Institut Mines-Télécom

Chaire
Valeurs et Politiques
des Informations Personnelles

Signes de confiance

l'impact des labels sur la gestion des données personnelles

coordonné par
Claire Levallois-Barth

Janvier 2018

TELECOM ParisTech

TELECOM Ecole de Management

TELECOM SudParis

Signes de confiance

l'impact des labels sur la gestion des données personnelles

ISBN 978-2-9557308-3-6 9782955730836 - version électronique - janvier 2018

Sommaire

Introduction

Armen Khatchatourov

Situés au centre de la construction de toute société, les liens de confiance concernent à la fois les relations entre les citoyens et les relations entre les individus et les organisations. En la matière, la confiance conditionne la possibilité même des échanges institutionnels et commerciaux et questionne le rôle que ces échanges peuvent avoir dans la structuration de notre vivre-ensemble. Or, nous assistons aujourd'hui à une crise de confiance – telle est du moins l'affirmation que l'on retrouve dans les domaines économique, politique et social. Le numérique est sans doute un des vecteurs de cette « crise », en bousculant aussi bien les modèles économiques que les mécanismes sous-jacents à la sphère publique.

En particulier, l'évolution récente de la problématique de la circulation des données personnelles montre bien une défiance de l'utilisateur à la fois à l'égard des acteurs économiques et des instances étatiques. Ceci est complexifié par la spécificité des biens numériques (dits biens « de confiance » en termes de la théorie économique) dont la « qualité » n'est pas connue par le consommateur, même après l'acte ponctuel de consommation.

Face à ce constat, on observe aujourd'hui l'émergence de nouveaux modes de régulation, allant de la légifération sur les « *marques de confiance* » ou « *labels* » (via le Règlement Général sur la Protection des Données – RGPD[1]) dont la gestion serait confiée à des instances publiques et / ou privées, à des démarches de type « *crowd-sourced* » dont les utilisateurs sont à l'initiative (cf. TOSDR[2]), en passant par une régulation technique *de facto* (par exemple à l'aide de bloqueurs de publicité). Nous pourrions être tentés de voir dans ces nouveaux modes un moyen de pallier la crise de confiance. Cette situation demande cependant à être examinée plus précisément, et de manière pluridisciplinaire. Une des questions essentielles, partagée à sa manière par plusieurs disciplines, est ici celle de la ***formalisation de la confiance***.

Ainsi, la notion de risque et celle de son évaluation formelle sont centrales dans l'économie, la confiance étant souvent associée au risque attribué à la contrepartie dans une transaction. À cet égard, le baromètre de la confiance de l'ACSEL-CDC[3] définit la confiance

---

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JOUE L 119/1 du 4 mai 2016, http://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=FR

2 « *Terms of Service; Didn't Read* » https://tosdr.org/

3 Baromètre de la confiance de l'ACSEL-CDC, 2016 http://www.caissedesdepots.fr/sites/default/files/medias/barometre_de_la_confiance_des_francais_dans_le_numerique_0.pdf

comme l'absence de ce type de risque. De même, la prime de réputation correspond à la différence entre le prix offert par un vendeur qui honore l'ensemble de ses obligations envers un acheteur, et le prix moyen observé sur le marché pour un service équivalent. Cette réputation peut être attribuée par un expert qui évalue le risque, comme Moody's ou S&P pour le risque de non-remboursement d'un emprunt, ou par les consommateurs qui notent les vendeurs d'une place de marché, comme celle d'Amazon ou d'eBay.

La formalisation de la confiance au sein des sciences informatiques repose également sur des méthodes d'évaluation de risque et sur la fourniture de preuves qualifiées d'infalsifiables. La confiance est classiquement qualifiée de « dure » ou de « molle ». Cette qualification varie en fonction des éléments de preuve de confiance, qui peuvent reposer sur des éléments techniques forts cryptographiques ou sur la participation de plusieurs entités pour évaluer collectivement, grâce à des outils de surveillance automatisés, le comportement « normal » ou « déviant » d'une entité, à la manière des systèmes de réputation. Les preuves « dures », quant à elles, reposent toujours sur des éléments cryptographiques et s'appuient soit sur une autorité de confiance (ou une chaîne hiérarchique d'autorités), comme c'est le cas pour la certification électronique ou la certification anonyme, soit sur un ensemble d'entités collaboratives à l'instar de la technologie blockchain.

De son côté, le droit définit classiquement la confiance comme une croyance en la bonne foi d'autrui. L'appareil législatif sert alors d'abord à protéger la partie faible, lorsque les liens sociaux préalables à l'échange marchand ne sont pas assez anciens ou assez forts pour que la transaction soit menée à bien. Il semble qu'aujourd'hui le droit s'oriente dans une démarche réglementaire dont le but a changé : il s'agit désormais de bâtir un cadre réglementaire qui permet d'assurer le bon fonctionnement du marché, on protège moins la partie faible « *en sa qualité de personne* » et « *on protège davantage la fonction économique que [la partie] incarne* »[4]. Dès lors, la légifération sur la confiance serait-elle guidée par les processus de même nature – de formalisation et de calcul de risque – que l'on observe en économie et en informatique ?

Enfin, du point de vue socio-philosophique, on peut se demander si ce mouvement de formalisation de la confiance ne comporte pas des risques qui lui sont propres. En effet,

4 Rochfeld, Judith. (2009). *De la «confiance» du consommateur ou du basculement d'un droit de protection de la partie faible à un droit de régulation du marché.* Conférences du CEJEC, Approche critique du vocabulaire du droit européen : la confiance, Oct 2008, France. pp. 7-11. <hal-00424954>

l'exemple de la régulation des données personnelles ne confirme-t-il pas un mouvement d'atténuation du rôle de l'État, en ceci que l'instance de régulation passe de l'appareil législatif proprement dit à un modèle nouveau, associant dans des proportions variables, l'État, le marché et les consommateurs ? On interprétera ce mouvement soit comme une capitulation de l'État quant à la possibilité de réguler certains aspects relatifs aux technologies numériques, soit comme un dialogue constructif avec les instances non-étatiques, que ces dernières soient strictement privées ou impliquent le consommateur. Dans les deux cas, il nous semble que dans l'espace ainsi ouvert, les mécanismes de délibération et de correction éventuelle des dysfonctionnements ne sont plus réglés sur le modèle du débat politique mais sur celui du marché : le sujet « agissant » est-il toujours le citoyen ? A-t-il été remplacé par le consommateur qui « vote avec le dollar » ?

En termes d'usages quotidiens, ce mouvement n'est pas sans effet sur la constitution même de l'individu ou du citoyen, et de sa capacité d'agir. L'exemple des labels en matière de protection des données personnelles nous semble à cet égard emblématique, en démontrant les tensions exacerbées par la transformation numérique et la « *datafication* » qui l'accompagne. En effet, d'un côté la généralisation des labels peut être vue comme une démarche de protection et d'encapacitation, dans le sens où les consommateurs sont mieux informés, et leurs données personnelles moins exposées à des logiques de capture. Mais d'un autre côté, en formalisant ainsi la confiance, en la réduisant à des signes extérieurs et en suggérant des produits et services présélectionnés, et en passant sous silence les mécanismes de la construction de la confiance, ne risque-t-on pas de manquer l'objectif d'encapacitation que l'on se fixe ? Là encore, les formes émergentes de régulation ouvrent un champ de questionnement nouveau devant être examiné attentivement.

Cet ouvrage se propose dans un premier temps de démontrer les transformations actuelles de la confiance et de ses formes (chapitres 1 à 4). Il étudiera ensuite ces changements dans la mise en œuvre des signes extérieurs de la confiance que sont les labels (chapitres 5 à 8), en évoquant en particulier le rôle des autorités publiques en la matière. Il abordera ensuite les effets potentiels de la labellisation sur les acteurs économiques et les utilisateurs finaux (chapitres 9 à 10). Enfin, il prendra l'exemple des blockchains pour se demander dans quelle mesure les technologies émergentes contribuent à la confiance (chapitre 11). De manière plus générale, le fil conducteur de la réflexion consiste à se demander si la thématique de la confiance ne soulève pas des enjeux sociétaux qui vont au-delà de la gestion du risque, de la transparence absolue, de la crainte des sanctions ou de la recherche de bénéfices.

Chapitre 1. La confiance dans le numérique. Des signes extérieurs vers la régulation de soi.

Armen Khatchatourov

1

Nous vivons dans des sociétés de plus en plus complexes, dans lesquelles la multiplication des indicateurs et des facteurs à prendre en compte pour toute action publique ou privée rend de plus en plus difficile toute opération de choix. Dans ces conditions, des mécanismes qui réduisent cette complexité, qui aident à la prise de décision, sont amenés à prendre une place prépondérante. Niklas Luhmann, sociologue de la deuxième moitié du XX^{e} siècle et fondateur de la théorie des systèmes sociaux, désigne la « confiance » comme un des principaux mécanismes de réduction d'incertitude. En effet, lorsque j'ai confiance en tel ou tel acteur, produit ou service, je suis naturellement amené à interagir avec cette entité de manière plus fréquente, mon incertitude quant à l'issue de l'interaction étant moindre.

Il convient néanmoins d'être plus précis dans la description des différents aspects qui sont en jeu dans la confiance. De quelle manière la confiance intervient-elle dans telle ou telle décision ? S'agit-il toujours d'un calcul des conséquences de l'action, calcul dont le rôle est de diminuer le risque encouru ? Quelle est l'articulation entre la volonté individuelle d'un acteur et les facteurs institutionnels qui peuvent l'influencer ?

La confiance dans le numérique. Des signes extérieurs vers la régulation de soi.

1.1. « Confidence » ou « Trust » ? Confiance assurée ou confiance décidée ?

Une des manières d'aborder la confiance, que nous devons à Luhmann, consiste à opérer une distinction entre deux aspects à l'œuvre dans la réduction de l'incertitude : « *confidence* » (terme anglais que l'on traduit en français par « confiance assurée ») et « *trust* » (que l'on traduit en français par « *confiance décidée* »)[1]. Illustrons cette distinction par quelques exemples.

Lorsque je dois acheter une voiture d'occasion auprès d'un vendeur que je ne connais pas suffisamment bien, je me trouve dans une grande incertitude quant à la qualité du produit. Je dois alors peser le pour et le contre, et faire un choix rationnel sur la base d'une multitude de facteurs : le prix que je trouve plus ou moins intéressant, ma connaissance de la mécanique, les informations que j'ai sur le vendeur, etc. Je dois me décider sur la base d'informations incomplètes et faire un saut dans l'inconnu en prenant un risque mesuré. Je suis alors dans une situation de *trust* / « *confiance décidée* » : je ***décide*** finalement de faire confiance à ce vendeur. Dans cette situation, des informations supplémentaires sur le vendeur peuvent faciliter mon choix.

1 Luhmann, N. (2001). Confiance et familiarité: Problèmes et alternatives. Réseaux, no 108,(4), 15-35. doi:10.3917/res.108.0015. Traduction de Louis Quéré.

Lorsque chaque matin je vais démarrer cette même voiture pour aller au travail, lorsque je vais arriver à une intersection avec une circulation dense, je vais aussi avoir besoin de réduire l'incertitude quant au bon déroulement des choses. Cependant, je ne vais pas être dans une attitude de comparaison permanente d'une multitude de facteurs, je vais plutôt compter sur le fait qu'un bon déroulement des choses est ***assuré***: le monde suit son cours, les moteurs démarrent et les ponts ne s'écroulent pas. Il y a là un aspect « systémique » de la confiance: l'ensemble du système fonctionne[2], je ne suis pas obligé de repartir à zéro pour toute action que je dois entreprendre.

La même logique peut être reprise dans le cas des technologies numériques: je décide d'effectuer un achat sur eBay auprès d'un vendeur plus ou moins bien noté (confiance décidée) mais mon action repose aussi sur la confiance assurée quant au bon déroulement de l'ensemble, ensemble qui comprend le bon fonctionnement de eBay lui-même, de la banque, du transporteur et du facteur, etc.

Sur un plan différent, la distinction *trust*/*confidence* permet d'aborder des enjeux plus complexes – et peut-être plus importants – de la société contemporaine dans son ensemble, société qui subit selon certains une crise de confiance dans la politique, voire dans les interactions sociales dans leur ensemble. Je peux en effet avoir une confiance décidée dans tel ou tel acteur politique en effectuant un calcul rationnel de bénéfices que je peux obtenir à titre individuel. Mais ce type de confiance dans un acteur politique ne préjuge en rien de la confiance assurée que je peux avoir dans le système global dont il fait partie, dans le bon déroulement du « vivre-ensemble ».

On l'aura compris, les deux types de « confiance », décidée et assurée, en réduisant la complexité de la situation à laquelle un individu est confronté, ont pour effet de lui permettre d'effectuer une action dans une situation d'incertitude et de non-familiarité. Pour autant, la confiance assurée et la confiance décidée fonctionnent de manières fondamentalement différentes. Ce fonctionnement peut être précisé selon une double articulation, selon deux lignes de partage.

---

2 Il y a là selon nous une source de confusion chez certains auteurs qui limitent la confiance assurée à la confiance en les systèmes ou institutions, alors que chez Luhmann celle-ci correspond à une modalité d'attitude et non à son objet. Une autre confusion consiste à définir la confiance assurée comme une confiance aveugle (éventuellement en systèmes) alors qu'elle obéit à un autre type de rationalité et de temporalité qui n'est pas de l'ordre de calcul de risque.

- (a) La première ligne de partage concerne les mécanismes impliqués dans la confiance et le rôle attribué à l'attitude rationnelle des acteurs.
  - Du côté de la confiance décidée, c'est la décision par la personne elle-même « en connaissance de cause » – ou en tous cas selon une évaluation du risque qualifiée de rationnelle – qui prend le devant de la scène.
  - Du côté de la confiance assurée, il s'agit de mécanismes institutionnalisés, de l'interaction dans laquelle le choix rationnel est peut-être moins important qu'une habitude socialement acquise. C'est le tissu local des interactions que les sociologues anglophones qualifient de « *grassroots* » (de base, de proche en proche) qui contribuent à ce que les choses commencent à « aller de soi », et que la confiance assurée soit établie. En ce sens, la confiance assurée a trait à l'histoire longue des interactions sociales, elle ne peut pas être décidée d'en haut, elle ne s'impose pas, et les mécanismes de sa facilitation sont plus difficiles à formaliser.

- (b) La deuxième ligne de partage concerne la manière dont l'acteur individuel guide son comportement futur. On pourrait parler ici d'une boucle de rétroaction selon laquelle une action donnée informe l'action future.
  - Dans la confiance assurée, l'échec d'une action particulière est attribué aux facteurs extérieurs sur lesquels l'acteur n'a que peu de prise : c'est le système dans son ensemble qui y est en jeu. En reprenant l'exemple de la voiture d'occasion, on dirait alors : pour comprendre tel ou tel incident, il faut comprendre en quoi c'est l'ensemble du système, qui comprend les vendeurs, les constructeurs des routes et les régulateurs de la circulation, pris dans leur histoire, qui est en jeu.
  - Dans la confiance décidée, l'échec est attribué au comportement de la personne elle-même, à un « mauvais » calcul qu'elle aurait effectué. En reprenant l'exemple de la voiture d'occasion, on dirait alors : je n'aurais pas dû acheter cette voiture, c'est en fin de compte moi qui ai fait un mauvais calcul. En ce sens, il n'y a pas de confiance décidée sans que l'acteur accepte la possibilité d'une perte et une part de non-visibilité ; à supposer que la transparence absolue soit possible, des mécanismes autres que la confiance seraient alors à l'œuvre.

La raison de cette distinction peut paraître extrêmement simple : l'attribution de son propre échec est au fond le reflet du concept même du ***risque*** et du fait que le calcul du risque est une opération interne à la personne qui tente de prendre en compte les facteurs externes. Pour autant, sa portée ne doit pas être sous-évaluée. En effet, mettre l'accent sur la confiance décidée ne consiste pas simplement à mettre l'accent sur une attitude qui correspond à un choix rationnel de l'individu à un moment donné. Il en va ici de la manière dont le comportement individuel sera guidé dans l'avenir. En d'autres mots, c'est le mécanisme de gouvernance de soi, de ce qui fait que l'individu devient ce qu'il est, qui est ici en jeu. Comme on le verra plus loin, c'est ce mécanisme particulier, dans lequel l'individu est ***tenu pour responsable***, qui devient aujourd'hui prépondérant.

Avant d'étudier cette mutation plus en détail, formulons ici de manière concise la question qui guide désormais notre réflexion : si tant est que nous assistons à une crise de la confiance, notamment vis-à-vis des entreprises ou des États qui collectent et utilisent nos données personnelles, s'agit-il d'abord d'une crise de la confiance assurée ou de la confiance décidée ? Si des politiques publiques ou des initiatives privées ont pour objectif de renforcer « la confiance » dans le numérique, lequel de ces deux aspects doit-on prendre soin en priorité ?

1.2. Petite histoire de la « confiance »

Tout d'abord, il convient de souligner le fait que la distribution entre les différents aspects que peut revêtir la confiance a subi, dans l'histoire, des modifications en lien avec des changements technologiques majeurs.

Si l'on suit Luhmann, le passage à l'imprimerie a rendu les savoirs plus disponibles et a atténué la distinction entre le familier et le non-familier. Les mécanismes d'habitus religieux, qui guidaient jusqu'alors l'action quotidienne, s'en sont trouvés déstabilisés. Par conséquent, les enjeux d'évaluation des actions individuelles et de participation dans le tout social ont pris le devant de la scène. Ces enjeux se sont justement structurés historiquement comme l'articulation entre la confiance assurée et la confiance décidée. C'est à partir de cette rupture historique que Luhmann peut alors faire cette distinction schématique : dans un monde de plus en plus complexe où l'individu doit faire des choix, la confiance décidée interviendrait pour réduire la complexité et ainsi pouvoir prendre des décisions ponctuelles (relations interpersonnelles, prise de risque calculée), la confiance assurée interviendrait dans le cadre de la participation des individus dans le système économique et politique

dans son ensemble. Il convient ici d'ailleurs de préciser que les deux n'obéissent pas à la même temporalité, l'une relevant de l'événement et l'autre de la continuité[3]. Ce tableau schématique est donc en réalité lui-même le résultat d'un processus historique long. Il n'y a donc pas de réalité psychologique ou organisationnelle de la confiance en dehors de son inscription dans les mutations sociétales.

Plus près de nous, l'avènement du libéralisme et du néolibéralisme perpétue ce mouvement en mettant l'accent sur la confiance décidée. En effet, dans l'exacte mesure où la société est entendue comme un ensemble d'acteurs autonomes, libres et responsables de leurs choix et dont le comportement correspond à un calcul de risque et de bénéfice potentiel, on accentue l'importance accordée à la confiance décidée dans les mécanismes à l'œuvre dans la société, et ce au détriment peut-être de la confiance assurée et de sa compréhension. Pourtant, comme le note Luhmann, si la diminution de la confiance décidée conduit au blocage des actions et de prises de risques individuelles (mes investissements, mes achats, mon consentement à la collecte et à l'utilisation de mes données personnelles…), l'appauvrissement de la confiance assurée conduit peut-être au « *sentiment diffus de non-satisfaction, de désaffection[4] ou même d'anomie*[5] ».

> *« Le défaut de confiance assurée provoque un sentiment de désaffection ; il conduit éventuellement à se retirer dans un univers restreint, aux dimensions purement locales, ou encore à aspirer à une vie indépendante, fut-elle modeste ; il engendre aussi de nouvelles formes d'« autogenèse », des attitudes fondamentalistes ou d'autres formes de milieux et de « mondes vécus » retotalisants. »*[6]

Ce sentiment d'aliénation a donc pour effet non seulement une influence négative sur la confiance décidée que je peux avoir lors de mes actions ponctuelles mais aussi sur

---

3 Les deux types de confiance répondent ainsi à deux types d'incertitude, l'une à l'échelle de l'évènement, l'autre à l'échelle de la continuité (« *uncertainty within the event temporality and uncertainty […] within the continuity temporality* », cf. Morten, Frederiksen. (2016). Divided uncertainty: A phenomenology of trust, risk and confidence, *in Søren Jagd and Lars Fuglsang (ed.) Trust, Organizations and Social Interaction*. Elgar.)

4 L. Quéré traduit ainsi en français le terme « *alienation* » présent dans le texte original.

5 La sociologie entend classiquement par *anomie* une absence des normes et une certaine désintégration de l'ordre social.

6 Luhmann, N. (2001). Confiance et familiarité : Problèmes et alternatives. Réseaux, no 108,(4), 15-35. doi:10.3917/res.108.0015.

(le sentiment de) l'appartenance à la société[7]. En d'autres termes encore, mettre l'accent sur la confiance décidée, c'est passer sous silence le fait que cette dernière repose sur la confiance assurée et qu'il s'agit là d'une de ses conditions essentielles.

En effet, comme on peut le soutenir en allant plus loin à partir de Luhmann, le *trust* lui-même ne comporte pas en soi ces conditions de possibilité, et présuppose toujours une base qui s'enracine dans le social. La monnaie en est un exemple : je fais confiance (sur le mode aussi « décidée » que l'on voudra) dans la monnaie parce que d'autres font confiance, parce qu'une histoire institutionnelle longue des échanges est ici à l'œuvre. Pour reprendre l'interrogation qui fait le titre de l'article bien connu de Gambetta paru en 2000 (« *Can we trust trust ?* »), nous pouvons en effet faire confiance à la confiance, mais il faut alors compléter cette formule : nous le pouvons à condition que les processus de confiance assurée soient également en présence.

On le perçoit ici, la confiance est un problème à la fois économique, technologique, de régulation et fondamentalement social dans ses conséquences. On remarque aussi qu'il est inexact de parler de la « crise de confiance », comme s'il s'agissait d'un simple changement quantitatif (moins de confiance aujourd'hui qu'hier) et comme s'il suffisait de mettre en œuvre des mesures bien choisies pour retrouver un niveau perdu. Il s'agit plutôt, comme nous essayons de le montrer, d'un changement de mode de gouvernance des acteurs et de mode selon lequel l'individu se construit à travers ses choix[8].

1.3. Confiance dans le numérique ?

La transformation numérique apporte à son tour une couche de complexité. À la lumière de ce qui a été dit, on peut supposer que le problème ne se résume pas à la simple réduction de « confiance » dans la situation actuelle où les interactions numériques prennent de plus en plus le pas sur les modalités classiques d'interaction. On assiste plutôt à une nouvelle redistribution entre des mécanismes de confiance assurée et de confiance distribuée.

---

7 Ou, selon l'expression de L. Quéré, « *une attitude générale d'adhésion* ». Quéré, L. (2001). La structure cognitive et normative de la confiance, p. 141.

8 En cela, la problématique de la confiance est intimement liée à celle de l'identité, et des modalités selon lesquelles quelque chose comme une « autonomie » du sujet dans les choix qu'il opère se met en place. Cf. à ce sujet Khatchatourov A., et Chardel, P.-A. (2016). La construction de l'identité dans la société contemporaine : enjeux théoriques. *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Reprenons ici les deux lignes de partage que nous avons évoquées et que sont d'une part (a) le rôle des interactions locales, et d'autre part (b) les mécanismes d'attribution de l'échec.

Il nous semble alors que dans la situation actuelle, dans laquelle la prévalence des formes néolibérales de régulation des activités économiques et techniques se conjugue à l'essor du numérique, sans que l'on puisse départager clairement leurs effets respectifs, le mouvement décrit par Luhmann se trouve accentué.

- (a) Le calcul de risque prend le pas sur les interactions locales, et ce à double titre. D'abord, ce calcul, et la prise de décision qui s'en suit, est de plus en plus éloigné des interactions locales. Il est souvent guidé par les instances de régulation centralisées dont la préoccupation est de légitimer des acteurs économiques ou institutionnels et qui de ce fait assurent la promotion de certains acteurs au détriment des autres. Par exemple, en sciences informatiques, et pour autant que la confiance soit abordée uniquement sous l'angle de la sécurité, on met de fait l'accent sur des risques bien spécifiques comme l'usurpation de l'identité au détriment d'autres types de considérations sociétales, notamment les conséquences de la surveillance généralisée. Ce faisant, on met au devant de la scène tel ou tel type de risque et les acteurs économiques et institutionnels qui lui sont associés, comme en témoigne encore la prévalence de la sécurité sur le respect de la vie privée.
  Ensuite, le calcul de risque est de plus en plus formalisé car il fait désormais appel non pas au débat public ou à la délibération législative (fut-il sur le mode de *trust*) mais aux procédures algorithmiques formelles, dont un des effets potentiels est justement d'atténuer le consensus et la cohésion sociale[9].

- (b) On fait reposer de plus en plus les résultats des actions sur l'individu-utilisateur, la boucle de rétroaction devient pour ainsi de plus en plus serrée, y compris dans les actions quotidiennes. Par exemple, je dois aujourd'hui faire du jogging avec mon capteur *FitBit* et analyser, voire rendre publiques mes données, car mes primes d'assurance ou mes remboursements de sécurité sociale en dépendent, et dans le même temps je suis invité à participer ainsi à la réduction globale des dépenses de santé, ainsi qu'à la prospérité économique de la société. Ici, dans

9 Cf. Rouvroy, A. & Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation. Réseaux 31.

l'exacte mesure où l'action individuelle apparaît comme une recherche de bien-être dans une palette des options dans lesquelles l'individu est amené à faire confiance (sur le mode supposé « décidé »), les conséquences de ses actions lui sont donc imputables, et le conduisent à se conformer à la boucle de rétroaction « préétablie » pour lui. Mais dans la mesure où la palette elle-même est définie par les instances extérieures, l'individu est « éduqué » à assumer sa responsabilité sans s'interroger sur le fait que le répertoire même de ses actions ne lui est pas imputable à proprement parler. C'est ici ce que nous pouvons appeler, à partir des travaux de Michel Foucault, la « responsabilisation » des individus par les sanctions et les récompenses[10].

C'est peut-être là une des limites de l'approche dite d'auto-détermination informationnelle[11] dans les conditions contemporaines, où l'utilisateur est amené à faire confiance aux acteurs qui sont présélectionnés et légitimés selon les processus dont la nature lui échappe le plus souvent[12]. En considérant que l'individu est responsable de ses choix, on tend à la « *contractualisation de la vie commune* »[13] sans pour autant s'interroger sur les effets des choix ponctuels sur la constitution de la subjectivité. Car pour l'utilisateur, choisir un service parmi tant d'autres c'est en effet « s'autogérer » dans ses actions ponctuelles, tout en assumant dans les faits les coûts du choix et le « risque » associé.

Le paradoxe actuel est que ce mouvement de ***responsabilisation*** de l'individu s'accompagne aussi d'une certaine ***déresponsabilisation*** de ce dernier. Dans la mesure où il est appelé à se conformer sans réserve aux prescriptions et signes provenant des instances extérieures, l'individu risque de perdre la capacité critique nécessaire, en mettant ainsi à mal le projet initial des Lumières et de l'individu autonome. Par exemple, la généralisation de la labellisation des services numériques ne risque-t-elle pas de conduire à

10 Comme le note Philippe Fournier en prenant l'exemple des politiques sociales, « *La gestion du risque, l'éducation des enfants, le fait d'habiter un certain quartier, etc. sont autant de facteurs liés à la responsabilité individuelle. Au bout du compte, les individus qui paraissent refuser d'assumer leurs responsabilités, en d'autres termes qui ne participent pas à l'optimisation du bien-être de la population […], se voient punis, disciplinés ou simplement laissés à eux-même*s ». (Fournier, P. (2015). La responsabilité comme mode de gouvernement néolibéral : l'exemple des programmes d'aide aux familles aux États-Unis de 1980 à nos jours. *in Les ateliers de l'éthique*, Volume 10, Numéro 1, Hiver 2015, p. 129–154)

11 On pourrait s'intéresser ici à l'histoire de cette approche, née en Allemagne dans les années 80, et désormais traduite dans le Règlement général sur la protection des données.

12 Ce point sera développé, sur l'exemple concret de la labellisation des acteurs du numérique, dans les chapitres qui vont suivre.

13 Foucault, M. (2004). Naissance de la biopolitique, Paris, Gallimard/Le Seuil, coll. « Hautes Études », p. 251.

terme à la généralisation des conduites qui ne font que suivre ce qui est prescrit, tout en se donnant bonne conscience de soutenir les acteurs qui se conforment eux-mêmes aux prescriptions légales en matière de données personnelles ?

Pour résumer cette situation relativement nouvelle, on pourrait alors tenter cette formule : là où « l'extérieur » dans la confiance assurée était imputable à l'habitus fondé dans le tissu des interactions sociales, « l'extérieur » devient une instance de prescription de comportements « rationnels » et en même temps « confiants », en basculant sur le territoire de la confiance décidée. Cependant, pour « rationnelle » qu'elle soit, la constitution et les mécanismes de légitimation de cette instance sont souvent passés sous silence.

La sociologie, au moins depuis Max Weber, se confronte à ce problème : comment rendre compte des processus de légitimation, des mécanismes qui instituent tel ou tel acteur comme digne de confiance ? Comment les comportements (de confiance, de choix économiques, de politiques publiques, de société…) sont à leur tour prescrits ? À quoi nous ajoutons : comment la confiance devient ainsi un mode de régulation particulier ? Et plus précisément encore : comment la confiance décidée – ou même « *suggérée* » – remplace les mécanismes de confiance assurée ?

Notons simplement que, à cet égard, Luhmann introduit la notion de légitimation par la procédure[14]. La nouveauté à laquelle nous sommes aujourd'hui confrontés est que les procédures reposent de plus en plus sur les technologies numériques, et que les rouages de cette légitimation, en raison même de la généralisation de la circulation des données, sont de plus en obscurs[15]. Dans la suite, nous distinguerons deux figures possibles – et problématiques – pour cette nouvelle confiance : la confiance *by design* et la confiance distribuée.

