Les labels visant à susciter la crédibilité : des pratiques existantes vers l'amélioration de qualité

Claire Levallois-Barth

Levallois-Barth, C.

«Les labels visant à susciter la crédibilité : des pratiques existantes vers l'amélioration de qualité»

dans **Signes de confiance – l'impact des labels sur la gestion des données personnelles** (Chapitre 7, pages 116 à 133).
Coordonné par Claire Levallois-Barth, Chaire Valeurs et Politiques des Informations Personnelles (France), Janvier 2018.

Livre disponible en version électronique sur http://www.informations-personnelles.org/
Une version papier est également disponible : ISBN 978-2-9557308-4-3

Les labels visant à susciter la crédibilité : des pratiques existantes vers l'amélioration de qualité

Alors que les labels de type CNIL et EuroPriSe poursuivent un objectif de conformité allant au-delà des obligations légales (cf. Chapitre 6), d'autres signes extérieurs de confiance s'inscrivent dans une toute autre démarche : celle de la recherche de confiance par la crédibilité de la marque (7.1.). Ces signes, délivrés par des prestataires privés, prennent place dans un marché fortement concurrentiel au sein duquel les organismes souhaitant être labellisés sont confrontés à une offre morcelée, peu connue du grand public (7.2.). En outre, une partie de l'offre se caractérise par une labellisation de pratiques susceptible d'induire l'utilisateur en erreur et, contrairement à l'objectif recherché, de susciter des réactions mitigées, si ce n'est de la défiance (7.3.).

7.1. La recherche de confiance par la crédibilité

Comme le souligne une personne interrogée dans le cadre des entretiens effectués pour cet ouvrage entre octobre 2015 et septembre 2017, « *donner de la confiance à l'utilisateur, ce n'est pas forcément par rapport à un texte de loi ou un cadre légal référencé, qui ne sont d'ailleurs pas connus de l'utilisateur final* ».

Le signe d'un engagement proactif à l'égard des données personnelles

Cette recherche de crédibilité peut aussi viser à réduire l'asymétrie d'informations[1] en communiquant auprès du public sur la politique de protection des données personnelles mise en place par l'organisation et les mesures adoptées pour y parvenir. Dans le contexte

1 La notion d'asymétrie d'informations est développée au début du Chapitre 9.

de la labellisation, elle se situe au-delà d'une simple déclaration marketing, qui peut s'avérer peu convaincante et parfois contre-productive, en apportant des garanties.

Parole d'un tiers de confiance

« *Le label, c'est un process qualité et commercial. Ce n'est pas une démarche de conformité. Ce n'est pas une assurance d'être conforme, et on peut atteindre la conformité autrement.* »

La démarche volontaire signifie que certaines mesures – certains diront un minimum d'exigences – sont mises en œuvre en interne et que cette implémentation est vérifiée, assurée par une intervention extérieure. Elle ne signifie donc pas qu'il n'existe ou qu'il n'existera pas de détournement éventuel de données personnelles, mais que l'organisme labellisé entend porter ses efforts sur la protection des données personnelles et qu'il en fait un argument commercial.

À cette fin, il adopte un engagement clair vis-à-vis de ses clients et choisit les éléments qu'il souhaite mettre en avant afin d'assurer la crédibilité de la marque sur le long terme. Ces éléments entendent garantir des engagements qui par nature diffèrent du seul respect de la réglementation. L'organisme définit ses axes de communication et l'argumentaire par lesquels il entend démontrer qu'il adhère de façon concrète à certaines normes techniques ou juridiques, à certaines valeurs ou certains principes éthiques. La stratégie n'est donc

pas si éloignée d'une démarche de développement durable et de responsabilité sociale d'entreprise.

Parole d'expert d'un organisme de certification

« *Un label, c'est le best effort. J'ai des imperfections mais je me donne les moyens de les traiter… on doit apporter des preuves qu'au moins, on essaie de faire.* »

Rédigés dans un langage qui se veut compréhensible, les critères sont axés sur le quotidien de l'entreprise et de l'utilisateur : les bonnes pratiques appliquées dans le cadre du *cloud* (par exemple, le fait que les données sont stockées uniquement en Europe), les garanties apportées dans l'utilisation des algorithmes ou de certains types de données personnelles (données relatives aux mineurs, données de santé), l'utilisation d'une technologie renforçant la protection de la vie privée comme une technique d'anonymisation, la participation au fonctionnement d'une liste d'opposition en matière de marketing direct.

