent en soi garantir que les produits TIC, services TIC ou processus TIC certifiés sont sécurisés du point de vue de la cybersécurité. Il s'git plutôt de procédures et de méthodologies techniques visant à attester que des produits TIC, services TIC ou processus TIC ont été soumis à des essais et qu'ils respectent certaines exigences de cybersécurité établies par ailleurs, par exemple dans des normes techniques* ».

[54] Article 58.1 et 58.2 du Règlement.

[55] Considérant 101 du Règlement.

[56] Article 58.7 du Règlement.

[57] Article 58.8 du Règlement.

Précisons que chaque État a la possibilité, sous réserve d'un accord conclu avec un autre État membre, de faire reposer les tâches de supervision sur la ou les autorités nationales de certification de cet autre État membre[58].

Par ailleurs, le règlement souligne l'importance de l'indépendance des autorités nationales par rapport aux entités surveillées tant dans leur organisation que dans leurs décision et structure juridique[59]. En *sus* de cette précaution, le législateur impose la séparation des activités liées à la délivrance des certificats de cybersécurité européens et des missions de supervision et leur exécution indépendante[60].

vi. Examen par les pairs

Les autorités nationales de certification doivent elles-mêmes faire l'objet d'un examen par les pairs, tous les cinq ans[61]. Cet examen doit porter sur i) le caractère bien distinct des activités de supervision et des activités de délivrance des certificats ; ii) les procédures permettant de superviser et d'assurer le respect des règles relatives au contrôle des prescriptions des certificats de cybersécurité ; iii) les procédures permettant de contrôler et de faire respecter les obligations des fabricants et des fournisseurs dans le cadre d'une auto-évaluation de conformité par ceux-ci ; iv) les procédures mises en place pour le contrôle, l'autorisation et la supervision des activités des organismes d'évaluation de la conformité et enfin v) le niveau de compétence du personnel délivrant les certificats de niveau élevé[62].

Cet examen est opéré par au moins deux autorités nationales de certification d'autres États membres et par la Commission. En outre, il est laissé à la libre appréciation de l'ENISA d'y participer[63]. Il nous semble qu'il aurait également été utile de préciser qu'une des autorités nationales de certification effectuant cet examen ne peut être celle de l'État membre ayant décidé de déléguer ses fonctions de supervision à un autre État membre.

Notons que l'article 59.5 du règlement laisse la faculté à la Commission européenne d'adopter des actes d'exécution pour éclaircir les critères concernant la composition de l'équipe chargée de cet examen, la méthodologie utilisée ainsi que son programme et sa fréquence.

vii. Groupe européen de certification de cybersécurité

Le GECC, organe nouvellement constitué, est composé de représentants des autorités nationales de certification.

Celui-ci a notamment pour mission i) de conseiller et d'assister la Commission dans une mise en œuvre cohérente de son programme de travail glissant et dans la préparation des schémas européens de certification ; ii) d'apporter son aide à l'ENISA dans la préparation d'un schéma candidat ; iii) de demander à l'ENISA la préparation d'un schéma candidat ; iv) la réalisation d'avis pour la Commission relatifs à la maintenance et au réexamen des schémas européens de

[58] Article 58.1 du Règlement.
[59] Articler 58.3 du Règlement.
[60] Article 58.4 du Règlement.
[61] Article 59.4 et considérant 99 du Règlement.
[62] Article 59.3 du Règlement.
[63] Article 59.4 du Règlement.

certification existants ; v) de suivre les évolutions dans le domaine de la certification et vi) de faciliter l'alignement des schémas européens de certification sur les normes internationalement reconnues[64].

viii. Site Internet sur les schémas européens de certification de cybersécurité

Dans un souci de publicité et de gestion globalisée au sein de l'Union, le législateur donne mission à l'ENISA de tenir à jour un site Internet spécialement réservé aux schémas européens de certification de cybersécurité. Ce portail doit fournir les informations relatives aux schémas européens de certification, aux certificats de cybersécurité et aux déclarations de conformité, en ce compris les schémas européens de certification et les certificats de cybersécurités expirés ou retirés. En outre, ce site Internet doit contenir un répertoire de liens vers des informations relatives à la cybersécurité[65].

