Glossaire

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information
CC: Critères Communs
CESTI: Centre d'Evaluation de la Sécurité des Technologies de l'Information
CISSP: Certified Information System Security Professional
COFRAC: Comité Français d'Accréditation
CSPN: Certification de Sécurité de Premier Niveau
CYBERACT : CybersecurityAct
ENISA: European Network and Information System Agency
GECC: Groupe Européen de Certification de Cybersécurité
HDS: Hébergement de Données de Santé
IoT: Internet of Things
(ISC)²
ISO
OSE: Opérateur de Service Essentiel
PCI-DSSI: ??
TIC : Technologies de l'Information et des Communications

Définitions

Examen par les pairs[1] désigne la procédure de vérification de la transparence et de cohérence de l'organisation des autorités nationales en charge de la certification nationale des produits, services et processus TIC de cybersécurité. L'objectif est d'assurer une harmonisation des normes au niveau des schémas de certification. L'examen par les pairs est réalisé au moins une fois tous les cinq ans par au moins deux autorités nationales de certification de cybersécurité d'autres États membres et par la Commission. L'ENISA peut participer à l'examen par les pairs.

Groupe des parties prenantes[2] désigne les membres sélectionnés parmi des experts reconnus représentant les parties prenantes concernées. La Commission, à la suite d'un appel transparent et ouvert, sélectionne, sur la base d'une proposition de l'ENISA, les membres du groupe des parties prenantes pour la certification de cybersécurité en assurant un équilibre entre les différents groupes de parties prenantes ainsi qu'un équilibre approprié entre les hommes et les femmes et un équilibre géographique.

Marché Unique numérique désigne le marché européen dans lequel la libre circulation des biens, des personnes, des services et des capitaux est garantie, et où les citoyens et les entreprises bénéficient d'un accès homogène et équitable aux biens et services en ligne[3]

---

[1] Art. 59 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013
[2] Art. 22 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013
[3] https://ec.europa.eu/commission/priorities/digital-single-market_fr

Niveau d'assurance[4] désigne 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 mais, en tant que tel, ne mesure pas la sécurité du produit TIC, service TIC ou processus TIC concerné;

Processus TIC désigne un un ensemble d'activités exécutées pour concevoir, développer ou fournir un produit TIC ou service TIC ou en assurer la maintenance[5];

Produits TIC désigne un élément ou un groupe d'éléments appartenant à un réseau ou à un schéma d'information[6];

Services TIC[7] désigne un service consistant intégralement ou principalement à transmettre, stocker, récupérer ou traiter des informations au moyen de réseaux et de systèmes d'information;

Logique d'intégration désigne la situation dans laquelle des élites de plusieurs cadres nationaux distincts sont persuadés de transférer leurs loyautés, attentes et activités politiques vers un nouveau centre, dont les institutions possèdent ou revendiquent des compétences supérieures à celle des Etats nationaux préexistants[8]

Logique de coopération désigne la situation dans laquelle des entités s'organisent ensemble par une logique de compromis et d'avantage afin de tirer des bénéfices d'une coopération, tout en préservant leur compétence nationale.

[4] Article 2, 21) du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013 :

[5] Art. 2, 14), du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[6] Art. 2, 12) du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[7] Art. 2 13) du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[8] HAAS Ernest B., « The uniting of Europe : political, social and economical forces 1950-1957 ", Stanford, Stanford university Press, 1958, 1968, 2004 (3ème edition), p.16.

PARTIE I L'ETAT DE L'ART DES CERTIFICATIONS DE CYBERSECURITE

Dans un contexte de numérisation croissante de la Société où le marché des technologies de l'information est en pleine explosion, la confiance des utilisateurs repose désormais sur des fournisseurs de produits et services, jugés experts dans leur domaine. Un déséquilibre des connaissances sur le produit ou service est alors apparent entre le côté demandeur (les utilisateurs) et les fournisseurs de produits et de services. En effet, la consommation des technologies des produits, services et processus TIC se fonde sur une relation de confiance et de garanties à respecter. Cependant, suite à de nombreux scandales comme celui du "*Cambridge Analytica*", liés à la sécurité des données collectées, les usagers tendent à perdre progressivement confiance en les acteurs et les produits du numériques. Cette remise en cause d'un marché numérique de confiance conduit à une prise d'acte de l'Union Européenne afin d'assurer une régulation du "*cyberespace*".