La labellisation se présente donc comme une stratégie marketing parmi d'autres. Certains organismes ont ainsi opté pour d'autres signes de confiance, notamment :

- en choisissant une forme purement déclarative en communiquant sur son « *Engagement envers la transparence* »[2], en adoptant sa propre charte des données personnelles[3] ou en adhérant à un code de conduite[4]
- en sensibilisant les internautes sur les risques liées aux données personnelles et en les accompagnant dans la (re)prise en main de leur identité numérique[5]
- en contribuant à la construction d'un écosystème de confiance en fournissant des outils techniques aux développeurs tiers d'applications afin que celles-ci informent l'utilisateur final sur le flux de données personnelles créé[6]

2 AXA, *Commitment to transparency*, https://group.axa.com/en/about-us/data-privacy

3 Charte d'Orange relative à la protection des données personnelles et de la vie privée - janvier 2010 (mise à jour : décembre 2014), https://bienvivreledigital.orange.fr/mes-donnees-mon-identite/charte-protection-des-donnees-personnelles-et-de-la-vie-privee ; Crédit agricole, Charte des données personnelles, https://www.credit-agricole.fr/nos-engagements/charte-des-donnees-personnelles.html

4 *Cloud Infrastructure Services Providers in Europe* (CISPE) *Code Of Conduct* qui entend anticiper la mise en œuvre du RGPD, https://cispe.cloud/code-of-conduct/

5 MAIF, *mesdatasetmoi*, https://www.mesdatasetmoi.fr/

6 *Orange Trust Badge*, https://partner.orange.com/trust-badge/

- en se situant dans un engagement de conformité juridique et en adoptant des règles internes d'entreprise approuvées par les autorités de contrôle[7]

D'autres entreprises préféreront simplement ne pas apporter de garanties et proposeront un prix plus compétitif.

Un des avantages de la labellisation visant à susciter la crédibilité est qu'elle est susceptible d'enclencher plus facilement une dynamique interne qu'une labellisation visant à prouver la conformité, plus exigeante ou moins adaptée à la culture de l'organisme. La décision de labellisation est une décision structurante pour l'organisme : très souvent prise au niveau de la direction générale, sa mise en œuvre impacte diverses fonctions ou divers métiers qui participent aux traitements de données personnelles (système d'information, juridique, marketing, audit, conformité, qualité, etc.) et mobilise les salariés.

La procédure d'évaluation permet d'identifier les forces et les faiblesses. À ce titre, elle est susceptible de déboucher sur une démarche d'amélioration de la gouvernance interne des données personnelles.

L'éventuel effet levier : la démarche d'amélioration

Cette démarche d'amélioration est le signe que nous nous situons non plus dans une approche purement réglementaire mais dans un système de gestion des risques encourus à la fois par le responsable du traitement et les personnes concernées par les données. Elle est notamment prônée par l'AFNOR Normalisation, laquelle préconise « *une approche par les risques, qui […] s'inscrit dans un processus itératif d'amélioration continue de la sécurité et de la protection des données personnelles* »[8].

On voit ainsi fleurir les offres commerciales des organismes de certification et des annonces qui entend accompagner l'entreprise pour identifier les risques, mettre en œuvre des mesures adaptées pour les diminuer et apporter des garanties de progrès à l'utilisateur.

Même si son référentiel n'est pas spécifiquement dédié à la protection des données personnelles mais porte en particulier sur la sécurité des informations alignée avec la norme

---

7 HP, Qu'est-ce que les BCR HP ?, http://www8.hp.com/fr/fr/binding-corporate-rules.html

8 AFNOR Normalisation, Guide Protection des données personnelles : l'apport des normes volontaires, janvier 2017, p. 6, http://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf

ISO 27001, le label « Cloud » est à cet égard emblématique. Il propose trois niveaux de garantie :

- **Niveau initial :** les déclarations du candidat qui prennent la forme d'une auto-évaluation sont vérifiées par un expert. Celui-ci peut exiger des informations ou documents faisant la preuve de l'évaluation.
- **Niveau confirmé :** l'entreprise doit obligatoirement fournir une liste de documents et l'auditeur peut exiger du candidat des informations ou documents complémentaires.
- **Niveau expert :** l'entreprise est auditée sur site par un auditeur et ses clients se prononcent sur leur perception du service rendu.

Selon son niveau, le label est délivré pour 2 ans (initial), 3 ans (confirmé) ou 4 ans (expert). Lors de sa première candidature, l'entreprise choisit le niveau de son choix. À l'occasion du renouvellement, elle peut opter pour le même niveau ou pour un niveau supérieur. Si elle demande le même niveau, la note obtenue lors du renouvellement doit être supérieure à celle obtenue lors de la précédente labellisation ; si elle candidate pour le niveau supérieur, le niveau d'exigences s'accroît tant pour la moyenne finale des caractéristiques, que pour la note minimum requise pour chaque caractéristique.

Le label ADEL recourt également à la notation, via un système de scoring et de rating par dimension, accompagné de recommandations et de préconisations[9].

Pour sa part, Bureau Veritas « *voit mal comment l'entreprise va pouvoir revendiquer, avec 100 % de certitude, que dans la totalité de ses systèmes et bases de données, sur un périmètre élargi à l'ensemble de ses filiales, à l'ensemble de ses fonctions, que la protection de la Privacy est sans faille* »[10]. C'est pourquoi l'organisme de certification a annoncé son intention de proposer un « *système de labels* » à « *trois niveaux permett[ant] aux entreprises d'être certifiées selon leur niveau de maturité* » :

- le label « Produit ou service Privacy by Design » permettrait à l'organisme, dans une démarche de conformité, de s'engager à l'échelle d'un produit ou d'un service

9 Label ADEL, Algorithm Data ETHICS LABEL, http://www.adel-label.com/label-adel/

10 Bureau Veritas, Rétablir la confiance dans le Big Data, novembre 2016, http://www.move-forward-with-privacy.bureauveritas.com/wp-content/uploads/2016/11/Bureau-Veritas-brochure-francais-donnees-personnelles-2016.pdf.