Par ailleurs, l'article 50.2 dispose que : « *Le cas échéant, le site internet visé au paragraphe 1 indique également les schémas nationaux de certification de cybersécurité qui ont été remplacés par un schéma européen de certification de cybersécurité* »[66].

ix. Schémas nationaux de certification de cybersécurité

Si le mécanisme de certification européen est mis en place pour assurer une harmonisation cohérente en matière de sécurité au sein de l'Union[67], le législateur laisse toutefois la possibilité de maintenir des schémas de certification nationaux s'ils ne sont pas couverts par un schéma européen de certification de cybersécurité[68]. Les certificats nationaux existants et couverts par un schéma européen restent également d'application jusqu'à leur date d'expiration[69]. Le site Internet de l'ENISA devrait informer le public des schémas nationaux de certification remplacés par un schéma de certification européen[70].

En revanche, le législateur enjoint les États membres de s'abstenir de créer de nouveaux schémas de certification nationaux pour les produits, services et processus TIC déjà garantis par un schéma européen[71]. Relevons toutefois que la disposition ne semble pas être une interdiction de principe[72]. En outre, l'article 57.4 de la réglementation impose aux États membres d'informer préalablement à toute création de nouveaux schémas de certification nationaux la Commission et le GECC. De manière abstraite, le considérant 94 indique que : « *La Commission et le GECC devraient évaluer l'incidence de nouveaux schémas nationaux de certification de cybersécurité sur le bon fonctionnement du marché intérieur, à la lumière de*

[64] Article 62 du Règlement.
[65] Article 50.1 du Règlement.
[66] Article 50.2 du Règlement.
[67] En effet, dans le considérant 66, le législateur dénonce la fragmentation géographique du niveau de cybersécurité dans les différents États membres. Par ailleurs, dans le considérant 67, il relève que les certifications sont majoritairement des problématiques nationales non cohérentes ou pilotés par les entreprises du secteur.
[68] Article 57.1 du Règlement.
[69] Article 57.3 du Règlement.
[70] Considérant 85 et article 50 du Règlement.
[71] Considérant 94 et article 57.2 du Règlement.
[72] Le considérant 94 du Règlement précise que : « *Toutefois, il convient de ne pas empêcher les États membres d'adopter ou de maintenir des schémas nationaux de certification de cybersécurité à des fins de sécurité nationale* ».

tout intérêt stratégique qu'il y aurait à demander, en leur lieu et place, un schéma européen de certification de cybersécurité »[73].

c. Auto-évaluation de la conformité

En plus de la certification européenne, le règlement prévoit le mécanisme d'auto-évaluation. L'article 53 prévoit la possibilité, à l'initiative du fabricant ou du fournisseur de produit services ou processus TIC – sauf en cas de présence d'une disposition du droit de l'Union ou du droit national imposant une auto-évaluation[74] et sous sa responsabilité, de délivrer une déclaration de conformité de l'Union européenne.

L'auto-évaluation est définie par le législateur comme « *une action effectuée par un fabricant ou un fournisseur de produits TIC, services TIC ou processus TIC, qui évalue si ces produits TIC, services TIC ou processus TIC satisfont aux exigences fixées dans un schéma européen de certification de cybersécurité spécifique* »[75].

Si l'auto-évaluation est également reconnue dans tous les États membres, son recours reste toutefois limité au premier niveau d'assurance de sécurité[76].

À des fins de vérification, le fabricant ou le fournisseur utilisant ce mécanisme doit mettre à disposition de l'autorité nationale de certification, toute la documentation technique et les autres informations pertinentes. À cet égard, ils doivent conserver ladite documentation pour la durée déterminée par le schéma européen de certification correspondant. De surcroît, une copie de la déclaration de conformité doit être transmise à l'autorité nationale de certification et à l'ENISA[77].

En outre, afin d'assurer la plus grande transparence possible et de renforcer la confiance des citoyens, l'article 55 de la règlementation prévoit une liste d'informations à mettre à disposition du public par le fabricant ou le fournisseur de produits, services ou processus TIC. Ces informations concernent i) les orientations et les recommandations pour aider les utilisateurs finaux à assurer une configuration, une installation, un déploiement ainsi qu'un fonctionnement et une maintenance sécurisée ; ii) la période pendant laquelle une assistance en matière de sécurité sera offerte aux utilisateurs, en particulier en ce qui concerne la disponibilités des mises à jour portant sur la sécurité du produit, du service ou du processus TIC ; iii) les informations de contact du fabricant ou du fournisseur et les méthodes acceptées pour recevoir des informations concernant des vulnérabilités de la part des utilisateurs du produit, service ou processus TIC et des chercheurs actifs dans la sécurité et enfin ; iv) une mention relative aux répertoires en ligne recensant les vulnérabilités publiquement divulguées liées au produit, service pou processus TIC ainsi que tout conseil pertinent en matière de cybersécurité[78].

