Référentiels et labels de sécurité et de confiance numériques : de la nécessité d'une stratégie de politique industrielle au service de la sécurité et de la compétitivité de la filière et des donneurs d'ordre !

Préambule

« *Le poids des normes, qui pénalise la croissance, (…) est de près de 4 % en France, soit dix fois plus que chez nos voisins. Cette contrainte constitue un frein insupportable à l'activité de notre pays (…). Le gouvernement s'engagera donc dans un puissant mouvement de débureaucratisation.* », déclaration de politique générale du Premier ministre, le 14 janvier 2025.

Dans cette perspective, le sujet des référentiels et des labels de sécurité et de confiance numériques présente des opportunités de simplification aptes à redonner de la compétitivité aux entreprises et des marges de manœuvre aux collectivités. Mais il nécessite un effort coordonné entre différents acteurs, pour clarifier en premier lieu les objectifs et les méthodes.

Ce sujet des référentiels et labels de sécurité numérique est d'autant plus d'actualité que la directive européenne « NIS 2 », votée par le parlement européen en 2022 et dont la transposition en droit national est en cours d'étude au Parlement, encouragent le recours à des normes et des spécifications techniques européennes et internationales. Cette directive indique que les États membres peuvent prescrire des produits et services certifiés dans le cadre de schémas européens afin de démontrer la conformité à certaines exigences[1].

Il existe aujourd'hui en France une multitude de référentiels traitant de la sécurité numérique répondant à différents objectifs (pas toujours clairement définis) avec, pour certains, la possibilité d'obtenir des labels de conformité. Force est de constater que cette multiplicité est contre-productive et coûteuse pour les donneurs d'ordre et les prestataires.

De ce fait, plusieurs questions se posent, et en particulier :

- Qui, au sein de l'État, **possède la compétence et la connaissance** pour porter efficacement le sujet des référentiels et des labels de sécurité et de confiance numériques ?
- Qui, au sein de l'État, a **en charge le sujet de la coordination** des référentiels et labels de sécurité et confiance numériques pour la France et **leur promotion** au niveau international ?
- Quels sont la **cohérence** et le poids des référentiels et des labels nationaux avec les standards internationaux (ISO[2] par exemple) et les réglementations françaises et européennes ?
- Qui a en charge **l'évaluation de l'efficacité**, tant sur le plan de la sécurité et de la confiance numériques que sur le plan économique, des référentiels et labels en France ? Quels sont, par exemple, les avantages compétitifs au regard des coûts engendrés par la mise en conformité aux référentiels ou à l'obtention de labels ?
- Enfin, pourquoi ne pas avoir développé en France **un schéma unique** de référentiels et de

1 articles 24 et 25 de la directive dite « NIS 2 » votée par le parlement européen en 2022 dont la transposition en droit national est en cours d'étude au Parlement

2 L'ISO est l'organisation internationale de normalisation.

labels de sécurité et confiance numériques, construit en plusieurs niveaux d'exigences[3] en adéquation avec les besoins des utilisateurs et la réglementation, ce qui est la logique semble-t-il retenue par l'Europe avec le règlement européen (UE 2019/881) Cybersecurity Act ?

Un panorama très partiel mais déjà trop complexe

La multitude de référentiels et de labels traitant de sécurité et de confiance numériques, ainsi que la diversité de leurs valeurs et finalités noient les donneurs d'ordre, parfois les prestataires, et sont coûteuses, tant en termes financiers que de délais.

Pour rappel, un label atteste de la conformité à tel ou tel référentiel, selon une organisation propre à chaque label. Il peut porter, dans le cas de la sécurité numérique, sur des produits de sécurité, des prestataires de services voire sur des systèmes numériques tout entiers.

Quelques exemples de labels…

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) produit de multiples référentiels d'exigences pour ses publics qualifiables de « haut du spectre » (administrations, opérateurs d'importance vitale, opérateurs de services essentiels, …). Elle a créé plusieurs labels pour des produits et des services, essentiellement de portée nationale, regroupés sous le terme générique pour plus de simplicité de « visas de sécurité ». Cette simplification de communication présente néanmoins une ambiguïté : avoir un « visa de sécurité » pourrait en effet être interprété comme un feu vert donné par l'État pour l'utilisation d'un produit ou d'un service. Ce qui n'est pas le cas. L'industriel chinois Huawei, par exemple, fréquemment pointé du doigt négativement par des États dont la France, possède un de ces « visas de sécurité » pour des produits de son catalogue[4].

Cybermalveillance.gouv.fr, « le dispositif national d'assistance et prévention du risque numérique au service des publics » qualifiés de « bas du spectre » (particuliers, petites collectivités, TPE-PME, associations, etc.), a créé un « Label Expert Cyber » de prestataires de proximité, qui est délivré par l'AFNOR.