---

14 Le concept de la *légitimation par la procédure* correspond, pour le résumer de manière excessivement rapide, à l'idée qu'à partir du moment où le droit n'a pas de fondement autre que lui-même (pas de fondement divin ou souverain), il tire sa légitimité de la procédure de sa propre effectuation. La procédure n'est donc pas à prendre dans le sens négatif, mais comme le mécanisme même par lequel le droit s'auto-légitime et acquiert sa validité. Luhmann concentre son ouvrage éponyme sur trois procédures (électorale, législative / parlementaire et judiciaire). Il paraît évident que ces procédures mêmes sont aujourd'hui substantiellement affectées par les technologies numériques, et que la confiance en elles-mêmes ou dans les acteurs qui y sont impliqués subit des changements majeurs.

15 Pour une approche plus philosophique de certains enjeux qu'une telle circulation pose aujourd'hui, cf. Khatchatourov A., (2016) Big Data entre archive et diagramme. Études Digitales n°2, Classiques Garnier, Paris.

1.4. **Le mirage du *Trust by design***

Ce double mouvement de fond selon lequel l'accent est mis sur la confiance décidée, que nous avons explicité dans les points (a) et (b) ci-dessus, s'accompagne aujourd'hui d'une idéologie particulière. Cette idéologie de « tout technologique » suppose que la solution technique ou au mieux technico-managériale soit en capacité de supplanter la construction sociale. Par exemple, on prône la transparence des algorithmes en la présentant comme une solution suffisante pour la reprise économique, voire pour l'équilibre social, en laissant dans l'ombre les processus plus larges dans lesquels leur conception et leur utilisation effective s'inscrivent[16]. On laisse aussi dans l'ombre le fait que l'examen d'un algorithme est hors de portée d'un utilisateur lambda, et il devrait faire confiance à d'autres instances – tels les « tiers de confiance » – qui en auront la charge, et ceci dans une spirale infinie de légitimation des acteurs, légitimation dont les rouages restent eux-mêmes à examiner. De même, on est tenté de croire que la mise en place d'une approche de type blockchain conduit à l'établissement de la confiance entre les acteurs grâce à la transparence absolue des échanges, sans analyser les rapports de conflit, de prise de position oligopolistique, les enjeux politiques sous-jacents, etc.[17]

Appelons cette idéologie le « *trust by design* ».

La transparence, l'ouverture du code et/ou des données, leur décentralisation sont-elles pour autant une garantie de regain de confiance ? Dois-je faire plus « confiance » à un acteur qui m'est bien connu, dont je peux raisonnablement supposer qu'il respecte ma vie privée sans que j'aie à consacrer des efforts croissants à la protection de mes données, ou bien à celui dont la solution technique semble se conformer à un moment donné à l'exigence désormais formelle de *trust by design* ?

Notre intuition ici est que ce mouvement de *trust by design* comporte en lui une ambiguïté fondamentale, et qu'il place l'accent encore plus sur la confiance décidée. Il cantonne ainsi l'individu-utilisateur dans toujours plus de choix présélectionnés par les instances extérieures, toujours plus de circulation et peut-être même de protection des données,

16 Cf. Khatchatourov A. (2016). Peut-on mettre la main sur les algorithmes ? Note sur la « culture algorithmique » de Dourish. Études Digitales, n°2, Classiques Garnier, Paris

17 Ce point sera développé dans le chapitre 11, consacré à la question de confiance dans les blockchains.

mais toujours moins de sentiment ou d'assurance de participer à quelque chose comme une société.

En effet, et pour ne prendre que les deux exemples ci-dessus, si tant est que le risque de divulgation des données que comporte l'action individuelle de souscription à un service soit diminué, et si tant est que la confiance décidée soit « rétablie », cela ne nous dit rien encore de la confiance assurée et de sa construction sociale.

Mais il y a plus. Cette tendance au *trust by design* pose fondamentalement la question de l'automatisation de la confiance, et de la production automatisée de ses signes extérieurs auxquels le comportement des individus est censé se conformer. Or, comme les ingénieurs concepteurs des systèmes informatiques le savent très bien[18], comme la philosophie ne cesse de le répéter à sa manière[19], la question cruciale est celle de la désautomatisation, du débrayage, de la suspension du sens commun et de ce qui va de soi, bref d'attitude critique face aux signes. C'est là la condition essentielle de la démocratie, du moins si l'on entend par là le projet des Lumières. En ce sens, et comme Luhmann aussi n'a cessé de le répéter[20], une certaine dose de défiance est essentielle au fonctionnement de la société pour que la confiance ne tourne à une confiance aveugle, pour que l'habitus ne tourne pas en simple automatisme.

1.5. De la confiance « distribuée »

Si l'on souhaite mettre en place des politiques publiques ou industrielles qui atténuent ce que Luhmann appelle « l'aliénation » il faut bien préserver – ou repenser à nouveaux frais – cet équilibre fragile entre les deux types de confiance, faute de quoi l'action individuelle guidée par la confiance décidée peut à son tour être bloquée. Car si la prise de risque est structurellement nécessaire (pour l'économie ou l'action politique), elle doit néanmoins s'articuler avec la confiance assurée dont les rouages ne relèvent pas de calcul ou de prescription. Or, en confondant les deux, en déplaçant le centre de gravité

18 Par exemple, dans le domaine de l'automatisation de la conduite des systèmes critiques (avion, centrale nucléaire, etc.), la question centrale est de ne pas « trop » automatiser, et d'élaborer un jeu dynamique de va-et-vient entre l'automatisation et le contrôle par l'humain. Parasuraman, R., Mouloua, M., & Molloy, R. (1996). Effects of adaptive task allocation on monitoring of automated systems. *in Human Factors: The Journal of the Human Factors and Ergonomics Society*, 38(4), 665-679.

19 Le geste même de la fondation de la philosophie occidentale chez Platon est celui de la suspension du jugement.

20 Luhmann, N. (2010). Le Pouvoir [« Macht »], Presses de l'Université Laval, 1975 / 2010.

vers la confiance décidée, le tournant actuel de *trust by design* peut très bien conduire à une dislocation encore plus grande de la confiance assurée.

Dès lors, la question semble être la suivante : comment imaginer des politiques (de confiance, de sa construction, de son « affichage » par les labels) qui *a minima* ne détériorent pas cet équilibre, ne rabattent pas la construction de la confiance assurée sur les mécanismes de calcul de risque et qui se contentent de « fonctionner » localement par exemple pour relancer la concurrence ? À ce titre, le chapitre qui suit évoquera le double rôle fonctionnel du droit, pour lequel il s'agit désormais non seulement d'assurer la protection de la partie faible (fonction qui historiquement ne se résume pas au champ des mécanismes économiques) mais aussi d'être partie intégrante du marché, en encadrant et en relançant la concurrence. Un des exemples parlants est ici la législation récente sur la portabilité des données, dont l'aspiration est de satisfaire la double injonction de protéger (ou « encapaciter ») le consommateur en lui donnant une certaine maîtrise sur ses données et dans le même temps relancer la concurrence entre fournisseurs, en facilitant le passage de l'une à l'autre, et la circulation des données. La question qui se pose ici est de savoir quelles sont les conditions sous lesquelles les processus institutionnels de légitimation des acteurs ne décrochent pas des processus sociaux à l'œuvre dans la confiance assurée.

Remarquons ici que même les sciences économiques, dont les postulats épistémologiques de base sont bien plus compatibles avec *trust* qu'avec *confidence* (i.e. bien plus avec la figure de l'acteur individuel qu'avec les processus sociaux), pointent comme malgré elles vers cette couche sociale qu'elles ne thématisent pas encore suffisamment. Ainsi, on évoquera dans les chapitres qui suivent l'intérêt relativement récent de l'économie pour des notions comme celles d'«équité» et de « réciprocité », ou encore celle des interactions répétées.

Il faut dès lors réfléchir aux conditions d'implication des citoyens dans ces processus. Mais l'enseignement que nous pouvons tirer de ce qui précède est que cette implication ne doit pas revêtir n'importe quelle forme. Certes, l'essor des systèmes participatifs, collaboratifs, distribués, mobilisant les multitudes, etc., nous indique quelque chose de cet ordre. On pourrait évoquer ici tout un éventail de mécanismes dont les individus-utilisateurs sont à l'initiative : les démarches « approvisionnées par la foule » ou *crowd-sourced*[21] ou l'utilisa-

21 cf. par exemple TOSDR : « *Terms of Service; Didn't Read* » https://tosdr.org/

tion par le grand public de bloqueurs de publicité (*adblocker*) qui opère de fait une forme de régulation technique via les sanctions qu'elle impose éventuellement aux acteurs du Web.

Cependant, la confusion terminologique dans laquelle baignent ces initiatives nous indique aussi que le spectre couvert est bien trop large pour que toutes les formes puissent répondre à l'exigence que nous évoquons. Car en effet, qu'y a-t-il de commun entre la notation de vendeurs sur *eBay* par un sous-ensemble d'acheteurs et les processus selon lesquels les participants à la communauté du logiciel libre acquièrent de la légitimité auprès de leurs pairs ? Certes, les deux procédures de légitimation peuvent être décrites comme contribuant à une réduction de l'incertitude à l'égard d'un acteur donné. Mais si les procédures à l'œuvre au sein du logiciel libre semblent faire place aux processus qui s'apparentent, au moins en partie, à la confiance assurée[22], la procédure de *eBay* nous semble reposer majoritairement sur la confiance décidée.

La tâche est donc désormais d'imaginer les voies non seulement pour donner la parole aux ***consommateurs*** dont le rôle fonctionnel dans le système social reste limité au champ de la confiance décidée mais également d'organiser les processus permettant aux ***citoyens*** d'être impliqués dans la confiance assurée.

Tels nous semblent être les enjeux soulevés aujourd'hui par la thématique de la confiance dans le numérique : une nouvelle articulation entre confiance décidée et assurée, entre responsabilisation et déresponsabilisation, entre confiance et défiance raisonnées. La difficulté de cette tâche ne saurait être surestimée. Il ne s'agit évidemment pas d'abandonner toute démarche de régulation, de laisser les individus-utilisateurs seuls face à la multitude des aspirateurs de données personnelles. Mais il s'agit bien d'essayer de parvenir à une approche critique de la régulation elle-même, l'objectif étant que cette dernière ne serve ni à réguler outre mesure les comportements des citoyens, ni à devenir une composante de « *privacywashing* ».

---

22 Comme le montre O'Neil (2014) dans Hacking Weber: Legitimacy, critique, and trust in peer production « *Legitimate domination in collaborative online projects was defined as overlapping regimes of hacker-charismatic, index-charismatic and procedural authority which coexist in hybrid formations* ». Ici, nous assistons à une forme qui joue sans doute sur le *trust* (le choix de l'*open source* peut se justifier rationnellement par la « confiance » dans la qualité du produit, par des aspirations personnelles de réputation, etc.) mais aussi sur *confidence* (du moins pour les membres participant de la communauté). Notons que dans cette citation l'expression « *index-charismatic authority* » correspond à une composante algorithmique, à un calcul automatisé d'« autorité » dans un réseau dont Barabàsi fût un des pionniers (cf. Barabàsi, AL. (2002). Linked: The New Science of Networks, Perseus, Cambridge, MA), alors que « *procedural authority* » se rapproche, sans que Luhmann soit cité, de la légitimation par la procédure. On voit donc bien que les deux peuvent coexister et être distribuées dans des proportions variables.

Illustration de couverture : « La Confiance », pastel de Thierry Citron (www.thierrycitron.fr)

Chapitre 2. La confiance saisie par le droit

Claire Levallois-Barth

2

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.

La confiance saisie par le droit

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.

Chapitre 3. La notion de confiance en économie

Patrick Waelbroeck
Antoine Dubus

3

La notion de confiance en économie peut s'aborder dans un premier temps comme une réduction du risque lié à une transaction. Ainsi le baromètre de la confiance de l'ACSEL-CDC n'utilise jamais le mot confiance directement, mais pose des questions sur les risques liés au partage d'information en ligne et de sécurité des transactions. Une manière d'appréhender la notion de risque est d'analyser les facteurs qui le réduisent. La connaissance permettant de mieux distinguer les états de la nature[1] et de construire de meilleurs modèles économiques agit comme un réducteur d'incertitudes et de risque.

Deux mécanismes économiques fondamentaux apportent de la confiance. Le premier est la connaissance ; le second porte sur les notions d'équité et de réciprocité. Nous examinons tout d'abord les différentes notions de risques associées à une transaction (3.1). Nous montrons ensuite comment les stratégies de court terme peuvent devenir contre-productives lorsque l'on essaie de construire des équilibres de coopération sur le long terme où les interactions sont répétées (3.2). C'est l'occasion de mettre également en avant le rôle de mécanismes punitifs dans la construction de la confiance. Cet argument se retrouve dans le cas où ce sont les consommateurs qui réduisent les incertitudes et punissent les mauvaises entreprises en participant à un système de réputation collaboratif (3.3).

1 Les états de la nature sont définis en économie comme la situation dans laquelle se trouvent un ensemble de facteurs économiques, par exemple le coût de production d'un bien, ou encore le niveau de sécurité informatique d'un fournisseur de services en ligne. Les agents économiques ne connaissent pas nécessairement ces états.

La notion de confiance en économie

Nous présentons par la suite le deuxième pilier de la confiance en économie à travers les nombreuses études expérimentales autour de la notion d'équité (3.4). Nous développons l'argument que l'économie numérique est en train d'affaiblir les deux piliers de la confiance à travers la baisse de la connaissance et le sentiment d'impuissance face aux asymétries de pouvoir et d'informations dans l'économie numérique (3.5). Une présentation du rôle économique du label comme signe de confiance termine ce chapitre (3.6).

3.1. La confiance comme une notion subjective de réduction du risque

Les incertitudes impliquent des risques largement étudiés en économie, associés à et précisés par des notions telles que : le risque systémique, le risque idiosyncratique (propre à une situation particulière), le risque stratégique… On peut regrouper les risques en trois grandes catégories. La première catégorie correspond au ***risque probabiliste***, qui permet de faire des calculs d'utilité espérée, selon les différentes probabilités que l'on accorde aux états de la nature. La deuxième catégorie de risque est *non probabiliste*. Ce type de risques est lié à la notion d'***incertitude*** (correspondant à des situations où l'on ne peut formuler de probabilités que lorsque certains événements se produisent, ou lorsque ces probabilités sont subjectives). La troisième catégorie, elle, porte sur la notion d'***incomplétude***, qui correspond à une situation où un agent économique ne connaît pas ou ne parvient pas à distinguer tous les états de la nature.

Le risque probabiliste permet de comprendre la notion de confiance à travers l'apprentissage lié à des signaux ou à des interactions répétées. L'apprentissage bayésien[2], par exemple, combine une distribution a priori et une fonction de vraisemblance, pour former une distribution a posteriori. Cet apprentissage à travers l'observation de signaux permet de réduire les risques et d'augmenter la confiance dans la transaction. Cette approche est nécessairement subjective puisque les distributions a priori peuvent dépendre de facteurs variant fortement d'une personne à l'autre. Par ailleurs, la manière dont le risque est pris en compte varie également parmi les agents économiques. On parle alors de différentes formes d'aversion au risque, ou d'aversion à la perte, car les individus ne réagissent pas de manière symétrique aux risques liés à des gains et à ceux liés à des pertes.

La deuxième catégorie permet d'affiner ces comportements asymétriques dans la perception du risque à travers la théorie d'utilité non-espérée, qui prend en compte des raisonnements qui vont au-delà de la moyenne (la moyenne ne suffit pas en tant que critère d'appréciation du risque) tout en acceptant l'idée que certains risques sont subjectifs[3].

La troisième forme de risque, celle liée à l'incomplétude sur les états de la nature, est étroitement liée à la notion de connaissance, car ce type de risque dépend de ce qu'un agent sait sur l'ensemble des événements possibles. Prenons un exemple : un patient va voir son médecin. Il décrit des symptômes qui lui font penser qu'il est malade, mais ne connaît pas cette maladie. Il connaît donc à cet instant deux états de la nature : *être en bonne santé* ou *être malade*. Le médecin l'examine et l'informe que ses symptômes peuvent correspondre à deux maladies. Après avoir consulté le médecin, le patient connaît maintenant trois états de la nature : *être en bonne santé*, *souffrir de la maladie_1*, *souffrir de la maladie_2*.

2 Il s'agit d'apprentissage sur les paramètre d'un réseau bayésien, réseau dans lequel les probabilités modélisent des degrés de croyance subjectifs des agents étudiés.

3 Voir Machina, M., (2007). Non-expected Utility, *in Darity (Ed), International Encyclopedia of the Social Sciences*, Macmilan Reference USA, 2nd Edition.

3.2. Interactions répétées et mécanismes punitifs

La réduction du risque peut provenir d'un mécanisme punitif comme dans le cas des ententes tacites. On a aussi confiance car on sait que le système permet de corriger ou de punir des agents qui se comporteraient mal. Si l'on connaît mieux les termes de la transaction, on peut créer de la confiance entre les parties impliquées dans la transaction. La meilleure manière d'illustrer ce propos est de considérer la transformation des équilibres économiques à travers les interactions répétées. Le ***dilemme du prisonnier*** considère une situation où deux complices d'un méfait sont interrogés séparément par la police. Si les deux complices ne se dénoncent pas, ils sont condamnés à une peine minime. Si les deux coopèrent avec la police, ils purgent tous les deux une peine maximale. Si l'un coopère et l'autre ne coopère pas, le premier bénéficie d'un traitement favorable et le second purge une peine lourde. La meilleure situation pour les deux complices consiste à ne pas coopérer avec la police et à se faire mutuellement confiance. Cependant, l'un des deux complices a toujours intérêt à dévier de cette situation pour dénoncer son complice pour alléger sa peine, si bien que le seul équilibre qui tienne est celui où les deux complices se dénoncent mutuellement.

Le fait que cette situation ne se produit qu'une seule fois est crucial pour comprendre cet équilibre de défiance. Car si l'on répète cette situation un nombre infini de fois, il s'avère que des équilibres coopératifs émergent, où les agents économiques se font confiance.

Dans les modèles de ***collusion tacite***, plusieurs entreprises se rencontrent sur plusieurs périodes. Contrairement au dilemme du prisonnier, tant que le facteur d'escompte du temps (qui permet de convertir les euros de demain en euros d'aujourd'hui) est relativement faible, un équilibre d'entente tacite, où les entreprises ne communiquent pas directement entre elles et néanmoins coopèrent, émerge. La raison en est que lorsqu'un agent décide de dévier unilatéralement, les autres agents peuvent le punir de telle sorte que le gain de la déviation unilatérale de court terme ne soit pas profitable par rapport aux gains d'une collaboration durable. La compréhension du mécanisme de ***punition*** est cruciale pour appréhender l'émergence de cet équilibre de confiance.

3.3. Systèmes de réputation pour créer de la confiance

Une autre manière de créer la confiance dans la transaction passe par des systèmes de réputation. La réputation est définie comme un « *goodwill* »[4], c'est-à-dire un stock qui augmente avec les expériences positives. Ainsi, de nombreux articles de la littérature économique étudient spécifiquement la plateforme *eBay* compte tenu de son système de notation. Ces études établissent clairement l'existence d'une prime à la réputation : un vendeur ayant une bonne réputation peut fixer un prix au-dessus de la moyenne. De manière similaire, Bounie et al. (2012) calculent que la prime à la réputation sur Amazon Marketplace peut atteindre 10%. La réputation a également un effet sur la probabilité d'effectuer une transaction (pour un vendeur). Par exemple, Cabral et Hortacsu (2010)[5] expliquent qu'une augmentation d'un pourcent du nombre d'évaluations négatives conduit à une baisse de 7,5% du prix de vente. Ils montrent également que lorsqu'un vendeur reçoit sa première évaluation négative, son volume de vente baisse de 13%. Un vendeur qui reçoit plusieurs évaluations négatives a plus de chance de quitter la plateforme de vente. Ainsi, la gestion active de son profil de vendeur a une valeur économique et explique pourquoi les gens cherchent à se présenter sous leur meilleur jour.

3.4. Confiance par l'équité et la réciprocité

Les interactions répétées permettent également de créer des équilibres fondés sur la réciprocité et l'équité. Ces concepts sont illustrés par la littérature en économie expérimentale portant sur des variantes du jeu du dictateur. Dans le jeu du dictateur (qui n'est en fait pas un jeu car il n'y a qu'une seule personne qui choisit sa stratégie), le dictateur est un personnage qui choisit comment diviser un montant, disons 10€, entre lui et un bénéficiaire anonyme. Les résultats des études expérimentales montrent qu'un grand nombre de dictateurs choisissent une répartition équitable, où chaque participant reçoit une somme comparable, là où la rationalité individuelle sans préoccupation pro-sociale aurait dû conduire le dictateur à tout garder pour lui. La connaissance de l'identité et du

4 Le *goodwill* (survaleur, ou écart d'acqusition) figure à l'actif des bilans et chiffre la différence entre le prix d'une acquisition et la valeur des actifs réels. Le savoir-faire, les projets de R&D, le climat social, la valeur d'une marque et sa réputation sont parmi les éléments pris en compte pour l'établir.

5 Cabral, L, Hortascu, A. (2010). Dynamics of Seller Reputation : Theory and Evidence from eBay, Journal of Industrial Economics, v. 58, no.1, March 2010, pp. 54-78.

profil socio-économique des joueurs est importante : plus la proximité sociale est proche, plus le montant donné est équitable.

Le jeu de la confiance est une variante du jeu du dictateur où le montant donné par le dictateur au bénéficiaire est multiplié par un montant arbitraire, par exemple doublé, et où le bénéficiaire peut redonner tout ou partie du montant reçu. De nouveau, les expériences montrent que le bénéficiaire retourne un montant non nul correspondant à un comportement de réciprocité. On comprend qu'il faut à la fois faire confiance (au sens de *trust*) et être digne de confiance (*trustworthiness*).

3.5. L'impact du numérique : réduction des externalités de connaissances, de la cohésion sociale et augmentation des asymétries d'informations

En plus de créer de la confiance, l'échange de connaissances permet le développement économique et l'innovation. Les modèles de croissance (endogène) montrent comment la croissance économique de long terme dépend de la manière dont les connaissances s'accumulent dans l'économie. Ces modèles supposent que les entrepreneurs et innovateurs contribuent au stock de connaissance de l'économie dans lequel d'autres innovateurs présents et à venir pourront trouver les techniques nécessaires à la conception de nouveaux produits et services. Cette externalité de connaissance intertemporelle est le moteur de la croissance de long terme, car les entrepreneurs futurs puisent leurs inspirations dans les connaissances d'aujourd'hui. Il est intéressant de noter qu'un brevet est accordé à un inventeur en contrepartie de la divulgation du procédé technique sous-jacent à l'invention, la propriété intellectuelle n'étant alors plus protégée par le secret mais le brevet d'invention. De manière générale, les échanges humains de connaissances engendrent des externalités à travers les échanges sociaux (par exemple le « bouche à oreille » ou le système de réputation).

Paradoxalement, alors que nous vivons précisément dans une société de la connaissance, ces échanges de connaissances sont menacés par l'automatisation, le secret de fabrication des algorithmes et les algorithmes prédictifs. Premièrement, l'automatisation liée à l'utilisation des robots et des algorithmes réduit l'intervention humaine dans les processus productifs et diminue les connaissances des travailleurs et des artisans (voir les

travaux de Bernard Stiegler[6] par exemple). Par ailleurs, certaines compétences acquises ne sont pas en l'état facilement encodables, c'est-à-dire qu'elles sont difficiles à décrire par une séquence de procédures où par un algorithme (par exemple, les gestes sophistiqués d'un artisan tel qu'un ébéniste ou un luthier). On parle de connaissances tacites qui sont également perdues par l'automatisation. Deuxièmement, beaucoup d'innovations liées au *Big Data* et aux algorithmes sont pour l'instant gardées secrètes par les entreprises, si bien que le mécanisme décrit dans le paragraphe précédent n'est ni opérationnel ni vérifiable. Troisièmement, les algorithmes prédictifs peuvent conduire, à travers leur ciblage encodé et déterministe, à enfermer les internautes dans des bulles informationnelles. Indépendamment de savoir si c'est l'algorithme qui enferme ou si c'est l'individu qui s'enferme par ses comportements ou choix, le résultat est identique : l'individu risque d'être privé de la richesse des échanges d'information qui engendrent la confiance. Ainsi dans le secteur des médias, on risque une polarisation des opinions par le biais algorithmique qui peut manifestement ébranler les fondements de la société démocratique telle que nous la connaissons.

3.6. Le rôle des labels en économie

Le numérique bouleverse les conditions de l'échange à travers l'asymétrie d'informations qu'il engendre, ce que F. Pasquale appelle la *black box society*[7] : les utilisateurs d'outils numériques ne connaissent pas l'utilisation qui est faite de leurs données personnelles, ni le volume des données échangées par les entreprises qui les collectent. Pire encore, ces entreprises peuvent manipuler le contexte informationnel de la transaction pour mettre les individus dans un environnement qu'ils pensent être de confiance (voir les travaux de Acquisti[8]) afin de les inciter à divulguer plus d'informations personnelles.

Ces asymétries d'informations affaiblissent l'équité et la réciprocité dans la transaction, et créent un sentiment d'impuissance des internautes isolés face aux grands groupes du numérique (ce que les sociologues appellent le capitalisme informationnel).

---

6 Stiegler, B. (2015). La Société automatique. L'avenir du travail, Fayard

7 Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press

8 Acquisti, A. (2012). Nudging Privacy: The Behavioral Economics of Personal Information. *in Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides (eds), Digital Enlightenment Yearbook 2012*, IOS Press

Pour résoudre les problèmes informationnels, les labels et marques de confiance sont des signaux qui permettent aux internautes de mieux appréhender les risques de la transaction.

Ces labels et autres signes de confiance sont appréhendés en économie par la théorie du signal. Celle-ci cherche à résoudre des problèmes d'asymétries d'informations en émettant un signal coûteux que les consommateurs pourront interpréter comme un gage de bonne pratique. Ainsi, plus le signal est coûteux plus son impact sera important, à condition que les consommateurs soient évidemment au courant de son coût. Si le label est essentiel dans un environnement incertain dans une relation de court terme, la marque au contraire s'inscrit dans la durée. La marque opère plutôt comme un effet de réputation résultant d'interactions répétées donnant lieu à un *goodwill* de la part des consommateurs. Ainsi, labels et marques apparaissent, en économie du moins, comme substituables ou du moins émergents dans des durées temporelles différentes.

« Le Conciliabule » –Thierry Citron

Chapitre 4. La confiance en informatique par la gestion du risque

Maryline Laurent
Armen Khatchatourov

4

La confiance en informatique repose sur l'évaluation des risques engendrés par l'usage d'un outil (logiciel ou matériel) ou, plus largement, toute forme de prestation informatique (service, site web). Cette évaluation et le niveau de fiabilité associé sont d'autant plus critiques que les enjeux sont élevés. Elle prend tout son sens quand la sécurité du système d'information (SSI) d'une organisation est en jeu.

Pour l'essentiel, on distingue deux manières d'appréhender la qualification du risque.

L'approche la plus ancienne concerne les produits de SSI (logiciels, matériels) mettant en œuvre des fonctions de sécurité, et les prestataires de services de confiance (services d'horodatage, de signature, de certification électronique…). Souvent, elle implique l'intervention des autorités publiques dans le processus d'émission d'une qualification du niveau de risque. On suppose alors que la confiance est transitive : si l'utilisateur accorde sa confiance à l'acteur qui émet la qualification ou à un certificat électronique, il fera également confiance à l'objet qualifié. La qualification des produits ou des prestataires n'est pas toujours obligatoire. Mais elle est néanmoins incontournable lorsqu'il s'agit notamment de concevoir des solutions SSI critiques ou de remporter un marché public. Elle se présente donc, avec le niveau qui lui est associé, comme un signe extérieur volontaire visant à renforcer la confiance décidée des individus et des entreprises (4.1.).

La seconde approche, plus récente, s'appuie sur le nombre massif et toujours croissant d'informations disponibles dans les systèmes d'information : elle consiste à attribuer un

La confiance en informatique par la gestion du risque

score à des individus ou à des services numériques. Ce score, qui joue le rôle d'un indicateur de risque, est calculé sur la base d'une analyse comportementale qui mesure l'écart entre deux comportements, le comportement évalué et un comportement référence. La note obtenue est susceptible d'influencer directement la confiance décidée (4.2.).

Notons que les deux approches – qualification d'un produit ou d'un prestataire / analyse comportementale – peuvent être employées conjointement, par exemple pour authentifier un utilisateur à la fois sur la base d'un certificat électronique et de son comportement.

4.1. L'évaluation du risque associé à l'utilisation des produits et services SSI

La sécurité, un enjeu fondamental pour les États et les entreprises

La nécessité d'évaluer le risque associé à l'utilisation des produits et services SSI répond historiquement aux besoins forts des entreprises et des États d'assurer la fiabilité et la disponibilité de leurs infrastructures et services et de lutter contre des menaces de cybersécurité. Clairement de type *top-down*, elle prend place dans un cadre strict édicté par les instances nationales et/ou européennes. Ce cadre réglemente le niveau de fiabilité attendu des services, matériels, et logiciels participant à la mise en œuvre de la sécurité des systèmes d'information, chaque niveau de fiabilité étant reflété par un niveau de qualification. L'objectif consiste ici à maintenir un haut niveau de vigilance, les enjeux étant à la fois économiques, politiques et stratégiques. Ainsi, afin d'assurer notamment leur sou-

veraineté nationale, les États procèdent à la qualification des produits SSI et services de confiance qui sont susceptibles d'être intégrés par leurs administrations, des opérateurs d'importance vitale et des entreprises dites sensibles. La qualification la plus élevée correspond à une prise de risque faible ; elle est donc adaptée aux infrastructures critiques.

