La confiance saisie par le droit

Claire Levallois-Barth

Levallois-Barth, C.

«La confiance saisie par le droit»

dans **Signes de confiance – l'impact des labels sur la gestion des données personnelles** (Chapitre 2, pages 22 à 36).
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

La confiance saisie par le droit

Projet de loi pour la confiance dans la vie politique, loi pour la confiance dans l'économie numérique[1], règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[2], on ne compte plus les textes juridiques qui se donnent pour objectif de renforcer la confiance. Ces derniers semblent constituer une réponse à une crise de la confiance, crise à l'égard des institutions démocratiques et de leur capacité à résoudre les problèmes complexes auxquels les citoyens sont confrontés mais aussi à l'égard des technologies et de l'industrie qui font courir des risques, perçus comme de plus en plus menaçants.

Pour autant, et de manière surprenante, la notion de confiance n'est pas explicitement définie par le droit. Aucun texte ne s'attache à caractériser ce concept qui reste vague dans sa définition (2.1.) et qui poursuit en matière de données personnelles une double fonction que nous allons expliciter (2.2.). Parmi les signes de confiance extérieurs figurent les labels, que le droit encadre dans un continuum allant du droit dur au droit souple (2.3.), labels qu'il convient de distinguer de la certification et des marques (2.4.).

---

1 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN), JORF, 22 juin 2004.

2 Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (Règlement eIDAS), JOUE L 257, 28 août 2014, p. 73–114.

2.1. La notion de confiance

En absence de définition législative de la notion de confiance, il est possible de se tourner vers la doctrine. Notamment, le Doyen Gérard Cornu donne la définition suivante dans son *Vocabulaire juridique*[3] :

Confiance

1. Croyance en la bonne foi, loyauté, sincérité et fidélité d'autrui (tiers, contractant) ou en ses capacités, compétences et qualifications professionnelles (ex. : confiance envers un médecin),
2. Action de se fier à autrui, ou plus précisément de lui confier une mission.

Selon cette définition, qui relève plus du sens commun que du sens juridique, la confiance se déterminerait par référence à une personne. Il s'agirait de l'action de lui confier une mission, par exemple en droit des contrats spéciaux via le mandat[4] et le dépôt[5] ou, plus récemment en droit de la santé publique, avec la possibilité pour tout patient majeur de

3 Cornu, G., (2016). Vocabulaire juridique, Paris, PUF, 11e édition, 2016, V° Confiance.

4 Le mandat est un contrat par lequel une personne, le mandant, donne à une autre personne, le mandataire, le pouvoir de faire un ou des actes juridiques en son nom et pour son compte.

5 Le dépôt est une convention par laquelle une personne, le dépositaire, se charge gracieusement de la conservation d'un objet mobilier ou d'une somme d'argent que lui remet le déposant.

désigner une personne de confiance qui peut être consultée au cas où ce même patient serait hors d'état d'exprimer sa volonté et de recevoir l'information nécessaire à cette fin[6]. S'il le souhaite, le patient peut se faire accompagner par la personne de confiance dans ses démarches et ses entretiens médicaux afin de l'aider dans ses décisions.

La confiance personnelle s'entend également comme une « croyance » qui permettrait d'avoir foi en ou d'accorder un crédit à un proche, un expert ou un professionnel. Cette confiance se traduirait par référence à d'autres notions : la fidélité dans le mariage, la loyauté du salarié, ce dernier devant s'abstenir de porter atteinte aux intérêts de l'entreprise (comme se servir des moyens mis à sa disposition pour son usage privé ou vendre les secrets de fabrication à un concurrent) ou la bonne foi lors de l'exécution d'un contrat. Dans l'hypothèse où l'un des contractants n'a pas – ou a mal – rempli son obligation, on recourt à la notion de mauvaise foi pour sanctionner son comportement.

La confiance se définit donc aussi de façon négative comme l'indiquent les concepts de perte de confiance en droit du travail ou d'abus de confiance en droit pénal. Ce dernier désigne une infraction contre les biens, dont l'objet est de disposer du bien d'autrui, y compris d'un bien immatériel, dans un cadre qui n'a pas été convenu avec le propriétaire.