[73] Considérant 94 du Règlement.
[74] Article 53.4 et considérant 79 du Règlement.
[75] Article 2, 22) du Règlement.
[76] Article 53.1 du Règlement.
[77] Article 53.3 du Règlement.
[78] Article 55 du Règlement.

Par ailleurs, le législateur précise ces informations doivent être disponibles sous un format électronique et demeurer accessibles au moins jusqu'à l'expiration du certificat de cybersécurité ou de la déclaration de conformité[79].

d. Réclamation

Les personnes physiques ou morales ont la possibilité d'introduire une plainte auprès de l'émetteur d'un certificat de cybersécurité européen. Cette dernière doit, en revanche, être adressée à l'autorité nationale de certification de cybersécurité lorsqu'elle se rapporte à un certificat délivré par un organisme d'évaluation de la conformité[80].

Il est prévu que l'autorité ou l'organisme recevant la réclamation informe la partie demanderesse de l'état d'avancement de la procédure et de décision prise. De surcroît, la personne doit également être informée de son droit à porter sa réclamation auprès d'un juge[81].

En effet, nonobstant la démarche auprès de l'autorité de certification ou l'organisme d'évaluation, la personne physique ou morale conserve le droit à un recours juridictionnel effectif pour i) les décisions de délivrance non-justifiée d'un certificat de cybersécurité européen ; ii) la non-délivrance de celui-ci ; iii) la reconnaissance d'un certificat de cybersécurité européen détenus par cette personne physique ou morale ou encore ; iv) l'absence de réaction de la part de l'autorité de certification ou l'organisme d'évaluation face à une réclamation introduite en vertu de l'article 63[82]. La partie demanderesse doit introduire le recours juridictionnel auprès de l'État membre dans lequel se trouve l'autorité de certification ou l'organisme d'évaluation de conformité de la cybersécurité dont elle désire contester la décision ou l'inaction[83].

e. Sanctions

Les États membres doivent fixer le régime des sanctions applicables aux infractions relatives au cadre de certification de cybersécurité et aux violations des schémas européens de certification. Ils doivent également prendre toutes les mesures nécessaires pour assurer leur mise en œuvre. Le législateur prend soin de préciser que ces sanctions doivent être effectives, proportionnées et dissuasives. En outre, les États membres reçoivent l'obligation d'informer, sans retard, la Commission européen du régime déterminé et des mesures prises ainsi que toute modification qui y serait apportée ultérieurement[84].

IV. ENISA

a. Composition

[79] Article 55.2 du Règlement.
[80] Article 63 du Règlement.
[81] Article 63.2 du Règlement.
[82] Article 64.1 du Règlement.
[83] Article 64.2 du Règlement.
[84] Article 65 du Règlement.

Instituée par le Règlement 460/2004[85], l'Agence de l'Union européenne pour la cybersécurité[86] (ENISA) a vu son mandat successivement prolongé[87]. Le règlement 2019/881 confère à l'ENISA un mandat permanent[88], tout en prévoyant une évaluation de l'Agence au plus tard le 28 juin 2024 puis tous les cinq ans[89].

L'ENISA est composée d'un conseil d'administration, un conseil d'exécutif, un directeur exécutif, un groupe consultatif et un réseau des agents de liaison nationaux[90].

Le conseil d'administration est constitué d'un membre nommé par chaque État membre et de deux membres nommés par la Commission chacun pouvant prendre part au vote et disposant d'une voie[91]. Son corps constitutif doit rencontrer les qualités suivantes : des connaissances dans le domaine de la cybersécurité ainsi que des aptitudes managériales, administratives et budgétaires. Par ailleurs, le législateur invite les États membres à une pérennité de leur membre représentatif afin d'assurer une continuité dans le fonctionnement de l'Agence[92]. Leur mandat est de quatre ans renouvelable[93].