Notons toutefois qu'aucune qualification n'est obligatoire. En pratique cependant, elle est difficilement contournable. En particulier, elle facilite, à la manière des poupées russes, l'obtention de labels relatifs à la protection des données personnelles, car elle garantit la bonne prise en compte des obligations de confidentialité et de sécurité. Par ailleurs, il ne faut pas perdre de vue que certaines réglementations sont obligatoires, en particulier en ce qui concerne la fourniture, l'importation, l'exportation et le transfert intracommunautaire d'un moyen de cryptologie associé à un produit ou une prestation de services.

Dans ce contexte, les autorités publiques – en France, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) – publient un catalogue des produits qualifiés, le niveau de qualification qui leur est attribué ainsi que la liste des prestataires de services de confiance qualifiés. La garantie ainsi obtenue n'est cependant pas absolue. En effet, l'histoire récente a montré que certains produits SSI pouvaient comporter une porte dérobée (*backdoor*) ou intégrer des fonctions de sécurité volontairement dégradées pour permettre le déchiffrement de flux de données sans connaissance préalable de secrets. L'agence Reuters a ainsi révélé[1] fin 2013 que la National Security Agency américaine avait versé un pot de vin de 10 millions de dollars à la société RSA pour que cette dernière implémente par défaut dans sa solution de sécurité BSAFE l'algorithme de génération de nombres aléatoires faible Dual EC DRBG (*Dual Elliptic Curve Deterministic Random Bit Generator*), et ce, pour permettre le déchiffrement rapide de données de millions d'utilisateurs. Par ailleurs, la NSA serait à l'origine d'une modification de l'algorithme Dual EC DRBG qui est censée, du moins officiellement, renforcer la sécurité des informations chiffrées, alors que des chercheurs ont prouvé que les dites modifications avaient au contraire renforcé les vulnérabilités.

Les qualifications délivrées par l'ANSSI pour les produits

En France, l'ANSSI, rattachée au Secrétaire général de la défense et de la sécurité nationale (SGDSN), a développé son propre schéma de certification pour les produits SSI

1 http://www.numerama.com/magazine/28926-nsa-rsa-extended-random-chiffrement-mozilla.html

Objet		Désignation	Référentiel	Nombre de qualifications	Durée d'attribution
Produits		Qualification élémentaire	ANSSI	Plus de 70	Sans limitation pour une version précise
		Qualification standard	Critères communs EAL3+	Plus de 30	6 mois
		Qualification renforcée	Critères communs EAL4+	Plus de 70	
Prestataires de sevices de confiance	SecNum Cloud	Qualification simple, avancée, ou qualifiée, selon le type de services *cf. cahier n°1 de la Chaire Valeurs et Politiques des Informations Personnelles, sur les Identités numériques*	ANSSI	0	3 ans maximum
	PSCE			Plus de 240	
	PRIS			0	
	PDIS			0	
	PASSI			26	
	PSHE			Plus de 240	

Tableau 1. Qualifications de sécurité délivrées par l'ANSSI pour les produits et prestataires de services de confiance

SecNumCloud : prestataire de service d'informatique en nuage ; PSCE : prestataire de service de certification électronique ; PRIS : prestataire de réponse aux incidents de sécurité ; PDIS : prestataire de détection d'incidents de sécurité ; PASSI : prestataire d'audit de la sécurité des systèmes d'information ; PSHE : prestataire de service d'horodatage électronique

sur la base d'un schéma de corégulation (cf. au Chapitre 5, la section «Des labels nombreux et hétérogènes», page 64): ainsi, la qualification est délivrée par l'ANSSI tandis que l'évaluation est effectuée par des centres d'évaluations privés accrédités par l'Agence. Selon les produits et les niveaux, les qualifications sont attribuées sur la base des résultats d'un audit ou de tests techniques.

Trois niveaux de qualification sont octroyés[2] (cf. tableau page précédente) :

- **La qualification élémentaire** permet d'attribuer un label de premier niveau à un produit SSI, en un temps contraint et avec des ressources réduites. Après examen du dossier par l'ANSSI, un centre d'évaluations agréé par l'Agence pour la certification CSPN (Certificat de Sécurité de Premier Niveau) applique le schéma de certification CSPN. Les vérifications portent entre autres sur la conformité du produit vis-à-vis de ses spécifications de sécurité, et sur les menaces prises en compte.

- **La qualification standard** nécessite plus de temps et de moyens, ce qui confère une garantie à un produit pour traiter des informations sensibles non classifiées. Le produit est évalué par un centre d'évaluation appelé CESTI (Centre d'Évaluation de la Sécurité des Technologies de l'Information), lui aussi accrédité par l'ANSSI. L'évaluation est réalisée sur la base du référentiel des critères communs (cf. section suivante) et sous le contrôle de l'ANSSI. La qualification standard obtenue pour six mois impose que le produit obtienne au moins le niveau EAL3+ tel que déterminé par les critères communs. À cette fin, le constructeur doit fournir de nombreux éléments, en particulier les mécanismes cryptographiques (protection des clés privées, gestion des nombres aléatoires…).

- **La qualification renforcée**, également accordée pour six mois, se fonde sur l'obtention d'un niveau EAL4+ selon le référentiel des critères communs. Les produits français ayant obtenu cette qualification renforcée reçoivent l'agrément «confidentiel» et/ou «secret défense» rendant le produit apte à traiter des informations classifiées.

2 Chochois, M., Magnin, N., (2015). Qualité des produits de SSI, les labels français, Techniques de l'ingénieur, H5825 v2, octobre 2015.

La reconnaissance mutuelle internationale

On distingue deux types d'accords internationaux de reconnaissance mutuelle qui permettent à un État A d'accepter une qualification émise par un État B.

Les premiers accords découlent de l'arrangement de reconnaissance mutuelle selon les critères communs (*Common Criteria Recognition Arrangement* – CCRA), dont le plus récent a été signé en 2014. Ainsi, vingt-huit pays reconnaissent actuellement la validité d'une qualification délivrée à un produit SSI par une de leur autorité de certification et évaluée selon le référentiel des critères communs. Il s'agit de l'Allemagne, de l'Australie, de l'Autriche, du Canada, du Danemark, de l'Espagne, des États-Unis, de l'Éthiopie, de la Finlande, de la France, de la Grèce, de la Hongrie, de l'Inde, d'Israël, de l'Italie, du Japon, de la Malaisie, de la Norvège, de la Nouvelle Zélande, du Pakistan, des Pays-Bas, du Qatar, de la République de Corée, de la République tchèque, du Royaume-Uni, de Singapour, de la Suède, et de la Turquie.

Les critères communs permettent de certifier un produit SSI via un niveau de certification appelé EAL (*Evaluation Assurance Level*), la note EAL1 étant la plus faible et la note EAL7 la plus élevée. Ce référentiel est très utilisé pour imposer des niveaux de certification en fonction des usages. Par exemple, une carte à puce pour un usage interbancaire doit être certifiée au moins EAL4+.

Les accords internationaux de reconnaissance mutuelle comportent néanmoins certaines limites établies en fonction du type de démarche d'évaluation mise en œuvre. Pour une évaluation réalisée selon les critères communs génériques, la reconnaissance mutuelle s'appliquait uniquement jusqu'au niveau EAL2. L'accord CCRA signé en 2014 a assoupli cette règle en définissant des profils appelés « *collaborative protection profile* » (cPP) qui disposent d'une méthode d'évaluation dédiée raffinant les critères communs. Désormais, pour une évaluation conforme à un cPP, la reconnaissance mutuelle peut être étendue jusqu'au niveau EAL4[3].

Un second type d'accord, l'accord européen de reconnaissance mutuelle du *Senior Officials Group Information Systems Security* (SOG-IS) signé en 1999 et mis à jour en 2010, a mis en place la reconnaissance de validité des certificats pour différents domaines

3 https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/les-accords-de-reconnaissance-mutuelle/#sogis-v3.

techniques. Par défaut, cette reconnaissance s'applique jusqu'au niveau EAL4 comme pour l'accord des critères communs, certains domaines tels que les « microcontrôleurs sécurisés et produits similaires » et les « équipements matériels avec boîtiers sécurisés » pouvant bénéficier d'une reconnaissance étendue au niveau EAL7. Onze pays sont actuellement concernés par cet accord, à savoir l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, la Pologne, le Royaume-Uni et la Suède. Pour chaque domaine technique, l'accord précise les pays désignés comme organismes de certification pour émettre une qualification de haut niveau.

La qualification des prestataires de services de confiance

Si l'intervention de l'ANSSI peut parfois sembler éloignée des préoccupations quotidiennes de l'utilisateur final, la situation évolue avec la mise en œuvre depuis le 1er juillet 2016 du règlement (UE) n°910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (*Electronic IDentification And trust Services* – eIDAS)[4].

Le texte instaure un cadre juridique commun à l'ensemble des États membres de l'Union européenne, en ce qui concerne les services d'identification électronique et cinq services de confiance – à savoir les signatures électroniques, les cachets électroniques, les horodatages électroniques, les services d'envoi recommandé électronique et de certificats relatifs à ces services, les certificats pour l'authentification de sites internet. Il nécessite d'être décliné dans chaque État membre, sa déclinaison nationale étant confiée en France à l'ANSSI. L'Agence établit actuellement les référentiels eIDAS et accrédite les organismes d'évaluation de la conformité[5]. Comme l'y autorise le règlement eIDAS, elle a par ailleurs défini quatre types de services qu'elle estime utiles : les prestataires de service informatique en nuage, les prestataires de réponse aux incidents de sécurité, les prestataires de détection d'incidents de sécurité et les prestataires d'audit de la sécurité des systèmes d'information.

---

4 Règlement (UE) no 910/2014 du Parlement européen et du Conseil du 23 juill. 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 : JOUE L 257/73 du 28 août 2014. 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.

5 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-reglement-eidas/documents-publies-par-lanssi/

Cependant, si le règlement a établi un certain niveau d'harmonisation et notamment un lexique commun relatif aux services de confiance décidée (*trust services*), il comporte néanmoins des lacunes et des ambiguïtés notables quant à la protection des données personnelles et de la vie privée des utilisateurs, en particulier en ce qui concerne la possibilité de leur traçage et de leur surveillance. À ce sujet, on se reportera aux chapitres 7, 8, 9 du cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**.

4.2. Vers de nouvelles formes d'analyse du risque associé aux services et utilisateurs

L'analyse comportementale

En informatique, l'analyse comportementale a pour but premier de détecter des intrusions informatiques et des comportements à risque. À l'origine, elle s'appuyait sur l'établissement d'un modèle de comportement « normal » d'un système d'information nécessitant une longue phase d'apprentissage du système. Depuis, la technique et son usage ont évolué pour se centrer sur le comportement des utilisateurs (UBA – *User Behavior Analytics*) et intégrer les dernières avancées en lien avec le *Big Data* et l'apprentissage statistique (*Machine Learning*).

Le tableau page suivante offre un aperçu des tendances actuelles selon lesquelles s'opère aujourd'hui l'évaluation des risques : on distingue les individus, services et plateformes faisant l'objet d'une analyse comportementale menée soit collectivement par des individus (II.), soit par des algorithmes de façon automatisée (III.). Afin d'identifier la véritable finalité de l'usage de l'approche comportementale, il est fondamental de connaître à la fois l'organisation qui définit la norme et le type de critères qui caractérisent cette norme. Ces informations permettent de mieux identifier la nature du risque informatique, le type de confiance mise en jeu, et de discuter des dérives possibles.

Une analyse menée collectivement par des individus (II.) permet, par exemple, de noter un service rendu par un individu ou une entreprise, qu'il s'agisse de vente comme Amazon, Ebay, ou de restauration ou d'hôtellerie au travers du site Tripadvisor. La crédibilité associée à la réputation résultante est d'autant plus grande que le nombre de notes et avis émis est important, car l'effort nécessaire pour corrompre le système, soit par des

	Analyse du risque associée aux services numériques	***Établissement d'un score associé aux services/ utilisateurs : analyse comportementale***		
Signe extérieur	Certificat électronique, services qualifiés	Scoring		
Qui évalue ?	Organismes de certification (I)	Humain (II)	Algorithme (III)	
Qui est évalué ?	Matériel / Logiciel / Services numériques	Service rendu	Individus (III.1)	Individus / sites web (III.2)
Qui fait la norme ?	Commission européenne, institutions	Ensembles d'individus	Gouvernement/ services	Institutions/ plateformes
Volume de données		Masse de données	Masse de données d'un individu	Masse d'invidus / sites web
Formes de confiance	Certification EAL ou eIDAS	Scoring	Profiling / scoring	Profiling / ranking
Confiance en…	Organisme de certification / Prestataire de services	Opérateur / plateforme / gouvernement		
Gages de confiance	Liste de prestataires et produits qualifiés publiée par l'ANSSI	Nombre d'évaluations	Algorithme et nombre de traces	Algorithme
Finalités	Confiance++	Évaluation d'un service	Authentification++ / Surveillance	Cyber-surveillance / Ranking de sites web

Tableau 2. Deux approches de la gestion du risque en informatique

campagnes d'autopromotion, soit par le dénigrement de concurrents, devra être d'autant plus important. Notons que ces systèmes de notation influencent d'ores et déjà de façon importante le choix des consommateurs. Selon une étude de PhoCusWright[6], 83% des personnes interrogées affirment que les avis postés sur Tripadvisor les aident à choisir le « bon » hôtel. Même si le système technique mis en place est pauvre, ces concepteurs entendent instaurer une relation de confiance entre offreurs de services et consommateurs en fournissant un indicateur de risque ; pour autant, il ne garantit qu'une confiance que certains pourraient être tentés de qualifier de « faible ».

L'analyse comportementale peut également être automatisée par un algorithme pour offrir une meilleure efficacité et précision (III.). Il peut s'agir de cibler un individu particulier (III.1). Dans ce cas, l'analyse peut servir à renforcer le niveau d'authentification d'une personne vis-à-vis d'un système d'information. En plus d'une authentification par mot de passe, clé USB, le fait que le comportement de l'individu soit proche de son comportement habituel va apporter un critère supplémentaire au processus d'authentification et limiter les risques. C'est donc le comportement habituel de la personne qui sert de référence, la nature et la grandeur des écarts autorisés étant définies par l'instance qui met en place le système. La fiabilité associée à cette évaluation comportementale repose sur la richesse et la qualité des traces laissées par l'individu dans le système et donc la précision avec laquelle il est possible de caractériser son comportement (sa géolocalisation, l'utilisation d'applications à certaines heures de la journée, les terminaux qu'il utilise…). Elle repose aussi sur la capacité de l'algorithme à détecter un comportement inhabituel. Pour ce faire, il est nécessaire de régler plus ou moins finement l'outil en fonction de l'individu ciblé, le but étant d'éviter un trop grand nombre de fausses alertes (faux positifs) et d'empêcher les usurpations d'identité (faux négatifs).

La finalité première de l'analyse automatisée individualisée peut cependant être détournée, notamment pour contrôler de façon généralisée le comportement d'une population (III.1). Ainsi, chaque individu pourrait se voir attribuer une note en fonction de son comportement et se voir allouer des avantages ou des pénalités. Par exemple, l'État chinois travaille sur un nouveau service de « crédit social », dont la mise en œuvre est annoncée pour 2020. Les citoyens chinois seraient alors « classés » selon leurs agissements et le niveau de comportement à « risques » de chaque citoyen serait mesuré.

6 https://www.tripadvisor.fr/TripAdvisorInsights/w733

Enfin, l'analyse automatisée peut porter sur une masse d'individus, de plateformes, de sites web (III.2), les finalités étant ici aussi d'ordre commercial ou politique.

Les systèmes de notation de Google notamment classent les sites web les plus populaires selon certains mots clés ; ceux d'Apple concernent la popularité de ses applications dans l'App Store. Cependant, le fonctionnement des algorithmes qui sont censés classer des produits, des applications ou des sites web selon un critère de popularité reste très opaque et ne permet pas toujours d'éviter certaines dérives. Par exemple, moyennant la somme de 11 000 dollars US, la société Taobao a pu positionner son application dans le top 10 des applications mobiles de l'App Store[7].

L'analyse automatisée sert également de support à la mise en œuvre d'une législation, par exemple la loi HADOPI2 ou la loi relative au renseignement. Cette dernière, votée en 2015 en France suite aux attaques terroristes de janvier 2015, autorise les autorités à collecter et analyser des données de connexion dites méta-données et définit les cas où ces mesures sont autorisées. Cette détection, qui vise notamment à assurer la défense nationale, à prévenir le terrorisme ou à défendre les intérêts économiques de la France, est réalisée de façon automatisée par un algorithme sur la base d'un comportement normatif prédéfini.

De façon classique, on constate donc que les techniques d'analyse comportementale sont à double tranchant. Elles servent à la fois un objectif louable consistant à améliorer la sécurité de l'environnement numérique et des ambitions commerciales ou institutionnelles plus inquiétantes.

7 https://recombu.com/mobile/article/manipulate-apple-app-store-rankings-for-money-in-china

4.3. Vers des systèmes de confiance hybrides, distribués et plus respectueux de la vie privée

En informatique, trois directions sont actuellement explorées pour limiter les risques de sécurité et de fuite de données et accroître le niveau de confiance dans les produits et services numériques.

- Des ***approches hybrides*** pour renforcer le niveau de sécurité des solutions SSI classiques à l'aide des méthodes d'analyse comportementale. Avec les progrès opérés dans le domaine du *Machine Learning* et du *Big Data*, couplés à la collecte massive de données, de plus en plus de services de sécurité s'appuient sur des méthodes d'analyse comportementale pour caractériser le comportement d'une personne, d'un système d'information, de façon à mesurer les écarts. On constate par exemple que les banques mettent en place une authentification forte de leurs clients sur la base d'éléments cryptographiques forts usuels couplés à une authentification comportementale où sont prises en considération des informations contextuelles (géolocalisation, horaire de connexion, adresse IP du terminal, *fingerprint* du terminal[8]), et des informations issues de l'interaction entre l'utilisateur et son terminal (habitude de navigation sur un site web, manière de bouger la souris, de frapper au clavier). La tendance dans le futur sera d'obtenir une plus grande finesse dans la caractérisation d'un comportement et une plus grande précision quant au niveau de risque encouru.

- Plus de ***transparence*** et une ***gouvernance décentralisée***. Cette direction est prise par les travaux sur la blockchain. L'objectif premier de la blockchain est d'offrir un service qui, au lieu d'être centralisé dans les mains d'une même autorité, se trouve administré par plusieurs autorités. L'algorithme de mise en œuvre du service est publiquement accessible, lisible et donc interprétable par tous ; ainsi le moindre changement dans le fonctionnement et la gouvernance du service doit être approuvé par consensus par l'ensemble des autorités participantes avant sa mise en application. En résultent une plus grande transparence, une (a priori) plus grande

8 La signature numérique d'un terminal (*fingerprint*) est composée d'une multitude d'informations (version du système d'exploitation, résolution de l'écran…) qui, prises individuellement sont sans importance, mais dont la combinaison permet d'identifier très précisément un terminal parmi des millions.

stabilité, le sentiment des utilisateurs de mieux contrôler les services et acteurs et donc un niveau de confiance plus élevé (ceci est développé au chapitre 11).

- Un meilleur **respect de la vie privée** des individus. Des briques technologiques se développent pour garantir à la fois des propriétés de sécurité et la protection des données personnelles. Parmi ces briques, on peut nommer la ***certification anonyme***[9] qui vise à minimiser la collecte des données par un fournisseur de services tout en garantissant à ce même fournisseur que l'internaute répond bien aux critères de restriction d'accès (être majeur, de la région Île-de-France…). On peut également citer le ***chiffrement homomorphique*** qui vise à déléguer à un tiers un certain type de traitement sur des données sans que les données en clair ne soient révélées, ou bien encore le ***calcul multipartite sécurisé*** qui permet à un ensemble de participants de réaliser un calcul collectivement tout en cachant le type d'opérations effectuées ou bien les valeurs brutes sur lesquelles porte le calcul. Ces approches peinent cependant à s'imposer en pratique. Les obstacles sont à la fois d'ordre technique, avec des coûts énergétiques encore trop importants, et d'ordre économique, avec la difficulté de s'orienter vers un modèle autre que celui de la marchandisation des données personnelles.

Si la technologie blockchain, les systèmes à gouvernance décentralisée et les travaux en faveur d'un meilleur respect de la vie privée sont moteurs dans l'établissement de la confiance décidée, il serait intéressant d'identifier plus précisément l'ensemble des éléments techniques qui pourraient faire émerger un environnement favorable à l'expression de la confiance assurée. Ces travaux en constituent, à n'en pas douter, une condition nécessaire, mais ils posent à nouveau la question de l'intervention et du rôle des autorités publiques dans ce champ.

9 Laurent, M., et Kaâniche, N. (2016). Les preuves d'identités ou d'attributs préservant le pseudonymat ; *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Les quatre chapitres qui viennent présentent les enseignements majeurs qu'il est possible de déduire à partir du recensement d'une centaine de labels, à la fois au niveau national, européen et américain (listés au chapitre 5). Ces signes de confiance extérieurs ont pour principal objet la collecte et l'utilisation des données personnelles de façon générale ou dans un cadre sectoriel, comme l'informatique en nuage ou le commerce en ligne.

► Notamment, le label belge BeCommerce, consacré au commerce électronique, porte sur la sécurité et la qualité de la transaction, la procédure de réclamation, les informations transmises aux clients, la protection des mineurs tout en garantissant la protection des données personnelles des clients.

Par exemple, il nous est apparu important de retenir des labels qui participent à la labellisation de certains principes de protection des données personnelles, comme les signes de confiance portant sur la sécurité (voir le chapitre 4 pour un aperçu plus complet). Si la confusion est souvent faite entre « *sécurité des données* » et « *protection des données personnelles* », il convient cependant de bien distinguer les deux notions.

Protection des données personnelles et sécurité des données

En matière de données personnelles, la sécurité est une composante parmi d'autres, un principe-clé certes mais un principe parmi d'autres principes tels que le principe de finalités du traitement, de durée de conservation des données, de légitimation, de protection des données sensibles, etc[1]. Principalement, la sécurité se traduit en terme d'obligation pour le responsable de traitement de données personnelles et le sous-traitant, à savoir la mise en place de mesures techniques et physiques propres (chiffrement des données, gestion des autorisations d'accès, etc.) pour protéger les données des personnes et empêcher tout traitement non autorisé. Le droit à la protection des données personnelles se conçoit dans un périmètre plus large comme un droit fondamental et un droit de l'Homme garanti par de nombreux textes nationaux et internationaux, notamment la Charte des droits fondamentaux de l'Union européenne.

1 Levallois, C. (2016). Identités numériques et gestion des données personnelles. *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Afin de faciliter les comparaisons, l'étude se focalise sur les signes de confiance proposés dans les États membres de l'Union européenne et traite le cas des labels suisses qui présentent un exemple intéressant, dans la mesure où ils s'appuient sur des principes proches de ceux contenus dans le RGPD.

► En outre, l'étude s'appuie sur plus d'une vingtaine d'entretiens qualitatifs effectués entre octobre 2015 et septembre 2017 auprès de représentants d'entités labellisées ou labellisatrices, de cabinets de conseils et d'avocats français. La liste de ces entretiens est détaillée en Annexes, page 218.

De façon générale, on constate que la labellisation se trouve à la croisée de deux conceptions : la première cherche à encourager les acteurs économiques à rendre compte de leur conformité juridique à travers des mécanismes de régulation et de responsabilité dans lesquels interviennent fortement les autorités publiques. À l'instar des labels délivrés par la CNIL et EuroPriSe, ces signes de confiance adressent l'ensemble des principes de protection des données personnelles, dans le cadre d'une conformité globale (cf. Chapitre 6). La seconde conception entend impliquer les acteurs économiques dans leur propre régulation à travers une démarche d'auto-régulation. Dans un contexte sociétal et numérique en perpétuelle évolution, l'objectif ici est d'agir comme un complément aux structures juridiques traditionnelles dans le cadre d'une recherche de crédibilité et de compétitivité qui met en avant certains critères dit de « qualité » (cf. Chapitre 7).

Chapitre 5. Panorama national et international des labels relatifs aux données personnelles

Claire Levallois-Barth,
Delphine Chauvet

5

Parmi la centaine de signes de confiance que nous avons retenus, certains emploient le terme de « label », d'autres celui de « certification » ou de « marque »[1]. Si on constate une hétérogénéité entre les différents signes de confiance extérieurs délivrés par différents types d'entités (5.1.), il n'en reste pas moins vrai que les procédures présentent des similitudes (5.2.).

5.1. Des labels nombreux et hétérogènes

Nous avons répertorié une centaine de labels, nationaux, européens et américains. Cet aperçu comprend 75 labels délivrés en Europe et 22 en Amérique du Nord (États-Unis et Canada) et Japon. On constate que ***des entités labellisatrices multiplient la création de labels*** différents. Certains labels disparaissent à peine créés, d'autres semblent répondre à un simple effet d'annonce. D'où la difficulté à rendre compte de façon exhaustive d'un panorama des labels en matière de protection des données personnelles.

1 Voir Chapitre 2, section 2.4, page 32.

Panorama national et international des labels relatifs aux données personnelles

L'une des explications à cette multiplication des labels est sans doute à rechercher du côté des différents métiers disposant de compétences pour créer un référentiel sur les données personnelles et apprécier la concordance entre les critères définis et les pratiques de l'entité qui souhaite être labellisée. On compte notamment des consultants, des juristes et avocats spécialisés, des auditeurs travaillant entre autre dans le cadre des certifications ISO, des informaticiens en ce qui concerne la sécurité des données ou l'informatique en nuage, des personnes issues du marketing et de la communication, et des économistes. Chaque spécialité va ainsi orienter son type de signe de confiance à la fois selon le domaine couvert et selon les objectifs poursuivis.

Pour autant, il est possible de constituer un panorama en retenant certaines caractéristiques concernant le périmètre géographique, le champ d'application et le type d'entités qui délivrent un label en matière de données personnelles.

Des labels essentiellement délivrés par des organismes allemands

En premier lieu, on note une répartition géographique inégale. Ainsi, l'Allemagne et les États-Unis sont les plus importants créateurs de labels. Sur 75 labels recensés en Europe, on compte, sans prétendre à l'exhaustivité :

1. 41 labels en Allemagne
2. 9 en France dont 4 labels délivrés par la CNIL
3. 4 en Espagne et en Suisse
4. 3 en Italie et aux Pays-Bas
5. 2 au Royaume-Uni
6. 1 en Autriche, en Belgique, au Danemark et au Luxembourg
7. 5 labels de dimension européenne

On compte par ailleurs 22 labels en dehors de l'Europe (États-Unis, Canada et Japon).

En Europe, c'est l'Allemagne qui a développé le plus de labels (voir la liste des labels dans le Tableau 4, page 68 et suivantes), à la fois pour des raisons juridiques et culturelles. Si ce pays encadre strictement la protection de la vie privée et des données personnelles, notamment pour des raisons historiques, l'explication est aussi à rechercher du côté de la structure juridique de cet État fédéral. En effet, chaque Land a la possibilité d'édicter sa propre loi en matière de protection des données personnelles. Par exemple, la loi du 9 février 2000 du Land Schleswig-Holstein a introduit une possibilité de certification par l'autorité de protection des données de ce Land, l'*Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (ULD).