► Dans un arrêt rendu le 22 octobre 2014, la chambre criminelle de la Cour de cassation a qualifié d'abus de confiance le fait pour un salarié d'avoir « *en connaissance de cause détourné en les dupliquant, pour son usage personnel, au préjudice de son employeur, des fichiers informatiques contenant des informations confidentielles et mis à sa disposition pour un usage professionnel* »[7].

À côté de la ***confiance accordée*** à une personne, le droit participe à l'instauration de la confiance à l'égard des institutions. La confiance légitime notamment renvoie, en droit de l'Union européenne, à l'attente de la part du justiciable d'une prévisibilité et d'une stabilité des normes émanant des autorités tant européennes qu'étatiques, tandis que la ***sincérité*** en droit budgétaire impose que « *les lois de finances présentent de façon sincère l'ensemble des ressources et des charges de l'État* »[8].

---

6 Loi n° 2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JORF, 5 mars 2002.

7 Cass. crim., 22 oct. 2014, n° 13-82.630.

8 Art. 32 de la loi organique n° 2001-692 du 1er août 2001 relative aux lois de finances, JORF, 2 août 2001.

Enfin, le législateur cherche à établir les conditions de la confiance à l'égard des entreprises, notamment dans le contexte du numérique qui ne peut se réclamer d'une pratique sociale ancienne et suffisamment assise.

Il est en particulier intéressant de noter que les textes nationaux ou communautaires qui utilisent dans leur intitulé le terme de confiance ne définissent pas cette notion, qu'il s'agisse du règlement adopté par l'Union européenne eIDAS sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur[9] ou de la loi française pour la confiance dans l'économie numérique (LCEN), adoptée le 21 juin 2004. Concernant cette dernière, le terme de confiance, ajouté au dernier instant dans le titre même de la loi, semble à tout le moins faire référence au processus psychologique de la confiance, tel que décrété par le législateur[10]. Bien que loi « pour » la confiance dans l'économie numérique ou règlement « sur » les services de confiance (*trust services* dans la version anglaise), les deux textes ont pour principal objectif de réguler le marché du commerce électronique. À cette fin, ils mettent en place des mécanismes propre à contrer les risques ressentis par l'utilisateur à l'égard de la technologie et de sa dimension mondiale, afin d'assurer une expérience « rassurante » pour pallier l'insuffisante construction du lien social (cf. Chapitre 1).

Ici, la confiance se construit à la fois autour de la notion de sécurité, qu'elle soit juridique, technique ou organisationnelle (par exemple via la certification des produits et services comme nous le verrons dans le chapitre 4) et de celle de responsabilité des acteurs de l'économie numérique[11], en particulier des prestataires techniques. « *Être responsable n'est-ce pas « répondre de » ? Et « installer » quelqu'un comme devant répondre d'une situation donnée n'est-ce pas le moyen de créer de la confiance ?* »[12]. Ainsi, tout un jeu de

9 Règlement eIDAS, précité. Nous encourageons les lecteurs à se référer à Levallois, C. (2016). La réglementation mise en place par l'Union européenne en matière d'identification électronique et des services de confiance (règlement eIDAS). *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

10 En ce sens, Castets-Renard, C., (2006). Le formalisme du contrat électronique ou la confiance décrétée, Defrénois, 30/10/2006, n°20, p. 1529.

11 Agosti, P., Caprioli, E.A., (2005). La confiance dans l'économie numérique (Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) (LCEN), Petites affiches, 03/06/2005, n°110, p. 3.

12 Vivant, M., (2004). Entre ancien et nouveau, une quête désordonnée de confiance pour l'économie numérique, Cahier Lamy Droit de l'informatique et des réseaux, n°171, juillet 2004, p. 2 et s.

la responsabilité se dessine à travers la régulation juridique, qui peut être appréhendée comme un instrument au service de la confiance.

