Les labels visant à prouver la conformité : de l'implémentation du cadre réglementaire et au-delà

Claire Levallois-Barth, Delphine Chauvet

Levallois-Barth, C., Chauvet, D.

«Les labels visant à prouver la conformité : de l'implémentation du cadre réglementaire et au-delà»

dans **Signes de confiance – l'impact des labels sur la gestion des données personnelles** (Chapitre 6, pages 92 à 114).
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 prouver la conformité : de l'implémentation du cadre réglementaire et au-delà

Parmi les labels conçus comme le prolongement de la législation relative aux données personnelles, nous avons retenu deux expériences riches d'enseignements : les labels délivrés en France par la CNIL (6.1) et en Allemagne par EuroPriSe (6.2).

- Ce dernier, développé sous l'égide d'un projet de recherche financé par la Commission européenne en 2007 et piloté par l'autorité de protection des données du Land allemand du Schleswig-Holstein (*Unabhängiges Landeszentrum fuer Datenschutz* – ULD), est désormais délivré par une société privée en partenariat avec les autorités de contrôle.

Pour l'essentiel, on retiendra que ces labels de conformité sont aussi exigeants l'un que l'autre. Cependant, leurs champs d'application, à la fois matériel et territorial, se recoupent peu. Alors même que l'on pourrait penser que l'implication des autorités de protection des données est perçue par le grand public et les entreprises comme un signe fort de confiance et de pérennité, ces labels « niches » sont peu connus et sont attribués à un nombre relativement faible d'entités. Cette situation s'explique principalement par le fait que leur obtention engendre un coût élevé, voire très élevé dans certains cas, et que leurs référentiels sont trop stricts selon certains acteurs. Le retour sur investissement est loin d'être incitatif (6.3.).

6.1. Les labels délivrés par la CNIL

En pratique, la labellisation constitue un enjeu complexe, à la fois pour le législateur et pour l'autorité de protection des données. À cet égard, on constate que les pouvoirs de labellisation de la CNIL ont été définis par étapes. L'expérience a commencé en 2004, et est loin d'être terminée puisqu'il s'agit à présent pour l'autorité d'adapter les référentiels aux exigences du RGPD (cf. Chapitre 8).

Les quatre types de labels progressivement proposés

À la date du 31 juillet 2017, il existe quatre types de labels délivrés par la CNIL.

C'est une loi de 2004 qui permet à la Commission «*à la demande d'organisations professionnelles ou d'institutions regroupant principalement des responsables de traitements*» de délivrer «*un label à des produits ou à des procédures*»[1]. Il faudra cependant attendre 2011 pour que la CNIL délivre son premier label.

1 Art. 11, 3-c) de la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF, 7 août 2004..

En effet, l'exercice du pouvoir de labellisation impliquait que soit adopté un décret d'application. Or, ce décret n'a jamais été publié, son rédacteur, la Direction des Affaires Civiles et du Sceau (DACS), ayant rencontré des difficultés quant à la façon de traiter « *la problématique concurrentielle de différenciation par la qualité* »[2]. La situation est débloquée en 2009 par la loi lorsque la CNIL peut elle-même préciser dans son règlement intérieur « *les modalités de mise en œuvre de la procédure de labellisation* »[3], ce qui rend inutile le recours au décret.

À la même époque, la Commission est autorisée à recourir à des tiers évaluateurs qualifiés et indépendants « *lorsque la complexité du produit ou de la procédure le justifie* », étant précisé que « *le coût de cette évaluation est pris en charge par l'entreprise qui demande le label* »[4]. Il lui faut cependant deux ans pour modifier son règlement intérieur[5].

Puis en 2014, la loi Hamon accorde à la CNIL le pouvoir de « *déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label* »[6] (voir ci-contre le c du 3° de l'article 11 de la loi Informatique et Libertés).

Enfin, depuis le 7 octobre 2016, la Commission peut certifier des procédés d'anonymisation de données personnelles et homologuer les référentiels liés et des méthodologies générales[7]. Cette possibilité offerte par la loi Lemaire s'inscrit notamment dans le cadre de l'*open data* où le recours à des procédés d'anonymisation doit permettre de concilier, d'une part, l'intérêt général à disposer des données et à informer les citoyens et, d'autre part, l'intérêt individuel de la personne concernée en protégeant ses données personnelles. En l'état, il reste à savoir quand la CNIL exercera ce nouveau pouvoir et dans quelles conditions (voir ci-contre le g du 2° de l'article 11 de la loi Informatique et Libertés).

---

2 Interview de Yann Padova, secrétaire général de la CNIL de 2006 à 2011.

3 Art. 105 de loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures, JORF, 13 mai 2009.

4 Art. 105 de loi n° 2009-526, précitée.

5 Délibération n° 2011-249 du 8 sept. 2011 portant modification de l'article 69 du règlement intérieur de la Commission nationale de l'informatique et des libertés et insérant un chapitre IV bis intitulé « Procédure de labellisation », JORF, 22 septembre 2011. Voir la dernière version du règlement intérieur de la CNIL, Délibération n° 2013-175 du 4 juillet 2013 portant adoption du règlement intérieur de la Commission nationale de l'informatique et des libertés.

6 Art. 17 de la loi n° 2014-344 du 17 mars 2014 relative à la consommation, JORF, 18 mars 2014.

7 Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF, 8 octobre 2016.