Dans cette perspective, nous étudierons dans ce premier article l'état de l'art des certifications en cybersécurité et les enjeux soulevés entre les modèles publics et privés. Nous poursuivrons sur une dimension européenne de ces enjeux dans un deuxième article.

I) Une certification selon les besoins

La certification est délivrée par un organisme agréé et extérieur à l'entité demandeuse, à l'issue d'un processus visant à s'assurer de la conformité du produit, service ou processus TIC avec un référentiel de normes de sécurité défini. Le processus est similaire pour la certification de personne, qui permet d'attester des connaissances d'un individu sur un domaine déterminé.

Dans un premier temps il est nécessaire de s'accorder sur la définition de ces normes. Puis d'évaluer objectivement selon un référentiel commun[9] pour délivrer une certification. Pour s'assurer de la conformité dans le temps il est nécessaire de renouveler périodiquement la certification.

Les tiers de confiance en charge de ce processus sont appelés les centres de certification, qui réalisent les analyses selon une méthode accréditée[10]. Ces centres de certification sont eux même "certifiés" (on parle "d'accréditation" dans ce cas) par une autorité française, le COFRAC[11].

1. Les domaines de certification

Il existe plusieurs domaines de certification, par exemple: l'environnement[12], la santé[13], l'agroalimentaire[14]. Mais qu'en est-il de la sécurité du secteur récent de l'information et des technologies numériques ? Nous proposons ci-dessous quelques exemples de certification de sécurité de l'information selon les besoins:

- La certification ISO 27001[15] pour attester du management de la sécurité de l'information dans un organisme. Elle s'intéresse à la prise en compte des exigences de sécurité des processus et des systèmes mais surtout à la mise en place d'un processus d'amélioration continue.

[9] https://fr.wikipedia.org/wiki/Certification; https://www.iso.org/fr/standard/46568.html
[10] https://www.cofrac.fr/qui-sommes-nous/notre-organisation/la-section-certifications/
[11] https://www.cofrac.fr/qui-sommes-nous/
[12] https://agriculture.gouv.fr/certification-environnementale-mode-demploi-pour-les-exploitations
[13] https://www.has-sante.fr/portail/jcms/c_411173/fr/mieux-connaitre-la-certification-des-etablissements-de-sante
[14] https://certification.afnor.org/secteur/agroalimentaire
[15] https://www.iso.org/fr/isoiec-27001-information-security.html

- La certification CISSP maintenue par l'organisation International Information System Système Security Certification Consortium(ISC)², vérifie le niveau de connaissance d'une personne.
- L'hébergement de données de santé doit être certifié Hébergement de Données de Santé HDS[16], et les applications bancaires doivent être conforme à Payment Card Industry Data Security Standard PCI-DSS[17].

En France l'Agence Nationale des Systèmes d'Information (ANSSI) est en charge de définir les référentiels de sécurité pour les TIC, et a autorité sur les évaluateurs tiers, les CESTI[18]. Le schéma français offre deux types de certification de la sécurité des TIC[19]:

- La certification Critères Communs (CC), standard internationalement reconnu, évalue la robustesse d'un produit selon 7 niveaux (de EAL1 à EAL7)[20]. Plus le niveau d'assurance visé est élevé, plus les éléments de preuve attendus sont précis et l'effort d'évaluation important. La durée de l'évaluation peut varier de 6 à 18 mois.
- La Certification de Sécurité de Premier Niveau (CSPN) est une alternative aux CC, lorsque le niveau de confiance visé est moins élevé, l'analyse étant réalisée en temps contraint avec un cahier des charges moins exhaustif[21] (un délai de 2 mois).