Dès lors, dans le numérique aussi, la confiance se traduit par référence à d'autres notions, notions que l'on retrouve dans le domaine des données personnelles. La ***sécurité*** des réseaux et des informations, la ***responsabilité*** des responsables de traitements et des sous-traitants mais aussi la ***loyauté***. Cette dernière est d'ailleurs reconnue par de nombreux textes[13] même s'il n'existe pas de définition légale du ***principe de loyauté***. Librement appréciée par le juge et la CNIL, elle s'entend au stade de la collecte essentiellement comme une obligation de transparence vis-à-vis des personnes dont les données sont collectées et traitées. Ainsi, ces dernières doivent être informées de l'identité du responsable de traitement, des finalités du traitement, de leurs droits, etc. À défaut, l'article 226-18 du Code pénal prévoit que «*le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende*» (1,5 millions si l'auteur est une personne morale). En l'absence de transparence, la collecte de données est jugée déloyale : par exemple, la collecte d'adresses électroniques personnelles de personnes physiques à leur insu sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition[14], la notation d'un professeur sans que cette possibilité soit limitée aux seuls élèves ayant ce professeur comme enseignant[15] ou la collecte par Facebook de données personnelles relatives à la navigation sur des sites tiers de personnes non-inscrites à son service[16].

Depuis peu, la loyauté des plateformes en ligne est aussi comprise en termes de transparence. Ainsi, la loi du 7 octobre 2016 pour une République numérique oblige les plateformes (Facebook, Twitter, Airbnb, Uber…) à «d*élivrer au consommateur une information loyale, claire et transparente*», notamment sur les modalités de référencement[17]. Cette même loi introduit également la notion de ***tiers de confiance numérique***, le tiers étant ici

13 Notamment, art. 8§2 de la Charte des droits fondamentaux de l'UE ou art. 5§1 du RGPD.

14 Cass. crim., 14 mars 2006, pourvoi n° 05-83.423.

15 CA Paris, 25 juin 2008, n° 08/04727, affaire «note2be».

16 CNIL, déc. n° 2016-007, 26 janvier. 2016 : «*À l'occasion de la navigation sur la page d'un site tiers sur lequel figure un module social FACEBOOK (bouton J'aime par exemple), … la société collecte des données relatives à la navigation des internautes qui ne sont pas inscrits sur le site FACEBOOK.COM […]. Si la finalité avancée par la société peut apparaître légitime (assurer la sécurité de ses services), la collecte des données relatives à la navigation sur des sites tiers des non-inscrits au site FACEBOOK.COM est réalisée sans qu'ils en soient informés.*»

17 Art. 49 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, JORF, 8 octobre 2016.

désigné comme un organisme certifié par la CNIL chargé d'enregistrer à la demande d'une personne ses « *directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès* »[18].

Par son ancrage dans les processus sociaux, le droit joue à la fois sur la confiance assurée et la confiance décidée : ce faisant, il laisse entrevoir deux tendances de fond qui se croisent et se recroisent, comme nous allons le voir, et qu'il cherche à encadrer.

2.2. Les fonctions de la confiance

La confiance naît essentiellement de l'existence d'un lien social qui s'est construit dans la durée. Comme nous venons de le voir, elle tiendrait dans l'action de se fier à autrui, cette croyance amenant la personne à interagir de manière plus fréquente et contribuant à réduire l'incertitude quant à l'issue de l'interaction (cf. Chapitre 1). Si autrui n'est pas digne de confiance, s'il n'est pas sincère, le droit intervient pour protéger la partie faible et sanctionner. Cette protection est le reflet de la prise en charge par la société d'une forme d'assurance du « vivre-ensemble » dans des conditions supportables. À cette fin, le droit édicte certaines obligations et réprime certains comportements pour apporter une garantie à toutes les parties quant au bon fonctionnement minimal de la société. Il participe ainsi à la confiance assurée.

Sur un plan différent, le droit cherche également à assurer le bon fonctionnement de l'économie. Lorsque l'on passe à un droit dont l'objectif devient la régulation du marché caractérisé par la libre circulation, en particulier des données au sein de l'environnement numérique, le législateur cherche à instaurer la confiance non plus de la partie faible mais du consommateur. La protection de ce dernier est, en effet, une condition préalable pour qu'il « accepte » la société de l'information, cette dernière ayant pris la forme de « *l'économie numérique, une vision présentée comme sociale cédant le pas aux impératifs économiques, mais qui intègre également les mêmes aspects sociaux* »[19].

---

18 Art. 40-I de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, tel que modifié par l'article 63 de la loi pour une République numérique, précitée.

19 Agosti, P., Caprioli, E.A., (2005). La confiance dans l'économie numérique (Commentaires de certains aspects de la loi pour la confiance dans l'économie numérique) (LCEN), Petites affiches, 03/06/2005, n°110, p. 4.