« *en mettant en œuvre une conception d'offre, une architecture de données et des moyens de type* « pseudonymisation » *ou autres* ». Ce label permettrait « *de démarrer dans la certification Privacy sans transformer l'ensemble de l'architecture IT* »

- le label « Certification Gouvernance » se situerait dans une approche qualité plus large dans laquelle l'organisme ferait labelliser son système de management de la donnée
- le label « RGPD » proposerait une certification volontaire de conformité décernée sur la base d'un référentiel découlant du règlement ; il permettrait à l'organisme de démontrer qu'il respecte la législation (cf. Chapitre 8)[11]

Cependant, les entreprises qui souhaitent s'orienter vers un label de « qualité » rencontrent actuellement des difficultés pour trouver une offre adaptée à leurs besoins. Certaines renoncent même à se faire labelliser alors même que le marché est fortement concurrentiel.

7.2. Un marché fortement concurrentiel

Dans le cadre de sa démarche d'auto-régulation, l'entreprise va être confrontée à une offre éclatée, peu connue du grand public. Comme le souligne Bureau Veritas, « *la multiplication des labels pourrait produire l'inverse de l'effet visé : au lieu de restaurer la confiance, augmenter la confusion* »[12].

Une offre éclatée

En France, le marché entend principalement répondre au besoin d'une profession, ou rassurer sur l'emploi d'une technologie. Aucun label n'a été attribué en ce qui concerne les récents labels « E-vote » de la FNTC et le label « ADEL ». Le label « Cloud » de France IT est délivré à neuf entités et le label « Cloud Confidence » à deux entreprises (voir tableau page suivante). On constate donc que peu de labels sont attribués à des organismes. Une première explication possible est celle liée à la concurrence entre prestataires.

---

11 Cette intention a été concrétisée par la publication début octobre 2017 du *Technical Standard for Data Protection Technical Standard related to personal data protection in compliance with the regulation* (EU) 2016/679, http://www.bureauveritas.com/home/news/business-news/worlds-first-personal-data-protection-standard.

12 Bureau Veritas, Rétablir la confiance dans le Big Data, novembre 2016, op.cit. p. 11

Parole d'un avocat

« *C'est la concurrence qui fait que ça ne marche pas dans le secteur privé. Celui qui a monté un label a beaucoup travaillé avant de présenter son offre à un premier client. Il a donc fortement investi. La perspective qu'il puisse fusionner avec un éventuel concurrent qui va se tirer la part du lion sur la capacité à vendre des prestations fait que l'on n'a que des boutiques.* »

Organisme	*Nom du label*	*Objet*	*Référentiel*	*Créé en…*	*Nombre de labellisés*
Adel	ADEL (*Algorithm Data Ethic Label*)	Services / Algorithmes	Règles éthiques	2016	0
Cloud Confidence	Certification Cloud Confidence	Services / Cloud	Normes légales + bonnes pratiques en matière de sécurité de l'information	2014	2
FEVAD	Marque de confiance FEVAD	Services / Commerce électronique	Normes légales + code déontologique du e-commerce et de la vente à distance – FEVAD	1957	400+
FNTC	E-Vote	Services / Vote électronique	Recommandation CNIL relative à la sécurité des systèmes de vote électronique	2016	0
France IT	Label Cloud	Services / Cloud	200 bonnes pratiques en matière de *cloud*	2012	9

Tableau 9. Labels de « qualité » proposés par les organismes privés français

Par exemple, le label « Site » lancé en 1999 par la FEVAD et la Fédération des entreprises du commerce et de la distribution (FCD) pour les sites de e-commerce n'a pas émergé alors même que ses vingt-sept règles avaient été élaborées en concertation avec la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) et la CNIL. L'explication avancée par un tiers de confiance viendrait du fait que les entreprises bénéficiant d'une grande notoriété ne percevaient pas la nécessité de la labellisation car elles étaient déjà membres d'autres fédérations professionnelles dont elles respectaient les règles déontologiques. Dès lors, elles préféraient bénéficier uni-

quement de la marque de confiance FEVAD. Le label « Site » restait intéressant pour les petites entreprises qui souhaitaient se faire connaître du grand public, mais qui finalement renonçaient à l'obtenir car il leur demandait un effort financier trop important en raison de la rémunération d'un tiers certificateur (qui s'ajoutait au prix de 1000 euros de la cotisation à la FEVAD).

Dans le secteur de l'informatique en nuage, on compte deux labels français rivaux, qui de surcroît sont en concurrence avec l'initiative européenne CISPE (*Cloud Infrastructure Service Providers in Europe*) qui depuis 2016 regroupe une vingtaine de fournisseurs d'infrastructures *cloud* en provenance d'une quinzaine de pays.

Une autre difficulté réside dans la nature des acteurs impliqués. Les labels « Cloud » sont portés par des organismes et sociétés français. Or le marché est dominé par des fournisseurs américains (Amazon, Google, IBM, Microsoft, Oracle, Salesforce…) qui ne soutiennent pas ces initiatives, ce qui en limite grandement la portée. Google, notamment, refuse d'indiquer la localisation des données.

