Labels de sécurité et confiance numériques : clés de compréhension et perspectives

Stéphane MEYNET
Président
CERTitude NUMERIQUE

Dans notre société de consommateurs souvent peu avertis mais toujours pressés, les labels occupent une place de premier ordre. Marque, voire garantie ou assurance de qualité, de sérieux et de confiance, les labels représentent pour un fournisseur un différenciant vis-à-vis de ses concurrents et pour le consommateur un critère de choix.

Tout ou presque tout devient aujourd'hui « labellisable », si bien que le but initial recherché par les labels tend à s'effacer devant la complexité produite par la multitude de labels et leur hétérogénéité. Trop de labels tuent les labels. Ce célèbre adage s'applique là encore à merveille !
Pour que les labels leur soient utiles, les consommateurs doivent en comprendre a minima les rouages et ce qu'ils recouvrent. S'assurer que les labels qu'ils retiennent comme critère de sélection, lorsqu'ils ne sont pas imposés réglementairement, répondent bien à leurs attentes. Sans cela, quelle est l'utilité des labels si ce n'est de s'entendre prononcer la très célèbre remarque : « c'est labellisé donc c'est bien ».
Le domaine de la sécurité et de la confiance numériques n'échappe pas à ce constat. Nous voilà rassurés !

Mais que signifie exactement labelliser et qu'est-ce qu'un label ?

Le Larousse propose une définition éclairée du verbe labelliser et du nom label.
Labelliser : attribuer un label.
Label : nom masculin (anglais label, étiquette, de l'ancien français label, ruban, du francique labba). Étiquette ou marque spéciale créée par un syndicat professionnel et apposée sur un produit destiné à la vente, pour en certifier l'origine, en garantir la qualité et la conformité avec les normes de fabrication.

Tout est dit dans cette définition ou presque. Les termes de « syndicat professionnel » pourraient être remplacés par « organisation », « produit » complété par « services ou personnes » et « normes de fabrication » résumé à « normes ».

Quid des labels de sécurité de de confiance numériques ?

Ainsi nos labels de sécurité et de confiance numériques entrent parfaitement dans la définition qui recoupe d'ailleurs celle proposée par le COFRAC[1].

En effet, de manière générale, les labels et en particulier les labels de sécurité et de confiance numériques s'appliquent à des organisations, des produits, à des services et prestataires de services et sont délivrés par des associations ou des organismes publics.
En France, l'ANSSI et cybermalveillance.gouv.fr, deux organismes publics, portent des labels de sécurité numérique : les « Visa de sécurité »[2] pour l'ANSSI et plus récemment, le label « ExpertCyber »[3] pour cybermalveillance.gouv.fr.
Le succès des visas de sécurité est indéniable au regard du nombre de visas attribués depuis plus de dix ans maintenant et cela pour un large gamme de produits et de prestataires. Pour s'en convaincre, il suffit de consulter sur le site de l'ANSSI le catalogue des visas de sécurité attribués à des produits couvrant un spectre allant de la carte à puce aux automates programmables industriels et développés par des entreprises aussi diverses que Thales, Atos, Stormshield, Huawei, Schneider Electric, Sogeti, Siemens, Idemia, pour n'en citer que quelques-unes. La liste des visas de sécurité attribués aux prestataires de service impressionne également par son ampleur.
Quant au label « ExpertCyber », créé en 2020, son déploiement est en cours et rencontre un véritable intérêt.
Une des premières leçons que nous enseignent les labels est qu'il est nécessaire de laisser du temps pour qu'ils deviennent pleinement opérationnels et utiles. Donnons donc rendez-vous à cybermalveillance.gouv.fr dans quelques années pour mesurer le succès de son label. « Rome ne s'est pas faite en un jour »...

Une deuxième leçon porte sur la lisibilité et la compréhension des labels par le marché, et en particulier par les utilisateurs. Cette problématique récurrente préoccupe bon nombre d'acteurs. Non avertis ou non familiers des labels, un utilisateur peut rapidement se sentir démuni et perdu devant les labels existants. Pire encore, il peut être amené à choisir un produit ou un prestataire simplement parce que celui-ci affiche un label sans s'assurer que le label correspond bien à son besoin et à ses conditions d'usage.
J'ai en tête plusieurs exemples d'utilisateurs - pour des raisons évidentes de confidentialité leurs noms ne seront pas cités - qui indiquaient fièrement avoir fait l'acquisition d'un produit labellisé mais dont les conditions d'emploi ne correspondaient absolument pas à leur environnement. Résultat : un faux sentiment de sécurité et un mauvais investissement… qu'il faudra justifier auprès de la hiérarchie.