Le conseil exécutif reçoit la mission d'assister le conseil d'administration. Il est ainsi chargé de préparer les décisions devant être adoptées par le conseil d'administration et de l'aider dans le suivi des dossiers[94]. Celui-ci n'est composé que de cinq membres nommés parmi les membres du conseil d'administration. Leur mandat a, pareillement au régime prévu pour le conseil d'administration, une durée de 4 ans renouvelable[95].

La gestion quotidienne de l'ENISA repose sur son directeur exécutif[96]. Il a notamment pour fonction d'adresser une proposition au conseil d'administration pour la création du groupe consultatif de l'ENISA. Ce dernier est composé d'experts représentant les parties prenantes concernées, notamment les entreprises actives dans le secteur des technologies de l'information et de la communication, les fournisseurs de réseaux ou de services de communication

[85] Règlement (CE) 460/2004 du Parlement européen et du Conseil du 10 mars 2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information, *J.O.*, L 11, 13 mars 2004, p. 1.
[86] Pour le site Internet de l'ENISA, voyez https://www.enisa.europa.eu/.
[87] Règlement (CE) 1007/2008 du Parlement européen et du Conseil du 24 septembre 2008 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, *J.O.*, L 293, 31 octobre 2008, p. 1 ; Règlement (UE) 580/2011 du Parlement européen et du Conseil du 8 juin 2011 modifiant le règlement (CE) n° 460/2004 instituant l'Agence européenne chargée de la sécurité des réseaux et de l'information en ce qui concerne sa durée, *J.O.*, L 165, 24 juin 2011, p. 3 et le Règlement (UE) 526/2013 du Parlement européen et du Conseil du 21 mai 2013 concernant l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et abrogeant le règlement (CE) n°460/2004, *J.O.*, L 165, 18 juin 2013, p. 41.
[88] Article 3 du Règlement.
[89] À cet égard, l'article 67 du Règlement dispose que : « *La Commission évalue l'incidence, l'efficacité et l'efficience de l'ENISA et de ses méthodes de travail, ainsi que la nécessité éventuelle de modifier le mandat de l'ENISA et les conséquences financières d'une telle modification. L'évaluation tient compte de toute information communiquée en retour à l'ENISA en réaction à ses activités. Lorsque la Commission estime que le maintien du fonctionnement de l'ENISA n'est plus justifié au regard des objectifs du mandat et des tâches qui lui ont été assignées, elle peut proposer que les dispositions du présent règlement relatives à l'ENISA soient modifiées* ».
[90] Article 13 du Règlement.
[91] Article 18 du Règlement.
[92] Article 14 du Règlement.
[93] Article 14.4 du Règlement.
[94] Les fonctions du conseil exécutif sont détaillées à l'article 19 du Règlement.
[95] Article 20 du Règlement.
[96] L'ensemble des tâches du directeur exécutif sont énumérées à l'article 20 du Règlement.

électroniques accessibles en ligne, les organisations de consommateurs, des universitaires étudiant la cybersécurité et les autorités de contrôle de la protection des données[97].

Le règlement crée également le groupe des parties prenantes pour la certification de la cybersécurité. Il est constitué de membres choisis, par la Commission européenne, parmi des experts représentant les parties prenantes concernées. À l'instar du groupe consultatif de l'ENISA[98], le législateur invite la Commission à une réelle représentativité au sein du groupe en assurant un équilibre des forces en présence tant sur le plan du genre, de la répartition géographique que du secteur d'activité. Ses missions consistent principalement dans le conseil à la Commission portant sur les questions stratégiques relatives au cadre européen de certification et sur des questions générales et stratégiques concernant les tâches de l'ENISA relatives au marché, à la certification et à la normalisation. En cas d'urgence, il doit donner un avis à la Commission et au GECC sur le besoin, pour l'Union, de disposer de schémas de certification additionnels au programme de travail glissant[99].

Enfin, le conseil d'administration doit créer, sur proposition du directeur exécutif, un réseau des agents de liaison nationaux. Ce dernier regroupe les représentants de tous les États membres et a pour principale mission d'assurer l'échange et la communication entre l'ENISA et les États membres[100].

b. Tâches

L'objectif principal de l'ENISA est d'être le point de référence en matière de cybersécurité de l'Union. À cette fin, plusieurs tâches lui sont confiées par le règlement.