Cette tension visant à assurer le fonctionnement efficace du marché en instaurant des règles aux bénéfices du consommateur est clairement perceptible dans le titre même du RGPD, lequel est « *relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* ». Elle est mise en exergue par la Commission européenne dans sa communication de 2012 « Protection de la vie privée dans un monde en réseau » :

> *« L'instauration d'un climat de confiance dans l'environnement en ligne est essentielle au développement économique. S'ils n'ont pas confiance, les consommateurs hésiteront à effectuer des achats en ligne et à recourir à de nouveaux services. Dès lors, il est également impératif de garantir un niveau élevé de protection des données pour accroître la confiance des consommateurs dans les services en ligne et réaliser le potentiel de l'économie numérique, ce qui stimulera la croissance économique et la compétitivité des entreprises de l'Union. »* [20]

Il s'agit donc bien ici de susciter la confiance dans le marché au sens de la confiance décidée, le terme *trust* figurant notamment au considérant 7 de la version anglaise du RGPD[21].

Un autre signe de ces tendances qui se croisent et se recroisent est perceptible à travers l'évolution des bases juridiques des textes législatifs. La directive 95/46/CE Données personnelles adoptée en 1995[22] a pour base juridique l'article 100A du traité instituant la Communauté européenne relatif au rapprochement des dispositions législatives ayant pour objet l'établissement et le fonctionnement du marché intérieur. Pour sa part, le RGPD, adopté en 2016, se base sur l'article 8§1 de la Charte des droits fondamentaux de l'Union européenne et l'article 16§1 du traité sur le fonctionnement de l'Union européenne qui

---

20 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Protection de la vie privée dans un monde en réseau – Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle, COM(2012)9 final, Bruxelles, 25 janvier 2012, p. 2.

21 Selon lequel "*Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market*".

22 Directive n°95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JOCE, L. 281 du 23 novembre 1995, p. 31.

disposent que « *toute personne a droit à la protection des données à caractère personnel la concernant* ».

On interprétera cet état de fait soit comme une mainmise des mécanismes du marché sur le domaine initialement du ressort du droit, soit au contraire comme une réconciliation entre la protection de la partie faible (la personne dont les données personnelles sont collectées) et la libre circulation des informations afin de stimuler la croissance économique et la compétitivité industrielle.

On notera toutefois les signes de l'inversion du rapport entre lien social et échanges marchands en constatant le rôle croissant du droit de la consommation. La loi pour une République numérique du 7 octobre 2016, par exemple, inscrit le droit à la récupération de l'ensemble de ses données dans le code de la consommation, à l'article L. 224-42-2. On note alors que ce même article précise que « *cette récupération s'exerce conformément aux conditions prévues à l'article 20 du [RGPD] pour les données ayant un caractère personne*l ». Dès lors, pourquoi ne pas avoir choisi d'insérer le droit à la portabilité directement dans la loi Informatique et Libertés ? L'objectif principal est ici de « *réduire la viscosité du marché* »[23]. Clairement, nous nous situons dans le domaine de la gestion des risques, via l'instauration de règles censées réduire l'incertitude et permettre à la personne de décider elle-même en connaissance de cause. La nouvelle rédaction de l'article 1er de la loi Informatique et Libertés, telle qu'introduite par l'article 54 de la loi pour une République numérique, en constitue une parfaite illustration : désormais, « *toute personne dispose du* ***droit de décider*** *et de contrôler les usages qui sont faits des données à caractère personnel la concernant* ».

Ce droit de décider entend traduire l'idée d'encapacitation (*empowerment*) du citoyen en lui donnant davantage de capacité d'agir et de contrôle, notamment en renforçant les obligations d'information et de transparence quant aux actions des autres parties. Ce serait donc la personne qui déciderait de l'usage qui doit être fait de ses données personnelles et non plus le législateur ou la CNIL. On peut s'interroger sur les conséquences de cette évolution, sur l'accent mis davantage sur la confiance décidée, dans sa forme la plus individualisée, que la confiance assurée. Ainsi, selon Nicolas Ochoa, « *donner plus de pouvoir à la personne fichée revient à la laisser de plus en plus démunie face à des auteurs de*

23 Projet de loi pour une République numérique enregistré à la Présidence de l'Assemblée nationale le 9 décembre 2015, 14e législature, n° 3318.