La marque de confiance FEVAD du secteur de la vente à distance, proposée depuis 1957, se distingue cependant par le nombre d'organismes labellisés, environ 400. Ce constat n'est pas propre à la France. En Europe, les marques de confiance en matière de commerce électronique se détachent par le nombre de membres qu'elles fédèrent. Dans ce secteur, la protection des données personnelles des clients constitue une des composantes de la confiance, à côté de garanties concernant notamment la livraison, le retour des produits, leur remplacement ou leur réparation. Ces marques fournissent des niveaux de protection des données personnelles hétérogènes, cette hétérogénéité étant principalement liée aux obligations légales nationales et aux objectifs poursuivis par l'association professionnelle qui délivre le label. Elles présentent l'avantage de sensibiliser les adhérents.

► Le Code de déontologie du e-commerce et de la vente à distance de la FEVAD rappelle les principales dispositions légales et exige que l'entreprise adhérente respecte deux listes d'opposition : l'une relative à la prospection commerciale téléphonique et l'autre à la prospection par courrier postal dite « Liste Robinson – Stop Publicité ».

► Un exemple intéressant concernant la fourniture de signes tangibles de confiance est constitué par la marque espagnole *Confianza Online*. Son code éthique de trente-deux pages a été officiellement approuvé par trois organismes publics : l'Agence espagnole de protection des données, l'Institut national de la consommation et le Ministère de l'industrie, du commerce et du tourisme.

Ces marques se sont fédérées au niveau européen. Ici aussi, la concurrence domine entre deux organisations aux ambitions similaires : l'*European Multichannel & Online Trade Association* (EMOTA) et l'association dissidente Ecommerce EUROPE.

- L'association européenne Ecommerce EUROPE représente 25 000 entreprises et fédère dix-neuf associations nationales, notamment la FEVAD / France avec environ 400 adhérents, BeCommerce / Belgique, Thuiswinkel / Pays-Bas avec 2 217 labels, E-maerket/Danemark avec 2 200 labels. Elle délivre gratuitement sa marque *ECommerce Europe trust mark* à 10 000 boutiques en ligne[13], laquelle doit être affichée conjointement avec une marque nationale accréditée. L'entreprise qui en bénéficie s'engage à respecter le code de conduite Ecommerce Europe pour le moins sommaire en ce qui concerne les données personnelles[14] et celui de l'association nationale fondé sur le droit national.
- De même, seuls les commerçants certifiés par un label national partenaire de l'EMOTA peuvent afficher le label européen EMOTA sur leur site.

Des prix compétitifs

Si les prix sont très variables, car fonction notamment du périmètre de la labellisation et du niveau d'exigences des référentiels, ils dépendent le plus souvent de la taille de l'organisme candidat ou de son chiffre d'affaires annuel :

- l'adhésion à la FEVAD est payante, la cotisation annuelle allant en fonction du chiffre d'affaire de 1 000 à 35 000 €

13 https://www.ecommerce-europe.eu/ecommerce-europe-trustmark/

14 https://www.ecommercetrustmark.eu/the-code-of-conduct/ qui, en matière de données personnelles, se contente d'affirmer : « *Nous respectons votre vie privée, nous protégeons vos données et nous veillons à un environnement Internet sans danger. Nous sommes transparents et nous vous informons de la collecte et du traitement de vos données ainsi que des fins auxquelles nous les utilisons, y compris les informations sur notre politique en matière de cookies. Les données sont collectées pour exécuter le contrat et améliorer notre offre à votre intention ainsi que votre expérience d'achat. Vos données sont collectées conformément à la législation en matière de protection des données et de respect de la vie privée, et uniquement avec votre consentement explicite, dans la mesure où la loi l'exige* ».

- le prix du label belge BeCommerce, en plus de l'adhésion à cette association qui commence à 150€ et qui s'élève à 11000€ au-delà d'un chiffre d'affaire de 25 millions d'euros, est de 500€ pour le premier audit de certification d'un site web, puis de 200€ pour les sites suivants
- pour *Confianza Online*, les frais annuels commencent à 295€HT pour les entreprises dont le chiffre d'affaires est inférieur à un million d'euros et augmentent progressivement jusqu'à 3500€ HT si le chiffre d'affaires dépasse 25 millions d'euros
- le coût du label « Cloud », entre 1000 à 5500€HT, varie en fonction de l'adhésion ou non du candidat à France IT et du niveau de labellisation demandé
- la déclaration d'un service *cloud* auprès de CISPE (*Cloud Infrastructure Service Providers* in Europe) revient à 990€, celles de trois services et plus à 2990€

On trouve cette même logique pour les labels américains :

- pour obtenir le label TRUSTe, il fallait compter 399$ (pour un chiffre d'affaire inférieur à 500000$) et 8999$ (pour un chiffre d'affaires de 2 milliards de dollars ou plus)
- pour le label BBBonline, 200$ pour un total des ventes inférieur à 1 million de dollars, et 6000$ pour un total de vente égal à 2 milliards de dollars ou plus.

La première labellisation est souvent plus chère : les frais de certification sont par exemple de 550€ pour le label BeCommerce et de 300€ pour la recertification tous les deux ans.