Premièrement, l'ENISA est chargée d'apporter sa contribution dans l'élaboration et la mise en œuvre de la politique européenne en matière de cybersécurité. En substance, il est prévu qu'elle apporte son expertise pour l'élaboration et la révision de la politique européenne. En outre, elle a également pour mission d'aider les États membres dans l'application cohérente et harmonisée de la politique européenne[101].

Sa seconde tâche est d'apporter son appui à l'élaboration et à la mise en œuvre de la politique de l'Union en matière de certification[102]. Pour ce faire, elle est chargée de cinq activités principales. Premièrement, elle doit notamment surveiller en permanence les évolutions dans les domaines de la normalisation.
Deuxièmement, l'Agence doit élaborer des recommandations relatives aux spécifications techniques d'utilisation appropriées dans le développement des schémas européens de certification dans les cas où il n'existerait aucune norme. Elle doit également préparer, à la demande de la Commission ou du GECC dans certains cas[103], des schémas européens de

[97] Pour le fonctionnement et les objectifs du groupe consultatif de l'ENISA, voyez l'article 21 du Règlement.
[98] En effet, l'artiche 21.1 du Règlement dispose que, pour le groupe consultatif de l'ENISA, *« le conseil d'administration s'efforce d'assurer un équilibre approprié entre les hommes et les femmes et un équilibre géographique, ainsi qu'un équilibre entre les différents groupes de parties prenantes* ».
[99] Article 22 du Règlement.
[100] Article 23 du Règlement.
[101] Article 5 du Règlement.
[102] Article 8 du Règlement.
[103] Sur l'intervention du GECC, *infra* et voyez également les articles 48.2 et 49.2 du Règlement.

certification de cybersécurité. De manière un peu particulière, ces schémas de certification sont appelés « schémas candidats ». Lors de la préparation d'un tel schéma, l'ENISA doit coopérer avec le GECC – dont l'avis n'est cependant pas contraignant[104] - et entendre toutes les parties prenantes au moyen d'un processus de consultation formel, ouvert, transparent et inclusif. En tout état de cause, les schémas de certification candidats préparés par l'ENISA doivent rencontrer toutes les exigences des schémas européens de certification traditionnels, à savoir principalement la rencontre des objectifs de sécurité fixés par le législateur, les niveaux d'assurance élémentaire, substantiel et élevé et comprendre les éléments devant se trouver dans tous schémas de certification énumérés à l'article 54 de la règlementation[105]. Troisièmement, il revient également à l'ENISA d'évaluer chacun des schémas européens de certification de cybersécurité. Cette évaluation doit avoir lieu au minimum tous les cinq ans et tenant compte des informations reçues en retour des parties intéressées. Le législateur donne la possibilité à la Commission et au GECC de lui demander le démarrage du processus d'élaboration d'un schéma candidat révisé[106]. Le conseil d'administration de l'ENISA conserve toutefois la possibilité, s'il motive sa décision, de rejeter la demande[107]. Quatrièmement, l'ENISA peut décider de participer à l'examen par les pairs des activités et du fonctionnement des autorités nationales de certification.
Cinquièmement et enfin, l'ENISA doit rédiger des lignes directrices relatives aux exigences de cybersécurité des produits, services et processus TIC en coopération avec les autorités nationales de certification et les entreprises du secteur[108] ainsi que des lignes directives relatives également au renforcement des capacités en matière de processus d'évaluation et de certification[109].

Une troisième tâche consiste en une obligation de connaissance et d'information. En effet, l'ENISA est en charge i) d'analyser les technologies émergentes et de fournir des évaluations sur les conséquences potentiels de nouvelles innovations technologiques en matière de cybersécurité, du point de vue tant sociétal que juridique, économique et réglementaire, ii) de produire des analyses stratégiques à long terme des cybermenaces et des incidents, iii) d'informer et de fournir des avis, des orientations et des meilleures pratiques en matière de sécurité des réseaux et des systèmes d'information et iv) de rassembler et traiter les informations du domaine public sur les incidents importants en vue de les transmettre aux citoyens, organisations et entreprises[110].