Art. 11-3 c) de la loi Informatique et Libertés

« Elle [la CNIL] délivre un label à des produits ou à des procédures tendant à la protection des personnes à l'égard du traitement des données à caractère personnel, après qu'elle les a reconnus conformes aux dispositions de la présente loi dans le cadre de l'instruction préalable à la délivrance du label par la commission ; la commission peut également déterminer, de sa propre initiative, les produits et procédures susceptibles de bénéficier d'un label. Le président peut, lorsque la complexité du produit ou de la procédure le justifie, recourir à toute personne indépendante qualifiée pour procéder à leur évaluation. Le coût de cette évaluation est pris en charge par l'entreprise qui demande le label ; elle retire le label lorsqu'elle constate, par tout moyen, que les conditions qui ont permis sa délivrance ne sont plus satisfaites. »

Art. 11-2 g) de la loi Informatique et Libertés

« g) Elle [la CNIL] peut certifier ou homologuer et publier des référentiels ou des méthodologies générales aux fins de certification de la conformité à la présente loi de processus d'anonymisation des données à caractère personnel, notamment en vue de la réutilisation d'informations publiques mises en ligne. »

En pratique, comme on peut le constater, la labellisation s'avère constituer un sujet complexe pour l'autorité de protection. En 2009, il s'agissait d'un nouveau métier qui impliquait que la Commission dispose des moyens techniques pour labelliser des produits et des ressources juridiques, particulièrement en droit de la concurrence. Par exemple se posait la question de la « discrimination positive » de certains produits et services[8].

L'un des mérites de la CNIL a donc été d'oser se lancer dans l'aventure, faute de solutions proposées à l'époque par le secteur privé. En effet, et contrairement à l'Allemagne (cf. Chapitre 7), la France n'est pas un pays créateur de labels.

8 Naftalski F.et Desgens-Pasanau G., (2010). Enjeux et perspectives du pouvoir de labellisation de la CNIL, Revue Lamy Droit de l'Immatériel, N°63, août-septembre 2010, 12 pages.

Pour des raisons exprimées de neutralité, et sans doute d'impact probable sur le marché, la CNIL a décidé de commencer par ce qui lui semblait le moins complexe en terme d'interaction et conséquences. Ainsi adopte-t-elle de sa propre initiative en octobre 2011 deux référentiels : l'un consacré à la formation, l'autre portant sur les audits. Le ***label «Formation»*** est délivré à des entités proposant, en interne ou en externe, des formations relatives à la protection des données personnelles, y compris des formations en *e-learning*. Le ***label « Audit de traitement »*** peut être demandé par des prestataires (cabinets de conseils, avocats, etc.) qui commercialisent des procédures d'audits de traitements des données personnelles ou par des organismes qui mettent en œuvre en interne de telles procédures. Ces procédures décrivent les différentes étapes et processus selon lesquels un audit doit être préparé, réalisé et finalisé. Ces deux premiers labels ne s'appliquent donc pas directement aux traitements de données personnelles mis en œuvre par un organisme.

Suivent en janvier 2014 l'adoption du référentiel sur le coffre-fort numérique et en décembre 2014 celui sur la gouvernance Informatique et Libertés. Le ***label « Coffre-fort numérique»*** porte sur les services de coffre-fort numérique stockant des données personnelles (documents, certaines métadonnées). Ces données ne sont accessibles qu'au seul titulaire du coffre, ainsi qu'aux éventuelles personnes qu'il a mandatées. Le ***label «Gouvernance Informatique et Libertés»*** concerne pour sa part les procédures mises en place par un organisme pour la protection des données personnelles, notamment un audit interne ou externe régulier. L'ambition de ce label est donc plus élevée par son périmètre.

Les deux types de labels ont été élaborés à la demande d'organisations professionnelles ou d'institutions regroupant des responsables de traitements. Concrètement, le label « Gouvernance Informatique et Libertés » émane d'une demande de l'Association Française des Correspondants aux Données Personnelles (AFCDP), et le label « coffre-fort numérique » de la Fédération des Tiers de confiance du numérique (FNTC). Dans ces quatre cas, la CNIL a estimé que le label correspondait à un besoin du marché.

Les quatre référentiels d'évaluation se fondent sur les normes légales et, selon les cas, les recommandations de la CNIL ou les normes ISO. Ils ont été élaborés par le comité

de labellisation de la CNIL[9], composé de trois commissaires choisis par le président de la CNIL, puis adoptés par voie de délibération par son assemblée plénière. Ainsi, le référentiel du label Gouvernance a été en partie élaboré à partir du projet de règlement RGPD et des normes ISO/IEC 27001:2013 sur les systèmes de management de la sécurité de l'information et ISO/IEC 29190:2014 sur la maturité dans le domaine de la protection de la vie privée qui ont été adaptées aux pratiques des correspondants Informatique et libertés. Le label « Gouvernance » se distingue également par son mode d'élaboration, les vingt-cinq exigences de son référentiel ayant été élaborées avec le concours de l'Association Française des Correspondants à la protection des Données Personnelles (AFCDP).

Nom du label	*Objet*	*Référentiel*	*Créé en…*	*Durée d'attribution*	*Nombre de labellisés*
Label CNIL « Formations »	Services / Formations	Normes légales + ISO 29990	2011	3 ans	54
Label CNIL « Audit de traitements »	Services / Audit	Normes légales + ISO 19011	2011		25
Label CNIL « Coffre-fort numérique »	Services / Coffre-fort numérique	Recommandations CNIL	2014		1
Label CNIL « Gouvernance Informatique et Libertés »	Procédures	Normes légales + ISO/IEC 27001:2013 + ISO/IEC 29190:2014 + projet RGPD	2014		13

Tableau 8. Labels délivrés par la CNIL au 17 octobre 2017 [10]

9 Le comité de labellisation a pour mission de proposer des orientations relatives à la politique de labellisation. Il élabore notamment les projets de référentiels et évalue la conformité des demandes de délivrances. Il se réunit en pratique tous les trois mois environ.

10 Norme NF ISO 29990 : services de formation dans le cadre de l'éducation et de la formation non formelles – exigences de base pour prestataires de services, 2010.

Norme NF ISO 19011 : lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental, 2002.

Normes ISO/IEC 27001:2013 sur les systèmes de management de la sécurité de l'information et ISO/IEC 29190:2014 sur la maturité dans le domaine de la protection de la vie privée en les adaptant aux pratiques des correspondants Informatique et libertés.