À l'échelon fédéral, une disposition juridique adoptée en 2001, la Section 9a de la loi fédérale sur la protection des données, prévoit qu'« *afin d'améliorer la protection des données et la sécurité des données, les fournisseurs de systèmes de traitement de données et de programmes et les organismes chargés du traitement des données peuvent faire examiner et évaluer leurs stratégies de protection des données et leurs installations techniques par des évaluateurs indépendants et approuvés, et peuvent publier le résultat de la vérification. Les exigences détaillées relatives à l'examen et à l'évaluation, la procédure,*

(suite page 78)

Organisme	*Nom du label*	*Objet*	*Type d'organisme*	*Site web*
Adel	ADEL (*Algorithm Data Ethic Label*)	Services/ Algorithmes	Privé	www.adel-label.com
Cloud Confidence	Certification Cloud Confidence	Services / Cloud	Association	www.cloudconfidence.eu
CNIL	Label CNIL Formations	Services / Formations	Public Autorité de contrôle Données personnelles	www.cnil.fr
	Label CNIL Audit de traitements	Services / Audit		
	Label CNIL Coffre-fort numérique	Produits / Coffre-fort numérique		
	Label CNIL Gouvernance Informatique et Libertés	Procédures		
FEVAD (Fédération du e-commerce et de la vente à distance)	Marque de confiance FEVAD	Services / Commerce électronique	Association	www.fevad.com
FNTC (Fédération des Tiers de Confiance du numérique)	Label E-Vote	Services / Vote électronique	Association	www.fntc-numerique.com
France IT	Label Cloud	Services / Cloud	Association	www.label-cloud.com

Tableau 3. Labels délivrés par des organismes français

Organisme	*Nom du label*
ADCERT Privacy Audit GmbH	ADCERT-geprüfter Datenschutz
Althammer & Kill GmbH & Co	Geprüfter Datenschutz
	Zertifizierter Datenschutz
a.s.k. Datenschutz	a.s.k. compagnysecure
	a.s.k. websecure
BNT GmbH	Geprüfter Datenschutz
Check 11 - GDD-Fachgruppe Externe Daten-schutzbeauftragte	Datenschutzzertifikat Check11
Conformity Trust GmbH	Trust in Privacy
Datenschutz cert GmbH	Zertifikat für Auftragsdatenverarbeitung
	Zertifikat für das Datenschutz-Management - Priventum
	Gütesiegel IPS (internet privacy standards)
Deutscher Dialogmarketing Verband e. V.	QuLS-Siegel Listbroker QuLS-Siegel Datenverarbeitung QuLS-Siegel Lettershop, QuLS-Siegel Adressverlag QuLS-Siegel Fulfillment
DQS Deutsche Gesellschaft zur Zertifizierung von Management-systemen GmbH	DQS-Gütesiegel Datenschutz Plus
	DQS-Gütesiegel Datenschutz
DSZ Datenschutz Zertifizierungs-gesellschaft mbH	Datenschutzsiegel

Tableau 4. Labels délivrés par des organismes allemands

Objet	*Type d'organisme*	*Site web*
Procédures, produits et services	Privé	www.adcert.eu
Procédures, produits et services	Privé	www.althammer-kill.de
Procédures, produits et services	Privé	www.bdsg-externer-datenschutzbeauftragter.de
Services / Sites web		
Procédures, produits et services	Privé	www.bntgmbh.de
Personnes / Experts Données personnelles	Association	externer-datenschutz.de
Procédures, produits et services	Privé	www.conformitytrust.de
Procédures, produits et services	Privé	www.datenschutz-cert.de
Procédures		
Services/Services en ligne		
Procédures, produits et services	Privé	www.ddv.de
Procédures	Privé	www.dqs.de
Procédures, produits et services	Privé	www.dsz-audit.de

(source : https://stiftungdatenschutz.org/aufgaben/zertifizierung, février 2017)

Organisme	*Nom du label*	
ePrivacy GmbH	ePrivacySeal	
	ePrivacyApp	
editco GbR	IT-Security- und Datenschutz-Audit	
EuroPriSe GmbH	EuroPriSe (European Privacy Seal)	
Datenschutz Mecklenburg-Vorpommern	Privacy Seal Gütesiegel Datenschutz Mecklenburg-Vorpommern	
GDD (Gesellschaft für Datenschutz und Datensicherheit)	Zertifizierung der Datenschutzqualifikation	
GDI Gesellschaft für Datenschutz und Informationssicherheit mbH	GDI - zertifizierter Datenschutz	
GenoTec GmbH	Datenschutz-CheckUp mit Zertifikat	
Greeneagle certification GmBH	Datenschutzkonform	
	Geprüfte Auftragsdaten- verarbeitung	
IITR (Institut für IT-Recht) GmbH	Datenschutz-Status Qualifizierter Datenschutz	
INOIS (Institut für organisatorische Informationssysteme)	Zertifizierter Datenschutz	
Interev GmbH	Geprüfter Datenschutz durch Interev	

Objet	*Type d'organisme*	*Site web*
Procédures, produits et services	Privé	www.eprivacy.eu
Services / Applications mobiles		
Procédures, produits et services		
Produits, services/sites web	Public avec les autorités de contrôle Données personnelles puis privé depuis 2014	www.european-privacy-seal.eu
Procédures et produits	Public Autorité de contrôle Données personnelles en lien avec EuroPriSe	
Personnes / Expert Données personnelles	Association	www.gdd.de
Procédures, produits et services	Privé	www.gdi-mbh.eu
Procédures, produits, services et personnes	Privé	www.geno-tec.de
Procédures, produits et services	Privé	www.greeneagle-certification.de
Procédures, produits et services	Privé	www.iitr.de/zertifizierung.html
Procédures, produits et services	Privé	www.inois.de/leistungsspektrum/zertifizierung
Procédures, produits et services	Privé	www.interev.de

Organisme	*Nom du label*	
Legitimis GmbH	Statement of Compliance	
MediaTest digital GmbH	Trusted App	
Privacy Stiftung	ADV Compliance Checked	
SCHUFA Holding AG	SCHUFA-DatenschutzSiegel	
Tacticx GmbH	Geprüfter Datenschutz	
Tekit Consult Bonn GmbH (TÜV Saarland Gruppe)	TÜV Geprüfter Datenschutz	
Trusted Shops GmbH	Trusted Shops	
TÜV Informationstechnik GmbH	TÜVIT-Zertifikat Trusted Site Privacy	
TUV Rheinland	Data Privacy Certification for Companies	
TÜV SÜD sec-IT GmbH	S@fer-shopping	
TÜV SÜD sec-IT GmbH	Zertifizierte Auftrags-datenverarbeitung	
Verband für Berater, Sachverständige und Gutachter im Gesundheits- und Sozialwesen e.V.	VBSG-Datenschutzsiegel	
ULD (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein)	Datenschutz-Gütesiegel	

Objet	*Type d'organisme*	*Site web*
Procédures	Privé	www.legitimis.de
Services/ Applications mobiles	Privé	www.mediatest-digital.com
Procédures, produits et services	Privé	www.privacy-stiftung.de
Procédures, produits, services et personnes	Privé	www.schufa.de
Procédures, produits et services	Privé	www.tacticx.de
Procédures, produits et services	Privé	www.tekit.de/zertifizierung/
Procédures/ Commerce électronique	Privé	www.trustedshops.com
Procédures, produits et services/ sites internet	Privé	www.tuvit.de
Procédures	Privé	www.tuv.com
Procédures/ Commerce électronique	Privé	www.safer-shopping.de www.tuev-sued.de/sec-it
Procédures	Privé	www.tuev-sued.de www.tuev-sued.de/sec-it
Procédures	Association	www.vbsg.org
Procédures, produits et services	Public Autorité de contrôle Données personnelles	www.datenschutzzentrum.de

Origine	Organisme	Nom du label
Autriche	Handelsverband	TrustMark Austria
Belgique	BeCommerce	Label Becommerce
Danemark	E-handelsfonden	E-maerket
Espagne	APEP (Asociación Profesional Española de Privacidad)	APEP-CertifiedPrivacy
Espagne	Confianza Online	Confianza Online
Espagne	ISMS Forum Spain	CDPP (Certified Data Privacy Professional)
Espagne	Seriedad Online	Seriedad Online
Italie	Bureau Veritas (Italie)	Certificazione del Personale Data Protection Officer
Italie	KHC (Know How Certification)	Certificazione data protection officer e privacy consultant
Italie	TÜV Italia/TÜV SUD GROUP	Certificazione di privacy officer e consulente della privacy
Luxembourg	EuroCloud Europe a.s.b.l.	EuroCloud Self Assessment EuroCloud Star Audit
Pays-Bas	Alliander NV	Data Privacy and Security certification
Pays-Bas	Thuiswinkel	Thuiswinkel Waarborg
Pays-Bas	Veiligheidsbranche	Keurmerk Particulier Onderzoekbureau
Royaume-Uni	Comodo CA Limited	Comodo Secure
Royaume-Uni	The Market Research Society	Fair Data
Suisse	APPD (Association des Professionnels de la Protection des Données)	CAPD (Certificat d'Aptitude à la Protection des Données)
Suisse		CIPD (Certificat d'Implémentation de la Protection des Données)
Suisse	SQS (Association Suisse pour Systèmes de Qualité et de Management)	Good Priv@cy
Suisse		SQS-OCPD (OCPD:2014; avant OCPD:2008)

Tableau 5. Labels délivrés par des organismes établis dans d'autres pays européens

	Objet	Type d'organisme	Site web
	Services / Commerce électronique	Association	www.handelsverband.at
	Services / Commerce électronique	Association	www.becommerce.be
	Services / Commerce électronique	Association	www.emaerket.dk www.emaerket.dk/english
	Personnes / Experts Données personnelles	Association	www.apep.es
	Services / Commerce électronique	Association	www.confianzaonline.es
	Personnes / Experts Données personnelles	Association	www.ismsforum.es
	Services / Sites web	Privé	www.seriedadonline.es
	Personnes	Privé	www.bureauveritas.it
	Personnes / Experts Données personnelles	Privé	www.khc.it
	Personnes / Experts Données personnelles	Privé	www.tuv.it
	Services / Cloud	Association	www.eurocloud-staraudit.eu
	Produits / Compteurs intelligents	Privé	www.alliander.com
	Services / Commerce électronique	Association	www.thuiswinkel.org
	Procédures / Investigation des agences de détectives privés	Association	www.veiligheidsbranche.nl
	Services / Sites web	Privé	www.comodo.com
	Procédures / Études de marché	Association	www.fairdata.org.uk
	Personnes / Experts Données personnelles	Association	www.appd.ch
	Personnes / Experts Données personnelles	Association	www.appd.ch
	Procédures et produits	Association	www.sqs.ch
	Procédures et produits	Association	www.sqs.ch

Origine	Organisme	Nom du label
États-Unis/ Canada	AICPA (American Institute of Certified Public Accountants) et CICA (Canadian Institute of Chartered Accountants)	WebTrust
Canada	Deloitte et Ryerson University	Privacy by design Certification
États-Unis	Better Business Bureau	BBB Accredited Business Seal or the Web
États-Unis	BuySAFE Inc.	Buysafe Guaranteed Shopping
États-Unis	CSA (Cloud Security Alliance)	CSA STAR (Security, Trust and Assurance Registry)
États-Unis	ESRB (Entertainment Software Rating Board)	ESRB Privacy Certified
		ESRB Privacy Certified for Kids
		ESRB Privacy Certified for Mobile
États-Unis	Gigya, Inc.	Gigya's Social Privacy Certification
États-Unis	Google	Trusted Store
États-Unis	IAPP (International Association of Privacy Professionnals)	Certified Information Privacy Professional (CIPP)
		Certified Information Privacy Manager (CIPM)
		Certified Information Privacy Technologist (CIPT)
États-Unis	McaFee Secure	McaFee Secure
États-Unis	PRIVO (Privacy Vaults Online, Inc.)	Privo Privacy Certified
		PRIVO's Safe Harbor Privacy Assurance Program Seal
États-Unis	TRUSTArc	TRUSTe Certification APEC
		TRUSTe Certification Enterprise Privacy certification
		TRUSTe Certification TRUSTed Data
		TRUSTe Certification TRUSTed Downloads
		TRUSTe Certification Children's Privacy
Japon	JIPDEC (Japan Institute for Promotion Of Digital Economy and Community)	PrivacyMark System

Tableau 6. Labels délivrés par des organismes situés en dehors de l'Europe

Objet	*Site web*
Services / Audits	www.webtrust.org
Procédures et produits	www2.deloitte.com/ca/en/pages/risk/articles/Privacybydesign.html
Services / Sites web	www.bbb.org
Services / E-commerce	www.buysafe.com
Services / Cloud	www.cloudsecurityalliance.org cloudsecurityalliance.org/star/
Services / Sites web	www.esrb.org et www.esrb.org/privacy.asp
Services / Applications mobiles, sites web et jeux vidéo en ligne pour les enfants	www.esrb.org
Services/ Applications mobiles	
Services / Sites internet et applications mobiles	www.gigya.com
Services / E-commerce	www.google.com/trustedstores/
Personnes / Experts Données personnelles	www.iapp.org/certify/cipp
	www.iapp.org/certify/cipm
	www.iapp.org/certify/cipt/
Services/Sites internet	www.mcafeesecure.com/
Services/Sites web, jeux, applications pour les enfants	www.privo.com
Procédures et produits	
Procédures	www.trustarc.com/privacy-certification-standards/
Procédures	
Services / publicité en ligne	
Services / Logiciel	
Services/ Enfants de moins de 13 ans	
Procédures	www.privacymark.org

(cas les plus connus – liste non exhaustive)

Organisme	*Nom du label*	*Objet*	*Type d'organisation*	*Site web*
EMOTA (European Multichanel and Online Trade Association)	Label de confiance de l'EMOTA	Services / Commerce électronique	Association	europeantrustmark.eu/fr
Ecommerce Europe	Ecommerce Europe Trustmark	Services / Commerce électronique	Association	www.ecommerce-europe.eu
EDAA (European Interactive Digital Advertising Alliance)	Trust Seal	Services / Publicité en ligne	Association	www.edaa.eu
	OBA Certification (Online Behavioural Advertising)	Service / Publicité comportementale		
European Schoolnet	eSafety Label.eu	Services / Écoles	Association	www.esafetylabel.eu

Tableau 7. Labels de dimension européenne

la sélection et l'approbation des évaluateurs sont stipulées dans une loi distincte.»[2] En pratique, cette loi spécifique n'a pas été adoptée. Aujourd'hui, 41 schémas de certification sont proposés en Allemagne. Seuls deux labels sont délivrés par les autorités de contrôle, les autres étant délivrés par des entités privées et visant à implémenter le cadre légal au-delà (cf. Chapitre 6).

2 Traduit librement de l'anglais : "*In order to improve data protection and data security, suppliers of data processing systems and programs and bodies conducting data processing may have their data protection strategies and their technical facilities examined and evaluated by independent and approved appraisers, and may publish the result of the audit. The detailed requirements pertaining to examination and evaluation, the procedure and selection and approval of the appraisers shall be stipulated in a separate act*", Federal Data Protection Act in the version promulgated on 14 January 2003 (Federal Law Gazette I p. 66), as most recently amended by Article 1 of the Act of 14 August 2009 (Federal Law Gazette I p. 2814), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html. Source en anglais : https://databeskyttelsesdag.files.wordpress.com/2017/01/dk_privacy-seals-and-certifications_2017-2.pdf.

En dehors de l'Union européenne (voir Tableau 6, page 76), l'offre de labels, marques et sceaux s'est fortement développée aux États-Unis. Les plus connus sont TRUSTe, avec ses différents programmes fournis désormais par TrustArc et portant notamment sur les principes définis par la Coopération économique pour l'Asie-Pacifique (*Asia-Pacific Economic Cooperation* – APEC), la publicité en ligne ou la protection des enfants de moins de 13 ans, le *Better Business Bureau* (BBB) qui s'adresse aux sites web des entreprises établies aux États-Unis et au Canada et se conformant au *BBB Code of Business Practices*, l'*Entertainment Software Rating Board* (ESRB) et son *Privacy Online Seal*, et enfin *WebTrust*.

Certains proposent à leurs clients des programmes visant à intégrer les dispositions du RGPD, comme TrustArc et PRIVO.

Des labels délivrés dans des domaines et secteurs variés

De manière générale, le marché des labels ne compte pas ou peu de labels généraux applicables à l'ensemble des secteurs. En effet, il se focalise sur :

- les ***produits***, avec notamment le label « Coffre-fort numérique » délivré en France par la CNIL

- les ***services***, comme les applications mobiles (*ePrivacyApp* de l'entité allemande ePrivacy GmbH) et l'informatique en nuage (*CSA STAR* de l'entité américaine *Cloud Security Alliance*)

- les ***processus***, comme *Good Priv@cy* de l'association suisse pour les systèmes de Qualité et de Management (SQS) et *Datenschutz-CheckUp mit Zertifikat* de l'entreprise allemande GenoTec Gmbh

- la ***formation***, qui peut être dispensée sur des textes nationaux et européens (label CNIL « Formation »)

    - à des experts spécialisés en matière de données personnelles : en Espagne avec *Certified Data Privacy Professional* (CDPP) de l'organisme ISMS Forum Spain, en Italie avec *Certificazione del personale-Privacy* de l'organisme *Know How Certification* (KHC), et aux États-Unis avec *Certified Information Privacy*

Professional (CIPP) de l'*International Association of Privacy Professionnals* (IAPP)

- mais aussi, de façon plus spécifique, à une profession comme les détectives privés (aux Pays-Bas avec le label *Keurmerk Particulier Onderzoekbureau* de l'organisme *Veiligheidsbranche*)

- ***Les audits, avec un label CNIL spécifique*** (cf. Chapitre 6)

De fait, les labels concernent ***des secteurs multiples et variés***, ainsi qu'en témoignent les domaines suivants :

- le ***commerce électronique*** : la marque danoise *E-maerket*, le label *BeCommerce* en Belgique, *Trusted Shops* en Allemagne ou le *European Trustmark label* délivré par Ecommerce Europe

- la ***publicité en ligne*** : *OBA Certification* de l'entreprise allemande Privacy GmbH

- le ***cloud computing*** : *CSA STAR* délivré par la *Cloud Security Alliance* aux États-Unis, le label « Cloud » de France IT

- les ***sondages*** : *Fair Data* délivré par *The Market Research Society* au Royaume-Uni

- les ***sites web*** et les jeux en ligne accessibles aux mineurs : *Privo Privacy Certified* délivré par Privo aux États-Unis

- les ***réseaux sociaux*** : *Gigya's SocialPrivacy Certification* de Gigya aux États-Unis

- les ***écoles*** : *eSafety Label* de l'*European Schoolnet* délivré au niveau européen

Des labels délivrés par des entités de natures diverses

Les labels sont délivrés par des entités de différentes natures. En Europe, il s'agit d'***organismes privés*** (56%). On observe aussi des labels créés par des ***associations spécialisées*** (34,66%) dans un domaine déterminé.

► Par exemple, l'association française Cloud confidence délivre un label sur l'informatique en nuage. À ce titre, ses membres sont composés de fournisseurs de *cloud*, de prestataires de services, d'experts mais aussi d'utilisateurs.

La particularité d'un label délivré par une association est que le candidat doit en règle générale adhérer à l'association pour être labellisé. Par ailleurs, on observe que les labels liés au secteur du commerce électronique sont généralement délivrés par des associations de professionnels regroupant des e-commerçants et des prestataires.

► Tel est le cas du label espagnol *Confianza Online* ou du label belge *BeCommerce*.

Il existe des labels délivrés par des ***organismes publics*** (9,33%). Plus précisément, ceux que nous avons retenus sont délivrés par des autorités nationales de protection des données. Il en va ainsi de la France (CNIL), et de deux Länder allemands : le Schleswig-Holstein et le Mecklembourg-Poméranie.

Si les labels sont délivrés soit par des entités publiques, soit par des entités privées, le schéma donnant lieu à leur délivrance peut revêtir ***une nature mixte***, fonction de la nature et du degré d'intervention des autorités publiques. Ainsi, on distingue les schémas :

- directement gérés par les autorités publiques, typiquement les labels délivrés par la CNIL, ou qui revêtent une valeur légale

- dit d'auto-régulation auxquels les autorités apportent leur soutien sans intervenir directement (par exemple les labels privés TÜV IT et TÜV Rheinland, SQS, DEKRA, MRS/Fair Data, *Trusted shops* ou OBA)

- dit de corégulation où les autorités publiques sont parties prenantes pour élaborer les exigences et/ou participer à la gestion opérationnelle ou financière, notamment EuroPriSe

Le cas de la Suisse qui présente un schéma de certification semi-public est emblématique : l'autorité de protection, le Préposé Fédéral à la Protection des Données et à la Transparence (PFPDT), participe aux procédures d'accréditation, de contrôle et de révocation des organismes de certification. Précisément, il s'agit des organismes qui délivrent des certifications pour les produits et procédures de traitements des données en application de l'Ordonnance Suisse sur les Certifications en matière de Protection des Données (OCPD) adoptée par le Conseil fédéral Suisse[3]. Par exemple, l'association Suisse pour les Systèmes de Qualité et de Management (SQS) est accréditée pour délivrer la certification OCPD:2014. Elle délivre par ailleurs le label « Good Priv@cy ».

5.2. Des schémas de labellisation présentant de fortes similarités

Les schémas donnant lieu à la délivrance d'un label présentent tous ***un référentiel***, ***une procédure d'évaluation***, ***un logo***, ***une procédure de vérification*** *a posteriori*, ainsi qu'***une procédure de résolution des conflits***. Leur but est de délivrer une attestation de conformité. Comme le fait remarquer Eric Lachaud, cela n'est pas typique à la protection des données[4]. Cet auteur démontre que « *la certification des données personnelles est une forme de certification comme une autre* » présentant des similarités en ce qui concerne à la fois les composantes et la procédure.

Un référentiel

Le terme de référentiel étant employé par la CNIL, nous utilisons ici cette notion, qui est définie par l'article L 433-3 du code de la consommation comme étant « *un document technique définissant les caractéristiques que doit présenter un produit, un service ou une combinaison de produits et de services, et les modalités de contrôle de la conformité*

3 Conformément à l'article 11, alinéa 2 de la loi fédérale suisse sur la protection des données du 19 juin 1992 (modifiée en dernier lieu le 1er janvier 2014) (CH301).

4 Lachaud, E. (2017). The General Data Protection Regulation and the rise of certification as a regulatory instrument. Computer Law & Security Review.

à ces caractéristiques. L'élaboration du référentiel de certification incombe à l'organisme certificateur qui recueille le point de vue des parties intéressées. » De manière générale, un référentiel fixe donc des caractéristiques, autrement appelées critères, exigences, spécifications ou normes. Ces caractéristiques, qui doivent être impérativement respectées, déterminent le périmètre des activités visées par le label, définissent les critères à respecter et fixent les valeurs pour chaque critère. Parfois, elles précisent le degré d'écart qu'un évaluateur peut accepter pour ces valeurs.

Dans le domaine des données personnelles, le référentiel s'appuie sur des sources diverses, juridiques ou non. Son contenu s'inscrit dans un continuum allant d'un référentiel très complet à des exigences pour le moins succinctes.

Tout d'abord, les spécifications se basent sur des ***obligations légales***, la directive 95/46/CE Protection des données et le RGPD, ainsi que les législations nationales. Tous les labels ne reprennent pas forcément l'ensemble des principes de protection des données personnelles définis dans ces textes mais ils se réfèrent toujours aux principaux (licéité, proportionnalité, finalité, transparence).

Les différents labels délivrés par Datenschutz cert GmbH sont fondés sur la loi fédérale allemande de protection des données, ceux délivrés par la CNIL sur la loi Informatique et Libertés et désormais le RGPD.

- Afficher un label qui garantit la conformité à une réglementation pose question car, par définition, la réglementation est obligatoire. Son non-respect expose le contrevenant à des sanctions. À cet égard, « *présenter les droits conférés au consommateur par la loi comme constituant une caractéristique propre à la proposition faite par le professionnel* » peut être considéré comme une pratique commerciale réputée déloyale[5].

5 Annexe 1 point 10 de la directive 2005/29/CE du Parlement européen et du Conseil du 11 mai 2005 relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur et modifiant la directive 84/450/CEE du Conseil et les directives 97/7/CE, 98/27/CE et 2002/65/CE du Parlement européen et du Conseil et le règlement (CE) n° 2006/2004 du Parlement européen et du Conseil, JOUE, n° L 149, 11 juin 2005, p. 22.

Les exigences peuvent également s'appuyer sur les ***recommandations de l'autorité de contrôle***[6].

- La conformité du label français « E-vote » délivré aux prestataires de vote par Internet par la FNTC à la loi Informatique et libertés a été attestée par la CNIL dans une délibération du 17 mars 2016[7].

- En Suisse, les certifications *GoodPriv@cy* et OCPD:2014 délivrées par l'Association Suisse pour les Systèmes de Qualité et de Management (SQS) ont notamment pour référentiel les directives du Préposé sur les exigences minimales qu'un système de gestion de la protection des données doit remplir[8].

Le référentiel peut aussi se référer à des normes internationales, en particulier celles établies par l'Organisation internationale de normalisation (*International Organization for Standardization* – ISO). Une norme est ici entendue comme un « *document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné* »[9]. Son respect est volontaire.

En matière de protection des données personnelles, on trouvera des labels dont les critères sont créés en partie à partir d'une interprétation des normes[10] :

---

6 Délibération n° 2010-371 du 21 oct. 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, JORF, 24 novembre 2010.

7 Délibération n° 2016-071 du 17 mars 2016 portant avis sur un projet de label « E-vote » présenté par la Fédération des tiers de confiance, JORF, 28 avril 2016.

8 Préposé fédéral à la protection des données et à la transparence (PFPDT): directives sur les exigences minimales qu'un système de gestion de la protection des données (SGPD) doit remplir du 19 mars 2014, https://www.admin.ch/opc/fr/federal-gazette/2014/3015.pdf

9 Directives ISO/IEC, Partie 2 — Principes et règles de structure et de rédaction des documents ISO et IEC, 2016-04-30.

10 Pour appréhender l'éventail des normes en matière de protection de la vie privée, voir AFNOR Normalisation, Guide Protection des données personnelles: l'apport des normes volontaires, janvier 2017, http://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf

- ISO 27001 portant sur le système de management de la sécurité de l'information[11] : par exemple le label suisse SQS-OCPD précité, le label « Cloud » de l'association France IT pour les aspects sécurité ou le label *Datenschutzsiegel* de la société allemande d'audit DSZ Datenschutz Zertifizierungs GmbH

- ISO 17024 relative au fonctionnement homogène et fiable des organismes de certification qui mettent en œuvre des dispositifs particuliers de certification de personnes[12] avec l'*APEP-CertifiedPrivacy* en Espagne ou en Italie le *Certificazione del Personale Data Protection* délivré par Bureau Veritas Italie

- ISO 19011 relative à l'audit des systèmes de management[13] avec le label CNIL « Audit de traitements » et les labels allemands *Trust in Privacy* de la société Conformity Trust GmbH et *SCHUFA Datenschutz Siegel* de la SCHUFA Holding AG

- ISO 29190 qui propose une méthodologie qui permet à une organisation d'évaluer ses progrès dans le domaine de la protection de la vie privée[14] avec le label CNIL « Gouvernance Informatique et Libertés »

- ISO 29990 relative aux services de formation[15] avec le label CNIL « Formation »

- ISO 27018 relative aux bonnes pratiques pour la protection des informations personnelles identifiables dans l'informatique en nuage public[16] avec « EuroCloud Star Audit »

---

11 ISO/IEC 27001:2013 : Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences.

12 ISO/IEC 17024 :2012 : Évaluation de la conformité. Exigences générales pour les organismes de certification procédant à la certification de personnes publiée.

13 ISO/IEC 19011:2011 : Lignes directrices pour l'audit des systèmes de management.

14 ISO/IEC 29190:2015 : Méthodologie pour la maturité dans le domaine de la protection de la vie privée.

15 ISO/IEC 29990 :2010 : Services de formation dans le cadre de l'éducation et de la formation non formelles – exigences de base pour prestataires de services, 2010.

16 ISO/IEC 27018:2014 : Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII.

Enfin, le référentiel peut se fonder sur des instruments d'***auto-régulation***. Ces instruments, au processus d'élaboration très variable, sont généralement limités aux membres d'un groupe. Dans le cas des données personnelles, il s'agit principalement d'associations professionnelles rassemblant les acteurs du secteur du commerce et de la publicité en ligne.

► On trouve ici le code éthique de la marque de confiance espagnole *Confianza Online*[17], le code de conduite du label *BeCommerce* pour la vente à distance en Belgique[18], et le code déontologique de la FEVAD[19].

Le code déontologique de la FEVAD

Ce code précise que « *les entreprises adhérentes s'engagent à respecter les dispositions légales et réglementaires relatives à l'Informatique, aux Fichiers et aux Libertés, à la vie privée et à la protection des données* » ainsi que « *la déontologie mise en place par les professionnels du marketing direct et digital* »[20]. À cette fin, il rappelle certaines obligations légales et impose à tout adhérant FEVAD le respect du Système Liste Robinson – Stop Publicité.

Ce type d'instrument n'est cependant pas élaboré uniquement par des associations professionnelles, mais aussi par des sociétés.

► La *Market Research Society* (MRS) propose à travers sa marque « éthique » *Fair Data* de certifier dix principes fondamentaux qui viennent compléter la législation britannique sur la protection des données et des normes ISO[21].

17 https://www.confianzaonline.es/documentos/Ethical_Code.pdf

18 https://www.becommerce.be/files/Code_de_conduite_du_Label_de_Qualite_BeCommerce.pdf

19 http://www.fevad.com/wp-content/uploads/2016/09/FEVAD_Codepro_Vsept2015.pdf

20 https://www.fevad.com/le-code-professionnel-de-la-fevad-se-met-de-nouveau-a-jour/

21 http://www.fairdata.org.uk/10-principles/

Une procédure d'évaluation

La procédure d'évaluation permet d'apprécier la concordance entre les critères définis dans le référentiel et les pratiques de l'entité qui souhaite être labellisée. Lorsqu'elle est effectuée par une entité privée, elle donne généralement lieu à la conclusion d'un contrat de service entre le labellisateur et le candidat à la labellisation. La particularité juridique de ce contrat est que sa réalisation demeure incertaine.

De manière générale, l'appréciation d'une politique de protection des données personnelles prend la forme soit d'une auto-évaluation, soit d'un audit.

L'***auto-évaluation***, consiste simplement pour l'entreprise candidate à faire part de ses démarches en matière de protection des données personnelles, par exemple en répondant à des questions : ***l'organisme dit ce qu'il fait***. Le label est attribué si la déclaration correspond aux exigences du référentiel, ce qui n'est pas sans poser question lorsqu'il n'existe pas de vérification (cf. «L'effet potentiellement trompeur», page 126).

- Cette forme « souple » de signe de confiance est très présente dans les labels américains à l'instar du label *TRUSTe Privacy Seal* (désormais délivré par TrustArc) ou de BBBOnline. L'*European Interactive Digital Advertising Alliance* (EDAA) propose également une auto-certification aux entreprises participant au programme d'auto-régulation de l'*Online Behavioural Advertising* (OBA)[22].

- Les accords conclus entre l'Union européenne et les États-Unis, qu'il s'agisse du *Safe Harbor* invalidé par la Cour de l'Union européenne ou du *Privacy Shield*, reposent également sur une auto-évaluation, ce qui ne manque pas de faire l'objet de débats et d'interrogations au sein des États Membres de l'Union européenne[23].

22 Le formulaire est accessible à : https://www.dropbox.com/s/lqkvhl31vcab2si/Self-certification%20form.pdf?dl=0. Sur le *Privacy Shield*, voir Lettre n°5 de la **Chaire Valeurs et Politiques des Informations Personnelles**, décembre 2016 : *Privacy Shield : un bouclier à peine brandi déjà ébréché ?*, https://cvpip.wp.imt.fr/2016/12/05/privacy-shield-un-bouclier-a-peine-brandi-deja-ebreche/

23 Voir https://www.privacyshield.gov/article?id=Self-Certification-Information

De son côté, l'***audit*** vise à obtenir des preuves : ***l'organisme prouve ce qu'il fait*** en fournissant les dites preuves via des documents ou en permettant l'accès à son système d'information[24]. Sa nature diffère donc de celle d'un contrôle.