D'après un tiers de confiance, la barrière des 10000€ serait assez forte pour les petites et moyennes entreprises qui sont néanmoins prêtes à investir 5000€. Cette somme dépend bien entendu des avantages que l'entreprise entend retirer de la labellisation. Un avocat cite le cas d'une start-up pour laquelle le prix de 40000€ ne paraissait pas excessif : cette entreprise développait une technologie « *extrêmement agressive vis-à-vis des données personnelles* » et cherchait à rassurer à la fois ses investisseurs et ses clients.

Parfois, le montant ne reflète pas le coût réel que devraient facturer les auditeurs. Selon un tiers de confiance, ces derniers se situeraient dans une logique de marché de « *première approche* » et proposeraient des prix « *très raisonnables* » pour capter la clientèle. Ils factureraient ensuite d'autres prestations, dans le cadre d'un processus d'amélioration.

Dans le même temps, de nouvelles formes d'automatisation d'audit sont en train d'apparaître. La machine, à travers les algorithmes, permet en effet d'automatiser certaines évaluations et d'en diminuer le coût. Star Audit, par exemple, facture 400€ l'auto-évaluation et la publication du rapport.

La labellisation en matière de données personnelles est donc une activité économique convoitée par un certain nombre de prestataires. « *Il en résulte qu'elle comporte une certaine ambivalence attestée, dans les champs classiques où un retour d'expérience a pu être établi, par le constat de pratiques de certification à la fois non conformes aux exigences de la protection des consommateurs et néfastes sur un plan concurrentiel.* »[15]

7.3. L'effet potentiellement trompeur

La démarche de « qualité » est susceptible d'effets qui portent à confusion et qui risquent d'induire l'utilisateur en erreur.

D'une part, le référentiel de « qualité » peut revêtir un niveau d'exigences variable. En ce qui concerne le cadre légal, on soulignera de façon positive que l'on y trouve les principales obligations en matière de protection des données personnelles (licéité, proportionnalité, finalité, transparence) issues de la directive (UE) 95/46/CE et, à partir du 25 mai 2018, du Règlement général sur la protection des données (désignées dans le schéma ci-contre par OB_RGPD). La garantie apportée par le label porte sur ces exigences (OB_RGPD1, OB_RGPD2) ; elle ne signifie pas pour autant que l'organisme labellisé a fait évaluer sa conformité en ce qui concerne ses autres obligations légales (OB_RGPD3, OB_RGPD4).

Quant aux critères de « qualité » désignés par CR_Q, qui par définition ne relèvent pas du champ législatif, ils offrent difficilement des points de comparaison entre les différents référentiels : un critère peut par exemple porter sur l'adhésion à une liste d'opposition et sa mise en œuvre pratique (CR_Q1), un autre sur l'hébergement des données sur le territoire de l'UE (CR_Q2), un autre encore sur la désignation d'un Correspondant Informatique et

15 Penneau, A. (2014). Certification et codes de conduite privés : article 38 et 39 (dans leur version originelle), *in La proposition de règlement européen relatif aux données personnelles : propositions du réseau Trans Europe Experts*, sous la direction de Nathalie Martial-Braz, Société de législation comparée, volume 9, 2014, p. 351.

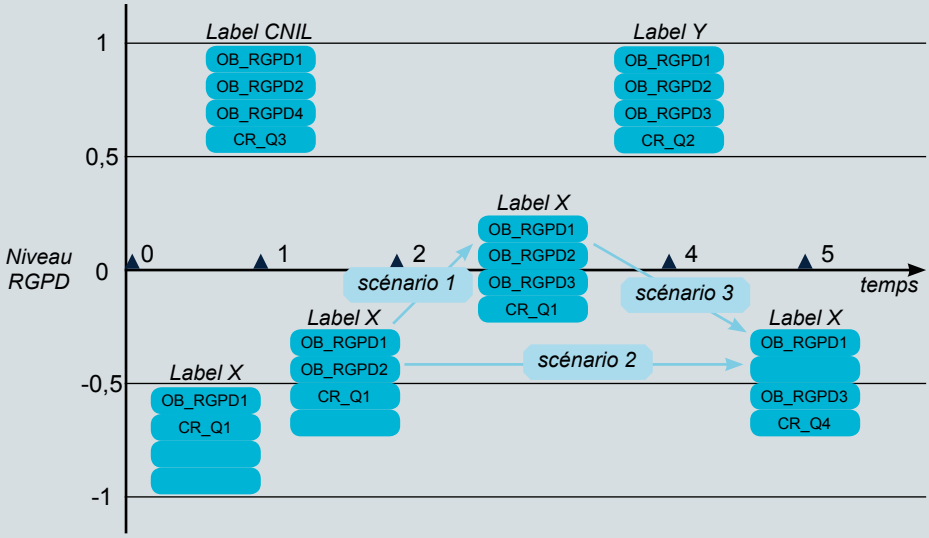

Figure 1. *Les effets de confusion*

Libertés dans des cas où cette désignation n'est pas juridiquement obligatoire (CR_Q3) ou la simple existence d'une politique d'entreprise (CR_Q4).