Par ailleurs, la CNIL n'a pas donné suite à plusieurs demandes, notamment celles relatives à des labels « Cloud », « Cookie » ou « Paiement en ligne ». Si l'on prend le cas des applications mobiles e-santé porté par le Conseil National de l'Ordre des Médecins, le refus de la CNIL était motivé par la complexité de labelliser une application mobile dont le fonctionnement dépend du système d'exploitation et du design de ce dernier, notamment en matière de paramétrage.

Si donc le périmètre des quatre labels pouvant être délivrés par la CNIL est inégal, leur délivrance suit en revanche une procédure identique.

La procédure de délivrance par la CNIL elle-même

Bien que la loi autorise la CNIL à recourir à des tiers indépendants, c'est elle qui endosse la responsabilité de l'évaluation et de la délivrance selon une procédure en quatre étapes[11] :

1. **Demande :** un label peut être sollicité par toute personne morale et, pour le label « Formation », par une personne physique. Deux ou plusieurs entités peuvent déposer une demande conjointe. Celle-ci s'effectue en téléchargeant le dossier de candidature via le site de la CNIL[12], puis en l'envoyant dûment rempli par voie postale ou en ligne.

2. **Recevabilité :** à compter du dépôt de la demande formalisée par un numéro d'enregistrement, le président de la CNIL dispose d'un délai de deux mois pour se prononcer sur la recevabilité du dossier. À défaut de réponse dans ce délai, le silence de l'autorité vaut rejet. La demande peut ainsi être refusée si elle n'entre pas dans le domaine du référentiel ou si le dossier est incomplet.

3. **Analyse par la CNIL :** une fois la demande déclarée recevable, le pôle « Labels » de la CNIL composé de deux personnes rattachées à la direction de la conformité, examine le dossier. Le site www.cnil.fr indique que « *la durée d'instruction varie en fonction du taux de conformité initiale et du nombre d'échanges avec la Commission* ». En pratique, les agents instructeurs établissent des évaluations

11 Pour un schéma détaillé voir : Naftalski F., (2011). Label CNIL et conformité « informatique et libertés » : publication des premiers référentiels, Revue Lamy Droit de l'Immatériel, 8 pages.

12 Pour un aperçu, le dossier de candidature pour le label CNIL « Gouvernance Informatique et Libertés », https://www.cnil.fr/sites/default/files/atoms/files/labelsCNIL-gouvernance-demande_0.docx.

successives, jusqu'à ce qu'une conformité totale soit atteinte. La durée de l'analyse varie en fonction de la complexité du dossier présenté, des demandes d'informations complémentaires et des auditions éventuellement pratiquées par le pôle Label ou le comité de labellisation. Elle est d'environ sept mois. Le comité de labellisation prend ensuite le relais pour juger de la conformité du dossier.

4. **Délivrance :** le label est délivré pour une durée de trois ans renouvelable par la CNIL réunie en formation plénière. En cas de refus de délivrance, ce dernier n'est pas rendu public et les dossiers de demandes de délivrance, qui peuvent par exemple comprendre les questionnaires d'audit, ne sont pas communicables au titre de la loi sur la liberté d'accès aux documents administratifs[13] ; le demandeur peut saisir le Conseil d'État dans un délai de deux mois. Jusqu'à présent, ce cas de figure ne s'est jamais présenté. Le demandeur, informé par voie postale, reçoit les logos personnalisés et le règlement d'usage de ces derniers. La délibération de la CNIL est publiée au journal officiel via le site Légifrance, et également sur le site www.cnil.fr. Ainsi, le public peut accéder à la liste des produits et procédures labellisés accompagnés du nom de l'entité bénéficiaire et de la date d'expiration du label.

Exemple de logo attribué, avec sa date d'expiration.

13 La Commission d'Accès aux Documents Administratifs (CADA) a ainsi confirmé à la CNIL que ces dossiers relevaient de l'exception de l'article 66-II de la loi du 17 juillet 1978 au regard de la protection du secret en matière industrielle et commerciale.

À l'issue de la première année de délivrance, le titulaire du label a ***l'obligation de transmettre à la CNIL un rapport d'activités*** qui permet à la Commission de vérifier le respect du référentiel et de l'utilisation du logo « Label CNIL » conformément au règlement d'usage de la marque collective label CNIL. Ainsi, ce règlement prévoit que « *le logo doit être utilisé en lien direct avec le produit ou la procédure labellisé. L'apposition du logo de manière générale et indéterminée est strictement interdite* »[14]. Ceci permet d'éviter que l'entreprise dont un service a été labellisé soit tentée de l'étendre à l'ensemble de ses services, faits pouvant notamment être réprimés sous la qualification de publicité mensongère ou de concurrence déloyale.

La Commission peut également vérifier à tout moment que le référentiel est bien respecté. Dans les faits, le titulaire du label est prévenu ; il ne s'agit donc pas d'un contrôle « surprise » car le but de la CNIL est « *d'accompagner, de guider, d'encourager les comportements des organismes qui veulent faire la différence* »[15]. Jusqu'à maintenant, quelques vérifications ont été opérées uniquement sur le label « Formation ».

Lorsqu'une plainte est déposée par un tiers ou si la CNIL estime qu'il existe un doute sur un éventuel manquement, l'entité labellisée doit présenter ses observations dans un délai d'un mois. Si ses réponses sont jugées insatisfaisantes, un rapporteur est désigné parmi les membres du comité de labellisation. La formation plénière décide (ou non) de retirer le label, chose qui pour l'instant n'est pas arrivée.

Lors du renouvellement du label, la procédure est allégée : six mois avant expiration, le labellisé doit informer la CNIL de son souhait et indiquer éventuellement l'existence de changements, lesquels sont vérifiés sur dossier.