L'étude des visas de sécurité par exemple indique que cette appellation, séduisante et simple à comprendre pour le quidam par la similitude avec les visas tamponnés sur des passeports pour voyager, regroupe en fait deux ensembles : certification et qualification.

Peu d'utilisateurs connaissent la distinction, pourtant essentielle, entre ces deux termes. De même, rares sont les utilisateurs qui vérifient le

[1]https://www.cofrac.fr/quest-ce-que-laccreditation/certification-et-accreditation-quelles-differences/

[2]https://www.ssi.gouv.fr/administration/visa-de-securite/
[3]https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/label-expertcyber

périmètre sur lequel porte le visa de sécurité et quelles sont les conditions ou restrictions d'usages qui y sont associées. Encore plus rares sont ceux qui étudient la cible de sécurité ou le référentiel d'exigences, c'est à dire, pour reprendre la définition du Larousse, la norme que le produit ou le service labellisé doit respecter.

Du point de vue des offreurs de solutions, les labels apportent certes un différenciant commercial, mais nécessitent un investissement en temps et argent non négligeable pour leur obtention, pouvant parfois même en décourager de s'engager dans la voie de la labellisation. En effet, si certains labels reposent sur une démarche déclarative, peu coûteuse, d'autres en revanche, reposent sur une évaluation de conformité effectuée par un tiers qu'il faudra bien évidemment rémunérer. Cette évaluation, de quelques milliers d'euros à plusieurs dizaines de milliers d'euros, s'étend bien souvent sur une période de plusieurs mois et nécessite un investissement en ressources humaines non négligeable. Ces contraintes doivent donc être mises en balance au regard du marché des produits et services de sécurité et de confiance numériques, fortement concurrentiel et en pleine consolidation. Les coûts et délais « administratifs » nécessaires à l'obtention des labels doivent impérativement être cohérents avec les exigences du marché et le « time to market ».

L'intérêt indiscutable des labels ne doit ainsi pas conduire à des discriminations et distorsion de concurrence, comme cela est malheureusement parfois le cas.

Revenons aux fondamentaux des labels et à leurs caractéristiques.

Pour résumer, certes de manière simplifiée, un label se construit sur 3 piliers :

- un périmètre : un produit, un système, un service, un prestataire
- un référentiel : une norme , un standard, une cible de sécurité, etc.
- un schéma : un organisme (une association, une entité publique ou privée) qui porte le label, en définit les caractéristiques et notamment le mode d'attribution.

Un label peut ainsi être porté par une entité à vocation commerciale ou non, se limiter à une (auto)déclaration de conformité à un référentiel ou recourir à une évaluation rigoureuse par un tiers, être reconnu au niveau national, européen ou international, porter sur un périmètre extrêmement variable et s'appuyer sur une multitude de référentiels.

Les labels, inventés pour apporter une marque de différenciation à la fois pour les fabricants et des critères de choix simplifiés pour les utilisateurs semblent, devant ce champ des possibles, s'être égarés de leur objectif et n'apportent plus aussi efficacement les réponses attendues. Une étude plus approfondie confirmerait certainement ce constat.

S'il faut travailler sur le temps pour qu'un label s'impose, s'il faut des labels lisibles et compréhensibles par l'ensemble des acteurs, s'il faut être vigilant aux coûts et délais administratifs, il semble également fondamental de définir sur le plan stratégique à quoi doivent servir les labels de sécurité et de confiance numériques avant de les construire. Sont-ils un outil au service de l'économie pour soutenir la « filière », pour soutenir les organismes de labellisation ? Sont-ils

un outil au service de la souveraineté nationale ? Sont-ils un outil pour la sécurité dans le cyberespace ? Sont-ils un outil pour renforcer la sécurité des installations numériques des institutions et des entreprises ? Sont-ils un outil d'information au service des utilisateurs ? Sont-ils tout cela en même temps ? Etc.