La garantie apportée ici signifie que les experts ont simplement vérifié que l'entreprise a bien mis en place des bonnes pratiques pour atteindre des exigences. Typiquement, un label portant sur la gouvernance des données personnelles est un engagement à respecter des procédures de qualité, et non pas à effectuer un traitement de données personnelles de qualité. Cela y participe, certes.

► L'exemple emblématique est ici le label américain TRUSTe qui labellise l'existence d'une déclaration de l'entreprise : il ne vérifie pas que la politique mise en place est la bonne.

Parole d'expert d'un organisme de certification

« *On est très « bonne pratique ». On restreint les exigences à l'existence d'une politique d'entreprise mise en œuvre réellement. On vérifie qu'il y a bien une substance derrière l'engagement. C'est plus une approche anglo-saxonne.* »

D'autre part, la temporalité intervient de façon non négligeable. L'évaluation est effectuée à un temps T0 pour une durée qui varie de un à cinq ans. Les contrôles *a posteriori* semblent rares pendant cette période. On trouve en effet parmi les labels existants peu d'informations sur un quelconque suivi alors même que le produit, service ou les règles de gouvernance qui ont été évalués ont certainement évolué entre-temps. Les labels qui prévoient une vérification ne communiquent pas sur la réelle mise en œuvre de celle-ci, si bien que l'on s'interroge sur leur matérialité. Le contrôle se fait principalement à travers le renouvellement. On relève cette ambiguïté notamment dans le domaine des marques de confiance de commerce électronique où le suivi du respect des exigences par le commerçant peut aller du renouvellement de la labellisation à un contrôle sporadique ou continu.

► Par exemple, le label BeCommerce (Belgique) énonce dans son règlement : « *chaque début d'année, 20% des sociétés qui ont obtenu le label de qualité et qui, par conséquent, sont liées par les règles de certification de BeCommerce, seront sélectionnées au hasard par un huissier de justice pour faire l'objet d'une procédure de certification de contrôle. Ces certifications seront réparties sur toute l'année et les sociétés impliquées ne seront évidemment pas informées de ce contrôle.* »[16]

Les critères eux-mêmes peuvent varier sur la durée, ce qui est classique dans le domaine de la certification : le niveau global de protection peut augmenter ou, au contraire, diminuer si certaines exigences sont supprimées ou si, plus subtilement, elles sont modifiées.

La crédibilité passe aussi par l'information du public. Elle se matérialise par la mise en place dans l'intérêt de toutes les parties des mécanismes de résolution des conflits dans le cas où un litige surviendrait entre l'entreprise labellisée et la personne dont les données personnelles sont utilisées. Or, tout comme la CNIL, certains labels n'indiquent qu'une

16 https://www.becommerce.be/upload/Label_FR_Reglement201420140313144711.pdf

adresse mail de contact sans autre précision ; les marques de confiance du secteur du commerce électronique et de la vente à distance privilégient une procédure de médiation et communiquent largement à son propos, comme *Confianza online*, *Trust Shops* et ESRB. Cette question des réclamations ou plutôt de l'absence de possibilités de réclamations crédibles se pose également dans le cadre de l'accord sur le *Privacy Shield*. Si l'accord a permis d'introduire le mécanisme de l'*Ombudsperson*, l'effectivité et l'indépendance de ce médiateur pose question[17].

Un problème particulier est donc le manque de volonté et de pouvoir de la part des organismes de certification à prendre des mesures pour faire face aux abus, à l'encontre de leurs adhérents lorsqu'il s'agit d'une association ou de leurs clients en ce qui concerne les organismes privés de certification. Les sanctions, du moins annoncées, vont du simple avertissement, à une suspension temporaire ou un renvoi, ou une sanction financière[18].

Les révocations sont rares. La publicité qui en est faite encore plus (la FEVAD précise que les sanctions ne sont pas rendues publiques) alors même que le retrait est supposé fonctionner comme un incitateur à se conformer aux engagements. Lorsque l'américain TRUSTe a retiré son label à *Gratis Internet of Washington* en 2005 pour non-respect de la politique d'information relative aux mineurs, l'organisme de labellisation n'a pas rendu public la nature des violations. L'argument avancé était qu'il était lié par un accord de confidentialité[19]. Or, comme le souligne un avocat, « *sanctionner les vilains petits canards paraît être la condition de la crédibilité et de la durée des labels* ».

Cependant, dans un contexte concurrentiel, il s'agit d'abord pour certains prestataires de parvenir à labelliser un nombre critique de clients. Ceci implique de « *laisser passer avec de très larges fourches* » les candidats pour créer une première base de données clients. Ce n'est que dans un deuxième temps, lorsque le nombre de clients labellisés est

---

17 Voir à ce propos le discours du député européen Claude Moraes dans le cadre de 13e Rencontre de la **Chaire Valeurs et Politiques des Informations Personnelles** : « Les données personnelles dans les traités et accords internationaux : le *Privacy Shield* » du 6 janvier 2017, https://cvpip.wp.imt.fr/2017/02/06/privacy-shield-claude-moraes-speech/

18 European Parliament, Directorate General for Internal Policies, A Pan-European Trustmark for E-Commerce: Possibilities and Opportunities, study, IP/A/IMCO/ST/2012-04, July 2012, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/492433/IPOL-IMCO_ET(2012)492433_EN.pdf

19 Associated Press, 'Privacy-Assurance Seal Yanked', Wired, 2 September 2005, http://www.wired.com/techbiz/media/news/2005/02/66557

suffisant, que l'organisme peut envisager d'élargir certaines exigences et de sanctionner les mauvais élèves.