Une certification CC est reconnue internationalement, alors que la certification CSPN est reconnue en France avec un objectif européen à court-moyen terme[22]. Dans les deux cas l'évaluation passe par une analyse de la conformité et une analyse des vulnérabilités d'un produit.

2. Les avantages et inconvénients de la certification

Outre le gage de confiance auprès des utilisateurs, l'objectif d'une certification est de répondre à des exigences sécuritaires, réglementaires, contractuelles ou commerciales.
Il est donc intéressant pour un organisme de s'appuyer sur la certification pour avoir l'assurance d'un produit, service, sans avoir à réaliser à sa charge la vérification de la conformité. Il en va de même pour les organismes fournisseurs de s'appuyer sur la certification afin d'attester de la complétude à un référentiel de leurs produits, services ou processus, le tout vérifié par un tiers de confiance indépendant.
La certification d'une conformité à la sécurité par exemple peut fortement orienter le choix du client au détriment d'un produit, service ou processus certifié plus faiblement voire non contrôlé. Cela peut donc représenter un atout de poids face à la concurrence. Cependant, ce processus peut mobiliser d'importantes ressources temporelles, financières et humaines, et peut se révéler coûteux pour une reconnaissance parfois limitée. La certification peut alors dans certains cas être un facteur d'inégalité et revêt en cela un élément d'investissement stratégique.
Outre la confiance les objectifs d'une certification peuvent être de répondre à des exigences réglementaires, contractuelles ou commerciales. Cependant selon le niveau d'assurance visé, suivant le niveau d'assurance visé ce processus est coûteux en temps, argent et ressources humaines pour une reconnaissance limitée (périmètre du service, version du produit ou reconnaissance par un État).

Comme nous le remarquons des acteurs du secteur public et du secteur privé proposent différentes certifications qui parfois se recoupent. Pour des certifications à périmètre ISO, quels sont les points différenciants? Sur quels critères sélectionner le modèle adéquat à la stratégie du fournisseur ?

[16] https://esante.gouv.fr/labels-certifications/hds/certification-des-hebergeurs-de-donnees-de-sante
[17] https://www.pcisecuritystandards.org/
[18] https://www.ssi.gouv.fr/administration/produits-certifies/
[19] https://www.ssi.gouv.fr/uploads/2018/01/certification_securite_produits_visa_securite_anssi.pdf
[20] https://www.ssi.gouv.fr/administration/produits-certifies/cc/
[21] https://www.ssi.gouv.fr/administration/produits-certifies/cspn/
[22] https://www.ssi.gouv.fr/administration/produits-certifies/certification-faq/

II) Les enjeux inhérents aux schémas de certification public et privé.

Après avoir vu le panorama des certifications existantes, nous pouvons nous demander quels sont les enjeux de ces deux modèles de certification (public et privé).

La cybersécurité étant un domaine récent, la littérature scientifique à ce sujet est encore limitée. Afin de présenter une analyse pertinente et pour appuyer notre démonstration, nous nous sommes tournés vers l'exemple de la sécurité des biens et des personnes dans le domaine de l'agroalimentaire, bien plus fournis en écrits. La logique régissant la certification dans ces deux domaines est identique à celle que nous souhaitons étudier en cybersécurité puisqu'elle est motivée par la protection des personnes utilisant ces produits, services ou processus.

Si nous classons les méthodes de certification, l'on peut distinguer deux grandes catégories:

- Le tampon approbateur d'un organisme public.
- La mise en place par des acteurs privés de leur propre certification.

Intéressons-nous à présent aux caractéristiques de ces deux modèles de certification qui présentent chacun des avantages et des inconvénients, pouvant représenter des atouts comme des faiblesses pour l'organisme certifié.

Quand choisir une certification issue des organismes publics ?