L'***audit sur pièces*** consiste pour le candidat à fournir des documents attestant la véracité de ses déclarations. À l'instar de la CNIL ou d'EuroPriSe, un auditeur vérifie la concordance en examinant les documents au regard du référentiel. À cette fin, il se réfère au guide d'audit qui décline chaque critère du référentiel et indique comment l'exigence peut être acceptée de façon objective. L'appréciation peut être effectuée de façon stricte. Parfois, des écarts sont tolérés : ils doivent être prévus et spécifiés.

Enfin, un ***audit sur site*** peut être mené par un évaluateur en ce qui concerne la conformité des organismes et des systèmes de management. Cet audit s'ajoute à l'examen des pièces par ce même expert au regard du référentiel. Tel est le cas des labels suisses *GoodPriv@cy* et DPCO délivrés par l'Association Suisse pour Systèmes de Qualité et de Management (SQS).

De manière générale, en matière de protection des données personnelles, la procédure d'évaluation est habituellement menée en interne par le labellisateur, à l'instar de la CNIL[25]. Ce dernier peut cependant recourir à des experts externes, comme EuroPriSe ou le label *BeCommerce* qui a choisi le certificateur Bureau Veritas. L'évaluateur externe peut être un organisme privé dont l'activité est la certification ou un expert. Le plus souvent, il doit être accrédité, ce qui renforce sa crédibilité. Notons que la Fédération des Tiers de Confiance du Numérique (FNTC) accrédite des évaluateurs externes qui ne sont pas choisis par le futur labellisé mais désignés via un système de tirage au sort afin de garantir une certaine indépendance. En Suisse, les organismes suisses ou étrangers qui effectuent des certifications au sens de l'article 11 de la loi sur la protection des données sont accrédités par le Service d'accréditation suisse, qui est associé au Préposé fédéral à la protection des données et à la transparence.

---

24 L'audit est défini par la norme NF ISO19011 comme un « *processus systématique, indépendant et documenté en vue d'obtenir des preuves et de les évaluer de manière objective pour déterminer dans quelle mesure des critères prédéterminés sont satisfaits* ».

25 Fair Data, Trusted Shops, confianza Online, TÜV Rheinland, DEKRA Certification, TÜV IT, SQS, etc.

Une attestation de conformité

Après avoir réalisé l'évaluation en matière de protection des données, le certificateur conclut à la conformité de l'entité dans l'hypothèse où elle satisfait les exigences du référentiel. Celui qui certifie peut être l'évaluateur comme la CNIL. Si tel n'est pas le cas, la mission du certificateur revient à vérifier les résultats de l'évaluation, à conclure à la conformité des procédures de traitement, du produit, du service analysés et à délivrer l'attestation de conformité.

L'approbation se traduit par une preuve matérielle, l'attestation de conformité, qui peut être délivrée pour une durée très variable (entre un an et cinq ans) soit par l'évaluateur lui-même, soit par le certificateur. Les attestations délivrées par les organismes privés sont en général payantes.

Sur le plan juridique, l'attestation de conformité est souvent une marque de conformité, c'est-à-dire une marque légalement déposée. Il en existe deux types : la marque collective et la marque de certification, huit États membres (l'Allemagne, la Belgique, l'Espagne, la France, le Luxembourg, les Pays-Bas, le Portugal et le Royaume-Uni) ayant mis en place un cadre juridique spécifique dédié à la marque de certification.

Une transparence

Pour instaurer la confiance à l'égard du client, un label implique la transparence et donc sa publicité. Concrètement, l'entreprise labellisée peut se voir attribuer un logo à l'effigie du label, qui peut être personnalisé avec mentions du numéro du label et de sa date d'expiration. Le labellisé peut faire apparaître le logo sur son site web ou ses documents de communication afin de se différencier de ses concurrents. Pour prévenir les fraudes (car on observe des tentatives d'usurpation de logos[26]), le logo peut aussi être numériquement distribué par une source située sur le site du labellisateur : le labellisé insère alors un lien hypertexte sur son site qui renvoie vers site du labellisateur[27]. Le logo peut aussi être hébergé sur un serveur contrôlé par l'organisme qui délivre le label[28].

---

26 Aux États-Unis, TRUSTe a fait condamner pour contrefaçon de marque les sites American-Politics.com et and SurfAssured.-com qui n'avaient pas été labellisés. *Standards in Electronic Transactions v Underwriters Digital Research Inc.*, US DC (Columbia), Civil Action No. 00–02574(CK).

27 Notamment PrivacyMark (online), Danish E-maerket, MRS Fair Data.

28 Par exemple, la marque de confiance Ecommerce Europe est liée à un certificat, tout comme les marques de confiance nationales de ses associations nationales membres. Pour utiliser le certificat, le logo doit être lié à l'adresse : https://ecommercetrustmark.eu/name-of-your-national-association.

Le logo est le signe physique à destination du public et des clients de l'entité labellisée, parce qu'il traduit la conformité de l'entreprise au référentiel, pour lui accorder leur confiance. Encore faut-il que cette marque de confiance soit connue, reconnue et facile à repérer, ce qui suppose en amont la mise en œuvre d'une politique de communication. Dans les faits, celle-ci est quasi-inexistante. Pourtant, la médiatisation est un outil important pour le succès du label. Preuve en est avec le label rouge.

Le logo ne constitue pas le seul indice visible de l'octroi d'un label. Dans certains cas, le public et les clients ont accès aux éléments qui motivent la labellisation comme par exemple le rapport de l'évaluateur et les conclusions de conformité du certificateur. Mais il est rare, si l'on excepte EuroPriSe et EuroCloud Star Audit qui publient les rapports de certification, d'en trouver une quelconque publication. Toutefois, certaines organisations mettent en ligne à disposition du public un registre des entreprises[29] auxquelles elles ont délivré un label, ainsi que les attestations de conformité[30].

Des contrôles, recours et sanctions

L'information du public implique aussi de mettre 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, il s'avère que la plupart des labels existants taisent leur existence (cf. Chapitre 7).

29 Par exemple, Confianza online, Seriedad online, Good Priv@cy.

30 Par exemple, Danish E-maerket, ePrivacySeal.

Chapitre 6. Les labels visant à prouver la conformité : de l'implémentation du cadre réglementaire et au-delà

Claire Levallois-Barth
Delphine Chauvet

6

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.).

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

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.* »

Chapitre 7. Les labels visant à susciter la crédibilité : des pratiques existantes vers l'amélioration de qualité

Claire Levallois-Barth

7

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.

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

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.* »

Rédigé 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 » désigné 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.

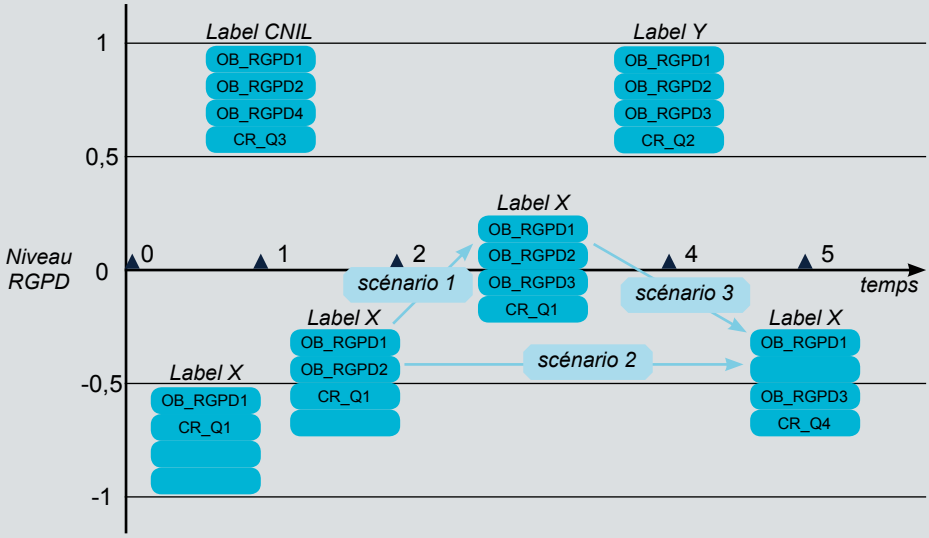


Figure 1. *Les effets de confusion*

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/.

«Assemblée» – Thierry Citron

Chapitre 8. Les mécanismes de labellisation issus du Règlement général sur la protection des données (RGPD)

Claire Levallois-Barth

8

Le 27 avril 2016, l'Union européenne a adopté le règlement (UE) 2016/679 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, abrogeant la directive 95/46/CE (Règlement général sur la protection des données ou RGPD)[1]. Le texte, entré en vigueur le 25 mai 2016, est applicable à partir du 25 mai 2018. À cette date, la loi française Informatique et Libertés devrait être en grande partie modifiée.

Le RGPD se situe dans la continuité de la directive européenne 95/46/CE (Directive Protection des données)[2] : il reprend les principes de protection existants (licéité, loyauté, transparence, limitation des finalités, minimisation et exactitude des données, limitation de la conservation, niveau de protection adéquat pour les flux transfrontières de données, protection renforcée des données sensibles, etc.) tout en ajoutant de nouvelles obligations (droit à la portabilité des données personnelles, droit à l'oubli numérique, etc.)[3]. Une des

1 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JOUE, n° L 119, 4 mai 2013, p. 1.

2 Directive 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, n° L 281, 23 novembre 1995, p. 31.

3 Voir Levallois-Barth, C. (2017). Données personnelles : une réforme européenne pour un 21e siècle numérique, Revue TELECOM 185, juin 2017, https://cvpip.wp.imt.fr/062017-donnees-personnelles-une-reforme-europeenne-pour-un-21eme-siecle-numerique/

Les mécanismes de labellisation issus du Règlement général sur la protection des données (RGPD)

nouveautés est constituée par la possibilité de « *certifications, labels ou marques en matière de protection des données personnelles* ».

En effet, le RGPD utilise les trois termes : ***certification***, ***label*** et ***marque***. Dès lors, existe-il une différence entre ces trois notions et si oui, laquelle ?

De façon classique, le règlement conçoit la certification comme un signe de conformité, signe qui prendrait la forme d'un label. Il stipule ainsi que « *lorsque les critères sont approuvés par le comité [Comité Européen de Protection des Données ou CEPD], cela peut donner lieu à une certification commune, le label européen de protection des données* »[4].

En ce qui concerne le terme « marque » et la confusion qu'il peut apporter, deux interprétations sont possibles. Selon la première, son emploi pourrait être interprété comme la volonté de laisser la porte ouverte à l'éventuelle inscription des signes de confiance au sein du droit européen des marques[5]. En France par exemple, il s'agit d'une marque déposée protégeant les droits des parties tierces autorisées à les utiliser. La reconnaissance juridique confère au propriétaire un droit exclusif d'utiliser la marque dont l'utilisation non autorisée et déloyale peut donner lieu à une action civile pour contrefaçon[6]. Selon la seconde interprétation, et au vu de certaines propositions avancées lors des négociations

4 Art. 42-5 du RGPD.

5 Dans ce sens, Lachaud, E., (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. Computer Law & Security Review 32, 814–826. https://doi.org/10.1016/j.clsr.2016.07.001

6 Art. L. 716-1 du Code de propriété intellectuelle.

sur le Règlement, on peut penser que la différence entre les « labels » et les « marques en matière de protection des données » reste essentiellement rhétorique[7]. Ainsi, le Parlement européen a assimilé les deux notions lorsqu'il a proposé que « *les autorités de contrôle octroient […] la marque standardisée de protection des données dénommée label européen de protection des données* »[8]. Concrètement, on note que les articles 42 « Certification » et 43 « Organismes de certification » du RGPD se focalisent dans leurs intitulés sur la seule certification.

Plus précisément, l'article 42 énonce l'objectif de la certification, qu'il conçoit comme un outil de démonstration de la conformité (8.1.). Pour autant, les modalités même de délivrance d'une certification, d'un label ou d'une marque ne sont pas à ce jour entièrement connues, le RGPD comprenant certaines options (8.2.) et laissant entrevoir plusieurs perspectives de mis en œuvre (8.3.).

8.1. Les mécanismes de certification, éléments participant à la démonstration du respect de la législation

Ainsi, le label, à côté de la certification et de la marque en matière de données personnelles, permet à l'entité de « prouver » (il s'agit ici d'une présomption de preuve) qu'elle a mis en place des mesures appropriées et efficaces pour respecter la législation. Cette faculté s'inscrit dans le cadre d'une nouvelle obligation, l'obligation de « responsabilité » ou « *accountability* » (voir ci-contre).

Parfois traduite par « *l'obligation de rendre des comptes* », elle implique de « *met[tre] en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est effectué conformément au […] règlement* »[9]. L'objectif est de s'assurer que l'entité qui collecte et traite des données personnelles a mis en place des outils pratiques en vue de garantir la protection effective des données[10].

---

7 Dans ce sens, Lachaud, E., (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. Computer Law & Security Review 32, 814–826. https://doi.org/10.1016/j.clsr.2016.07.001, précité.

8 Résolution législative du Parlement européen du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil 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 (Règlement général sur la protection des données) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), art. 39 1 sexies

9 Art. 24-1 du RGPD.

10 Dans ce sens, Groupe de travail « Article 29 » sur la protection des données, avis n° 3/2010 sur le principe de responsabilité adopté le 13 juillet 2010, WP 173, p. 3, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf

Le principe de responsabilité (« accountability »)

Dès 1980, le principe de responsabilité est reconnu explicitement dans les lignes directrices régissant la protection de la vie privée de l'Organisation de Coopération et de Développement Économiques (OCDE). Ainsi, le point 14 précise : « Principe de la responsabilité » : « *Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.* » Il est l'un des principaux concepts du cadre défini par l'Organisation Économique pour l'Asie-Pacifique (APEC) pour la protection de la vie privée (point 26 de l'*APEC Privacy Framework*). Il figure également dans la dernière version du projet de norme ISO 29100 établissant un cadre pour le respect de la vie privée.

Ces outils peuvent notamment consister à appliquer une politique de protection des données, un code de conduite approuvé ou des mécanismes de certification approuvés. Ainsi, la certification n'est pas obligatoire mais conçue comme un élément laissé au choix du responsable de traitement et tenant à la situation particulière des opérations de traitements qu'il opère. Elle lui permet de prouver qu'il a mis en place des mesures appropriées et efficaces pour respecter la législation, en particulier pour attester du respect des deux exigences : celle, classique, de sécurité du traitement, et l'obligation nouvelle de garantir que la protection des données est assurée dès la conception du traitement (*Data Protection by design*) et par défaut (*Data Protection by default*)[11]. La certification va également permettre au responsable de traitement de prouver qu'il a fait appel à un sous-traitant présentant des « *garanties suffisantes* »[12]. Enfin, elle intervient lors du prononcé des sanctions, les autorités de contrôle devant la prendre en compte pour décider, s'il y a lieu, d'imposer une amende administrative et pour en fixer le montant[13].

Ce faisant, ce système de présomption simple est conçu comme un outil qui doit :

- engendrer au niveau du responsable de traitement une sécurité juridique en lui permettant de prouver que les données personnelles qu'il transmet à un autre responsable de traitement ont été collectées et peuvent être utilisées en toute légalité.

11 Voir *« Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth, p.67.

12 Voir considérant 81 et art. 28-5 du RGPD.

13 Art. 83-2(j) du RGPD.

- aider les utilisateurs-consommateurs à visualiser rapidement le niveau de protection de leurs données[14].

Le renforcement de la transparence s'opère à un double niveau : celui de la personne concernée (B2C) et celui des responsables de traitements (B2B). Elle concerne ainsi toute la chaîne d'utilisation des données personnelles, de leur collecte à leur transmission, en passant par leur sous-traitance.

La certification s'adresse en effet aux responsables de traitement et aux sous-traitants, qu'ils relèvent ou non du champ d'application du RGPD. Il s'agit d'un aspect important : offrir la possibilité à un organisme établi dans l'Union européene de transférer de façon légale des données personnelles à un organisme certifié RGPD, même si le pays dans lequel sont envoyées les données ne dispose pas d'un niveau de protection adéquat. Cette forme d'***exportation de la norme européenne*** de protection des données doit permettre aux entreprises non européennes d'entrer plus facilement sur le marché européen.

Transfert de données personnelles en dehors de l'Union européenne (articles 45 et 46 du RGPD)

Lors d'un transfert de données personnelles en dehors de l'Union européenne, le RGPD stipule, à l'instar de la directive 95/46/CE Protection des données, que le transfert ne peut avoir lieu que vers un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, ou une organisation internationale, qui assure un niveau de protection adéquat. Ce niveau de protection est reconnu par la Commission européenne, chargée de publier des décisions dites d'adéquation.

En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant peut transférer des données s'il prévoit des « *garanties appropriées* ».

14 Cons. 100 du RGPD.

Parmi ces garanties, figurent des règles internes d'entreprise, des clauses contractuelles, un code de conduite approuvé ou « *un mécanisme de certification approuvé […] assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées* ». Les garanties peuvent aussi prendre la forme d'un accord international, à l'instar de l'accord conclu en juillet 2016 entre les États-Unis et l'UE, le *Privacy Shield* et dont les modalités mêmes de mise en œuvre ne sont pas sans poser question[15].

8.2. Les options de mise en œuvre

Le RGPD retient une formulation souple qui permet à tous les schémas de labellisation existants de coexister, qu'il s'agisse d'un label public délivré au niveau national ou de l'UE, ou bien d'un label délivré par une association ou un organisme privé. De son côté, l'organisme de certification privé devra obtenir un agrément qui, lui aussi, pourra être accordé de différentes manières.

Des labels délivrés soit par une autorité publique, soit par une entité privée

Selon les règles fixées par le RGPD, un label pourra être délivré sur la base de critères approuvés et publiés par l'autorité de contrôle compétente, sur son territoire (en France, la CNIL)[16]. Les critères pourront également être approuvés par le Comité Européen de la Protection des Données (CEPD)[17]. Dans ce cas, ils donneront lieu à une certification commune, le label européen de protection des données[18]. Cependant, le RGPD ne précise pas la façon dont les critères seront définis. Notamment, il ne prévoit pas une consultation des parties prenantes (l'industrie, les organisations non gouvernementales…), contrairement à

15 Voir Levallois-Barth, C., Meseguer, I. (2016). *Privacy Shield* : un bouclier à peine brandi déjà ébréché ?, Éditorial de la lettre d'information trimestrielle n° 5 de la **Chaire Valeurs et Politiques des Informations Personnellles**, décembre 2016 : https://cvpip.wp.imt.fr/2016/12/05/privacy-shield-un-bouclier-a-peine-brandi-deja-ebreche/

16 Art. 58-3(f) du RGPD.

17 Composé du chef d'une autorité de contrôle de chaque État membre et du Contrôleur européen de la protection des données, ou de leurs représentants respectifs, le CEPD disposera notamment de la personnalité juridique et de pouvoirs renforcés.

18 Art. 42-5 du RGPD.

ce qu'il prévoit pour l'élaboration d'un code de conduite[19]. Ce type de consultation, qui a été proposé par le Parlement européen en première lecture, constitue pourtant une pratique établie dans le domaine de la certification.

Afin d'obtenir un label valide pour une durée maximale de trois ans, avec possibilité de renouvellement, un responsable de traitement ou un sous-traitant pourra s'adresser soit à une autorité de contrôle, soit à une entité privée par exemple AFNOR certification, *British Standard Institut* ou Bureau Veritas. Les deux types d'entités (publique ou privée) pourront délivrer des labels sur la base de critères approuvés au niveau national (par l'autorité de contrôle) ou de l'UE (par le CEPD).

Les possibilités seront donc :

- un label européen établi au niveau de l'UE délivré par une autorité de contrôle nationale
- un label européen établi au niveau de l'UE délivré par un organisme privé de certification
- un label basé sur des critères nationaux délivré par une autorité de contrôle nationale
- un label basé sur des critères nationaux délivré par un organisme privé de certification

Ce recours aux entités publiques et privées reflète le compromis adopté : tandis que le Parlement européen proposait que ce rôle soit conféré aux seules autorités nationales de contrôle en matière de protection des données personnelles (désignées également dans cet ouvrage comme « autorité de protection des données »), la Commission européenne et le Conseil européen préféreraient accréditer des auditeurs privés.

19 cf. cons. 99 du RGPD « *Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations.* »

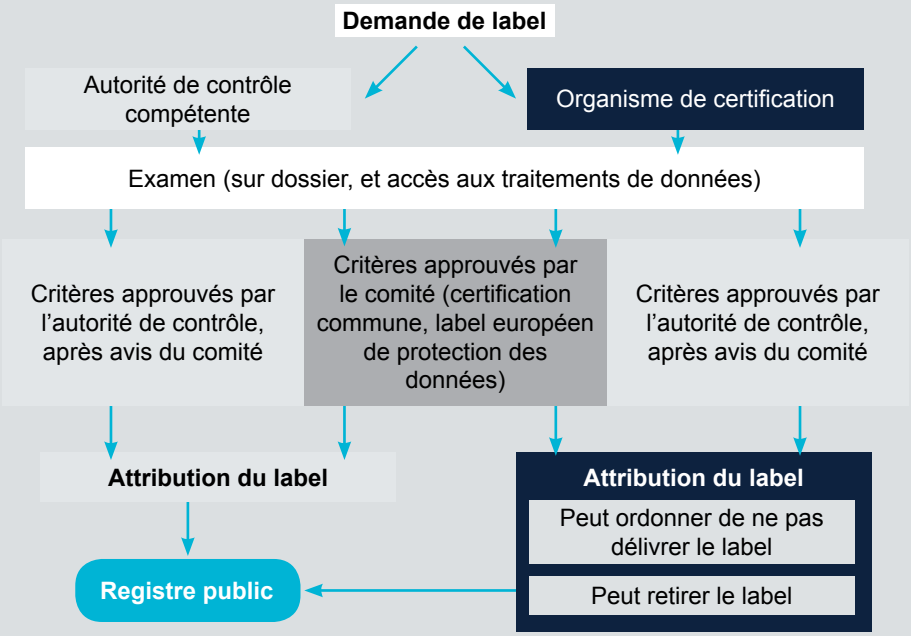


Figure 2. RGPD : délivrance d'une certification / d'un label

Autorité de contrôle compétente (Article 56 du RGPD)

L'autorité de contrôle compétente est l'autorité de l'établissement principal ou de l'établissement unique du responsable du traitement ou du sous-traitant. Si le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres, son établissement principal correspond en principe au lieu de son administration centrale dans l'Union.

Ces principes connaissent toutefois des exceptions.

En ce qui concerne le responsable de traitement : lorsque les décisions quant aux finalités et aux moyens du traitement sont prises dans un autre de ses établissements et que cet établissement a le pouvoir de faire appliquer ses décisions, cet établissement doit être considéré comme l'établissement principal ;

En ce qui concerne le sous-traitant : s'il ne dispose pas d'une administration centrale dans l'Union, il convient de retenir l'endroit où se déroule l'essentiel des activités de traitement.

Pour autant, le RGPD ne mentionne pas les modalités de reconnaissance mutuelle : on ignore quel statut une autorité de contrôle compétente dans un État A accordera à un label délivré conformément au RGPD dans un État B par une autorité compétente ou par un organisme privé[20]. Il prévoit, en tout cas, que les labels ainsi que tous les mécanismes de certification seront consignés dans un registre public tenu par le CEPD[21].

Que le label soit délivré par une entité publique ou privée, le responsable de traitement devra fournir toutes les informations pertinentes ainsi que l'accès à ses activités de traitements. Lorsque l'évaluation sera effectuée par un organisme de certification, cet organisme devra communiquer à l'autorité de contrôle les raisons de la délivrance du label et, le cas échéant, les éléments justifiant son retrait. L'autorité pourra retirer une certification ou ordonner à l'organisme de certification de ne pas délivrer un label si les exigences applicables ne sont pas ou plus satisfaites. Les autorités de contrôle acquièrent donc avec le RGPD de nouveaux pouvoirs.

On note, à cet égard, que le RGPD n'aborde pas la question du coût de la certification, alors que le Parlement européen avait proposé de préciser qu'elle puisse s'effectuer « *moyennant le paiement de frais raisonnables tenant compte des coûts administratifs* », « *au travers d'un processus transparent et ne présentant pas de complications injustifiées* » via « *des redevances harmonisées* »[22].

Comme nous venons de le voir, l'harmonisation proposée par le RGPD est loin d'être totale, la certification pourra être délivrée au choix soit par une autorité de contrôle, soit par un organisme de certification « *disposant d'un niveau d'expertise approprié* »[23]. Dans ce dernier cas, l'entité privée sera mise « *sous surveillance* ».

Des organismes de certification privés mis sous surveillance

Ainsi, le RGPD fixe des critères communs pour les organismes de certification. Il illustre une tendance générale qui fait évoluer « *le modèle actuel de la certification vers*

20 En Suisse, l'article 7 de l'Ordonnance sur les certifications en matière de protection des données (OCPD) du 28 septembre 2007 intitulé "Reconnaissance des certifications étrangères » précise que la reconnaissance est effectuée par le Préposé, après avoir consulté le Service d'accréditation suisse, https://www.admin.ch/opc/fr/classified-compilation/20071826/index.html

21 Art. 42-8 du RGPD.

22 Art. 39 1 sexies, 39 1bis et 1ter « Certification » de la résolution législative du Parlement européen du 12 mars 2014, précitée.

23 Art. 42-5 du RGPD.

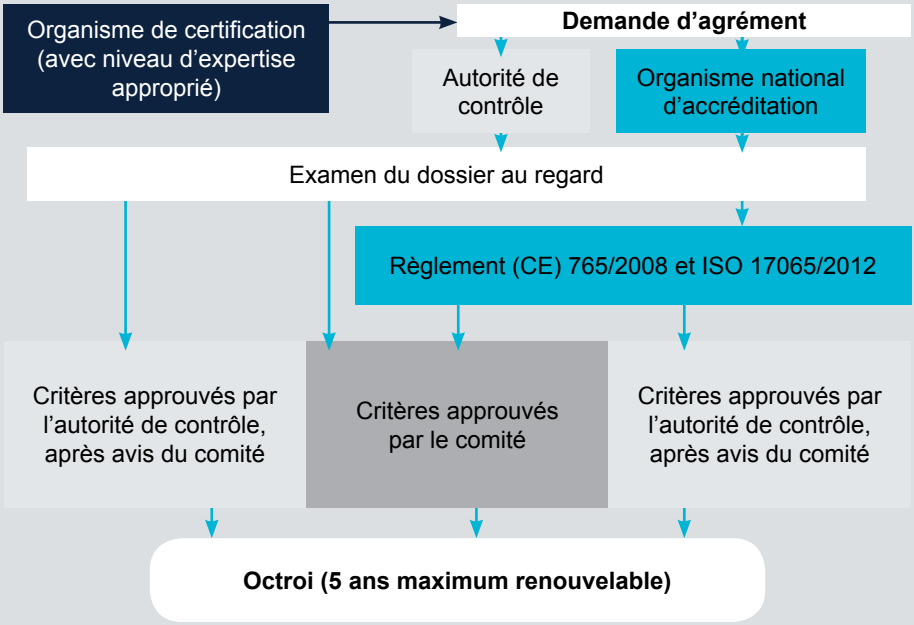


Figure 3. RGPD : agrément d'un organisme de certification

une posture interventionniste visant à écarter l'influence des organismes de certification insuffisamment compétents, indépendants ou impartiaux… »[24]. En la matière, il laisse le choix à chaque État quant aux modalités de mise sous surveillance des organismes de certification. Ainsi, un organisme pourra être agréé pour cinq ans maximum :

- soit par une autorité de contrôle nationale (en France, la CNIL qui voit ainsi ses pouvoirs d'autorisation renforcés)
- soit par le CEPD
- soit par l'organisme national d'accréditation[25]

24 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. 353.

25 Art. 43-1 du RGPD et article 70-1(o) du RGPD.

Pour ce troisième cas, le RGPD précise que l'organisme national d'accréditation sera « *désigné conformément au règlement (CE) no 765/2008 du Parlement européen et du Conseil*[26]*, conformément à la norme EN-ISO/IEC 17065/2012*[27] *et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56* ». Ainsi, cet organisme, en France le Comité français d'accréditation, le Cofrac, devra de façon classique se conformer aux exigences d'un règlement UE, le Règlement (CE) n°765/2008, et ce qui est beaucoup moins courant, d'une norme ISO. Cette exigence n'est pas sans poser question puisqu'il s'agit par définition d'une norme volontaire adoptée par consensus au sein d'une organisation internationale et non d'un organe de l'UE.

Par ailleurs, le Règlement (CE) no 765/2008 exige qu'un État membre désigne un seul et unique organisme d'accréditation afin de prévenir toute concurrence. Or, le RGPD laisse la possibilité aux États membres de choisir entre deux options : un organisme de certification pourra se faire agréer soit par une autorité de contrôle, soit par un organisme national d'accréditation. Sur quels critères son choix se basera-t-il ? La vigilance s'impose à cet égard.

Quelle que soit l'option retenue, l'organisme de certification sera agréé sur la base de critères rédigés et publiés par l'autorité de contrôle, après avis du CEPD, ou par le CEPD lui-même. Il sera soumis à certaines obligations institutionnelles et procédurales : non seulement il devra s'engager à respecter les critères approuvés par l'autorité de contrôle ou le CEPD, mais aussi démontrer son indépendance et son expertise en matière de protection des données personnelles, ainsi que l'absence de conflit d'intérêt dans l'accomplissement de ses missions.

Par ailleurs, il devra mettre en place des procédures qui concerneront « *la délivrance, l'examen périodique et le retrait d'une certification* », le traitement « *des réclamations relatives aux violations de la certification ou à la manière dont [elle est] appliquée* »[28]. Il devra « *définir la façon dont ces procédures et structures sont rendues transparentes à l'égard*

---

26 Règlement (CE) n°765/2008 du 09/07/08 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil, JOUE, n° L 218, 13 aout 2008, p. 1.

27 ISO/CEI 17065:2012 relative à l'évaluation de la conformité – Exigences pour les organismes certifiant les produits, les procédés et les services.