Face à ce risque de nivellement par le bas de la certification en matière de données personnelles, la question est alors de savoir quels types de règles il convient d'adopter pour encadrer ce marché et selon quel mode de régulation. À cet égard, le RGPD laisse la porte ouverte à plusieurs options (cf. Chapitre 8).

Le cas américain

Aux États-Unis, les labels ou marques de confiance sont nombreux et d'origine privée, le législateur préférant laisser le marché se réguler par lui-même. En l'absence de cadre légal général à l'instar de l'Union européenne, le pays dispose de quelques lois fédérales sectorielles[20]. Certains États, comme la Californie, ont adopté des législations plus exigeantes ou imposé la notification des failles de sécurité[21]. Le législateur n'intervient donc que dans des secteurs et pour des usages spécifiques car, comme l'a souligné Isabelle Falque-Pierrotin, présidente de la CNIL, lors d'une rencontre organisée par la **Chaire Valeurs et Politiques des Informations Personnelles** le 8 janvier 2016[22], «*la protection des données est très marquée par les sensibilités culturelles de chaque pays. Cette conception a des conséquences sur la régulation : nous [les européens] pensons que les données personnelles sont un droit fondamental tandis que les États-Unis se rattachent davantage à la protection des consommateurs.*»

La protection des consommateurs et de la concurrence est assurée par la Commission fédérale américaine du commerce (*Federal Trade Commission* – FTC). À ce titre et sous ce prisme, cette agence fédérale indépendante intervient en matière de protection des don-

---

20 Comme le *Privacy Act* de 1974 pour les traitements des données effectués par le gouvernement fédéral et ses agences, l'*Health Insurance Portability and Accountability Act* (HIPAA) de 1996 dans le domaine de la santé, le *Children's Online Privacy Protection Act* (COPPA) de 1998 en ce qui concerne les enfants de moins de 13 ans ou encore le Gramm-Leach-Bliley Act de 1999 pour les activités financières.

21 La loi californienne *Online Privacy Protection Act of 2003 – Business and Professions Code* oblige les sites de commerce électronique ou encore les sites collectant des données personnelles d'habitants californiens à afficher une déclaration de confidentialité. D'autres lois, telles que celles du Nebraska ou de Pennsylvanie, sanctionnent les déclarations trompeuses en matière de protection des données personnelles.

22 **Chaire Valeurs et Politiques des Informations Personnelles**, 10e rencontre *Personal Data in the International Treaties and Agreements*, 8 janvier 2016.

nées personnelles[23]. Son premier et principal outil consiste à exiger d'une entreprise qu'elle mette fin à ses pratiques illégales et, le cas échéant, à adopter des mesures coercitives.

- La FTC peut exiger la mise en place de politiques claires de protection des données personnelles et de sécurité ou l'effacement des données des consommateurs obtenues illégalement. En 2011, elle a par exemple imposé à Facebook d'informer les internautes quant aux changements de ses conditions générales d'utilisation qui pouvaient affecter leur vie privée et leur faire approuver.

- La FTC peut également imposer à une entreprise de se soumettre à des évaluations annuelles effectuées par des experts indépendants, ou encore une réparation pécuniaire en faveur des consommateurs.

En cas d'irrespect de ses injonctions, la Commission peut chercher à obtenir des condamnations pécuniaires. Outre l'atteinte à l'image de marque des entreprises, les amendes sont relativement dissuasives : suite aux négociations entreprises avec la FTC, Google a dû s'acquitter en 2012 de la somme de 22,5 millions de dollars pour mettre fin aux poursuites liées à la surveillance des utilisateurs du navigateur Safari[24].

Dans ce contexte, les labels fondés sur des systèmes d'auto-évaluation indiquent simplement au consommateur que le site partage ouvertement sa politique de confidentialité. Celle-ci précise, par exemple, comment les informations sont collectées, utilisées et partagées et la façon dont la personne peut effectuer un certain contrôle sur ses données. Cet affichage a donc pour objectif d'informer le consommateur et ainsi lui permettre de faire un choix éclairé quant à l'utilisation de ses données. Des entreprises internationalement connues comme Apple, Ebay, The New York Times ou encore Cisco, Disneyland, EA games, Hewlett Packard, IBM, McDonalds, Oracle ou Verizon sont labellisées. Certaines cumulent même plusieurs labels.

---

23 Notamment en ce qui concerne l'application de lois sectorielles spécifiques comme le *Fair Credit Reporting Act* de 1970 ou le COPPA. En particulier, la section 5 du *Federal Trade Commission Act* interdit les pratiques illégales ou trompeuses.

24 Le réseau social Path avait en 2013 négocié avec la FTC une amende de 800 000 $, soit près de 588 000 € à l'époque, qui s'ajoutait à l'obligation de se soumettre à un audit sur la protection des données. En 2014, Yelp avait dû s'acquitter d'une amende de 450 000 $ pour avoir collecté des données d'enfants âgés de moins de 13 ans, sans le consentement des parents.