Il existe en France une volonté de certains acteurs (CCI, AFNOR…) de créer de nouveaux référentiels, voire de nouveaux schémas de labellisation, pour couvrir les manques actuels entre les publics visés par l'ANSSI et ceux traités par Cybermalveillance.gouv.fr. Ces démarches visent à développer un marché local ou spécifique, tout en permettant d'une mise en lumière en termes de communication**.** Certains territoires français envisagent par ailleurs de développer leurs propres référentiels et labels, via leur CSIRT ou campus cyber régionaux[5]. La Revue Stratégique de Cyberdéfense de 2018 avait d'ailleurs identifié ce risque de foisonnement en indiquant que le développement de ces activités devait être découragé[6], dans un souci de cohérence avec la démarche menée au niveau national et les travaux d'harmonisation européenne défendue par la France dans ce domaine.

Dans le même temps, l'Europe travaille depuis plusieurs années à la définition de référentiels partagés pour le cloud, pour la 5G, pour les objets connectés, etc. ainsi qu'à la définition d'un méta schéma de certification. L'application du Cyber Resilience Act (CRA), voté récemment, est notamment très

3 Trois niveaux semblent se dessiner en France : « important », « essentiel » et « vital ».
4https://cyber.gouv.fr/produits-certifies/logiciel-de-controle-dacces-du-huawei-oceanstor-dorado-storage-system-modele-de
5 dispositifs créés dans la dynamique de la stratégie d'accélération de cybersécurité de février 2021
6 paragraphe 2.3.4 de la revue stratégique de cyberdéfense du 12 février 2018

attendu pour la définition d'exigences de sécurité applicables aux produits comportant des éléments numériques.

Face à ce développement de référentiels et labels en tous genres, le Darwinisme évoqué dans certaines conférences pourrait, de fait, conduire à un tri « naturel » parmi toutes ces initiatives. Mais à quelle échéance ? A quel coût pour les finances publiques ? Et avec quels impacts pour la compétitivité de nos entreprises ?

Il serait temps de se coordonner.

Des effets négatifs des référentiels et des labels

Certains pays utilisent les référentiels et labels comme un outil de politique industrielle et d'intelligence économique. Ce n'est manifestement pas le cas de la France, qui ne l'affiche pas comme tel et n'investit pas massivement les comités internationaux de normalisation comme le font d'autres pays, qui peuvent ainsi imposer leurs propres standards et favoriser leurs écosystèmes.

Certains référentiels et labels sont aujourd'hui exigés par de grands donneurs d'ordre auprès de leurs fournisseurs, mais aussi des assurances auprès de leurs assurés et par certains organismes privés, notamment financiers. Ces derniers tendent à s'appuyer sur des entreprises essentiellement nord-américaines se positionnant de façon similaire aux agences de notation financières. Pour répondre à ces « agences », les entreprises doivent répondre à des questionnaires souvent intrusifs et consommateurs de temps et fournir de nombreux éléments relatifs à leurs systèmes d'information. Se pose alors la question de l'utilisation des données transmises, qui doit déjà éveiller les craintes des spécialistes nationaux de l'Intelligence Économique (IE)[7].

Enfin, les réglementations actuelles comme l'article 22 de la Loi de programmation militaire 2014-2019 (LPM), la transposition en 2018 de la directive européenne NIS et la transposition à venir de la directive NIS 2 imposent au travers de décrets ou d'arrêtés des mesures de sécurité, c'est à dire in fine un référentiel d'exigences, aux opérateurs concernés. Pour répondre à ces besoins réglementaires, l'offre de produits et de service de prestataires labellisés par l'ANSSI s'est récemment étendue[8].
Néanmoins, la **masse critique** pour que ces prestataires répondent efficacement à la demande ne semble pas atteignable à court terme. En effet, il est question de plusieurs dizaines de milliers d'organisations qui devront se mettre en conformité à NIS 2, voire d'autres réglementations pour certaines d'entre elles. Cela supposerait des centaines de prestataires labellisés pour les accompagner. Ajoutons que le niveau des exigences techniques mais aussi les coûts et délais pour l'obtention de ces labels ne sont pas toujours cohérents avec la réalité et les exigences du marché. Les chiffres fréquemment évoqués sont des processus durant plusieurs mois et un coût de plusieurs dizaines de milliers d'euros pour les labels de l'ANSSI les moins contraignants et jusqu'à plus d'un an, et plus d'une centaine de milliers d'euros pour les labels plus exigeants. Et ce, pour certains, pour une durée de vie de quelques années. Le **risque de déséquilibre** entre l'offre et la demande ainsi que de **« distorsions » de concurrence** est ainsi bien réel. Enfin, n'oublions pas le **surcoût** pour les donneurs d'ordre contraints de recourir à ces prestataires ou produits labellisés, qui grèvent d'autant leur compétitivité, dès lors que ces dépenses ne s'imposent qu'aux acteurs soumis à la réglementation française.