Les premières normes sont définies par des organismes publics afin de garantir une impartialité sur la prise de décision. Son objectif premier est de protéger les utilisateurs. Dans le cadre de l'agroalimentaire dont l'objectif est de garantir que le produit peut être consommé sans crainte d'empoisonnement alimentaire et satisfait un niveau de qualité suffisant. Dans la cybersécurité les certifications disponibles valident bien la qualité d'un produit ou d'un service mais elle n'est pas destiné au grand public. Même la PCIDSS est destiné aux assureurs pour leur garantir un niveau de risques de vols de données minimal. Les autres certifications dites "tampons" sont plutôt destinés pour les industriels ou bien le marché de la Défense.
Les exigences sont fixées par l'organisme public et diffusées afin que chacun puisse en prendre connaissance. Il est possible pour tout le monde de vérifier le contenu de la certification et de la challenger si nécessaire. Ainsi chacun peut connaître les exigences pour se faire certifier ou réaliser une évaluation préliminaire. La certification quant à elle est délivrée par l'organisme public ou bien par des organismes privés dépositaires de l'autorité. Ce second aspect permet de libérer les coûts du processus de certification auprès d'organismes privés. Nous retrouvons le CSPN comme type de données ou bien plus habituellement toute la protection liée au personnes comme la ceinture de sécurité pour une voiture.

Avec le temps il arrive que des organismes privés, en général des acteurs importants du marché, décident de se mobiliser pour proposer leur propre certification. Ceci répond à un besoin d'adapter plus rapidement les dispositifs existants aux nouvelles technologies. Le cycle de décision plus court des organismes privés permet en effet de revoir régulièrement la liste des exigences mises à jour.
Ces mises à jour régulières créent des niches pour les acteurs qui ont la capacité de s'adapter rapidement. Ainsi lorsque les exigences sont trop élevées ou différentes des exigences précédentes, la capacité de se mettre rapidement en conformité représente un critère voire une condition permettant à l'acteur de s'assurer une place sur le marché, en particulier si celui-ci est régulé par la

norme en question. Il arrive parfois que le régulateur s'approprie la norme "privée" pour contrôler les organismes sous sa tutelle. C'est ce qui se passe avec le lait sur le marché vénézuélien.
De plus, proposer sa propre certification implique stratégiquement une connaissance du marché global (concurrents, environnement, opportunités et obstacles) sur le domaine concerné et témoigne donc d'une vision proactive et d'une volonté de s'imposer sur ce marché.
Enfin, la certification privée permet aux acteurs de garantir un niveau de qualité attendu. Cela permet de fluidifier le marché entre les différentes entités. C'est ce qui permet par exemple de garantir un niveau minimum de qualité pour le lait afin de les mélanger plus facilement. Dans les technologies de l'information ces normes permettent de garantir un niveau d'interconnectivité entre les différents systèmes.

Les schémas de certification sont multiples, permettant ainsi de choisir celle convenant le mieux à notre besoin. Cette pluralité permet de conserver un marché dynamique et concurrentiel. Dans cet environnement, l'Union européenne s'engage à proposer ses propres schémas de certification.
Pour comprendre la genèse de ce modèle et les enjeux qui en découlent, nous vous invitons à lire la deuxième partie traitant du CybersecurityAct.

PARTIE II Le modèle européen du cadre de certification

La législation européenne est le jeu de négociation des Etats membres qui œuvrent par le moyen du compromis. Cet objectif du compromis articule compétences exclusives, partagées ou d'appuis, afin de concilier intérêt national et l'intérêt général de l'Union européenne (UE).
Le CybersecurityAct, règlement européen, directement applicable en droit national, est porteur d'enjeux cruciaux en termes de cyber sécurité, mais aussi politique et économique pour l'ensemble de ses Etats membres. Nous découvrirons d'abord la création du modèle européen de certification, en présentant un historique de sa législation, ses enjeux et son contenu. Puis, nous proposerons une mise en perspective de ce cadre européen des schémas de certification.