traitements de données toujours plus puissants […] Ce principe revient donc sciemment à instrumentaliser la faiblesse du libre arbitre de tout un chacun sur des questions éminemment techniques, sujets sur lesquels, au regard de ce degré de technicité, l'individu non spécialiste doit être considéré comme un majeur incapable pour son propre bien. »[24]

Dans le même sens, on peut se demander ce qui sous-tend le passage d'un système d'autorisations des traitements de données personnelles par l'autorité de contrôle (tel que mis en place par la loi Informatique et Libertés en 1978) à un renforcement de la place du consentement de la personne concernée par le RGPD. L'individu exerce-t-il réellement son libre arbitre lorsqu'il consent à n'importe quelle utilisation de ses données personnelles ? Lorsqu'il accepte en un clic les conditions générales d'utilisation d'un site, surtout quand son refus bloque tout accès au site ? Comme le fait remarquer Nicolas Ochoa, « *au regard de la vigueur de l'économie numérique et de la nécessité de son usage massif et croissant des données personnelles, cela se tient* » et fait partie de la logique qui se donne pour objectif premier d'augmenter la circulation des données.

2.3. La mise en œuvre de la confiance ou l'imbrication du droit dur et du droit souple

Cette nouvelle tendance, qui appelle à la libre circulation des données, prend place dans un paysage juridique lui-même en profonde reconfiguration.

On constate en effet que les règles de droit ne sont désormais plus caractérisées par la seule contrainte mais qu'elles cherchent également à orienter les comportements. Dans ce contexte, le label occupe une place particulière, en tant que signe extérieur et visible de la confiance.

Classiquement, le droit se définit par un ensemble de normes de conduite, édictées par l'autorité publique et assorties de sanctions en cas de non-respect. Cette conception traditionnelle telle que l'enseigne Hans Kelsen, ce droit « dur » symbolisé par la contrainte, les pouvoirs publics et la sanction, est relayé aujourd'hui par une forme de droit qualifié de « souple ».

---

24 Nicolas Ochoa, « La libre disposition des données personnelles : retour sur un braquage discret des droits et libertés », 27/01/2016, https://www.lesechos.fr/idees-debats/cercle/cercle-147345-la-libre-disposition-des-donnees-personnelles-retour-sur-un-braquage-discret-des-droits-et-libertes-1195601.php

Le droit souple se définit comme un ensemble de règles non contraignantes émanant d'une entité publique ou privée et exemptées de sanctions si elles ne sont pas suivies. Invitant à une redéfinition de la norme, le droit souple est critiqué au regard de la conception rousseauiste de la règle de droit, laquelle se caractérise principalement par sa force obligatoire. À l'inverse du droit dur, il s'agit d'un droit « *qui invite plus qu'il ne contraint, qui propose plus qu'il n'impose, qui dirige plus qu'il ne force* »[25]. En 2013, le Conseil d'État a défini cette notion dans son étude annuelle comme « *l'ensemble des instruments répondant à trois conditions cumulatives :*

- *Ils ont pour objet de modifier ou d'orienter les comportements de leurs destinataires en suscitant, dans la mesure du possible, leur adhésion ;*
- *Ils ne créent pas par eux-mêmes de droits ou d'obligations pour leurs destinataires ;*
- *Ils présentent, par leur contenu et leur mode d'élaboration, un degré de formalisation et de structuration qui les apparente aux règles de droit.* »[26]

À titre d'exemple, les avis et les lignes directrices, notamment ceux du G29, les recommandations et les packs de conformité de la CNIL, les codes de conduite, les chartes déontologiques, les règles internes d'entreprises (qui permettent aux sociétés mères des multinationales de produire un droit applicable à l'ensemble de leurs filiales), les standards techniques sont autant d'instruments hétérogènes pourvus d'une certaine autorité normative. Cette autorité certes n'est pas celle de la contrainte, mais elle incite à l'adoption de certains comportements.

Sans force contraignante, les instruments de droit souple s'inscrivent dans une chaîne de normativité graduée allant du « strict » droit contraignant au « véritable » droit souple. Il est ainsi fréquent que les textes de droit dur prévoient l'existence de ce type d'instruments, voire leur confèrent un rôle dans la définition de leurs règles d'application.