28 Art. 43-2 du RGPD.

des personnes concernées et du public». Alors seulement, son nom figurera dans le registre public tenu par le CEPD[29].

L'autorité de contrôle compétente ou l'organisme national d'accréditation pourront retirer un agrément si ces conditions ne sont pas ou plus réunies. Si les mesures prises constituent une violation du RGPD, l'organisme de certification pourra, en outre, faire l'objet d'une amende administrative pouvant s'élever jusqu'à 10 000 000€ ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu[30].

8.3. Les perspectives de mise en œuvre du RGPD et le rôle des instances publiques

Pour les raisons que nous venons d'évoquer, le RGPD n'impose pas la mise en place de mécanismes de certification, labels ou marques en matière de protection des données, mais «encourag[e]» simplement les États membres, les autorités de contrôle, le CEPD et la Commission européenne dans cette démarche[31]. Le feront-ils? Et surtout quelles formes cet «encouragement» prendra-t-il? En pratique, le RGPD implique d'être décliné dans la législation secondaire soit au niveau national, soit au niveau européen.

L'harmonisation du référentiel

Pour l'instant, la Commission européenne s'interroge sur la pertinence d'adopter des actes délégués ou des actes d'exécution[32] et a choisi la voie classique de la normalisation pour travailler sur un référentiel commun, face à l'inaction de l'industrie. Déjà en 2006, la Commission européenne a demandé au secteur privé «*d'élaborer des systèmes abordables pour la certification de sécurité des produits, processus et services qui répondent à des besoins spécifiques de l'UE (notamment en ce qui concerne le respect de la vie*

29 Art. 70-1(o) du RGPD.

30 Art. 83-4b du RGPD.

31 Art. 42-1 du RGPD.

32 Cette possibilité est introduite par les articles 43-8 et 43-9 du RGPD.

privée)», favorisant une approche d'auto-régulation[33]. En l'absence de réaction tangible, elle a annoncé en 2010 son intention d'examiner «*la possibilité d'instaurer des régimes européens de certification (par exemple, des «labels de protection de la vie privée») pour les processus, technologies, produits et services*»[34]. Début 2015, elle a adopté un mandat chargeant les organismes européens de normalisation d'élaborer «*des normes européennes et des publications en matière de normalisation européenne pour la gestion du respect de la vie privée et de la protection des données à caractère personnel*»[35]. Le mandat se focalise sur le respect de la protection des données dès la conception et par défaut et ainsi que sur les obligations de sécurité[36]. Pour y répondre, le Comité européen de normalisation (CEN) et le Comité européen de normalisation en électronique et en électrotechnique (CENELEC) ont créé un comité de travail conjoint, le JWG 8 «*Privacy management in products and services*»[37].

De son côté, le G29, qui avait prévu d'adopter fin décembre 2016 des lignes directrices sur la certification, en a reporté la publication.

Il est vrai que le sujet se révèle complexe, notamment parce que seules les autorités de contrôle françaises et allemandes possèdent une certaine pratique en matière de labellisation. De son côté, l'autorité de contrôle britannique, l'*Information Commissioner Office* (ICO), a annoncé qu'elle travaillait à la création d'un label «Vie privée» reposant sur un

33 Communication de la Commission au Conseil, au Parlement européen, au Comité économique et social européen et au Comité des régions, Une stratégie pour une société de l'information sûre – Dialogue, partenariat et responsabilisation, COM(2006) 251 final, Bruxelles, 31.05.2006, p. 11, http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:52006DC0251

34 Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, Une approche globale de la protection des données à caractère personnel dans l'Union européenne, COM(2010) 609 final, Bruxelles, le 4.11.2010, p. 14, http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_fr.pdf

35 Décision d'exécution de la Commission européenne du 20 janvier 2015 relative à une demande de normalisation aux organisations européennes de normalisation concernant des normes européennes et des publications en matière de normalisation européenne pour la gestion du respect de la vie privée et de la protection des données à caractère personnel, conformément à l'article 10, paragraphe 1, du Règlement (UE) n° 1025/2012 du Parlement européen et du Conseil à l'appui de la directive 95/46/CE du Parlement européen et du Conseil et à l'appui de la politique industrielle en matière de sécurité de l'Union, C(2015) 102 final, Bruxelles, le 20 janvier 2015, http://ec.europa.eu/transparency/regdoc/rep/3/2015/FR/3-2015-102-FR-F1-1.PDF

36 Annexe de la décision d'exécution de la Commission du 20 janvier 2015, C(2015) 102 final, précitée, http://ec.europa.eu/transparency/regdoc/rep/3/2015/FR/3-2015-102-FR-F1-1-ANNEX-1.PDF

37 http://www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Privacy/Pages/default.aspx

logo déposé sous forme de marque commerciale[38]. La certification serait effectuée par des organismes tiers privés accrédités par l'organisme national *UK Accreditation Services* (UKAS). Les autorités de contrôle doivent donc d'abord partager leurs expériences pour acquérir une culture commune. Concrètement, la certification a fait partie des thèmes discutés lors du premier Fablab organisé par la Présidence du G29 le 26 juillet 2016, ce qui démontre son importance. Partie intégrante du processus de co-construction, ce Fablab a réuni une centaine de personnes – représentant à la fois les autorités de protection des données, la société civile et les industriels – afin d'alimenter la réflexion.

L'adoption des lignes directrices par le G29

Afin de préciser la mise en œuvre du RGPD, le G29 élabore des lignes directrices en recourant à une méthode particulière. Tout d'abord, il sélectionne les thèmes de travail. Une consultation publique est ensuite organisée. Puis le contenu du texte est discuté lors d'une réunion appelée « Fablab » à Bruxelles avec les représentants des autorités de protection des données, la société civile et les industriels. Une première version des lignes directrices est ensuite publiée (v1). Elle est soumise à une deuxième consultation des parties prenantes, pour aboutir à la publication d'une deuxième version (v2) [39].

L'harmonisation des schémas de certification

Sur le fond, il s'agit de préciser les modalités d'application du RGPD, mais aussi de réguler le marché intérieur des services de certification en matière de protection des données personnelles. En effet, ainsi que le souligne le G29, « *l'expérience dans d'autres domaines, et notamment dans la certification des marchandises, a montré une tendance au nivellement par le bas. La concurrence entre prestataires pourrait conduire à une baisse des prix, ainsi qu'à une certaine souplesse, voire à un assouplissement des procédures… des règles semblent nécessaires pour garantir la bonne qualité des services et des conditions égales pour tous* »[40]. Les interrogations portent alors sur les modalités et le niveau

38 https://iconewsblog.wordpress.com/2015/08/28/whats-the-latest-on-the-ico-privacy-seals/

39 Pour consulter les différentes lignes directrices adoptées : http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

40 Groupe de travail «Article 29» sur la protection des données, avis n° 3/2010 sur le principe de responsabilité adopté le 13 juillet 2010, WP 173, n° 67, p. 20, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_fr.pdf

d'intervention des autorités publiques européennes et nationales, compte tenu des nombreuses marges de manœuvre laissées aux États membres[41].

À cet égard, Eric Lachaud examine la possibilité de prendre en compte l'expérience du marquage CE dans le cadre de l'Internet des objets[42] qui se fonde sur le schéma suivant[43] :

- le législateur européen émet des exigences dites de « haut niveau » via les directives « Nouvelle approche »
- les organismes de normalisation les complètent avec des normes techniques
- les fabricants ou les organismes de certifications privés vérifient et certifient la conformité aux normes techniques
- les autorités nationales des États membres surveillent les fabricants et les organismes de certifications sur leur propre marché

Dans ce modèle de corégulation, la Commission européenne adopterait une norme obligatoire en matière de données personnelles et l'organisme s'auto-certifierait, ce qui aurait pour avantage d'introduire une certaine flexibilité, faciliterait l'implication des petites et moyennes entreprises et réduirait le coût de la labellisation. Cette solution présente toutefois deux inconvénients. D'une part, le marquage CE introduit une certaine confusion auprès du consommateur : il atteste qu'un produit est présumé conforme à une norme européenne et non que le produit est fabriqué dans l'Union européenne. D'autre part, son schéma ne concerne actuellement que les produits. Il devrait donc être adapté aux services, personnes et procédures en matière de données personnelles. En outre, le silence du RGPD sur ce sujet semble plutôt augurer du choix d'un label spécifique « Données personnelles ».

41 Voir Tambou, O., (2016). L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ?, Revue Lamy de Droit de l'Immatériel, avril 2016, pp. 51-54 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2768093.

42 Voir E. Lachaud qui propose d'élargir le périmètre du marquage CE à la protection des données personnelles, in Lachaud, E., (2016). Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things? *In Data Protection on the Move* (pp. 135-162). Springer Netherlands.

43 Décision du conseil 93/465/EEC du 22 juillet 1993, concernant les modules relatifs aux différentes phases des procédures d'évaluation de la conformité et les règles d'apposition et d'utilisation du marquage «CE» de conformité, destinés à être utilisés dans les directives d'harmonisation technique, JOCE, n° L 220, 30 août 1993, p.23.

Rowena Rodrigues propose quant à elle un schéma qui n'est pas si éloigné de celui du marquage CE : il s'agirait d'adopter une norme obligatoire relative aux analyses d'impact[44]. L'organisme effectuerait son analyse et s'auto-certifierait. La vérification serait confiée soit aux autorités de protection des données qui effectueraient des contrôles, soit aux organismes de certification privés chargés de conduire des audits une ou deux fois par an. Les plaintes et réclamations seraient d'abord déposées auprès de l'organisme labellisé, avant d'être introduites devant une juridiction ou une autorité de contrôle.

Il peut aussi être envisagé d'établir des labels au niveau national. Cette solution ménagerait à la fois les autorités de contrôle et les marchés nationaux de la certification mais poserait des difficultés d'articulation. Le risque est que les entités souhaitant être labellisées se tournent vers des labels moins exigeants, plus faciles à obtenir et au retour sur investissement plus important, la certification étant « *une activité marchande ordinaire pleinement ouverte à la concurrence* »[45].

Si l'option de la labellisation délivrée par les autorités de contrôle est retenue, ces autorités devront avoir les moyens humain et financier de leur ambition. Cela sera-t-il vraiment le cas dans un contexte de restriction budgétaire ? Elles devront également veiller à éviter toute discrimination, à ne pas être « juge et partie », cet écueil étant souvent avancé par les personnes interrogées.

Parole d'un avocat

« *Celui qui sanctionne ne peut pas être le labellisateur… car la tentation serait naturellement de privilégier ceux qui ont le label CNIL au détriment de ceux qui ne l'ont pas mais qui pourraient avoir… d'autres labels plus exigeants que le label CNIL sans pour autant créer de présomption de conformité.* »

Afin de démultiplier les possibilités de labellisation, ne vaut-il pas mieux dédier les moyens à la surveillance du niveau d'indépendance et de compétence des experts travail-

44 Voir Rodrigues, R., Wright, D. and Wadhwa, K. (2013). Developing a privacy seal scheme (that works), International Data Privacy Law Advance Access, published February 1, 2013, 17 pages,. p. 15.

45 Avis de l'Autorité de la concurrence n° 15-A-16 du 16 novembre 2015 portant sur l'examen, au regard des règles de concurrence, des activités de normalisation et de certification, point 51, http://www.autoritedelaconcurrence.fr/pdf/avis/15a16.pdf

lant pour les organismes de certification privés ? Il faut en tout cas veiller à établir les modalités de coopération entre les autorités de contrôle et les organismes nationaux d'accréditation. Il s'agit à la fois de contrôler l'ensemble des schémas de labellisation et d'articuler la labellisation « Données personnelles » avec les certifications proposées dans d'autres domaines, comme celui de la sécurité.

Reste l'épineuse question du niveau de protection : faut-il concevoir la certification comme un facilitateur permettant à un organisme de démontrer sa conformité à des critères de qualité ou positionner le label sur un niveau de protection globale allant au-delà de la législation à l'instar des labels délivrés par la CNIL ? L'écueil est alors de réglementer « dans les détails », de trop réguler et de ne pas répondre aux attentes des parties prenantes, en particulier des petites et moyennes entreprises.

Un long parcours reste donc à accomplir pour voir un jour exister des « labels » européens apportant en un seul coup d'œil une information précise et crédible au citoyen. Le risque est au contraire d'ajouter de la confusion dans un domaine particulièrement complexe.

Chapitre 9. Analyse économique des marques de confiance

Patrick Waelbroeck
Antoine Dubus

9

Nous analysons à présent les défis économiques associés aux labels de protection des données personnelles et aux marques de confiance. Nous développons tout d'abord la notion d'asymétrie d'informations, qui fait que les consommateurs sont en recherche de signaux pour évaluer la confiance qu'ils peuvent avoir dans les produits ou services proposés (9.1.). Nous poursuivons par l'analyse de la demande de protection de la vie privée et des données personnelles : quelles sont les sources d'externalités négatives et la forme qu'elles prennent (9.2.) ? Quelle est en regard l'offre de sécurité et de protection des données clients proposée par les entreprises (9.3.) ? Nous terminons ce chapitre en discutant les différents modèles économiques associés au processus de labellisation (9.4.).

9.1. La notion d'asymétrie d'informations

L'économie numérique est désormais « axée sur les données ». Les entreprises Internet telles qu'Amazon ou Criteo utilisent les données personnelles pour développer leurs modèles commerciaux en fonction de recommandations de produits et du ciblage publicitaire[1]. Ces informations peuvent résulter de contributions volontaires (un consommateur commentant un blog ou évaluant la qualité d'un produit ou la réputation d'un vendeur) ou de traces involontaires (laissées par un internaute dans son historique de navigation). Cela soulève la question de savoir quels types de données sont utilisés par les entreprises et quels sont les risques pour les consommateurs. Les données utilisées à mauvais es-

1 Voir www.criteo.fr pour une description de leurs offres d'affaires

Analyse économique des marques de confiance

cient peuvent conduire à des externalités négatives telles que la fraude, le harcèlement, le spam, le piratage, le vol d'identité, etc. Ces externalités négatives résultent d'une défaillance du marché lorsque les actions d'un agent économique exercent un effet négatif sur d'autres agents sans compensation liée à un mécanisme de marché.

Ces risques sont présents au stade de la collecte, de l'exploitation et de la transmission des données. Néanmoins, ils sont difficiles à appréhender pour le consommateur. D'une part, il lui est difficile de vérifier comment ses données sont utilisées par les compagnies qui les collectent et les traitent et de savoir si cette utilisation est conforme ou non à la législation. Ceci est d'autant plus vrai à l'ère du *Big Data* où des bases de données indépendantes avec peu d'informations personnelles peuvent être combinées facilement pour identifier une personne. D'autre part, un individu est difficilement capable d'évaluer techniquement le niveau de sécurité informatique dont font l'objet ses données pendant leur transmission et leur stockage.

Cette situation conduit à des asymétries d'informations qui portent sur le volume de données personnelles stockées par l'entreprise et ses partenaires, les traitements effectués et les territoires qui hébergent ses données. L'asymétrie d'informations survient lorsqu'un agent économique a plus d'informations sur les états de la nature et les différents types

d'incertitudes qu'un autre agent. Cela peut entraîner une disparition du marché, comme l'a montré George Akerlof[2] dans ses travaux qui lui ont valu son prix Nobel.

L'impact économique des asymétries d'informations a d'abord été analysé sur les marchés d'occasion, où un vendeur connaît la qualité du produit qu'il vend mieux que le prospect, puis a été appliqué sur le marché du travail et sur les marchés financiers. Ce concept peut être appliqué aux données personnelles car l'entreprise qui traite les données de ses clients dispose de plus d'informations sur le niveau de conformité juridique et sur la sécurité de son infrastructure informatique que l'utilisateur. Cependant, les entreprises elles-mêmes ne sont pas toujours en mesure d'évaluer totalement la sécurité de leur système d'information : elles ignorent ainsi parfois si elles ont subi une cyberattaque. Dans ce cas, l'intégrité du système de données n'est pas vérifiable et l'état de sécurité et de protection peut être inconnu tant pour les entreprises que pour les consommateurs. On parle alors de biens de croyance dans la mesure où l'état de la nature n'est vérifiable pour aucun agent économique impliqué dans la transaction.

L'état de sécurité d'une transaction comme un bien de croyance

Le cas de Yahoo[3] illustre ce phénomène à grande échelle, puisque la firme n'a pris connaissance (selon ses dires) qu'en 2016 du vol de plus d'un milliard de comptes utilisateur qui avait eu lieu trois ans auparavant.

L'asymétrie d'informations peut encourager les vendeurs peu scrupuleux (à savoir ceux qui ne respectent pas la réglementation en vigueur ou les bonnes pratiques) à appliquer de mauvaises politiques de protection des données et réduire la participation des consommateurs au marché. En présence d'asymétries d'informations, les consommateurs cherchent des signaux pour évaluer le niveau de confidentialité, la protection des données et/ou la sécurité des sites Web, des produits et des services. Parmi ces signaux, les labels de confidentialité et les marques de confiance jouent un rôle central.

2 Akerlof, G. A. (1970). The market for lemons : Quality uncertainty and the market mechanism. The quarterly journal of economics, 488-500.

3 http://www.lemonde.fr/pixels/article/2016/12/14/plus-d-un-milliard-de-comptes-d-utilisateurs-yahoo-ont-ete-pirates_5049069_4408996.html

9.2. Comprendre la demande de sécurité et de protection des données personnelles : les sources d'externalités négatives

La principale justification économique pour protéger les données personnelles est fondée sur l'existence d'externalités négatives pour les consommateurs quand celles-ci circulent sans autorisation. Ces externalités négatives peuvent prendre les formes suivantes :

- la fraude d'identité et le vol d'identité
- l'utilisation de données personnelles par un tiers à des fins douteuses telles que le spam
- la perte de données personnelles telles que les numéros de carte de crédit en raison d'un manque de sécurité des serveurs où les données sont stockées

Ces externalités négatives (pour le consommateur) conduisent les entreprises à collecter trop de données par rapport à l'optimum social. Il existe plusieurs autres mécanismes économiques qui expliquent pourquoi les consommateurs souhaitent protéger leurs données personnelles. Nous les présentons ci-dessous.

Discrimination par les prix

Si les entreprises disposent d'informations précises sur leurs clients et leurs comportements, elles peuvent pratiquer la discrimination par les prix, à savoir vendre le même produit ou service à différents prix nets à des consommateurs différents. Le prix net comprend les frais de livraison et de production. Pour les produits numériques, la forme de discrimination la plus répandue consiste à développer des stratégies pour identifier plusieurs groupes de consommateurs et proposer différentes versions d'un même produit ou service à ces groupes. Par exemple, un fabricant de logiciels propose un même produit avec différentes fonctionnalités : une version professionnelle complète et une version basique (ou étudiante) pour laquelle certaines fonctions ne sont pas disponibles. Les informations personnelles des consommateurs peuvent donc être utilisées pour personnaliser les offres à des clients ciblés, souvent à un coût très faible. Certains consommateurs bénéficient de prix bas, mais d'autres se voient proposer des prix plus élevés et peuvent décider de protéger leurs données personnelles pour éviter d'être discriminés. Les logiciels permettant de masquer les adresses IP, les extensions de navigateur Internet bloquant les scripts rendent plus difficile l'identification des utilisateurs et donc la discrimination par les prix.

Ciblage et bulles informationnelles

Les consommateurs reçoivent des informations filtrées par les plateformes telles que Google ou Amazon. Par exemple, le moteur de recherche Google filtre les résultats de recherche en fonction de la géolocalisation, de l'historique de navigation et du profil publicitaire. Amazon exécute des algorithmes pour fournir des recommandations de produits personnalisés en fonction de l'historique de navigation et des achats d'une personne. Ces filtres d'information peuvent influencer le comportement des internautes. Ils soulèvent des problèmes économiques importants liés principalement au droit de la concurrence. En effet, comment garantir que le consommateur ne rate pas des opportunités commerciales et que ces filtres ne réduisent pas la concurrence en excluant certains contenus, produits ou services?

Les bulles informationnelles sont créées par des algorithmes qui créent un univers spécifique pour un internaute et vont potentiellement influencer la manière dont il pense, se comporte et achète. Encore une fois, certains internautes peuvent décider alors de protéger leurs données contre le ciblage dont ils peuvent faire l'objet.

Publicités et bloqueurs de pubs

De nombreux réseaux en ligne peuvent être décrits par ce que la littérature économique appelle « les marchés à deux faces ». Ils se caractérisent par des externalités de réseau croisées ou indirectes entre différents groupes d'agents. Par exemple, un moteur de recherche tel que google.com permet aux internautes d'accéder gratuitement à un contenu financé par la publicité. Le site met ainsi en relation les annonceurs avec des consommateurs potentiels. Ces derniers trouvent le moteur de recherche d'autant plus utile que le nombre d'annonces pertinentes est important. De même, un annonceur cherche une plateforme avec un grand nombre d'utilisateurs qui peuvent voir ses publicités ciblées. Il existe donc une externalité de réseau positive entre les utilisateurs d'Internet et les annonceurs. La dynamique des marchés à deux faces où les internautes et les annonceurs interagissent implique qu'un petit avantage comparatif initial d'un moteur de recherche peut conduire à sa domination du marché grâce à une boucle de rétroaction positive.

La littérature économique sur la publicité distingue deux types de publicité : les publicités informatives et persuasives. Les publicités informatives fournissent des informations sur les caractéristiques clés du produit, telles que les détails physiques, les caractéristiques techniques et les prix. Les publicités persuasives sont utilisées pour construire une

marque et ne fournissent pas forcément des informations utiles. Bien que les publicités informatives soient précieuses pour certains consommateurs, les publicités persuasives peuvent être considérées comme une nuisance pour d'autres. Ces derniers chercheront alors à les bloquer et à éviter d'être identifiés.

Les travaux empiriques sur la perception des publicités par les consommateurs sont rares, mais soulignent diverses attitudes des consommateurs : certains adorent la publicité alors que d'autres y sont extrêmement averses. Ces perceptions varient également d'un pays à l'autre. Selon une étude de Business Insider UK, un utilisateur Internet sur 4 utilise un bloqueur de publicité en France alors que seul 1 sur 10 en utilise aux États-Unis en 2015. Le taux de pénétration des bloqueurs de publicité est en forte augmentation en France et atteint plus de 50% d'après le sondage réalisé par la **Chaire Valeurs et Politiques des Informations Personnelles** au début de 2017[4].

Des CGU difficiles à lire, encore plus à comprendre

Des règles formelles et écrites, telles que des chartes ou des conditions générales d'utilisation d'un service (CGU) peuvent réduire les asymétries d'informations en spécifiant le niveau de sécurité informatique et de conformité juridique de la protection des données personnelles. Les CGU sont souvent utilisées par les entreprises qui vendent des produits et des services numériques. Cependant, comme l'ont souligné Olurin et al. 2012[5], Anton et al. 2003[6], ces CGU sont extrêmement difficiles à lire et à comprendre (Cranor et McDonald 2009[7], Becher et Zarksy 2015[8], Bakos et al., 2014[9]). En outre, elles sont toujours formulées dans un format « tout ou rien » où l'acheteur du produit ou l'utilisateur du service doit accepter toutes les conditions avant de pouvoir l'utiliser. En analysant l'impact économique de ces contrats, on peut penser que les termes des services qui protègent mieux les

4 https://cvpip.wp.imt.fr/files/2017/06/Donn%C3%A9es-personnelles-et-confiance-VPIP-Mediametrie-Synth%C3%A8se.pdf

5 Olurin, M., Adams, C., Logrippo, L. (2012). Platform for privacy preferences (p3p): Current status and future directions. IEEE, Tenth Annual International Conference on Privacy, Security and Trust (PST), pp 217-220. DOI : 10.1109/PST.2012.6297943

6 Anton, A., Earp, J. B., Bolchini, D., He, Q., Jensen, C., Stufflebeam, W. (2003). The lack of clarity in financial privacy policies and the need for standardization. IEEE Security & Privacy, 2(2):36-45. DOI : 10.1109/MSECP.2004.1281243

7 McDonald, A. M., Cranor, L. F. (2009). The cost of reading privacy policies. ISJLP, 4, 543.

8 Becher, S. I., Zarsky, T. (2015). Online Consumer Contracts: No One Reads, But Does Anyone Care?.

9 Bakos, Y., Marotta-Wurgler, F., Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. The Journal of Legal Studies, 43(1), 1-35. DOI : 10.1086/674424

données personnelles conduiront à un niveau de rentabilité inférieur à court terme. D'une part, la protection des données et la sécurité sont coûteuses à mettre en œuvre. D'autre part, les termes de service qui facilitent l'exploitation, la réutilisation et la vente de données personnelles engendrent plus de profits. Un contrat unique pour tous les utilisateurs permet à une entreprise d'imposer des règles flexibles en matière de protection des données personnelles et n'est certainement pas une garantie pour l'utilisateur du service que ses données personnelles seront protégées, créant ainsi et perpétuant d'autres asymétries d'informations.

9.3. L'offre de sécurité et de protection des données personnelles par les entreprises

Nous étudions maintenant les facteurs qui poussent les entreprises à sécuriser leur infrastructure de données et à protéger les données personnelles de leurs clients. Premièrement, la sécurité peut être analysée comme un bien public pour lequel il y a un sous-investissement par le secteur privé. Comme nous l'avons vu dans les sections précédentes, il existe des externalités négatives associées au manque de protection des données personnelles qui ne sont pas compensées par les mécanismes du marché et qui exacerbent ce phénomène de sous-investissement. Deuxièmement, les entreprises développent des stratégies commerciales pour atteindre rapidement une masse critique au détriment de la sécurisation de leur infrastructure de données. Enfin, les stratégies commerciales basées sur l'exploitation des données personnelles exigent souvent que les entreprises communiquent les données personnelles de leurs clients avec des tiers qui ne reçoivent pas forcément d'incitations à les protéger. L'asymétrie de l'information portant sur le niveau de sécurité de l'infrastructure des données permet aux entreprises de partager facilement des données sans que les clients n'en soient conscients.

La « sécurité » comme un bien public

La théorie économique caractérise un bien public par une utilisation non-rivale, c'est à dire que la consommation du bien par un agent ne nuit pas à sa consommation par un autre agent. La consommation du bien public est aussi non exclusive : il est impossible d'empêcher un agent de consommer le bien. Ainsi, l'entreprise qui sécurise son infrastructure de données ne peut généralement pas s'approprier la totalité des bénéfices induits par son investissement. En revanche, elle profite elle-même des investissements des

autres entreprises. Elle aura donc tendance à sous-investir dans le bien. Chaque agent suivant cette logique, l'ensemble des entreprises risquent de sous-investir en sécurité.

De plus, les entreprises ont moins d'incitations à sécuriser les données de leurs clients par rapport à l'optimum social, car elles ne tiennent pas compte des externalités négatives pour les utilisateurs de services numériques, comme argumenté dans la section précédente. Dans l'ensemble, le secteur privé ne fournit pas le niveau de protection optimal et les données personnelles sont sous-protégées dans l'écosystème.

Les conséquences des externalités de réseaux

Moore et Anderson (2012)[10] étudient l'effet des externalités de réseau sur le niveau de sécurité choisi par les développeurs de logiciels. Les externalités positives de réseaux émergent lorsque la valeur d'un produit ou service augmente avec le nombre d'utilisateurs. Par exemple, la valeur d'un logiciel augmente avec le nombre de ses utilisateurs, parce qu'il est plus simple d'utiliser le format associé pour l'échange de fichiers entre amis, collègues, et contacts de façon générale. Une entreprise a donc intérêt à atteindre une masse critique le plus rapidement possible afin de dominer son marché et de devenir la référence. Les incitations pour une entreprise à dépenser de l'argent et du temps pour protéger les données personnelles de ses clients sont réduites, par rapport à une situation sans externalité de réseau. La démarche consistant à laisser d'autres acteurs, comme des chercheurs en sécurité informatique, ou des professionnels de détection de failles indépendants, corriger les erreurs, semble plus rentable.

Les modèles d'affaires fondés sur l'échange de données

Les entreprises qui développent leurs stratégies commerciales autour de la publicité créent des revenus en vendant les données de leurs clients à des tiers. Ces entreprises sont incitées à rédiger des conditions de service très générales pour pouvoir utiliser (et réutiliser) de manière exhaustive les données disponibles. Lorsque les données personnelles sont transférées à des tiers, il est difficile pour le client de déterminer comment ses données sont utilisées, stockées et sécurisées. Les *Ad exchanges* avec enchères en temps réel exacerbent ces problèmes, car les données personnelles disponibles dans les cookies stockés sur les ordinateurs sont transmises et appariées par d'autres plates-formes et sociétés tierces. Les données personnelles peuvent ensuite être utilisées sans

10 Moore, T., Anderson, R. (2012). Internet security. The Oxford Handbook of the Digital Economy'(Oxford University Press 2011).

le consentement des clients par des entreprises qui sont parfois très éloignées de l'entreprise initiale et de ses clients.

Data lock-in

Les économies d'échelle dans le stockage et l'exploitation des données, l'existence d'externalités de réseaux sur les plateformes en ligne à plusieurs versants, c'est-à-dire qui servent d'intermédiaires entre plusieurs groupes d'agents économiques, ont créé des monopoles sur Internet. Par exemple, Google représentait en 2017 plus de 88% des recherches sur Internet dans le monde[11]. Par ailleurs, un utilisateur de services numériques bénéficie des informations stockées en ligne lui permettant d'automatiser sa connexion, d'enregistrer ses préférences et son historique de navigation. Ceci crée une situation de *lock-in* résultant d'une captivité des utilisateurs fidélisés au service et caractérisée par des coûts de changement élevés. Cette situation permet aux entreprises en monopole d'imposer des conditions d'utilisation de leurs services facilitant une exploitation massive des données de leurs clients parfois à leurs dépens (Mantelero, 2013[12]).