Une quatrième mission porte sur la coopération européenne et internationale. À cet égard, l'agence doit apporter son expertise à la coopération entre les États membres, entre les institutions, organes et organismes de l'Union ainsi qu'entre les parties prenantes. En particulier, l'ENISA doit soutenir les États membres dans la gestion des incidents ayant un impact significatif ou substantiel sur la sécurité des réseaux et des systèmes d'informations. La directive 2016/1148 détermine de manière non exhaustive cinq critères devant permettre

[104] Articles 49.5 et 49.6 du Règlement.
[105] Article 49.1 du Règlement.
[106] Article 49.8 du Règlement.
[107] Article 49.2 du Règlement.
[108] Article 8.3 du Règlement.
[109] Article 8.4 du Règlement.
[110] Article 9 du Règlement.

d'identifier l'importance d'un incident. Il s'agit du nombre d'utilisateurs touchés par l'incident, la durée de celui-ci, sa portée géographique, sa gravité pour le fonctionnement du service et l'ampleur de l'impact sur les fonctions économiques et sociétales[111]. Ainsi, à la demande d'au moins un États membre, l'ENISA est chargée d'aider dans l'évaluation de ces incidents et dans leurs gestions techniques[112]. Par ailleurs, toujours à la demande d'un ou plusieurs États membres, l'Agence doit venir en aide dans la réalisation des enquêtes techniques *ex post* relatives à ces incidents[113]. Le partage des informations et des solutions est vivement encouragé[114]. Ces obligations s'inscrivent dans la poursuite d'un renforcement de la coopération au sein du réseau des CSIRT, mise en place par la directive 2016/1148[115]. L'ENISA se voit également confier la tâche de participer activement à la réalisation d'une réaction concernée au niveau de l'Union et des États membres en cas d'incidents ou de crises transfrontières de cybersécurité majeurs, notamment par le rassemblement et le partage d'informations[116].

En outre, une coopération doit également se faire avec les autorités de contrôle de la protection de la vie privée et des données à caractère personnel, notamment par l'échange de lignes directrices et d'expérience[117]. Par ailleurs, l'ENISA doit également prendre activement part dans la coopération internationale. En ce sens, elle doit contribuer au travail de l'Union dans le renforcement de sa collaboration avec les pays tiers et les organisations internationales ainsi qu'au sein des cadres internationaux de coopération pertinents[118].

L'Agence de l'Union européenne pour la cybersécurité doit, en parallèle, assurer une mission de sensibilisation et d'éducation du public européen[119]. Elle reçoit également un mandat de participation à la recherche et l'innovation en matière de cybersécurité[120].

c. Transparence

Bien que l'article 26 du règlement dispose que l'ENISA fixe les modalités pratiques pour parvenir à la transparence dans ses règles internes de fonctionnement, il prévoit toutefois qu'elle exerce ses activités avec un niveau élevé de transparence. Elle est donc chargée de veiller à ce que le public et toute personne intéressée dispose d'informations appropriées, objectives, fiables et facilement accessibles, notamment en ce qui concerne le résultat de ses travaux. En

[111] Article 16.4 de la directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union, *J.O.*, L 194/1, 19 juillet 2016 (ci-après « directive 2016/1148)
[112] Article 7.4, b) du Règlement.
[113] Considérant 36 et article 7.4 d) du Règlement.
[114] Article 7.4 et considérant 34 du Règlement. La recommandation (UE) 2017/1548 encourageait déjà une coopération et un partage d'informations entre les États membres et l'ENISA ; recommandation (UE) 2017/1584 de la Commission du 13 septembre 2017 sur la réaction coordonnée aux incidents et crises de cybersécurité majeurs, *J.O*, L 239/36, 19 septembre 2017.
[115] Ce réseau des centres de réponse aux incidents de sécurité informatique est composé des représentants des CSIRT nationaux de chacun des États membre et du CERT-UE (centre de réponse d'urgence pour les institutions et agences de l'Union européenne). Pour plus d'informations relatives aux fonctionnements et aux missions du réseau, voyez les articles 12 et s. de la directive (UE) 2016/1148.
[116] Article 7.7 du Règlement. À ce propos, voyez également F. DUMORTIER, *op. cit.*
[117] Article 7 du Règlement.
[118] Article 12 du Règlement.
[119] Article 10 du Règlement.
[120] Article 11 du Règlement.

outre, son conseil d'administration[121] peut, sur proposition du directeur exécutif[122], autoriser des parties intéressées à participer en tant qu'observateurs à certaines activités de l'ENISA. Notons que le législateur européen n'apporte pas de précision quant aux activités pouvant être ouvertes à l'extérieur.

d. Accès aux documents et confidentialité

L'article 28 dispose que la règlementation relative à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission[123] s'applique également à aux documents détenus par l'ENISA. Pour le surplus, le législateur charge le conseil d'administration d'adopter les règles d'application concrètes de cette obligation de transparence au plus tard pour le 28 décembre 2019.