I) La genèse du modèle européen de certifications

A. Historique de la législation, les raisons, les moyens

La cyber sécurité est une composante de la sécurité-défense, relevant de la compétence des États qui dépend du ressort national.

En 2010 la Commission européenne estime que les TIC génèrent 5% du PIB européen, représentant une valeur marchande de 660 milliards d'euros, et près de la moitié des gains de productivité au sein de l'UE[1]. Souhaitant faire du numérique un facteur de croissance, l'UE organise l'harmonisation du cadre règlementaire du marché numérique. Toutefois, s'il est vecteur de productivité et de croissance, il est également la porte ouverte aux cyber menaces en constantes augmentation. A ce titre, le Conseil estime en effet que les cyberattaques coûteraient environs 400 milliards d'euros par an à l'économie mondiale[2].

En février 2013, l'UE s'ouvre ainsi un champ d'action propre à la cybersécurité avec sa stratégie pour un cyberespace ouvert, sûr et sécurisé[4]. Liant besoin de sécurité et opportunité économiques, en 2015, la commission Junker lance la Stratégie européenne du Marché unique numérique[5] afin de contrer l'hégémonie nord-américaine et d'exploiter le potentiel économique du numérique. Selon le Conseil, les dirigeants de l'UE « considèrent que la réforme de la cybersécurité est actuellement l'un des principaux volets du processus visant à compléter le **marché unique numérique** de l'UE »[6].

Le 13 septembre 2017, le président de la Commission européenne, Jean-Claude Juncker présente la stratégie « Résilience, dissuasion et défense : construire une cybersécurité forte en Europe »[8], lequel contient la proposition de Règlement Cybersecurity Act sur l'ENISA et pour la première fois un cadre européen de schémas de certification européenne.

Adopté le 12 mars 2019, avec 586 voix pour, 44 contre et 36 abstentions, le CyberAct constitue le terreau de l'Union européenne en cybersecurité, en quête de s'inscrire sur la scène internationale en tant qu'acteur prédominant du cyberespace. Le règlement a été publié le 7 juin 2019 au Journal Officiel de l'UE.

Ce système de certification prendrait la forme d'un ensemble de règles, d'exigences techniques et de procédures à respecter, dans un schéma de certification qui dépendrait du contexte d'utilisation du produit ou service, et du niveau d'assurance. Il aurait pour rôle de « réduire la fragmentation des

marchés et de supprimer les obstacles réglementaires, tout en renforçant la confiance. Ces schémas de certification seraient reconnus dans tous les États membres, ce qui permettrait aux entreprises de mener plus aisément des activités transfrontières »[10]. Les entreprises pourront ainsi commercialiser plus facilement leurs produits connectés au sein de l'UE et les consommateurs seraient en mesure de faire des choix davantage éclairés, poursuivant la logique de ce marché unique.
Pour arriver à ses fins, l'UE élargit le mandat donne à l'ENISA et lui alloue un budget de 8 millions d'euros par an et de double ses effectifs pour arriver à 125 personnels. De même le FED (Fond Européen de Développement) réserve 5% de son budget aux projets cyber communs.

B) La mise en place d'une certification européenne

1. La présentation du processus décisionnel

La Commission européenne établit un programme de travail de l'Union pour la certification européenne de cybersécurité. Celle-ci est appuyée par le GECC et par le groupe des parties prenantes (GEPP). Ce programme de travail inclut une liste de produits, services et/ou de processus TIC susceptibles d'entrer dans le champ d'application du futur schéma de certification européenne[23]. Leur référencement doit se justifier au regard de différents objectifs pris alternativement, tels que la disponibilité et le développement de schémas nationaux (risque de fragmentation), le droit ou la politique applicable de l'Union ou d'un État membre, la demande du marché, l'évolution de la situation concernant les cybermenaces, ou enfin, d'une demande de préparation d'un schéma candidat émanant du GECC.

Ces objectifs définis sont circonstanciés à l'évolution des sociétés. Toutefois, si en théorie ces derniers semblent ne présenter aucune difficulté de mise en oeuvre, en pratique la discorde peut se trouver au sujet de l'interprétation des différentes notions.