9.4. Une analyse économique de la protection des données personnelles et des marques de confiance

Les marques de confiance peuvent prendre différentes formes et spécificités. Nous étudions ces différentes combinaisons, en renvoyant à Rodrigues et al. (2013)[13] pour une approche plus systématique. Une ***marque de confiance par adhésion*** est délivrée par une association à ses membres contre des frais. Elle est généralement délivrée par une entreprise privée, comme TRUSTe aux États-Unis. Une ***marque de confiance publique***, quant à elle, est délivrée par une autorité publique en conformité avec un règlement, une loi ou une politique spécifique. Une ***marque de confiance binaire*** (publique ou privée) indique si l'entreprise a atteint un certain niveau de certification de conformité aux réglementations ou aux chartes existantes. Une ***marque de confiance continue*** (publique

11 http://www.journaldunet.com/ebusiness/le-net/1087491-parts-de-marche-des-moteurs-de-recherche-dansle-monde/

12 Mantelero, A. (2013). Competitive value of data protection: the impact of data protection regulation on online behavior, International Data Privacy Law 3(4): 229-238. DOI : 10.1093/idpl/ipt016

13 Rodrigues, R., Barnard-Wills, D., Wright, D., De Hert, P., Papakonstantinou, E. (2013). EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final Report. Publications Office of the European Union.

ou privée) possède plusieurs niveaux de conformité, généralement représentés par des lettres ou des couleurs.

Label délivré par adhésion et labels publics

Un label est moins crédible si ses membres doivent adhérer de manière volontaire, et ce pour des raisons évidentes. En effet, la relation entre l'organisation qui délivre le label et ses membres est ambiguë. Il s'agit d'une relation de type « principal-agents multiples » où les membres sont également des clients qui paient des frais d'adhésion au principal. Le principal est intéressé par l'acquisition de nouveaux membres et a donc moins d'incitation à vérifier la conformité de ses membres aux normes du label même si la charte de l'organisation stipule qu'elle s'engage à le faire. Par conséquent, les membres ne protègent les données de leurs clients que s'ils pensent que la probabilité d'être pris en défaut est suffisamment élevée.

Les labels publics ne souffrent pas du problème de clientélisme, mais la question du financement de l'audit se pose, comme nous le verrons plus loin. Par ailleurs, les labels publics co-existent souvent avec des labels par adhésion. Comment déterminer le niveau de qualité du label public ? Tout d'abord, une norme fournie par l'État qui serait trop faible par rapport aux meilleures pratiques de l'industrie perd son pouvoir de signal. Certaines entreprises préféreront alors payer un coût supplémentaire pour adopter un sceau privé de qualité supérieure afin de se signaler à leurs clients et d'obtenir un avantage concurrentiel et une meilleure réputation.

Si les normes étatiques sont proches de celles des sociétés ayant obtenu des labels de haute qualité, les entreprises s'appuieront sur le sceau public pour signaler la haute qualité de leur politique de protection des données personnelles, le label public se substituant alors au label privé. Enfin, s'il n'y a que des marques de confiance publiques, il existe un risque de sélection adverse qui peut conduire à l'exclusion des entreprises de haute qualité si la norme est trop faible (ou des entreprises de moyenne à haute qualité si la norme est trop élevée).

Par ailleurs, la cohabitation de marques de confiance internationales, soumises à des législations différentes, peut introduire de facto une cohabitation public-privé dans les écosystèmes de protection des données. ***La détermination du bon niveau de qualité pour la norme de protection est donc un élément essentiel à prendre en considération.***

Formats : volontaires, continus, binaires

Deux principaux formats de labels existent, qui ont différents effets économiques : continus et binaires. Les labels continus prennent différentes valeurs, représentées par des couleurs, des signes, ou des lettres. Une marque de confiance binaire signale uniquement si l'entreprise respecte un référentiel. Roe et Sheldon (2007)[14] constatent que les marques de confiance continues réduisent considérablement les asymétries d'informations et conduisent à des prix et une qualité sur le marché équivalents à ceux qui prévalent dans une situation d'information parfaite, même si les labels continus sont a priori plus difficiles à comprendre et à interpréter que les labels binaires. Pour les marques de confiance binaires, il existe un risque que les consommateurs à faible revenu et les entreprises de faible qualité préfèrent la norme de qualité inférieure, et que les consommateurs ayant des hauts revenus privilégient les entreprises offrant un niveau de protection élevé.

Procédures d'audit et résolution des conflits

Parfois, le contrat entre l'organisation qui délivre la marque de confiance et ses membres précise que les membres paient pour résoudre les conflits avec les clients. Parfois, ce sont les clients qui doivent régler les frais liés au litige. Cela peut entraîner des inefficacités si les frais sont élevés. Par exemple, Connolly (2008)[15] a démontré que l'application des termes du contrat entre TRUSTe et ses membres était rare. Il fournit de nombreux exemples de violations de la vie privée entre 1998 et 2007 (y compris des pertes de données chez AOL, Facebook, Hotmail, Microsoft et Real Networks) qui n'ont pas été suivies d'actions de rectifications.

Il est évident qu'un label privé sans politique d'audit régulier est voué à perdre son pouvoir de signal de qualité pour les consommateurs.

Les différents modèles d'affaires

La question suivante porte sur les frais facturés par l'organisation qui délivre la marque de confiance. D'une part, un prix élevé d'une marque de confiance exclut les petites entreprises qui n'ont pas les moyens de financer la labellisation. D'autre part, un prix élevé signale aux consommateurs que l'entreprise qui affiche la marque de confiance est financièrement saine et qu'elle dispose de ressources suffisantes pour protéger les données

14 Roe, B., Sheldon, I. (2007). *C*redence good labeling: The efficiency and distributional implications of several policy approaches. American Journal of Agricultural Economics 89(4):1020-1033. DOI : 10.1111/j.1467-8276.2007.01024.x

15 Connolly, C. (2008). Trustmark Schemes Struggle to Protect Privacy, Working paper.

personnelles de ses clients. Un prix élevé reflète également la bonne réputation de l'organisation qui délivre la marque de confiance et la fiabilité du processus de labellisation. Cet argument n'est évidemment valable que si les internautes connaissent les coûts de labellisation payés par les entreprises qui gèrent les sites Web qu'ils visitent.

Un prix faible ne permet pas à la marque de confiance de jouer son rôle de signal de qualité et pourrait réduire le budget de l'organisme délivrant la marque de confiance pour auditer ses membres. Une certification gratuite n'est possible que si elle est financée par un consortium ou une agence publique. La question du coût associé aux labels publics de protection des données publiques à grande échelle attend des réponses.

Plusieurs facteurs économiques mettent en évidence des inefficacités sur le marché de la protection des données personnelles. Premièrement, les asymétries d'informations créent des comportements opportunistes de la part des entreprises peu scrupuleuses qui développent des stratégies pour exploiter les données des clients parfois à leur insu (discrimination par les prix, CGU trop peu protectrices, captivité des clients). Deuxièmement, les entreprises qui investissent dans la protection des données clients ne prennent souvent pas en compte les externalités négatives pour les clients de la perte de leurs données (spam, vol d'identités, fraudes). Troisièmement, les forces du marché poussent certaines entreprises à atteindre une masse critique au détriment de la protection des données ou fondent leur modèle d'affaire sur la vente de données à des tierces parties qui n'ont pas nécessairement les mêmes incitations économiques à protéger les données clients. Les labels de protection des données agissent comme des signes de confiance dont l'impact économique est difficile à déterminer. D'une part, un label de haute qualité délivré par une institution publique génère de la confiance, mais possède des coûts élevés, à la fois pour les entreprises privées et pour l'institution publique, qu'il s'agit de financer. D'autre part, un label privé permet de résoudre le problème du financement, mais pose des problèmes de clientélisme et peut être plus facilement manipulé. Dans les deux cas, les questions de savoir quel est le bon niveau de qualité associé au label et quel est son prix sont essentielles pour que le label joue pleinement son rôle de signe de confiance sur le plan économique.

« En Chemin l'empreinte de l'autre » – Thierry Citron

Chapitre 10. Les impacts économiques des labels

Patrick Waelbroeck

10

Ce chapitre s'intéresse à l'impact économique des labels pour les entreprises et les consommateurs. Nous montrons tout d'abord comment les labels et les marques de confiance peuvent impacter les stratégies des entreprises (10.1.). Les résultats présentés sont essentiellement fondés sur des études américaines qui peuvent néanmoins servir d'enseignement dans le contexte européen. La section 10.2 présente les résultats d'une enquête que la **Chaire Valeurs et Politiques des Informations Personnelles** a réalisée en 2017 en collaboration avec Médiamétrie sur l'usage des données personnelles par les internautes français[1]. Le volet sur la perception des labels par les internautes est présenté en exclusivité dans ce chapitre.

10.1. Impact économique des marques de confiance

Les études empiriques sur l'efficacité économique des marques de confiance et des labels montrent qu'ils engendrent une faible augmentation des prix et un effet positif sur les ventes. Elles identifient également que les comportements adoptés par les consommateurs peuvent paraître risqués car issus d'une incompréhension des politiques sous-jacentes de protection des données personnelles et de leur vie privée. Pour déterminer un ordre de grandeur, nous pouvons nous référer à l'étude de Miyazaki et Krishnamurthy(2002)[2] qui

1 https://cvpip.wp.imt.fr/donnees-personnelles-et-confiance-quelles-strategies-pour-les-citoyens-consommateurs-en-2017/

2 Miyazaki, A. D., Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. The Journal of Consumer Affairs 28-49. DOI : 10.1111/j.1745-6606.2002.tb00419.x

Les impacts économiques des labels

ont constaté aux États-Unis que 32% des entreprises Fortune 50, près de 5% des entreprises Fortune 500 et 14% des entreprises de Information Week 100 étaient titulaires d'un label TRUSTe ou BBBOnLine, les deux principales marques de confiance américaines en 2002. Des études plus récentes indiquent des chiffres similaires pour la pénétration des marques de confidentialité et des marques de confiance parmi les sites Web les plus visités (environ 7 sur 50).

Augmentation du prix et des ventes

Les différentes études américaines montrent qu'après l'adoption d'une marque de confiance le produit labellisé voit son prix augmenter. L'impact varie selon des facteurs exogènes. Différents ordres de grandeur permettent d'apprécier ces impacts selon la nature du produit, la nature de la marque de confiance, le processus ou la composante identifiée, ou encore la localisation géographique du marché. La littérature portant essentiellement sur les marques de confiance agroalimentaires, les effets sont naturellement à modérer, mais ils permettent de saisir les écarts importants.

Kiesel et Villas Boas (2007)[3] étudient l'impact des marques de confiance du *National Organic Program* et du Département de l'Agriculture pour le lait biologique aux États-Unis sur les consommateurs. Ils constatent un changement dans les habitudes d'achat des

3 Kiesel, K., Villas-Boas, S. B. (2007). Got organic milk? consumer valuations of milk labels after the implementation of the USDA organic seal. Journal of agricultural & food industrial organization 5(1). DOI : 10.2202/1542-0485.1152

consommateurs après l'apparition des marques de confiance. Plus précisément, une majoration variant entre 192 cents et 224 cents est acceptée par les consommateurs pour un demi-gallon de lait biologique, ce qui correspond à une augmentation de 39,4% à 45,8% du prix.

Brounen et Kok (2011)[4], dans leur étude sur l'évolution des achats de biens immobiliers en fonction de la présence d'un label de consommation énergétique au Pays-Bas, observent une augmentation de la propension à payer de 3.7%, liée à la présence d'une marque de confiance garantissant une efficacité énergétique supérieure de l'habitation. Considérant que le prix moyen de vente d'un logement aux Pays-Bas lors de leur étude est de 231 000 €, ils évaluent la majoration tarifaire moyenne à 8 449 €.

Pour le cas des marques de confiance sanitaires, McCluskey et Loureiro (2000)[5] se réfèrent à une étude de 1997 en France (après la crise de la vache folle). Ils rapportent une disponibilité à payer de 22% plus élevée pour de la viande de bœuf garantie non infectée. Bjorner et al. (2004)[6] étudient quant à eux l'impact de la marque de confiance écologique « Nordic Swann » sur la consommation de 1 596 foyers danois. Le label environnemental a un effet positif sur le choix du papier toilette, avec une propension à payer un prix de 13% à 18% supérieur pour un produit garantissant qu'il est respectueux de l'environnement.

D'un point de vue commercial, Levy et al. (1985)[7] observent un impact positif du *Special Diet Alert*, un programme d'informations nutritives à l'initiative de supermarchés mené sur deux ans. Ils notent toutefois une différence d'impact du programme selon la zone géographique concernée : l'augmentation des ventes de produits favorisée par le programme fut de 4 à 8% supérieure à Washington par rapport à Baltimore, mettant en avant une plus grande sensibilité de la population concernée aux facteurs visés par les marques de confiance.

---

4 Brounen, D., Kok, N. (2011). On the economics of energy labels in the housing market. Journal of Environmental Economics and Management 62(2):166-179. DOI : 10.1016/j.jeem.2010.11.006

5 Loureiro, M. L., McCluskey, J. J. (2000). Consumer preferences and willingness to pay for food labeling: A discussion of empirical studies. Journal of Food Distribution Research 34(3):95-102

6 Bjørner, T. B., Hansen, L. G., & Russell, C. S. (2004). Environmental labeling and consumers' choice—an empirical analysis of the effect of the Nordic Swan. Journal of Environmental Economics and Management, 47(3), 411-434. DOI : 10.1016/j.jeem.2003.06.002

7 Levy, A. S., Mathews, O., Stephenson, M., Tenney, J. E., & Schucker, R. E. (1985). The impact of a nutrition information program on food purchases. Journal of Public Policy & Marketing, 1-13

Mai et al. (2015)[8] étudient l'impact des marques de confiance de garantie de protection des données personnelles sur les prix de vente. Ils évaluent à 1,5% la majoration du prix associée à l'introduction d'une marque de confiance, dans le cas des sites de vente. De façon similaire, Melnik et Alm (2002)[9] relèvent un impact significatif d'une bonne évaluation d'un vendeur sur eBay, mais associée à une très faible augmentation du prix.

Les évaluations que nous venons de citer varient donc de 1,5% à 45,8% du prix de vente d'un produit garanti par un label, par rapport à un produit sans garantie. Il ressort de la liste d'études ci-dessus que le lieu de vente, la nature du produit, et d'éventuels scandales liés au secteur étudié sont probablement à l'origine d'un tel écart. On peut résumer ce résultat par la notion intuitive de risque perçu. Un utilisateur sera d'autant plus prêt à payer une majoration tarifaire pour un produit si le risque associé à une qualité douteuse est important.

Plus précisément, McCluskey et Loureiro (2000)[10] montrent que la garantie d'absence d'OGM en Europe et au Japon augmente la disponibilité à payer des consommateurs, tandis que Li et al. (2003)[11] observent en Chine que les consommateurs sont prêts à payer 38% de plus pour du riz génétiquement modifié par rapport à du riz traditionnel, et 16,3% de plus pour de l'huile de soja génétiquement modifié par rapport à de l'huile de soja traditionnelle. Ceci pourrait s'expliquer par des différences de cultures et de politiques agro-alimentaires.

L'impact des marques de confiance porte plus sur un effet volume que sur un effet prix, en particulier pour des sites non marchands, où l'impact de la marque de confiance ne peut pas être observé sur le prix.

---

8 Mai B, Menon N M, Sarkar S (2010) No free lunch: Price premium for privacy seal-bearing vendors. Journal of Management Information Systems 27(2):189-212

9 Melnik, M. I., & Alm, J. (2002). Does a seller's ecommerce reputation matter? Evidence from eBay auctions. The journal of industrial economics, 50(3), 337-349. DOI : 10.1111/1467-6451.00180

10 Loureiro M L, McCluskey J J (2000) Consumer preferences and willingness to pay for food labeling: A discussion of empirical studies. Journal of Food Distribution Research 34(3):95-102

11 Li, Q., Curtis, K. R., McCluskey, J. J., & Wahl, T. I. (2003). Consumer attitudes toward genetically modified foods in Beijing, China

Marques de confiance et effets de confusion

Gao (2007)[12] se penche sur la comparaison des impacts selon différentes marques de confiance. Il énumère quatre caractéristiques relatives à un produit agricole et pouvant être garanties par une marque de confiance : la qualité à la consommation en termes de goûts, l'origine géographique, le respect de méthodes biologiques, la présence d'OGM.

L'originalité de l'approche réside dans l'étude comparée des marques de confiance existantes pour la viande les unes par rapport aux autres, et l'étude de l'impact supplémentaire d'une marque de confiance sur un produit déjà marqué. Ils notent, entre autre, que la date de péremption n'a un impact que secondaire, dépendant de la présence d'autres attributs. En outre, les marques de confiance portant sur la tendresse et la maigreur de la viande ont un effet positif significatif, contrairement à la date de péremption. De façon surprenante, les effets marginaux pour la qualité de la viande et l'origine du produit sont opposés à partir d'un certain seuil : le nombre de marques de confiance garantissant la tendresse de la viande a un effet marginal positif sur la propension à acheter. En revanche, la certification d'origine de la viande passe d'un effet positif pour le passage de 3 à 4 marques de confiance, mais a un effet négatif pour le passage de 4 à 5.

L'important ici est le changement d'effet d'une valeur positive à une valeur négative, laissant supposer que le nombre de marques de confiance peut être jugé négativement à partir d'un certain seuil. Finalement, il observe que, sans tenir compte de la nature précise des marques de confiance, leur nombre a un effet marginal positif.

Cette confusion est également relevée pour les marques de confiance écologiques. Leire et Thidell (2005)[13] étudient, pour leur part, l'impact du «Nordic Swann» ; ils constatent que cette marque est efficace. Si entre deux produits comparables, l'un d'eux possède la marque «Nordic Swann», les consommateurs le préféreront. Cependant, ce résultat qui semble fort en terme d'attitude annoncée, perd de sa signification dès que l'auteur considère l'achat effectif.

---

12 Gao, Z. (2007). Effects of additional quality attributes on consumer willingness-to-pay for food labels (Doctoral dissertation, Kansas State University)

13 Leire, C., Thidell, Å. (2005). Product-related environmental information to guide consumer purchases–a review and analysis of research on perceptions, understanding and use among Nordic consumers. Journal of Cleaner Production, 13(10), 1061-1070. DOI : 10.1016/j.jclepro.2004.12.004

Enfin, si l'on considère les données personnelles sur Internet, Larose et Riffon (2007)[14] confrontent les comportements de 227 étudiants et concluent que le « *Privacy Paradox* », à savoir le partage volontaire des données personnelles malgré la crainte qu'elles ne soient pas effectivement protégées, est dû à une trop grande confiance des utilisateurs. Ainsi, la confusion autour des risques que peut présenter un site entraîne une certaine vulnérabilité de l'internaute.

Cependant, Nouassair et al. (2002)[15] étudient un phénomène comparable au « *Privacy Paradox* », dans le contexte en France des produits génétiquement modifiés. Les consommateurs interrogés se déclarent contre les aliments avec OGM. Cependant, ils ne semblent pas prendre cette composante en compte lors de leurs achats. Leur étude portant sur un panel de 112 participants souligne que l'inattention aux marques de confiance est la cause de cette contradiction, et que le prix qu'ils sont prêts à payer décroît de 30% lorsque les consommateurs prennent connaissance de la présence d'OGM.

10.2. **Impact des labels sur les utilisateurs**

Afin de mieux appréhender la façon dont les Français gèrent leurs données personnelles, la **Chaire Valeurs et Politiques des Informations Personnelles** s'est associée à Médiamétrie pour réaliser une enquête en mars 2017. Celle-ci s'inscrit dans le contexte d'une lente érosion de la confiance sur Internet, de la collecte souvent abusive des données personnelles et de la surveillance mise en place par certains États ou acteurs privés.

L'échantillon, représentatif de la population internaute, était constitué de 2051 internautes âgés de 15 ans et plus. La représentativité a été assurée par la méthode des quotas (sexe, tranche d'âge en 5 classes, classe socio-professionnelle en 5 classes et région Paris-Province) sur la base de l'enquête de référence de la population d'internautes en France, l'Observatoire des usages de l'Internet. Le questionnaire a été auto-administré en ligne sur la période du 26 février au 16 mars 2017.

14 LaRose, R., Rifon, N. J. (2007). Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. Journal of Consumer Affairs, 41(1), 127-149. DOI : 10.1111/j.1745-6606.2006.00071.x

15 Noussair, C., Robin, S., Ruffieux, B. (2002). Do consumers not care about biotech foods or do they just not read the labels? Economics letters, 75(1), 47-53. DOI : 10.1016/S0165-1765(01)00594-8

Pour mieux comprendre les enjeux des signes de confiance, la série de questions rédigées par Patrick Waelbroeck, Armen Khatchatourov et Claire Levallois-Barth portait sur ***les formes que devrait prendre un label***, ***le type d'entité devant délivrer le label***, et ***l'impact d'un label sur les habitudes des internautes***.

La forme

Nous avons discuté des avantages et des inconvénients de différentes formes de labels, en particulier les labels à plusieurs niveaux et les labels binaires (cf. Chapitre 9). Nous y avons souligné à plusieurs endroits les risques de manipulations par les entreprises labellisées associés aux labels binaires. Nous en avons conclu qu'un label à plusieurs niveaux était préférable. Les réponses fournies par les internautes que nous avons interrogés confirment la préférence pour des labels nuancés.

Figure 4. *Type de label qui susciterait le plus la confiance*

Parmi les internautes qui affirment une préférence quant à la présence ou non d'un label de fiabilité, plus de la moitié ferait davantage confiance à un label nuancé, qui exprimerait le niveau de protection des données personnelles via une échelle (de notes ou de couleurs).

Un label nuancé ☑☑☑

C'est-à-dire un label qui indiquerait un niveau de protection des données personnelles via une échelle de notes ou de couleurs. *54%*

Un label unique ☑

C'est-à-dire que la présence de ce label indiquerait que le site protège les données personnelles, et l'absence de ce label ne donnerait aucune indication quant à la protection des données personnelles. *32%*

Aucun de ces deux types de labels *8%*

Je ne sais pas *7%*

► *Question : à quel type de label feriez-vous le plus confiance ?*

► *Base : internautes de 15 ans et plus qui se positionnent quant à la notion de label (n=1437)*

Qui doit labelliser ?

Nous avons identifié dans les chapitres 7 et 9 les risques de clientélisme et les effets potentiellement pervers d'un système de label délivré par un organisme privé.

La prédominance de l'organisme public

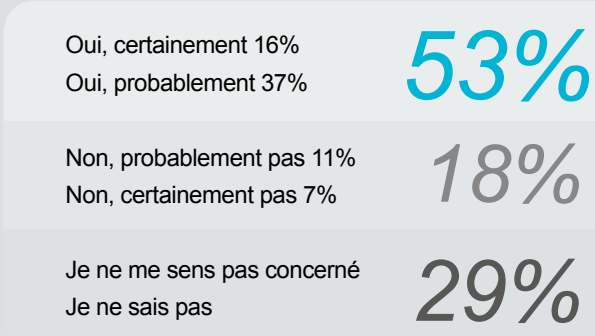
Les réponses à l'enquête montrent clairement qu'un organisme de l'État ou un organisme institutionnel constituerait un tiers de confiance pour délivrer un label numérique pour près de 7 internautes sur 10. La question du modèle d'affaires et du financement du coût de la labellisation n'a cependant pas été posée.

Le potentiel des notations collaboratives

En ce qui concerne le système de notations collaboratif, on remarque que 53% des personnes interrogées sont prêtes à y participer de manière active (sans incitations monétaires ou autre), ce qui correspond à un chiffre que l'on retrouve dans les systèmes de notation de sites comme eBay, où environ 50% des membres évaluent leurs transactions.

Figure 5. *Disposition à donner son avis sur la fiabilité d'un site*

Plus de la moitié des internautes serait prêts à donner leur avis sur la fiabilité d'un site, pour témoigner ou non que le site protège bien les données personnelles. En revanche, 3 internautes sur 10 ne se sentent pas concernés ou ne savent pas.



► *Question : pour démontrer qu'ils protègent bien les informations personnelles, certains sites affichent les avis des consommateurs sur la confiance qu'ils leur accordent et sur la fiabilité du site. Seriez-vous prêts à participer en donnant votre avis sur la fiabilité d'un site ?*

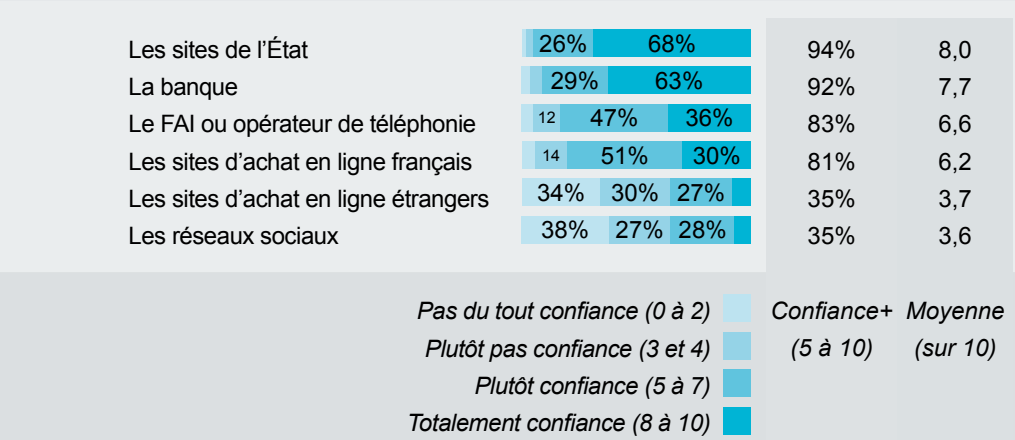
► *Base : internautes de 15 ans et plus (n=2051)*

Qui doit-on labelliser ?

L'enquête montre clairement que l'on doit labelliser en priorité les sites d'achat en ligne étrangers et les réseaux sociaux, pour lesquels les niveaux de confiance sont nettement inférieurs à la moyenne.

Figure 6. *Niveau de confiance vis-à-vis des acteurs sur Internet*

Les sites de l'État et la banque suscitent la confiance de la quasi-totalité des internautes. Les sites d'achat français sont jugés nettement plus fiables que les sites d'achat étrangers. Seulement un tiers des internautes font confiance aux réseaux sociaux (note moyenne de 3,6/ 10)



► *Question : sur une échelle de 0 à 10, quel est votre niveau de confiance pour chacun des acteurs suivants ?*

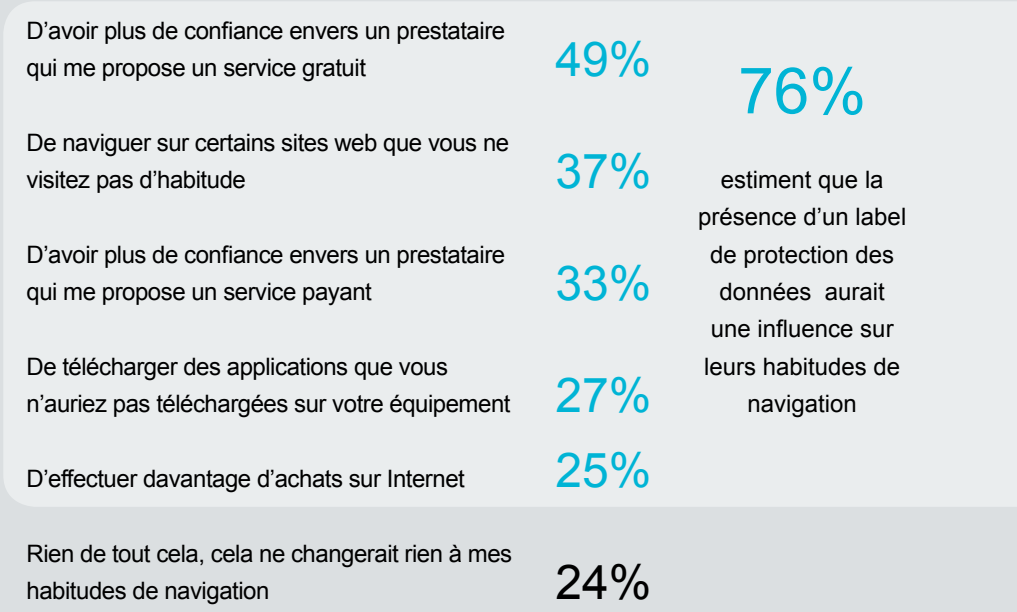
► *Base : internautes de 15 ans et plus (n=2051)*

Impact

Le label de protection des données permet d'améliorer le niveau de confiance dans les situations perçues comme risquées, comme l'utilisation d'un service gratuit ou un téléchargement. On constate également un effet positif d'exploration qui permettrait aux internautes de sortir de leurs bulles informationnelles. Un impact économique pour ¼ des personnes interrogées est également à souligner.

Figure 7. Impacts qu'aurait un label de protections des données

Parmi les internautes qui ont exprimé une préférence quant à la présence ou non d'un label de fiabilité, plus des trois quarts verraient leurs habitudes de navigation influencées par la présence d'un label. Cela améliorerait notamment la confiance envers les sites labellisés.



► *Question : si un label de protection des données personnelles se développait, pensez-vous qu'il permettrait…*

► *Base : internautes de 15 ans et plus qui se positionnent quant à la notion de label (n=1437)*

Pistes de mise en œuvre

L'expérience des labels dans les autres industries, telles que l'agro-alimentaire ou le secteur énergétique, montre qu'ils ont des impacts significatifs en termes de prix et de ventes pour les entreprises et produits labellisés. L'ampleur de ces effets économiques varie cependant d'une étude de cas à l'autre, les effets les plus forts étant observés lorsque les risques pour les consommateurs sont élevés (risque pour la santé par exemple).

Ainsi, la prise de conscience grandissante des enjeux sociétaux autour de la protection des données personnelles par les internautes peut conduire à penser que l'impact économique des labels de protection de données ira également en grandissant.