Les labels ainsi délivrés par la CNIL sont susceptibles d'intéresser essentiellement les organismes français. Si ces derniers souhaitent obtenir un label européen, ils ont la possibilité de se tourner vers EuroPriSe, qui compte la CNIL parmi ses partenaires.

---

14 Voir règlement d'usage de la marque collective label CNIL, https://www.cnil.fr/sites/default/files/atoms/files/label_CNIL-charte_dutilisation_du_logo.pdf

15 Carvais, J. (2015). Le label CNIL comme outil de conformité, *in AFCDP, Correspondant Informatique et Libertés, Bien plus qu'un métier*, pp. 504. .

6.2. Le label européen EuroPriSe

Le label transeuropéen EuroPriSe, pour *European Privacy Seal*, permet à un organisme de démontrer sa conformité aux lois et réglementations européennes. Ce label se distingue des labels attribués par la CNIL par le recours à des experts indépendants.

Un label « d'excellence » créé et soutenu par les autorités de protection des données européennes

Créé en 2007, EuroPriSe est issu du projet pilote eTEN, financé à hauteur de 1,2 millions d'euros par la Commission européenne. Le consortium, piloté par l'autorité de protection des données du Land allemand du Schleswig-Holstein (*Unabhängiges Landeszentrum fuer Datenschutz* – ULD), réunissait une dizaine de partenaires (autorités de protection des données, universités et cabinets de conseils[16]) provenant de huit pays européens.

Après deux ans de développement, EuroPriSe a publié son référentiel « Produits et services des technologies de l'information ». Les labels délivrés sur cette base concernent des entités de toute taille, qu'il s'agisse de PME ou de multinationales telles que Microsoft en 2008 ou SAP en 2012.

Le 1er janvier 2014, l'initiative a été transférée à une société privée, l'EuroPriSe GmbH, laquelle se compose désormais d'une autorité de certification chargée de délivrer les labels et d'un comité consultatif ayant pour principale mission d'assurer la qualité du label.

À cette fin, le comité est composé d'experts indépendants issus des autorités de protection, notamment un représentant de l'ULD et un représentant de la CNIL.

Notons qu'EuroPriSe agit depuis 2014 en tant qu'organisme de certification pour le label délivré par l'État fédéral allemand de Mecklembourg-Poméranie, en consultation avec le Commissaire à la protection des données et à la liberté d'information de ce Land[17]. Ce label appelé *Gütesiegel Datenschutz Mecklenburg-Vorpommern* (sceau de confiden-

16 Notamment les autorités de protection de données de Madrid (*Agencia de Protección de Datos de la Communidad de Madrid*, APDCM), de France (CNIL), le *Austrian Academy of Science*, la *London Metropolitan University* du Royaume-Uni, le *Borking Consultancy* des Pays-Bas, *Ernst and Young AB* de Suède, le *TÜV Informationstechnik GmbH* d'Allemagne et le VaF s.r.o. de Slovaquie.

17 https://www.european-privacy-seal.eu/EPS-en/News/n/7972/europrise-starts-work-as-certification-authority-for-the-new-privacy-seal-of-the-german-federal-state-of-mecklenburg-vorpommern

tialité d'approbation) est fondé sur l'article 5 de la loi sur la protection des données de Mecklembourg-Poméranie occidentale et certifie le respect de cette loi. Ce même texte oblige les organismes publics du Land à accorder la priorité au déploiement des produits et des procédures ainsi labellisés et doit donner un avantage concurrentiel aux entreprises certifiées.

En avril 2016, l'EuroPriSe GmbH a élargi son offre en proposant une labellisation des sites web dont le périmètre porte sur les parties d'un site accessibles au public et sur l'interaction entre le serveur web et le navigateur de l'utilisateur.

Contrairement à la CNIL, EuroPriSe dispose, non pas d'un référentiel par type de labels, mais d'un référentiel unique qui précise, dans les cas pertinents, si un critère s'applique à un produit, un service ou un site web[18]. Rédigé sous forme de questions, il est régulièrement mis à jour, ainsi qu'en attestent les 109 pages de la dernière version en date de janvier 2017. Celle-ci intègre notamment le RGPD, la directive « *Vie privée et communications électroniques* » et la législation en vigueur dans les États membres. Ainsi fondé sur un niveau élevé de protection des données personnelles, on serait tenté d'y voir l'influence des autorités de protection des données, en particulier de l'ULD considéré par certains comme l'une des autorités européennes les plus draconiennes. On comprend donc pourquoi EuroPriSe se présente comme une « *marque de confiance d'excellence* » (*trust mark of excellence*) ayant ouvertement vocation à procurer un avantage concurrentiel aux entreprises labellisées.

Et si le référentiel entend refléter une certaine excellence à la fois sur le plan juridique et technologique, il en va de même pour sa procédure de délivrance.

La procédure de délivrance faisant appel à des experts EuroPriSe

La procédure de délivrance d'un label EuroPriSe comprend, tout comme celle de la CNIL, quatre étapes. De manière générale, le processus complet de labellisation allant de la saisine des experts à la délivrance du label dure en moyenne entre huit mois à un an.

18 *EuroPriSe Criteria for the certification of IT products and IT-based services ("GDPR ready" version – January 2017):* https://www.european-privacy-seal.eu/EPS-en/Criteria

1. **Phase préparatoire :** le futur labellisé choisit parmi la liste des experts accrédités, dont les noms figurent sur le registre public d'EuroPriSe, un expert juridique et un expert technique. Il leur présente son produit, service ou site web et discute avec eux des modalités de l'évaluation, en particulier de la définition du périmètre de labellisation (*Target of Evaluation* – ToE). Il contacte ensuite l'autorité de certification EuroPriSe qui, lors d'une réunion préparatoire, valide l'objet de l'évaluation. Après avoir négocié la rémunération des deux experts, le futur labellisé conclut un accord avec l'autorité de certification.