Pour autant, l'apport réel de ces signes de confiance est questionné par les associations de protection de la vie privée d'outre-Atlantique. L'association *Privacy International* notamment estime qu'ils créent souvent une « *illusion de protection de la vie privée* » et n'ajoutent aucune plus-value aux obligations légales[25].

Le cas du label américain TRUSTe, le plus grand prestataire de certification en matière de *Privacy*, qui participe aux mécanismes d'auto-régulation mise en œuvre notamment par la loi américaine sur la protection de la vie privée en ligne des enfants (C*hildren's Online Privacy Protection Act* – COPPA), les accords *Safe Habor* et *Privacy Shield* conclus entre l'Union européenne et les États-Unis[26], et les règles transfrontalières de protection de la vie privée de la Coopération économique pour l'Asie-Pacifique (*Asia-Pacific Economic Cooperation* – APEC), est à cet égard emblématique. Cette organisation à but non lucratif, qui employait quatre-vingt salariés et comptait 4 000 clients, effectuait des contrôles auprès des détenteurs de son label qui, pour le moins, laissaient à désirer. Ainsi, la *Federal Trade Commission* (FTC) a condamné l'entreprise labellisée TRUSTe Toyssmart.com en juillet 2000 pour non-respect de sa politique de protection des données personnelles et revente de sa base de données clients[27]. Toyssmart.com n'est d'ailleurs pas la seule société dans ce cas.

- Une étude menée en 2007 a démontré que les sites web Microsoft, Yahoo, Chase Manhattan Bank, et Geocities pourtant labellisés TRUSTe pratiquaient des politiques de vie privée discutables. Il en allait de même pour Equifax qui disposait d'un label BBBOnLine[28].

---

25 Privacy International, 'Response to the European Commission's Communication on the 'Comprehensive Approach on Personal Data Privacy International, January 2011, p. 11 http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/pi_en.pdf : "*We have strong reservations about the value of 'privacy seals', which can often create an illusion of privacy protection without delivering anything additional to legal obligations, and we especially question the value of privacy seals operated by for-profit companies when the profits of the seal program are wholly dependent on the revenues from seal holders*".

26 Le 16 août 2016, TRUSTe a annoncé qu'il travaillait avec plus de 500 entreprises pour évaluer et vérifier le respect des nouvelles exigences du *Privacy Shield* et fournir des services de règlement des différends, https://www.trustarc.com/press/500-companies-working-truste-comply-eu-u-s-privacy-shield/.

27 *FTC v Toysmart.com, LLC, and Toysmart.com, Inc., District of Massachusetts, Civil Action* No. 00–11341-RGS, https://www.ftc.gov/enforcement/cases-proceedings/x000075/toysmartcom-llc-toysmartcom-inc.

28 LaRose, R. and Rifon, N., (2007). Promoting i-Safety: Effects of Privacy Warnings and Privacy Seals on Risk Assessment and Online Privacy Behavior (Summer 2007), vol. 41, Journal of Consumer Affairs 12.

► Une seconde étude issue de travaux menés à l'Université américaine de Carnegie Mellon en 2010 a mis en évidence que les sites web de Facebook, MSN, et AOL, qui disposaient du label TRUSTe EU Safe Harbor, n'utilisaient pas correctement la plateforme de préférence P3P : sur 2417 labellisés TRUSTe-certified websites, 134 sites pratiquaient une politique de gestion des cookies problématique, dont 21 figuraient parmi les cents premiers sites les plus fréquentés[29].

TRUSTe lui-même a fait l'objet d'une série de sanctions, dont une amende de 200 000$ par la FTC en novembre 2014, pour pratiques trompeuses : entre 2007 et 2013, l'organisme avait renouvelé tacitement le label de 1 000 sociétés sans effectuer la moindre vérification a posteriori [30]!

Il n'est donc pas surprenant que TRUSTe ait changé de nom. L'organisme s'appelle désormais TrustArc afin, du moins officiellement, « *de refléter notre transformation d'une société de certification en un fournisseur mondial de solutions de confidentialité fondées sur la technologie* »[31].

TrustArc propose certains labels TRUSTe et commercialise des solutions de gestion de la conformité au cadre juridique européen, en particulier au RGPD et au *Privacy Shield*. Ce type d'activité marchande emblématique du développement actuel du marché des prestataires de services de certification et de labels en matière de données personnelles doit-il être réglementé pour limiter les abus et, si oui, comment ? Quelles réponses nous apporte le RGPD à cet égard ?

---

29 Leon, P. G., Faith Cranor, L., McDonald, A. M., and McGuire, R., (2010). Token attempt : The Misrepresentation of Website Privacy Policies Through the Misuse of P3P Compact Policy Tokens, CyLab. Paper 73, http://repository.cmu.edu/cylab/73. Voir également Connolly, C., Greenleaf, G. and Waters, N. (2014). Privacy self-regulation in crisis? TRUSTe's 'deceptive' practices, 132 Privacy Laws & Business International Report, 13-17, December 2014.

30 FTC Approves Final Order In TRUSTe Privacy Case, https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.

31 The Leader in Privacy Compliance and Risk Management Solutions Has a New Name – TrustArc, https://www.trustarc.com/about/.