Remarques. A titre d'exemple, comment arbitrer la vérification de l'objectif "critère de marché"? Quel est le seuil à partir duquel un schéma de certification doit être lancé?

De plus, La référence à l'existence ou non de cybermenaces n'est-elle pas poreuse? Faut-il donc attendre que le risque soit beaucoup plus élevé et critique pour agir? Comment évaluer véritablement le besoin de la société en se référant à un critère ne matérialisant pas la situation réelle à un instant T ?

Une fois élaboré, le programme de travail est communiqué aux organismes de normalisation et de régulation, les entreprises du secteur des Etats Membres. Cette transparence permet aux entités nationales de bénéficier d'un aperçu du future cadre de travail de l'ENISA par référence au programme de travail précédemment établi par la Commission européenne.

De plus, sur demande de la Commission européenne, et dans certains cas, le GECC, l'ENISA peut être enjointe de préparer un schéma candidat ou de réexaminer un schéma existant. Si malgré les

[23] Art. 47 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

sollicitations de la Commission européenne et du GECC, l'ENISA atteste d'un refus, celui-ci doit être justifié[24].

Remarques.

Quels sont les cas particuliers auxquels il est fait référence? La Règlement spécifie seulement que "la Commission et le GECC devront évaluer le bien-fondé d'une telle demande en tenant compte des finalités et objectifs généraux du présent règlement et de la nécessité d'assurer la continuité en ce qui concerne la planification et l'utilisation des ressources par l'ENISA"[25].

Une fois le rôle de l'ENISA achevé, la Commission est habilitée à adopter le schéma européen de certification de cybersécurité par voie d'actes d'exécution. Le schéma de certification est conçu pour réaliser des objectifs de sécurité, préciser le niveau d'assurance concerné et certaines informations utiles aux utilisateurs[26].La délivrances des certifications demeurera sous la compétence des autorités nationales de certification.

En outre, l'ENISA devrait tenir informer les citoyens européens en indiquant différentes informations sur un site web, dont les schémas adoptés pour les produits, services, ou processus TIC spéficiques, puis détailler les schémas nationaux de certification de cybersécurité remplacés par un nouveau schéma[27].

2. Harmonisation des standards de sécurité : définition de niveaux d'assurance européens

Les schémas de certification actuels présentent des différences en termes de couverture des produits, de niveaux d'assurance, de critères de fond et d'utilisation effective, ce qui entrave les mécanismes de reconnaissance mutuelle au sein de l'Union[28]. De plus, l'adoption des nouveaux schémas européens remplacera, *de jure,* les schémas nationaux existants. Le Règlement Européen pallie à cette carence en précisant que les schémas de certification devront définir les niveaux d'assurance à atteindre[29]. Il se décomposent selon les trois niveaux suivants:

[24] Art. 49 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[25]Considérant 84 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[26] Art. 51 à 54 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[27] Considérant 85 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[28] Considérant 67) du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

[29] Art. 51-52 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013

Niveau d'assurance	*Elémentaire*	*Substantiel*	*Elevé*
Champ d'application	Minimisation des risques élémentaires d'incidents ou de cyberattaque connus. Est principalement concerné le marché de l'Internet des Objets ou IoT.	Minimisation des risques connus de cybersécurité, cyberattaques ou incidents et émanant d'acteurs aux aptitudes et aux ressources limitées. Est concerné le Cloud (le service informatique en nuage).	Minimisation du risque de cyberattaques de pointe soient menées par des acteurs aux aptitudes solides et aux ressources importantes, "significatives". Est concerné le marché des véhicules connectées ou des solutions de télémédecines (appareils informatiques médicaux).
Evaluation	1 examen de la documentation technique	Vérifier les exigences de l'examen élémentaire. Vérifier l'absence de vulnérabilités connues du public et la mise en œuvre des fonctionnalités de sécurité par les produits, services et processus TIC.	Vérifier les exigences de l'examen substantiel. Vérifier l'absence de vulnérabilités connues du public, que les produits, services ou processus TIC mettent correctement en œuvre les mesures de sécurité, au niveau de l'état de l'art.
Auto-évaluation[30]	Oui	Non Des tests sont réalisés par un tiers de confiance, étant le Conformity Assessment Body (CAB).	Non Évaluation de la résistance des produits, services et processus TIC aux attaques par des tests de pénétration. Ces tests sont réalisés par un tiers de confiance.
Examen par les pairs[31]	**Système général d'évaluation par les pairs.**		**Système spécifique d'évaluation par les pairs.** La Commission européenne adopte des actes d'exécution établissant un plan quinquennal d'examen par les pairs entre les autorités nationales de certification de cybersécurité.