► La certification, les labels et les marques en matière de données personnelles en sont une illustration : ces instruments sont reconnus par le RGPD comme ayant une valeur de référence à la fois dans le cadre de l'obligation de responsabilité et des transferts internationaux de données (cf. Chapitre 8). Une

25 Mekki, M., (2009). Propos introductifs sur le droit souple, *in Le droit souple*, Dalloz, Coll. « Thèmes et commentaires », 2009, p. 11.

26 Conseil d'État, Le droit souple, Les rapports du Conseil d'État, La documentation française, 2013, p. 61, http://www.ladocumentationfrancaise.fr/rapports-publics/144000280/index.shtml.

forme d'avantage est accordée aux entités qui y recourent, puisqu'elles sont dispensées de fournir d'autres justificatifs.

Dans ce contexte, les promoteurs du droit souple soulignent sa flexibilité. D'une part, il serait utile pour agir au niveau international ; d'autre part, il permettrait d'appréhender des phénomènes émergents en rapide évolution (notamment les mutations technologiques[27] en explorant des domaines prospectifs comme l'intelligence artificielle, les drones), et de préparer l'adoption ultérieure de textes contraignants. En revanche, ses critiques pointent le contournement des institutions démocratiques et la dégradation des qualités attendues du droit, telles que la clarté et la stabilité de la norme. Ainsi, dans un rapport de 1991, le Conseil d'État s'inquiétait pour la sécurité juridique menacée par une inflation normative sans précédent, affirmant dans une formule célèbre : « *Qui dit inflation dit dévalorisation : quand le droit bavarde, le citoyen ne lui prête plus qu'une oreille distraite* »[28]. Au cœur de ce bavardage, la haute juridiction dénonçait en 1991 le droit « mou », le droit à « l'état gazeux » qui, à vrai dire, présente un contenu identique au droit souple dont elle préférait pourtant souligner les qualités en 2013.

Aujourd'hui, le droit souple est partie intégrante de la régulation des données personnelles car, selon Isabelle Falque-Pierrotin, présidente de la CNIL, « *à la réglementation prescriptive s'ajoute la nécessité d'une régulation plus partenariale, fondée sur des instruments juridiques personnalisés* »[29]. Dans ce cadre, la CNIL entend privilégier le dialogue et l'appropriation par les acteurs. Le label apparaît alors comme un outil de mise en œuvre, un relais des principes de protection des données personnelles édictés par le droit dur, censé définir des bonnes pratiques et contribuer à la résolution de problèmes opérationnels. On constate le recours croissant à cet instrument situé en aval du droit « source » et qui se présente comme un signe extérieur de confiance.

2.4. Le label, signe extérieur de confiance

En droit français, le label ne fait l'objet d'aucune définition officielle. De même, la CNIL ne donne aucune définition technique, mais envisage le label comme un indicateur de

27 Dans ce sens, Le droit souple, Rapport du Conseil d'État, précité, p. 91.

28 Conseil d'État, De la sécurité juridique, Rapport public annuel 1991, La documentation française.

29 Isabelle Falque-Pierrotin, « Le droit souple vu de la CNIL : un droit relais nécessaire à la crédibilité de la régulation des données personnelles », in Le droit souple, Rapport du Conseil d'État, précité, p. 241.

confiance pour les consommateurs. Abstraitement, le label serait envisagé par la doctrine comme « *un mode de reconnaissance d'un niveau de qualité, délivré par une entité privée ou une autorité publique, adossé à un cahier des charges (référentiel)* »[30].

In concreto, le label se manifeste différemment dans plusieurs domaines, par exemple en matière environnementale ou agroalimentaire. En effet, l'article L. 115-21 du Code de la consommation dispose que « *les labels agricoles sont des marques collectives attestant qu'une denrée alimentaire ou qu'un produit agricole non alimentaire et non transformé possède un ensemble distinct de qualités et caractéristiques spécifiques préalablement fixées et établissent un niveau de qualité. Ce produit doit se distinguer des produits similaires de l'espèce habituellement commercialisés par ses conditions particulières de production, de fabrication et, le cas échéant, par son origine.* »

Le label suppose une démarche volontaire des entreprises. Il est adopté par ces dernières et n'est pas imposé. En ce sens, il fait partie du droit souple. Néanmoins, si la volonté s'exprime dans l'adhésion, l'aspect contraignant surgit au stade des sanctions bien que celles-ci ne soient pas pécuniaires. Le retrait du label peut être perçu comme une sanction morale préjudiciable à l'image de l'entreprise.