7 Traitée en France notamment par le Service de l'Information Stratégique et Sécurité Économique (SISSE).
8 Les prestataires d'assistance et de maintenance sécurisé (PAMS) et prestataires d'accompagnement et de conseils en sécurité complètent la liste des prestataires labellisés par l'ANSSI.

L'intérêt des référentiels et des labels est bien réel.

Les référentiels et labels peuvent néanmoins constituer un outil puissant de la France tant sur le plan de la sécurité et de la confiance numériques, que de la compétitivité et de la souveraineté.

A condition toutefois d'intégrer les éléments suivants :

- **L'implication des acteurs publics et privés concernés** pour l'élaboration de référentiels voire des labels, sur le modèle des travaux du Référentiel de Maturité Cyber (RMC)[9] menés par le ministère des armées et les grands donneurs d'ordre de la base industrielle et technologique de Défense (BITD). Il a été porté par la DGA, a été élaboré en collaboration avec des acteurs privés et contient plusieurs niveaux d'exigences adaptés aux besoins et au terrain.
- **La lisibilité et la transparence** de ce qu'apportent réellement les référentiels et labels pour les utilisateurs. Nombreux sont ceux qui choisissent des produits ou prestataires parce qu'ils sont labellisés bien qu'ils ne correspondent pas à leurs besoins.
- **Des coûts financiers et des délais de mise en conformité ou d'obtention des labels cohérents avec la réalité du marché.** Actuellement, les coûts et délais constatés constituent des freins majeurs comme cela a été évoqué précédemment.
- **La transparence dans les critères d'évaluation** pour l'obtention des labels. Si les référentiels d'exigences pour les visas de sécurité de l'ANSSI par exemple sont publics, les critères d'évaluation ne le sont pas nécessairement.
- **La définition d'une masse critique d'acteurs et de produits labellisés** pour répondre aux besoins en évitant les distorsions de concurrence et l'augmentation des coûts pour les utilisateurs finaux.

Enfin, le développement de **mécanismes d'autoévaluation basés sur des outils libres** dont le développement serait piloté par l'État, bénéficierait à de nombreuses organisations et permettrait d'atteindre une masse critique pour les premiers niveaux d'exigences de sécurité numérique en limitant les coûts. Cela positionnerait également la France comme leader au niveau européen voire plus largement. La France ne semble toutefois pas vouloir s'engager dans cette voie et préfère les mécanismes plus contraignants.

***

Face à ces questions et enjeux, **le Parlement pourrait se saisir de ce sujet stratégique**.
Par exemple à l'occasion de la transposition de NIS2, en évaluant le niveau d'efficacité des référentiels et labels de sécurité et confiance numériques existants afin de pouvoir dégager des orientations claires et profitables à tous.

L'objectif *in fine* d'une telle démarche serait de construire la meilleure stratégie possible en matière de référentiels et de labels de sécurité numérique et de confiance numériques, afin d'une part d'**élever significativement le niveau** de sécurité et de confiance numériques des organisations en France ; d'autre part de **créer un véritable différenciant économique** et un facteur de compétitivité reconnu ; et enfin, de **renforcer la dimension souveraineté**. Et ce, **en simplifiant les démarches de conformité** qui s'imposent aux entreprises.
Un cercle vertueux.

9 https://armement.defense.gouv.fr/securite-et-habilitation/securite-du-numerique/referentiel-de-maturite-cyber

Références du CyberCercle

- Matinale du CyberCercle « les certifications européennes de cybersécurité » avec Philippe BLOT, lead expert certification à l'ENISA, décembre 2021
- Matinale du CyberCercle « Sécurité numérique des produits intelligents – Travaux de l'OCDE » avec Laurent BERNAT, Cybersecurity Policy Analyst à l'OCDE, février 2022
- Parole d'Expert "Labels de sécurité et confiance numériques : clés de compréhension et perspectives", Stéphane MEYNET, président de CERTitude NUMERIQUE, février 2022
- Matinale Auvergne-Rhône-Alpes sur les exigences « minimales » pour les organisations, Matinale inversée, juin 2023
- Parole d'Expert "Certification européenne de Cybersécurité : bâtir un marché des TIC de confiance à 27", Chloé BLONDEAU, Experte Nationale Détachée de l'ANSSI auprès de l'ENISA, juin 2023