2. **Évaluation par les experts :** les deux experts évaluent le produit, service ou site web. En particulier, ils identifient tous les flux de données personnelles relatifs au périmètre de labellisation et s'assurent de leur conformité juridique à tous les textes européens. Puis, les deux experts rédigent conjointement deux rapports : un rapport d'évaluation confidentiel et un rapport plus court, qui sera rendu public. Ils sont également tenus, à ce stade, de déclarer par écrit, et lors de chaque évaluation, agir en toute indépendance.

Parole d'expert EuroPriSe

« *On doit cerner la cible, le périmètre de ce qu'on veut labelliser… c'est un travail compliqué, fastidieux. On appréhende tous les flux, on les identifie et on assure leur conformité à tous les textes européens… non seulement la directive, la jurisprudence, mais aussi les décisions du Groupe 29…* »

3. **Validation par l'autorité de certification :** l'entité candidate approuve les deux rapports. Elle les transmet ensuite à l'autorité de certification qui effectue une contre-évaluation consistant à vérifier rigoureusement si les critères pertinents ont été appliqués et si le demandeur a répondu de manière plausible aux questions.
   Dans le cas du label délivré par le Land de Mecklembourg-Poméranie, l'avis de l'autorité de certification EuroPriSe est transmis au Commissaire à la protection des données, qui donne son accord.

4. **Délivrance :** Le label est délivré pour une durée de deux ans renouvelable, la procédure de renouvellement étant moins contraignante. Il est rendu public via l'adresse https://www.european-privacy-seal.eu/EPS-en/awarded-seals qui précise notam-

ment sa durée de validité et permet de télécharger le rapport public d'évaluation. L'organisme labellisé dispose également d'une attestation de conformité.

Outre ce registre des entreprises certifiées, la transparence s'illustre également sur le terrain des règlements des litiges. À cet égard, le plaignant doit se conformer à une procédure en deux étapes : il doit d'abord s'adresser au titulaire du label. Si sa plainte n'est pas résolue, il doit ensuite remplir un formulaire en ligne afin qu'EuroPriSe GmbH mène l'enquête[19]. À notre connaissance, EuroPriSe n'a jamais eu recours à une procédure de retrait du label.

Le niveau « d'excellence » s'illustre également à travers les conditions strictes d'accréditation des experts qui s'articulent autour de trois critères : compétence, fiabilité et indépendance[20].

Les trois critères d'accrédition d'un expert EuroPriSe

Compétences : l'expert suit obligatoirement une formation spécifique de trois jours en anglais, notamment en matière d'évaluation et d'audit, à l'issue de laquelle il rédige avec son homologue, expert juridique ou technique, un rapport conjoint basé sur un cas pratique. Le temps passé pour être accrédité est estimé à 15 jours/homme par un expert déjà très pointu dans son domaine.

Fiabilité : l'expert est tenu d'effectuer une déclaration écrite portant sur sa situation financière (il ne doit pas, entre autres, avoir été soumis à une procédure d'insolvabilité), pénale (il ne doit pas avoir été condamné pour fraude ou falsification de documents dans les cinq dernières années), et sur son assurance responsabilité qui doit couvrir les éventuels dommages qui résulteraient de ses évaluations.

Indépendance : l'expert ne peut pas être le correspondant Informatique et Libertés du futur labellisé ou son consultant.

19 https://www.european-privacy-seal.eu/EPS-en/Dispute-Resolution-Complaint-Form

20 https://www.european-privacy-seal.eu/EPS-en/Expert-Admission

Une fois admis, l'expert dispose d'un logo spécifique précisant son champ d'expertise (voir ci-dessus). Sa cotisation annuelle s'élève alors à 390€ HT. S'il souhaite étendre son accréditation aux sites web, il doit passer un cas pratique spécifique et rédiger un second rapport d'expertise. Il lui en coûtera 150€ HT et, s'il n'est pas déjà accrédité, 600€ HT. Afin de prolonger son accréditation valable trois ans, il doit notamment avoir effectué une évaluation EuroPriSe. Dans le cas contraire, il doit mettre à jour ses connaissances en participant à un atelier.

Pour autant, le label EuroPriSe n'est pas plus connu que les labels délivrés par la CNIL. Il n'aide donc pas l'utilisateur-consommateur à se repérer dans la « jungle » des produits et services liés aux données personnelles. Pourquoi ?

6.3. Des labels peu connus au retour sur investissement encore limité

Qu'il s'agisse d'EuroPriSe ou des labels CNIL, on constate un nombre relativement faible d'entités labellisées. Il semble qu'une explication soit à rechercher du côté des coûts relativement élevés engendrés pour obtenir ce signe de confiance, alors que le retour sur investissement reste encore insuffisant.

Le nombre relativement faibles d'entités labellisées

En juin 2017, dix-neuf entités sont labellisées EuroPriSe, dont une majorité d'entreprises allemandes. Sur ces dix dernières années, on compte, en incluant les renouvellements[21] :

- 6 labels attribués en 2008
- 6 labels attribués en 2009 (et 1 label renouvelé)
- 3 en 2010

21 Tous les chiffres donnés ici sont actualisés de décembre 2017.

- 5 en 2011 (et 2 labels renouvelés)
- 3 en 2012 (et 2 labels renouvelés)
- 2 en 2013 (et 3 labels renouvelés)
- 8 en 2014 (et 3 labels renouvelés)
- 5 en 2015 (et 6 labels renouvelés)
- 3 en 2016 (et 3 labels renouvelés)
- 2 en 2017 (et 8 labels renouvelés)[22]

Comme le souligne un expert accrédité EuroPriSe, «*j'ai été très déçu du retour sur investissement*». Alors même que cette personne a investi temporellement (un mois minimum), intellectuellement (haute connaissance de toutes les décisions prises au niveau européen) et financièrement pour obtenir son accréditation, elle n'a obtenu aucune prestation. Elle n'est d'ailleurs pas la seule. En effet, fin juin 2017 le registre des experts EuroPriSe comprenait une centaine de personnes, présentes dans dix-neuf pays[23].