[30] Art. 53 du Règlement européen relatif à l'ENISA (Agence de l'Union Européenne pour la cybersécurité et à la certification de cybersécurité ds technologies de l'information et des communications et abrogeant le Règlement (UE) N° 526/2013.

[31] Note XXXX, Ibid.

*II . **Les perspectives issues du modèle européen de certifications***

Ce nouveau cadre législatif apporte de nouveaux enjeux et perspectives sur le marché du numérique et prête à de nombreuses controverses qui ont contribué à limiter la portée contraignante d'un cadre de certification harmonisé.

A. L' Europe à deux vitesses, facteur d'une législation harmonisée à double tranchants

L'élaboration des "futurs" schémas de certification est influencée par les autres modèles existants dont notamment ceux français. Les CESTI français, sont déjà au niveau requis mais également pour les entrants en certification qui vont ainsi gagner un avantage compétitif à l'échelle européenne. Cette harmonisation se fait-elle donc au détriment des entités nationales des autres Etats Membre. Harmoniser les cadre de certification en UE pourrait viser, selon le principe de concurrence accrue, à garantir un marché performant, incitant les Etats membres à offrir des produits et services TIC de qualité pour un coût abordable. Pourtant, sans prise de compte des écarts en dotation de cybersécurité des états membres au départ, sur un marché aussi disparate que celui de la cyber en UE, une réglementation communautaire en matière de cybersécurité pourrait s'avérer contraignante aux vues des intérêts commerciaux nationaux, qui dans le secteur de la sécurité peuvent se relever de la souveraineté des Etats membres. Cela pourrait conduire à exacerber la concurrence intra européenne et le repli national au lieu de générer une force européenne. Parallèlement des Etats membres offrant produits et services TIC au niveau de sécurité faibles (Roumanie, Bulgarie) auraient avantage à se faire certifier par des Etats membres à l'expertise moins développé (moins coûteuse et moins experte pour estimer), pour un niveau de sécurité reconnu in fine équivalent à celui des Etats membres avancés en cybersécurité (France, Allemagne, Estonie). Ce qui représente un risque d'instaurer un niveau de sécurité réel à la baisse au profit du commerce. (**à fusionner**) L'expertise cyber étant inégale même en Europe, il pourrait être plus simple de valider sa certification dans un pays moins strict. Cela entraînerait une course au moins disant et un abaissement du niveau de sécurité des pays les plus avancés. Cette hétérogénéité dans la mise en oeuvre pratique du processus de certification conduirait à un *cherry picking*[32] des autorités nationales de certification et cela contreviendrait à la raison d'être de la réglementation.

Afin de pousser cette volontée marquée par la Commission européenne de faire de la certification une cause européenne (reformuler) dans le domaine de la cybersécurité, on aurait pu envisager, une fois le modèle adéquat stabilisé, d'encourager les assureurs à accorder les assurances qu'aux produits et services TIC disposant d'un niveau de sécurité minimum référencé par l'UE.