Par précaution, l'article 27 précise que, sans préjudice de l'article 28, l'ENISA ne peut divulguer à des tiers les informations traitées ou reçues et pour lesquelles, sous réserve de motivation, une demande de confidentialité a été émise. À nouveau, la mise en œuvre de ces modalités pratiques est laissée à l'Agence[124].

[121] Sur la composition, le fonctionnement et les fonctions du conseil d'administration de l'ENISA, voyez les articles 14 à 18 du Règlement.
[122] Sur les tâches du directeur exécutif de l'ENISA, voyez l'article 20 du Règlement.
[123] Règlement (CE) 1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission, *J.O.*, L 145, 31 mai 2001, p. 43.
[124] Notons également que l'article 27.2 du Règlement dispose que « *Les membres du conseil d'administration, le directeur exécutif, les membres du groupe consultatif de l'ENISA, les experts externes participant aux groupes de travail ad hoc et les membres du personnel de l'ENISA, y compris les fonctionnaires détachés par les États membres à titre temporaire, respectent les obligations de confidentialité prévues par l'article 339 du traité sur le fonctionnement de l'Union européenne, même après la cessation de leurs fonctions* ».
À cet égard, l'article 339 du TFUE dispose que « *Les membres des institutions de l'Union, les membres des comités ainsi que les fonctionnaires et agents de l'Union sont tenus, même après la cessation de leurs fonctions, de ne pas divulguer les informations qui, par leur nature, sont couvertes par le secret professionnel, et notamment les renseignements relatifs aux entreprises et concernant leurs relations commerciales ou les éléments de leur prix de revient* ».

V. Conclusion

Dans la perspective de renforcer l'expertise de l'Union européenne en matière de cybersécurité, le règlement met en place un mécanisme inédit : le schéma de certification de cybersécurité. Il consacre un ensemble d'exigences techniques applicables à la certification et à l'auto-évaluation de conformité. Afin d'éviter une fragmentation territoriale, ce schéma est élaboré au niveau européen et est commun à tous les États membres. Par ailleurs, après leur réalisation, tant la certification que l'auto-évaluation sont reconnues par tous les États.

Si la certification ne peut être garante du risque zéro, le schéma européen établit néanmoins trois niveaux d'assurance en fonction du caractère plus ou moins poussé du contrôle effectué : élémentaire, substantiel ou élevé. Chacun de ces niveaux répond à des exigences particulières et peut être délivré uniquement par l'organisme compétent désigné par la réglementation.

Afin d'améliorer la culture commune de la cybersécurité entre tous les États membres, le législateur leur impose la désignation d'une ou plusieurs autorités nationales de certification. Ces autorités ont un rôle dans la délivrance des certifications d'un niveau d'assurance élevé et une mission de supervision des activités des fabricants ou fournisseurs de produits, services ou processus TIC.

En outre, le règlement dote l'ENISA d'un mandat permanent et non plus limité qui aurait dû venir à expiration en 2020. L'ENISA voit également ses missions renforcées. En effet, elle est en particulier chargée d'apporter son appui et son expertise à l'élaboration et à la mise en œuvre de la politique de l'Union en matière de certification.

À la lecture du règlement, force est de constater que le législateur, sensible aux évolutions technologiques et à la rapidité de détection des failles de sécurité par les *hackers*[125], insiste sur des évaluations permanentes de la situation de l'Union en matière de cybersécurité et met en place plusieurs corps au sein de l'ENISA afin de permettre des temps de réflexion et d'échanges d'information. Il revient désormais à la Commission européenne de mettre en place son programme de travail afin de déterminer les prochains axes stratégiques en matière de cybersécurité et de prioritiser les produits, services et processus TIC devant entrer dans le champ d'application du schéma européen de certification. Celui-ci est attendu, au plus tard, le 28 juin 2020. Gageons que l'Union parviendra à trouver un équilibre entre ambition et réalisme...

[125] Pour une approche critique de l'absence de la problématique des *ethical hackers*, voyez la contribution de V. VANDER GEETEN dans cet ouvrage.