Si pour certains Etats les labels relèvent clairement de la politique industrielle ou de l'influence stratégique, pour la France ils semblent d'avantage relever des intérêts fondamentaux de renforcer la sécurité des systèmes numériques, des institutions, des OIV, des OSE et progressivement de tous. Cette question de l'objectif stratégique des labels pourrait néanmoins se reposer dans le cadre de la stratégie nationale pour la sécurité numérique du prochain quinquennat.

Quid des travaux réglementaires ?

L'Europe, au travers de l'ENISA, travaille sur la questions des certifications de sécurité (des labels) au niveau européen[4]. Un objectif ambitieux et ô combien nécessaire, notamment sur le plan de la politique industrielle afin d'harmoniser les labels des différents Etats membres.

En France, le Sénat porte la proposition de loi n° 629 (2019-2020) pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public[5] en proposant notamment un cyberscore. Sur le modèle des nutriscores, le cyberscore informerait les utilisateurs sur le niveau de sécurité des produits et de l'usage qui sera fait de leurs données. Un tel label, potentiellement applicable à tous produits numériques, éclairerait le consommateur lors de ses achats et obligerait implicitement les fabricants à traiter la question de la sécurité et de la confiance numériques.

Vers un label de sécurité et de confiance numériques unique ?

L'idée d'un label unique n'est certes pas nouvelle. Un label, potentiellement décliné en trois niveaux (or, argent, bronze par exemple) suivant le mode d'attribution ou le niveau d'exigences à remplir, simplifierait les process et améliorerait la lisibilité pour toutes les parties prenantes.

Mais le label ne représente-t-il pas finalement que le sommet de l'iceberg ?
Le travail de fond à mener sur lequel nous devrions concentrer nos efforts ne serait-il pas dans la définition des normes, standards et référentiels utilisés pour les labels et leur déploiement sur le plan international ? La France produit une multitude de normes, standards, référentiels et réglementations mais dont le périmètre n'est le plus souvent que national. Or cette bataille se joue au niveau mondial, a minima au niveau européen : il est clair que la France reste malheureusement bien souvent en retrait des influenceurs en la matière.

L'ISO, organisme international, constitue une référence en matière de normalisation. La série de normes ISO270XX et plus particulièrement

[4]https://cybercercle.com/matinale-cybercercle-certification-europeenne-cybersecurite/
[5] Rapport de Mme Anne-Catherine LOISIER sur la proposition de loi n° 629 (2019-2020) pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public présentée par le sénateur Laurent LAFON et enregistrée à la Présidence du Sénat le 15 juillet 2020 https://www.senat.fr/dossier-legislatif/ppl19-629.html

l'ISO27001[6], dédiée au management de la sécurité des systèmes d'information, tend à s'imposer. Elle offre en outre la possibilité à des organisations d'être certifiées et de compléter ainsi leur tableau de chasse des labels dont un des plus célèbre et fréquemment rencontré est sans aucun doute l'ISO9001 dans le domaine de la qualité. Si la certification ISO27001 relève le plus souvent d'une démarche volontaire, plusieurs textes réglementaires français la citent comme exemple, voire l'imposent comme un préalable dans le domaine de la santé pour la certification des hébergeurs de données de santé.
Il est fort à parier que les assureurs exigeront demain que les entreprises soient conformes à cette référence internationale qu'est l'ISO 27001 pour les assurer contre les risques cyber.

En conclusion, le sujet des labels de sécurité et de confiance numériques mériterait un rapport d'information voire une thèse, au regard de ses multiples facettes et de l'étendue de son champ d'application.

Les labels représentent aujourd'hui à eux seuls un marché en pleine croissance. Néanmoins, s'il est certain que des travaux de simplification seraient nécessaires pour garantir un minimum de lisibilité et donc d'efficacité des labels, la question que nous devrions nous poser est bien l'objectif recherché.
En attendant une hypothétique réponse à cette question sensible, ne devrions-nous pas retrouver le chemin de la simplicité et de l'efficacité en nous concentrant sur la définition d'un socle « universel » d'exigences de sécurité et de confiance applicable à tous systèmes numériques et leurs données, de même pour les prestataires, ce que l'on retrouve finalement dans la quasi-totalité des standards, référentiels, normes et réglementation ?

[6]https://www.iso.org/isoiec-27001-information-security.html