B. Le soft power européen facteur d'inefficacité en matière de certification ?

La complexité de l'UE à imposer une réglementation contraignante implique entre autres une définition imprécise des notions de ressources importantes alors que le règlement stipule que la certification européenne pourrait ultérieurement être contraignante sur les niveaux de sécurité élevé pour les OSE. Le champ d'application des niveaux d'assurance élémentaire, substantiel et élevé repose sur des imprécisions. En effet, il est fait référence aux notions de ressources importantes / ressources limitées et au ratio relatif aux mesures de sécurité appréciées selon de l'état de l'art. Le modèle de certification et l'état de l'art sont définis à un instant T tandis que les enjeux de

[32] un choix à la carte

cybersécurité sont plus que jamais en essor et évolutifs. Il s'agit d'un modèle européen qui laisse beaucoup de marge à interprétation et donc une application hétérogène dudit règlement.

En effet, tel que finalement voté après le jeu de négociation entre les intérêts des Etats membres (le Conseil), ceux de la communauté (La Commission) et ceux des citoyens (le Parlement européen), l'on peut redouter une efficacité moindre de cette initiative pourtant forte de la Commission, puisqu'elle reste *in fine* cantonnée à du volontariat (soft power).

Cette limitation d'action et d'efficacité de l'UE est également démontrée par un projet d'envergure qui n'a à l'heure actuelle pas l'ambition de ses moyens. On constate en effet que l'effectif de l'ENISA devrait passer à 125 avec ce règlement alors que l'ANSSI dispose de 600 agents fin 2017 et l'Office fédéral de la sécurité des technologies allemande, le BSI, de 800. De plus l'ENISA est dotée par la Commission d'un budget de 23 millions en cybersécurité en 2022 soit de nombreux postes prioritaires autres que la certification. Ce qui peut paraître dérisoire au vu du défis et de l'impact que l'agence Européenne semble vouloir porter.

Au profit d'une certification européenne volontaire, le CESE[1] voue par exemple à l'Agence ENISA un rôle de support aux instances nationales. Celles-ci lorsqu'elles existent au sein des Etats membres, sont considérées comme davantage spécialisées, détentrices d'une expertise et d'une confiance des opérateurs[2] et acteurs cyber, dont l'agence européenne et l'UE à grande échelle, ne dispose pas. Au regard des enjeux de la certification entre les états membres, la "faible" dotation en moyens de l'UE témoigne de sa difficulté à appréhender et à concilier l'ensemble des données à prendre en compte, afin d' établir une certification harmonisée à la hauteur des défis cyber de nos jours.

CONCLUSION

Dans notre société mondialisée, l'ultra numérisation se développe un une vitesse exponentielle. Porteuse de progrès technique, d'opportunité économique et de développement sociétal et humain, l'essor des TIC s'accompagne de menaces dont il ne faut plus seulement les maîtriser mais également et de plus de plus les appréhender avec une longueur d'avance pour survivre et bénéficie de son caractère avantageux. Être proactif et résilient devient non plus une source d'avantage mais la condition de maintien dans l'arène de la concurrence et de la sécurité numérique. L'UE, reposant sur des fondations commerciales et économiques, se trouve en difficulté d'avancer dans le domaine du numérique de façon légitime et contraignante, face à 28 intérêts distincts qui peuvent peiner à voir leur intérêt communautaire comme égal; en témoigne l'épisode historique du Brexit. Les fondements de l'UE datent de 1945 et les préoccupations d'après guerre ne sont plus d'actualité au vu du changement de paradigme face à la nature numérique de la guerre au 21ème siècle. Au coeur de ces deux problématiques (commerce et sécurité) la certification européenne, instrument d'une tentative d'organisation communautaire pour se saisir des opportunités de notre ère au gré de ses fondations, pourrait mettre en lumière le besoin de faire évoluer une organisation à la racine, qui doit évoluer avec les problématiques qu'elle essaye de réglementer.
Au vue de l'écosystème de certification déjà existant, on peut s'interroger sur la pertinence d'un modèle supplémentaire à une échelle communautaire. Ce modèle arrivera-t-il à s'imposer et devenir une référence?