Le label doit être distingué de la certification définie par l'article L. 115-27 du Code de la consommation qui dispose que « *constitue une certification de produit ou de service soumise aux dispositions de la présente section l'activité par laquelle un organisme, distinct du fabricant, de l'importateur, du vendeur ou du prestataire, atteste, à la demande de celui-ci effectuée à des fins commerciales, qu'un produit ou un service est conforme à des caractéristiques décrites dans un référentiel et faisant l'objet de contrôles. Le référentiel est un document technique définissant les caractéristiques que doit présenter un produit ou un service et les modalités du contrôle de la conformité du produit ou du service à ces caractéristiques.* »[31] On remarque que les pouvoirs publics détiennent toujours un rôle, même si certains auteurs font allusion à une « privatisation » de la certification[32]. À l'échelon international, la certification est définie de façon quasi-similaire par l'Organisation internationale de normalisation (ISO – *International Organization for Standardization*) comme une

30 Naftaski, F., Desgens-Pasanau, G., (2010). Enjeux et perspectives du pouvoir de labellisation de la CNIL, Revue Lamy Droit de l'Immatériel 2010, n°63.

31 Loi n°94-442 du 3 juin 1994 modifiant le Code de la consommation en ce qui concerne la certification des produits industriels et des services et la commercialisation de certains produits, JORF, 4 juin 1994.

32 Pontier, J.-M. , (1996). La certification, outil de la modernité normative, D. 1996, p. 355.

« *assurance écrite (sous la forme d'un certificat) donnée par une tierce partie qu'un produit, service ou système est conforme à des exigences spécifiques* »[33].

La certification est un processus volontaire ou obligatoire mené sur la base d'exigences élaborées par un organisme reconnu et réalisées par un auditeur accrédité et externe au candidat. Il est impératif toutefois de ne pas oublier à ce stade que ces exigences n'intègrent pas nécessairement et uniquement des obligations légales. Le processus d'évaluation aboutit, s'il réussit, à la délivrance d'une attestation officielle de conformité aux exigences. Le résultat final peut prendre plusieurs formes qui indiquent que la certification a été obtenue : un label, une marque ou un certificat.

Soulignons qu'une entreprise peut aussi être certifiée sans pour autant disposer d'un label ou d'une marque : soit la certification est obligatoire, soit elle permet à l'organisme d'obtenir un diagnostic de ce qui se passe en interne afin d'améliorer ses propres processus.

Le caractère obligatoire de la certification est bien illustré en France par les exemples des données de santé et des jeux d'argent en ligne :

- à l'heure actuelle, les hébergeurs de données de santé doivent être agréés par le ministre chargé de la Santé après avis de la CNIL et du Comité d'Agrément des Hébergeurs pour une durée de trois ans[34]. Ils sont au nombre de 96. À partir de 2018, un hébergeur de données de santé sur support numérique devra obligatoirement être titulaire d'un certificat de conformité[35]. Celui-ci sera délivré par un organisme de certification accrédité choisi par l'hébergeur. Il pourra s'agir de l'instance française d'accréditation, le COFRAC, ou de son équivalent au niveau européen[36].

33 https://www.iso.org/fr/certification.html.

34 Art. L. 1111-8 du code de la santé publique créé par la loi n°2002-303 du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé, JORF, 5 mars 2002, texte n°1 et art. R. 1111-10 créé par le décret n°2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel et modifiant le code de la santé publique (dispositions réglementaires), JORF, 5 janvier 2006.

35 ASIP Santé, Évolution de la procédure d'agrément des hébergeurs de données de santé, http://esante.gouv.fr/services/referentiels/securite/le-referentiel-de-constitution-des-dossiers-de-demande-d-agrement-des

36 Ordonnance n°2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel modifiant l'article L. 1111-8 du code de la santé publique, JORF, 13 janvier 2017.

- de même, l'agrément des opérateurs de jeux par l'Autorité de Régulation des jeux en ligne (ARJEL) est obligatoire ; celle-ci s'appuie notamment sur une certification obligatoire par des organismes de certification[37].