Du côté de la CNIL, le nombre de labels délivrés est plus conséquent. On en dénombre 93 dont:

- 54 labels «Formation» (et 21 demandes de renouvellement)
- 25 labels «Audit» (et 9 demandes de renouvellement)
- 1 label «Coffre-fort» numérique
- 13 labels «Gouvernance»

Pour comparer, avec les limites que cela comporte, en France,

- dans le secteur de l'agriculture biologique, le label AB concernait 32 236 producteurs fin 2016
- dans l'agro-alimentaire, le label rouge est attribué à plus de 5000 éleveurs (soit 97 093792 poulets)
- en matière environnementale, la norme NF environnement concernait 142 entreprises en 2005

Les États-Unis comptent eux aussi un nombre conséquent d'entreprises labellisées en matière de protection des données personnelles: le label *TRUSTe certified Privacy*, dé-

22 https://www.european-privacy-seal.eu/EPS-en/awarded-seals

23 https://www.european-privacy-seal.eu/EPS-en/register-of-experts

sormais délivré par *TrustArc*, est décerné à plus de 1 000 clients[24], tandis que 145 700 sites Internet sont labellisés BBBonline. Ces chiffres sont cependant à considérer avec précaution dans la mesure où le degré d'exigences américain est bien éloigné de la rigueur européenne comme en atteste notamment le recours à la procédure d'auto-déclaration (cf. Chapitre 7).

On peut également se référer au nombre de labels attribués par l'ULD, l'autorité de contrôle du Land allemand Schleswig-Holstein. Dans ce cas, à l'instar d'EuroPriSe, l'évaluation est effectuée par des experts accrédités, ayant justifié de leurs compétences juridiques et/ou techniques. Elle donne lieu à un rapport qui est validé par l'ULD. Cette dernière délivre alors le label.

Sur cette base, depuis 2002 :

- 96 labels concernant des produits et services ont été attribués au niveau du Land (47 renouvellements)
- 84 experts ont été accrédités depuis 2002, dont 38 experts juridiques et 24 experts techniques, 22 experts ayant à la fois les compétences techniques et juridiques[25]
- aucun label n'a été délivré par le Land de Mecklembourg-Poméranie[26]

Dès lors, comment interpréter le faible nombre d'entités labellisées EuroPriSe ou CNIL ?

Selon un interviewé, nous ne serions qu'au début d'un long processus et leur nombre ira en augmentant avec la mise en œuvre du règlement sur la protection des données (cf. Chapitre 8). Un expert d'un organisme de certification souligne qu'il ne s'agit pas tant d'arriver à un certain nombre d'organismes mais d'attirer « *quelques marques connues et reconnues* » pour créer un effet d'entraînement à l'égard des demandes de labellisation.

Encore faut-il que plusieurs conditions soient remplies, notamment que les labels relatifs à la protection des données personnelles soient connus. Or, on observe que le seuil critique pour que le grand public et les organisations aient connaissance de ces indicateurs

---

24 *TrustArc by Numbers*: https://www.trustarc.com/resources/privacy-research/trustarc-by-the-numbers/

25 *Privacy Seals and Certifications*, Databeskyttelsesdagen 2017, Babara Körffer, *Unabhaengiges Landeszentrum fuer Date,schutz*, Schleswig-Holstein Tyskland, https://databeskyttelsesdag.files.wordpress.com/2017/01/dk_privacy-seals-and-certifications_2017-2.pdf

26 https://stiftungdatenschutz.org/aufgaben/zertifizierung, février 2017.

de confiance est loin d'être atteint. Qui en France connaît les labels délivrés par la CNIL comparé aux labels agro-alimentaires ou énergétiques ? Le public semble plus sensible à la qualité de son environnement, qui le renvoie à sa santé, qu'à la problématique de la protection de ses données personnelles qui représente certes un risque, mais un risque moins concret, plus lointain. On remarque d'ailleurs que les associations de consommateurs s'intéressent peu à la question, qui leur paraît technique, à la différence des États-Unis (cf. Chapitre 7). Pour autant, l'attitude des utilisateurs-consommateurs change à la fois en fonction des usages et des techniques comme le relève le récent sondage effectué par la Chaire Valeurs et Politiques des Informations Personnelles avec Médiamétrie (ce que nous verrons au chapitre 10).

Par ailleurs, la CNIL communique peu sur les labels qu'elle délivre, préférant médiatiser d'autres axes de travail ; pour sa part, EuroPriSe manque de moyens. Pourtant, de nombreux experts accrédités EuroPriSe exercent au sein d'importants cabinets de conseil ou d'avocats d'affaires, notamment en Espagne, au Royaume-Uni, en Suède. Plusieurs d'entre eux ont reconnu, lors des interviews, qu'ils ne communiquaient pas assez, faute de temps et par manque d'habitude.

Du côté des entreprises, les logos des deux types de labels ne semblent pas plus connus, et lorsque cela est le cas, ils ne présentent pas un véritable avantage. Conçus comme le prolongement de la législation, leur coût d'obtention s'avère élevé dans la plupart des cas.

Le coût d'obtention élevé sans véritable avantage concurrentiel

Si l'impartialité d'EuroPriSe est de mise, elle a toutefois un prix. À titre d'illustration :

- dans le cadre de la labellisation d'un périmètre « étroit » comme une solution biométrique, il faut compter trente jours de travail (15 jours pour l'expert technique et 15 jours l'expert juridique) et un coût de 40 000 € grand minimum

- pour un périmètre plus large, certains experts avancent le chiffre de 80 000 €, d'autres une fourchette allant de 100 000 à 200 000 €

- la simple labellisation d'un site Internet demande au moins vingt jours (10 jours pour l'expert technique et 10 jours pour l'expert juridique)

Ce prix dépend directement du périmètre de labellisation retenu, périmètre qui conditionne le temps facturé par les deux types d'experts. Or, celui-ci est difficile à déterminer. Il semble cependant poser moins de problème pour la partie juridique que pour la partie technique où « *tout dépend là du nombre de sous-traitants, du nombre de prestataires impliqués dans l'hébergement, dans la sécurité* ».

Parole d'expert EuroPriSe

« *Déjà identifier les flux … Ça, c'est le plus gros. Personne n'est au courant de rien, en plus ! … Le pire problème c'est que le contrôle d'informations n'est jamais bien fait, les consentements, n'en parlons pas ! Et après, dès que ça sort de la boîte… ça part à droite à gauche ! Si on veut vérifier les contrats, les trucs, les machins… on y passe un temps fou !* »

Pour diminuer le prix, une solution consisterait à réduire le périmètre de labellisation. Mais alors, selon les quatre experts interrogés, le label perd souvent sa signification et le dossier est rejeté par l'autorité de certification EuroPriSe. Des entreprises ont ainsi abandonné leur projet lors de la phase préparatoire. C'est d'ailleurs pour cette raison qu'EuroPriSe s'est diversifié en labellisant les sites internet « *pour que ce soit vendable car moins cher en termes d'expertise et ça parle plus aux clients* ».

Une seconde solution, avancée par un expert, pourrait consister à pratiquer en amont une analyse d'impact qui permettrait à périmètre constant de définir les risques, puis de sélectionner les critères à appliquer.

Parole d'expert EuroPriSe

« *Il y a une marge de risques qu'il faut accepter… avec comme principe directeur la proportionnalité. C'est-à-dire que, par rapport au traitement que l'on est en train d'auditer, on doit aller dans un degré de détails aussi important que celui qu'on ferait dans le domaine de la santé, ou s'il y a des données sensibles qui sont collectées…* »

La CNIL, de son côté, met en avant l'avantage de la gratuité. Cet argument doit cependant être relativisé, si l'on considère le temps passé qui, lui aussi, constitue un coût. La plupart des interviewés estime que l'obtention d'un label CNIL est « chronophage », leur démarche s'étant transformée dans certains cas en « *véritable parcours du combattant* ». Ici aussi, le coût varie essentiellement en fonction du périmètre retenu et de la taille de l'entreprise. Pour l'obtention du label « Formation », les chiffres avancés vont de « *quelques semaines* », à « *15 jours/homme* ». Le label « Audit » s'avère plus « chronophage » : une entreprise a estimé le temps passé à 143,5 jours (pour une équipe composée de cinq personnes), une autre a mis un an et demi « *à construire le label* », une troisième entre quatre et cinq mois.

Là où certains voient un signe fort de qualité et de confiance, d'autres soulignent une lourdeur administrative excessive. Il y aurait, selon un interviewé, « *une faute originelle qui consiste à vouloir faire plus, plutôt que de faire au moins à droit constant* ». Le label « Gouvernance », par exemple, impose que l'entité dispose d'un Correspondant Informatique et Libertés (CIL). Or, le CIL est une simple option évoquée par la loi Informatique et Libertés et le RGPD n'impose pas un Délégué à la Protection des Données dans tous les cas. Selon une personne interrogée, « *c'est confondre la finalité (le respect des données personnelles) et les moyens (avoir un CIL)… la question est : est-il possible d'arriver au même résultat sans CIL ?* ». Selon un autre interviewé, la CNIL chercherait à « *insuffler sa doctrine* », à ajouter des « *détails que la loi n'impose pas* » mais « *que le régulateur voudrait voir se généraliser et qui dissuade tout le monde d'en faire plus que ce que la loi exige en demandant un label public* ».

Ici, « *l'autorité de contrôle va exprimer ce qui fait sa spécificité c'est-à-dire prolonger une réglementation et donc réglementer dans les détails plus fort que ce que les entreprises sont prêtes à accepter* ». Cette tendance à réglementer « *dans les détails* » s'exprime notamment à travers les trente-trois exigences obligatoires (et les quarante-quatre exigences facultatives relatives aux modules complémentaires) du label « Formation » et les soixante-treize exigences du label « Audit ».

Parole d'expert à propos du label Formation de la CNIL

« *Cela rentre dans un degré de détails et de bureaucratie qui est dingue. Par exemple, on m'a dit : « Il manque la définition du consentement art. 2h de la directive. » Vu que c'est une justification sur pièces, le travers est que dans l'idée d'instruire vraiment le dossier toutes les pièces sont examinées et qu'il faudra tout faire.* »

Ici encore on retrouve le reproche du manque de flexibilité, de marge de manœuvre laissée au demandeur : un interviewé explique : « *ce n'est pas assez souple. Ensuite, il y a certaines exigences qui sont à côté de la plaque du besoin terrain* ». Un second souligne « *On est sur du théorique et théoriquement, on peut faire une belle procédure et remplir toutes les exigences sans même connaître ce qui se passe sur le terrain* ». En particulier, le label « Audit » ne tient pas compte de la taille de l'organisme et de sa nature (cabinets de conseils, entreprises, etc.). En outre, à l'inverse d'EuroPriSe, il impose de réunir en amont des compétences juridiques et techniques, ce qui suppose « *de trouver son âme sœur* » avant de déposer le dossier. Ce point est bloquant pour certaines personnes.

L'unique label décerné en matière de coffre-fort en juillet 2016 s'explique par le fait qu'une partie de l'une de ses vingt-deux exigences pose problème : en effet, les produits proposés par le marché ne chiffrent pas les noms des fichiers déposés dans les coffres-forts. La CNIL justifie sa doctrine par le fait que ces métadonnées présentent le même degré de sensibilité que le document lui-même.