En matière de protection des données personnelles, on retrouve l'emploi des termes de « label », « certification » et « marque ». En France, la loi Informatique et Libertés dispose que la CNIL « *délivre un label à des produits ou à des procédures* »[38]. On trouve également l'emploi du terme « label » (*Seal* en anglais) par des entités privées, par exemple en Allemagne le *ePrivacySeal* délivré par la ePrivacy consult GmbH, au niveau européen le *esafety label*, ou aux États-Unis le *Accredited Business Seal for the Web* du Better Business Bureau (BBB). Au Royaume-Uni, l'autorité de contrôle, l'*Information Commissioner Office* (ICO) envisage de délivrer des *Privacy Seals* qu'elle définit comme un sceau d'approbation qui démontre une bonne pratique en matière de protection de la vie privée et des normes élevées de conformité à la protection des données[39]. On peut également se référer, au niveau européen, au label *EuroPriSe* (*European Privacy Seal*) qui, selon ses promoteurs, offre une certification de conformité[40].

Ainsi, l'élaboration de labels en matière de données personnelles s'inspire fortement des procédures développées dans le domaine de la certification. En Allemagne par exemple, les procédures d'audits développées dans les années 1990 dans le domaine de l'environnement ont servi de modèle pour développer les labels en matière de données personnelles principalement proposés par des acteurs privés. Par ailleurs, on constate que dans ce domaine spécifique, il est aussi fait référence à la certification.

En France, si la CNIL délivre des « labels », la loi du 7 octobre 2016 pour une République numérique l'autorise aussi à publier « *des référentiels aux fins de certification de la conformité de processus d'anonymisation* » des données personnelles. De son côté, la Suisse a

37 Voir en particulier la partie V « Informations relatives aux comptes joueurs » de l'annexe II du Règlement relatif à la certification prévue à l'article 23 de la loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne, adopté par la décision n°2014-018 du collège de l'Autorité de régulation des jeux en ligne en date du 17 mars 2014, modifiée par la décision n°2016-006 du collège de l'Autorité de régulation des jeux en ligne en date du 18 février 2016, http://www.arjel.fr/IMG/rc/certification2.pdf.

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

39 *Stamp of approval which demonstrates good privacy practice and high data protection compliance standards*, voir https://ico.org.uk/for-organisations/resources-and-support/privacy-seals/.

40 *Offers certification to compliant […] products, […] services and […] processings*, voir https://www.european-privacy-seal.eu/EPS-en/Home.

adopté une ordonnance sur les certifications en matière de protection des données le 28 septembre 2007.

Les acteurs privés utilisent, eux aussi, le terme de certification :

- en Espagne, l'association professionnelle de protection de la vie privée (*Asociación Profesional Española de Privacidad* – APEP) délivre la certification *APEP-CertifiedPrivacy*,
- l'Allemagne dispose de nombreuses possibilités avec notamment la *Data Privacy Certification for Companies* de TÜV Rheinland et la *Zertifizierung der Datenschutzqualifikation* de la *Gesellschaft für Datenschutz und Datensicherheit* (GDD),
- en Italie, la *Certificazione di privacy officer e consulente della privacy* est fournie par TÜV Italia/TÜV SUD GROUP,
- au niveau européen, l'*OBA Certification* est délivrée par l'*European Interactive Digital Advertising Alliance* (EDAA).

Du côté des marques de confiance, on note qu'elles opèrent dans le secteur du commerce et qu'elles sont délivrées par des associations, avec notamment :

- en France, la marque de confiance FEVAD de la Fédération du e-commerce et de la vente à distance,
- en Autriche, TrustMark Austria de l'association *handelsverband,*
- et en Europe l'*Ecommerce Europe Trustmark* de l'association Ecommerce.

Le label en matière de données personnelles se présente donc comme le résultat final d'une assurance écrite. Signe extérieur d'un processus volontaire, il se base sur un référentiel déclinant certaines obligations légales. La confiance ainsi recherchée est définie par rapport à d'autres notions, notamment la loyauté, la sécurité et la responsabilité. Elle se situe à la croisée d'une ambiguïté essentielle entre l'exigence de la protection de l'utilisateur et celle de la circulation des données personnelles que l'on suppose indispensable au développement de l'économie numérique.