Cette « hyper-bureaucratisation » soulignée par un expert « *découle du fait que les labels CNIL ont été conçus comme des cahiers des charges dans un processus qualité, comme pour une entreprise fabriquant des produits alimentaires ou de grande distribution. C'est une logique qui segmente, décompose et met davantage l'accent sur les processus que sur le fond et la substance. En matière de formation, c'est particulièrement discutable, voire stérilisant* ».

Pour sa part, Johanna Carvais, Responsable du pôle Labels de la CNIL en 2015 explique : « *plutôt que de les [les labels] fonder sur le strict respect de la loi, la CNIL a pris pour habitude d'aller au-delà de la loi et de veiller à ce que les exigences qui vont servir de référence à l'analyse de conformité reflètent a minima les recommandations usuelles de*

la CNIL et les bonnes pratiques en règle générale. En effet, tout le monde est censé respecter la loi. Un label qui attesterait de la conformité à la loi devrait en théorie être délivré à tous. Or, ce qui fait la force et l'intérêt d'un label est justement qu'il va servir à distinguer les bons acteurs des moins bons. En ce sens, il ne pourra être délivré à tous les acteurs d'un même marché, sauf à perdre en crédibilité. Il doit permettre de discerner les acteurs et de mettre en avant ceux qui l'ont obtenu afin de leur donner un véritable avantage concurrentiel. Le label sera perçu à ce tire comme un atout économique. »[27]

Une fois le label obtenu, la question du retour sur investissement pour les labels CNIL suscite des avis divergents : pour certains, le label « *n'a pas permis de vendre plus* ». Pour d'autres, notamment des cabinets d'avocats et des cabinets de conseil, le fait d'être labellisé attirerait plus de clients. Le label est perçu positivement, comme un atout concurrentiel, notamment en B2B à l'égard des organismes publics dans le cadre de la passation de marchés publics. À cet égard, on note que la loi de protection des données du Land de Schleswig-Holstein dispose que la préférence doit être accordée aux produits certifiés[28]. Pour sa part, la loi fédérale suisse prévoit que le maître du fichier n'est pas tenu de déclarer son fichier s'il a obtenu un label de qualité[29].

Paroles d'experts à propos du label Formations

« *Je n'ai jamais vu un client dire : je suis venu chez vous parce que vous êtes labellisé. Je n'ai pas l'impression que ça m'a apporté plus de monde. C'est ça qui est curieux !* »

27 Carvais J., (2015). Le label CNIL comme outil de conformité, *in AFCDP, Correspondant Informatique et Libertés, Bien plus qu'un métier*, pp. 500.

28 Art. 4§2 de la loi de protection des données du Land de Schleswig-Holstein.

29 Art. 11a, al. 5, f de la loi fédérale suisse sur la protection des données du 19 juin 1992 (modifiée en dernier lieu le 1er janvier 2014) (CH301).

Pour autant, de manière paradoxale, de nombreux labellisés CNIL renouvellent leur demande : « *je vais redemander le label Formation pour des questions d'image* »[30]. Les experts accrédités EuroPriSe réitèrent leur accréditation pour la même raison.

En France, certains organismes labellisés CNIL qui ont investi en temps pour obtenir un premier type de label, envisagent d'en demander un second. Ayant déjà effectué le travail de « défrichage » et ayant appréhendé la méthode de travail de la CNIL, la demande d'un autre label leur paraît beaucoup moins « chronophage ».

Parole d'expert

« *J'ai mis 15 jours/homme à obtenir le label CNIL Formation. Je pense mettre 10 jours pour obtenir le label Audit.* »

Il est important de ne pas oublier que ces démarches et process de labellisation sont relativement récents, en ce qui concerne du moins les données personnelles. La généralisation de leur adaptation, à la fois sur le plan économique et sociétal dans les usages, s'inscrit nécessairement dans une temporalité plus longue. Comme le souligne un avocat, « *nous ne sommes qu'au début d'une longue histoire* ».

Qu'en est-il pour les organismes non-labellisés CNIL ?

À cet égard, le coût financier et temporel doit être mis en relation avec les bénéfices attendus par l'entreprise. D'une manière générale, ces bénéfices ne semblent pas pour l'instant suffisamment élevés, les risques liés à une non-conformité étant relativement faibles. Les sanctions civiles et pénales sont actuellement quasi-inexistantes. Les treize sanctions prononcées par la CNIL en 2016 (4 sanctions pécuniaires et 9 avertissements, dont 4 rendus publics) n'ont rien d'incitatif. La CNIL, en effet, n'est pas culturellement une autorité répressive. Le sera-t-elle lorsque le RGPD entrera en vigueur et qu'elle pourra prononcer une sanction financière pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial ?

30 Plus précisément, les taux de renouvellement sont quasiment de 100% pour le label « Formation » et de 50% pour le label « Audit ».

Paroles d'experts à propos du label Gouvernance de la CNIL

« *Personne n'a voulu y aller. … les entreprises sont très attentistes par rapport au nouveau règlement en France. C'est lié au fait qu'il n'y a pas de sanctions. C'est une gestion des risques en entreprise.* »
« *… la violation des données n'est pas assez sanctionnée, à défaut les entreprises iraient plus vers ce genre d'outil. Vu que ce n'est pas le cas, quel intérêt ?* »

Quand bien même les sanctions financières seraient élevées, les entreprises ne conçoivent pas le label uniquement comme un instrument de prolongation de la législation. En effet, le point de consensus est difficile à trouver « *entre le plus que souhaite la CNIL dans un label et le plus que l'entreprise souhaite mettre en avant* ». Ce ***plus*** va au-delà de la volonté de mettre en avant sa conformité.

Parole d'expert

« *Il y a une espèce de blocage sur la communication que l'entreprise souhaite développer car la seule chose qu'elle espère et qui est une monnaie forte est que ça soit conforme à la communication qu'elle développe.* »