En ce qui concerne la perception des utilisateurs d'un tel label, l'enquête que nous avons menée au sein de la **Chaire Valeurs et Politiques des Informations Personnelles** semble indiquer qu'un label à plusieurs niveaux délivré par un organisme public combiné à un système de notation collaboratif en co-construction avec les internautes semble prometteur. Il devrait en priorité renforcer la confiance des internautes lorsqu'ils utilisent des sites marchands étrangers et des réseaux sociaux.

Chapitre 11. La blockchain est-elle une technologie de confiance ?

Maryline Laurent

11

Ce chapitre présente le fonctionnement et les limites du « *trust by design* » exposé au chapitre 1, en s'appuyant sur un exemple particulier de technologie, celui de la blockchain.

Cette technologie a été inventée à la fin des années 2000. Plus précisément, elle a été développée au sein du projet d'échange de crypto-monnaie sur Internet Bitcoin, projet qui l'a rendue populaire et qui a permis de démontrer sa grande fiabilité. En 2014, la fondation à but non lucratif Ethereum dirigée par Vitalik Buterin décide d'étendre le principe de la blockchain à une blockchain programmable, ouvrant ainsi le champ à un nouveau type de transactions appelé « *smart contracts* ».

► Un exemple de transaction ou *smart contract* consiste à déclencher un virement (en crypto-monnaies) à la réception d'un colis, ou l'ouverture d'une porte (véhicule, location de maison…) après prépaiement du service.

En 2015, une première version du code source d'Ethereum est rendue publique, ce qui permet à de nombreux industriels et développeurs indépendants de proposer des services innovants. Citons par exemple le tout récent service Fizzy d'AXA qui assure les passagers contre les retards d'avion[1].

1 https://buff.ly/2xiTBId

La blockchain est-elle une technologie de confiance ?

La blockchain est souvent comparée à un gros livre de comptes, publiquement accessibles et auditables, tenu par des « membres ». Ces derniers ont la possibilité d'y ajouter des écritures, à condition que cette opération soit validée par plusieurs membres du groupe, voire la majorité des membres. Il est ainsi possible de tracer les écritures de chacun, sans pour autant connaître l'identité des entités impliquées, les membres agissant sous pseudonymat.

Après avoir introduit quelques techniques élémentaires utiles à la compréhension (11.1.), ce chapitre décrit le fonctionnement technique de la blockchain (11.2.). Puis, il identifie les propriétés clés qui permettent de lui conférer un certain degré de confiance (11.3.). Enfin, il dresse un état des lieux des risques et limites associés à cette technologie et discute de sa capacité à garantir la protection des données personnelles (11.4. et 11.5.).

La difficulté de l'exercice consiste à distinguer ce qui relève, d'une part, du concept propre à la blockchain et, d'autre part, des différentes instanciations qui en ont été faites, notamment les projets Bitcoin, Ethereum, Ripple et Litecoin[2]. Notons que les explications fournies dans la suite ont principalement trait au projet Bitcoin, qui fait l'objet d'une littérature fournie et stable.

2 On pourra alors écrire Blockchain Bitcoin, Blockchain Ethereum… pour désigner ces instanciations.

11.1. Les éléments techniques fondamentaux

La sécurité offerte par la blockchain repose pour l'essentiel sur des mécanismes cryptographiques standard, relevant principalement de la cryptographie à clés publiques, des fonctions de hachage et des signatures électroniques.

Mécanismes cryptographiques

La cryptographie à clés publiques suppose que chaque entité d'un système dispose de deux clés, une ***clé publique*** connue de tous et une ***clé privée*** maintenue secrète par l'entité qui en est propriétaire. Cette clé privée permet à son propriétaire de signer une demande de transaction et ainsi de prouver qu'il en est à l'origine. La clé publique permet à une autre entité de vérifier l'authenticité de la signature.

Le niveau de sécurité d'un cryptosystème se mesure à la difficulté de craquer les clés privées. Ce niveau dépend directement de la taille des paramètres : plus leur taille est grande, plus il est difficile de craquer la clé privée. Avec du matériel informatique de moins en moins cher et offrant de plus en plus de puissance de calcul et de mémoire, il est nécessaire de réviser régulièrement à la hausse la taille des paramètres, pour maintenir le niveau de difficulté. Aujourd'hui, une sécurité de niveau 100 est suffisante, ce qui correspond à un attaquant à qui on confère la capacité de réaliser 2^{100} opérations pour réaliser une attaque.

Le projet Bitcoin se fonde sur le cryptosystème ECC (*Elliptic Curve Cryptography*) qui utilise l'algorithme de signature ECDSA (*Elliptic Curve Digital Signature Algorithm*). ECDSA s'appuie sur les courbes elliptiques qui ont l'avantage d'utiliser, pour un même niveau de sécurité, des tailles de clés raisonnables par rapport à d'autres cryptosystèmes à clés publiques plus classiques tels que le RSA (du nom de ses inventeurs : Rivest, Shamir et Adleman). Ainsi, pour un niveau de sécurité de 112, les clés exigées sont de 3072 bits pour RSA et seulement de 256 bits pour ECC.

Fonctions de hachage

Les fonctions de hachage (*Hash*) sont très présentes dans les blockchains, en particulier la fonction SHA256. Elles permettent de fabriquer des signatures pour authentifier chaque transaction, de garantir un lien fort entre un membre de la blockchain et sa clé publique, et d'identifier une transaction ou un bloc injecté dans la blockchain. Elles servent

aussi à lier les blocs entre eux de manière à rigidifier l'enchaînement des blocs, ce qui offre une garantie de l'intégrité de la blockchain.

Propriétés d'une fonction de hachage (Hash) cryptographique

- Production d'un résultat (ou haché) de taille fixe : quel que soit le message fourni en entrée, la fonction retourne toujours un résultat de même taille. L'algorithme SHA256 retourne un haché sur 256 bits
- Irréversibilité du message haché : il est très difficile de trouver le message fourni en entrée à partir du résultat de la fonction
- Résistance aux collisions : il est très difficile d'obtenir à partir de deux messages le même haché
- Effet avalanche : la modification d'un bit dans le message en entrée a pour conséquence de modifier au moins la moitié des bits en sortie. Cette propriété est intéressante pour garantir l'intégrité.

Lorsque les propriétés d'irréversibilité et de résistance aux collisions sont qualifiées de « très difficiles », cela signifie que les outils algorithmiques et informatiques actuels ne permettent pas de réaliser une attaque sur une fonction de hachage en un temps raisonnable.

Signatures électroniques

La fabrication d'une signature suppose, pour le signataire, de commencer par appliquer une fonction de hachage sur les éléments de la transaction à authentifier, puis de chiffrer le résultat obtenu avec sa clé privée.

11.2. Le fonctionnement de la blockchain

Une blockchain est un ensemble de transactions individuelles regroupées en blocs, chaque bloc contenant les transactions émises à partir du dernier bloc. Chaque transaction est émise par un nœud préalablement enrôlé, qui la diffuse à tous les membres de la blockchain.

L'authenticité et la légitimité de la transaction sont alors vérifiées par les nœuds de la blockchain, qui se réfèrent à l'historique des transactions enregistrées depuis l'origine dans la blockchain. Puis, les mineurs agglomèrent sous la forme d'un bloc les transactions validées. Pour valider le bloc, ils doivent « miner », c'est-à-dire résoudre un problème

mathématique complexe appelé « Preuve de travail » (*Proof of Work* – PoW)[3]. Le mineur qui le premier résout le problème mathématique diffuse sa solution à tous les nœuds, qui vérifient alors la preuve PoW. En cas de validité avérée, chaque nœud ajoute le bloc dans la blockchain, et les mineurs commencent à miner le bloc suivant. Le fait d'inscrire massivement un bloc dans la blockchain signifie qu'un consensus a été atteint parmi les nœuds.

Les différents types de nœuds

D'un point de vue technique, les membres de la blockchain sont des ressources informatiques (par exemple des ordinateurs) qui ont été connectées à la blockchain lors d'une phase d'enrôlement. Mises en réseau au travers d'Internet, ces ressources sont couramment appelées des nœuds.

Pour être membre d'une blockchain, une personne doit donc enrôler un de ses équipements informatiques en tant que « nœud ». Il existe deux types de nœuds :

- les ***nœuds réguliers***, dotés pour la plupart de capacités informatiques ordinaires, à partir desquels des personnes physiques peuvent émettre des demandes de transactions
- les ***nœuds « miners »*** ou mineurs, dotés de grosses capacités de traitement, directement utiles au fonctionnement de la blockchain et capables eux aussi d'émettre des transactions

Les nœuds réguliers ou mineurs, pour peu qu'ils disposent de grosses capacité, peuvent stocker l'ensemble de la blockchain. Ils sont alors appelés « nœud entier » (« *full node* »). Notons que la Blockchain Bitcoin lancée en 2009 atteint en 2017 plus de 158GB.

La phase d'enrôlement dans la blockchain

Au cours de l'enrôlement, le nœud, qu'il soit régulier ou mineur, télécharge un logiciel qui lui permet de s'interfacer avec la blockchain. Ce logiciel est personnalisé grâce à un numéro de compte blockchain (par exemple, une adresse Bitcoin de 160 bits) et un jeu de clés publique et privée. Il est impératif que le propriétaire du nœud conserve le logiciel téléchargé et le mot de passe qui déverrouille sa clé privée. Dans le cas contraire, il perdra l'accès à son compte blockchain et ne pourra plus passer de transaction à partir de son compte.

---

3 Le procédé de validation par *Proof of Stake,* radicalement différent du *Proof of Work*, est expliqué page 190.

Il doit exister un lien évident et facilement vérifiable entre le numéro de compte et la clé publique. Dans le cas du Bitcoin par exemple, l'adresse Bitcoin correspond classiquement au résultat du hachage de la clé publique associée. Ainsi, tout nœud est en mesure de vérifier la cohérence entre la propriété d'un compte et la signature d'une transaction qu'il est supposé avoir émise. Cette caractéristique évite de recourir à une infrastructure de gestion de clés où la gestion des certificats électroniques est particulièrement lourde et coûteuse.

La phase de transaction

La phase de transaction comprend la validation de chacune des transactions, l'agrégation de ces transactions en un bloc, le travail de minage (PoW, PoS) qui peut prendre plusieurs minutes (environ dix minutes pour le projet Bitcoin), la diffusion du bloc miné, la validation d'un nouveau bloc par ses pairs et l'insertion du bloc dans la blockchain.

Chaque blockchain laisse une certaine latitude au nœud émetteur pour préciser les conditions à satisfaire pour qu'une transaction soit effective.

Pour le projet Bitcoin, la règle implicite consiste à vérifier qu'un nœud dispose de suffisamment de Bitcoins pour émettre la transaction. Le nœud émetteur quant à lui peut imposer, sous forme d'un programme écrit en script, ses propres conditions, par exemple que le bénéficiaire prouve son identité en émettant une signature valide ou plusieurs signatures dans le cas où le bénéficiaire disposerait par exemple de plusieurs comptes et souhaiterait augmenter le niveau de sécurité.

Dans le cadre d'Ethereum, les règles sont fixées par les développeurs de *smart contracts*.

Quelles que soient les règles particulières adoptées par chaque type de blockchains, dans tous les cas une transaction doit nécessairement contenir (voir Figure 8, page 186) :

- un identifiant de transaction
- des informations permettant de valider la légitimité de la transaction ou, plus largement, de situer le contexte de la transaction. Le projet Bitcoin fait référence à des entrées (*inputs*) qui permettent à l'émetteur Bertrand d'identifier plusieurs transactions antérieures (celles d'Anne et Alice) pour justifier d'un solde suffisant, et de prouver qu'il satisfait bien les conditions imposées par Anne et Alice (disposer de la clé publique et d'une signature) pour disposer des montants transférés
- des informations précisant le résultat de la transaction. Le projet Bitcoin définit des sorties (*outputs*) qui précisent les bénéficiaires du virement (Charles et Zoé),

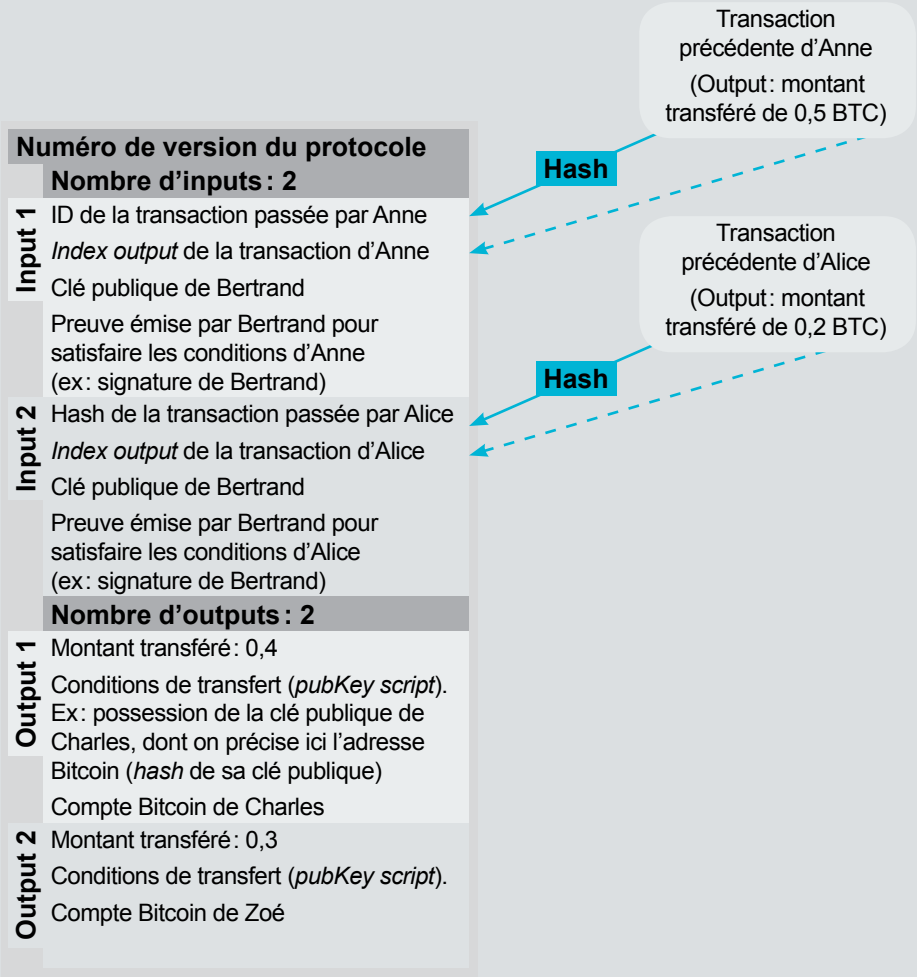


Figure 8. Format simplifié d'une transaction Bitcoin

le montant associé, et les conditions que les bénéficiaires doivent satisfaire pour récupérer le montant. À la manière d'un livre de compte, l'équilibre peut être atteint entre *inputs* et *outputs*, mais si le montant en *output* est moins élevé qu'en *input*, cela signifie que le mineur peut bénéficier de la différence pour son travail de minage. Parfois, les frais de transaction sont obligatoires, le montant alloué permettant d'inciter les mineurs à intégrer la transaction dans leur opération de minage.

La constitution des blocs

Un bloc regroupe un ensemble de transactions. Il vise à cristalliser le contenu des transactions et du bloc, ainsi que la position du bloc dans la blockchain, de manière à rendre impossible toute modification accidentelle ou malveillante du contenu de la blockchain. Cette cristallisation repose sur deux procédés essentiels complémentaires.

Le premier procédé cherche à rigidifier la structure de transactions et de blocs en venant souder tous ces éléments entre eux. À cette fin, les fonctions de hachage sont utilisées intensivement et sont parfois organisées pour produire un arbre de Merkle[4]. Mais si les fonctions de hachage empêchent de modifier partiellement un bloc de la chaîne, elles n'éliminent pas les actes d'écrasement éventuel des derniers blocs. Ce sont les mécanismes de minage couplés à l'architecture décentralisée de stockage et de calculs qui fournissent des garanties de confiance. Tous les éléments apportant structurellement et fonctionnellement de la confiance sont présentés en section 11.3, page 192.

Si l'on se réfère à la structure du projet Bitcoin (cf. Figure 9, page 188), un bloc est composé d'un entête incluant une signalétique utile au fonctionnement de la blockchain, d'un contenu regroupant les transactions et d'un nonce, c'est-à-dire un nombre aléatoire utile à l'opération de minage et d'autres éléments explicités ci-dessous.

Lors de chaque transaction, un identifiant (TxID) est calculé : il correspond au haché du contenu de la transaction. L'arbre de Merkle permet ensuite de solidifier l'ensemble des transactions en calculant des hashs successifs jusqu'à trouver la racine de l'arbre. Le résultat est alors inscrit dans l'entête du bloc. Le contenu de l'entête est alors fortement lié au contenu du bloc, ce qui ultérieurement servira à prouver l'intégrité du contenu du bloc.

---

4 « *En informatique et en cryptographie, un arbre de Merkle ou arbre de hachage est une structure de données contenant un résumé d'information d'un volume de données, généralement grand (comme un fichier)* .» Wikipédia

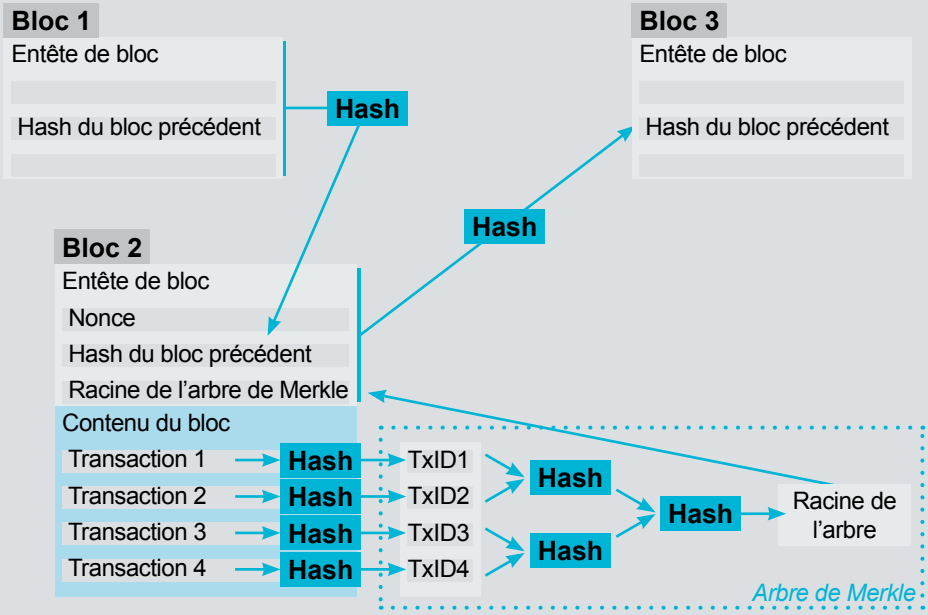


Figure 9. Format simplifié d'un bloc Bitcoin et de son chaînage dans la blockchain

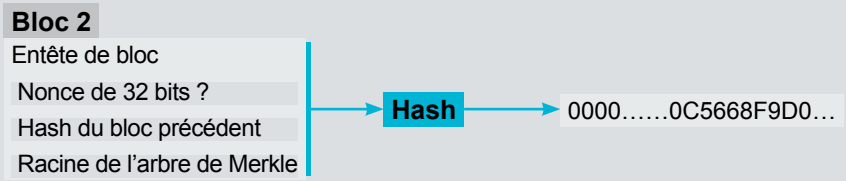


Figure 10. Travail de minage de type PoW sur l'entête du bloc Bitcoin

Le deuxième procédé de cristallisation garantit, quant à lui, l'intégrité de la place du bloc dans la blockchain. Cette propriété est assurée essentiellement en chaînant les blocs entre eux, à partir du premier bloc de la chaîne appelé « *Genesis Block* ».

► Sur la Figure 9, page 188, le bloc 2 est bien situé entre les blocs 1 et 3, ce qui peut être vérifié en s'assurant que le haché du bloc 1 est correctement renseigné dans l'entête du bloc 2. Il en va de même pour le haché du bloc 2 dans l'entête du bloc 3.

Lorsque le PoW est résolu simultanément par deux mineurs, les autres nœuds reçoivent alors deux blocs validés mais différents. Les deux blocs sont alors ajoutés à la chaîne au même niveau, ce qui crée un effet de fourche et démarre deux chaînes distinctes.

Ce problème de dédoublement s'auto-régule, tout simplement par le fait que l'effort de minage n'est pas réparti équitablement entre les deux blockchains temporairement distinctes. Ainsi la blockchain qui grandit plus vite que l'autre sera considérée valide. Pour Bitcoin, il est admis qu'au bout de cent blocs ajoutés à la blockchain, le problème de dédoublement est résolu. Bien entendu, cela suppose de réintégrer les transactions invalidées qui figurent dans la blockchain abandonnée. Il est également convenu qu'une transaction de type Bitcoin est considérée effectivement passée à la condition qu'elle soit « enterrée » sous six blocs, ce qui nécessite d'attendre une heure avant que le bénéficiaire ne puisse disposer de ses Bitcoins et réaliser lui-même une transaction. Cette condition est un frein très fort à l'utilisation des blockchains dans un environnement dynamique, ce qui amène les chercheurs à s'intéresser à des alternatives comme le *Proof of Stake*.

La validation de l'opération de minage

L'opération de minage permet au mineur de construire un bloc valide par la résolution d'un problème mathématique complexe et de se voir octroyer un gain. Avant de démarrer cette résolution, le mineur ajoute une transaction appelée transaction « *coinbase* » dans le bloc à traiter afin d'être rémunéré. À cette fin, la politique de la blockchain l'autorise à créer de la monnaie et à ne pas respecter la règle applicable aux transactions standard selon laquelle le montant de l'*output* doit être inférieur au montant en *input*. La transaction « *coinbase* » précise le mineur bénéficiaire et le montant de son gain. De la sorte, après résolution du problème, si le bloc est accepté par les autres mineurs de la blockchain, le mineur aura acquis le gain ainsi que l'ensemble des frais de transaction. Les concepteurs

du projet Bitcoin ont prévu que la récompense du bloc diminue avec le temps, et que les mineurs doivent de plus en plus compter sur les frais de transaction pour être rémunérés.

La validation par preuve de travail (*Proof of Work* – PoW)

Le problème à résoudre, pour valider un bloc, consiste à trouver la valeur du champ Nonce de 32 bits à renseigner (cf. Figure 10, page 188) dans l'entête du bloc de sorte que le hachage de l'entête du bloc aboutisse à un résultat inférieur à une certaine valeur. Plus cette valeur est petite, plus le problème est difficile à résoudre. Pour conserver la même complexité calculatoire au fil du temps, la politique de la blockchain ajuste le niveau de difficulté.

- Dans le cas du projet Bitcoin, un bloc est miné en moyenne toutes les dix minutes. Tous les 2016 blocs, soit une période théorique de deux semaines, une moyenne est calculée ; si le temps moyen est trop court, la difficulté est revue à la hausse ; s'il est trop long, la difficulté est revue à la baisse.

L'un des inconvénients majeurs du PoW est que le mineur doit effectuer de nombreux calculs. Un type de preuve plus simple, le *Proof of Stake* (PoS), a donc été développé.

La validation simple par preuve d'enjeu (*Proof of Stake* – PoS)

L'objectif de la validation par PoS est d'alléger la procédure de minage par PoW. Cet allégement va permettre à la fois de réduire les dépenses énergétiques et d'obtenir une meilleure réactivité de la blockchain. L'enjeu est donc à la fois écologique et économique, puisque la blockchain va pouvoir inscrire plus rapidement des transactions, et donc traiter de plus gros volumes.

- Le projet Ethereum développe actuellement un algorithme PoS appelé Casper. La migration vers Casper, prévue d'ici à deux ans, devrait permettre de valider des blocs en quelques secondes, voire moins d'une seconde, et ainsi de traiter 20 000 transactions par seconde.

D'un point de vue fonctionnel, la validation par PoS est encore plus décentralisée que celle par PoW. En effet, le PoW impose que les nœuds effectuent exactement les mêmes opérations de minage depuis la validation des transactions jusqu'à la résolution du problème. Ceci a pour effet de déséquilibrer le fonctionnement de la blockchain, et ce d'autant

plus que la Chine centralise aujourd'hui une grande partie du minage des Bitcoins. Pour sa part, l'approche PoS Casper répartit le volume de transactions à valider, non pas sur la totalité des nœuds, mais en plusieurs sous-groupes. Le système privilégie les nœuds qui ont le plus fort engagement, c'est-à-dire ceux qui ont un portefeuille le plus fourni (en Bitcoin par exemple) et qui ont donc le plus à perdre en cas de malveillance. De plus, un système d'amendes est prévu pour dissuader les mauvais comportements.

Si le principe PoS est à première vue prometteur, la prudence reste de mise. Même s'il est en test sur Ethereum, il n'a pas réellement fait ses preuves, contrairement au procédé PoW déjà testé dans les projets large échelle Bitcoin et Ethereum.

Les mécanismes d'incitation à miner

Sans le minage, la blockchain ne pourrait pas fonctionner. Il est donc primordial de proposer un gain appelé crypto-carburant suffisamment attractif pour inciter un nombre suffisant de mineurs à miner et à stocker la blockchain. Le gain doit compenser l'achat de matériel de fortes capacités (en calculs et/ou stockage) et son maintien en état ainsi que le coût de l'énergie.

Pour rappel, le mineur doit disposer de puissances de calculs importantes. Un gain lui est versé pour chaque minage réussi et accepté par ses pairs sous la forme d'une transaction qu'il ajoute dans le bloc (cf. «La validation de l'opération de minage», page 189).

Les concepteurs définissent librement la nature du crypto-carburant. Celui-ci est généralement lié à l'activité portée par la blockchain. Il peut s'agir de la crypto-monnaie Bitcoin ou ether pour le projet Ethereum, ou de techniques de fidélisation classiques : bénéficier d'espace de stockage, de ressources de calculs, de capacité de votes plus importante, de quelques heures de location de voiture, d'un séjour dans un hôtel ou d'un voyage.

Dans tous les cas, ce procédé d'incitation implique de définir une unité virtuelle qui permet d'accumuler des gains en fonction des efforts fournis, au même titre qu'une carte de fidélité.

11.3. Les facteurs de la confiance

Une blockchain dispose de plusieurs atouts pour susciter la confiance. Cette confiance n'est cependant pas absolue.

L'architecture décentralisée et la neutralité de la gouvernance

En premier lieu, la confiance repose sur une ***architecture décentralisée*** composée d'un grand nombre de nœuds dépendant d'organisations variées. Contrairement à une architecture centralisée où les décisions peuvent être prises unilatéralement, il faut parvenir à un consensus ou contrôler plus de 50% des nœuds (ou de la puissance de calcul) pour agir sur le système. Le fait que l'architecture repose sur une multitude de nœuds, garantit une plus grande impartialité dans le travail de validation et de stockage de la blockchain, une meilleure disponibilité du service et donc une confiance accrue dans le service.

Si la confiance suppose que la répartition des ressources informatiques utiles aux calculs et au stockage soit équilibrée entre organisations, on observe cependant une tendance inverse dans le cas du Bitcoin avec la création de fermes de minage (*mining pool*). À plusieurs reprises, les trois plus grosses fermes ont réussi à détenir à elles seules plus de 50% de la puissance du réseau. Or, cette barre des 50% est critique car elle permet à une organisation ou un regroupement d'organisations de réaliser l'attaque des 51%, c'est-à-dire de censurer des transactions avant le processus de minage, de favoriser le travail de minage de ses propres mineurs pour empocher les gains à la place de mineurs plus rapides, de réussir en cas de dédoublement de la chaîne à imposer une chaîne plus longue avec une probabilité raisonnable de succès, et donc de maîtriser l'historique de la chaîne. Cependant, l'attaque des 51% ne permet ni de voler des gains, ni d'émettre des transactions frauduleuses.

En second lieu, la confiance repose sur la ***neutralité de la gouvernance***. Avant d'investir de son temps et son argent dans une blockchain, il est nécessaire de se poser les questions suivantes : « *la neutralité de la gouvernance est-elle garantie ?* » Les acteurs, c'est-à-dire le petit groupe de personnes impliquées à faire évoluer le code et le protocole, sont-ils réellement indépendants dans leurs prises de décision et capables de résister à des pressions politiques, industrielles… ? Si ce n'est pas le cas, le principe fondamental de décentralisation n'est plus respecté. De plus, si l'ensemble de ces acteurs contrôle plus de la moitié de la puissance de calcul de la blockchain, alors le principe de consensus

n'est lui non plus pas respecté pour les raisons suivantes. Quand une mise à jour du code de la blockchain impliquant de nouvelles règles de fonctionnement est diffusée dans la blockchain, l'administrateur d'un mineur a le choix d'accepter ou de refuser la mise à jour. Il peut s'agir d'une transformation des règles mineure et rétrocompatible – on parle alors de « *soft fork* » - ou d'une transformation importante et sans compatibilité ascendante – on parle alors de « *hard fork* ». Pour devenir fonctionnel, un « *soft fork* » doit recueillir le soutien d'une majorité de mineurs, tandis que le « *hard fork* » nécessite un consensus beaucoup plus large. En cas d'absence de consensus avec deux populations conséquentes de mineurs, la blockchain initiale se scinde en deux. Les deux blockchains suivent alors leur propre chemin. Un regroupement d'acteurs qui détiendraient la majorité de la capacité de minage, peut donc, par collusion, modifier les règles de gouvernance, créer des « *forks* » qui créent de la confusion, de la double dépense (voir plus bas) et un risque de dévaluation de la crypto-monnaie.

La transparence pour une meilleure auditabilité

La confiance repose également sur le ***principe de transparence***. Ce principe se décline en plusieurs éléments tant au niveau des chaînes de transaction que des algorithmes.

- **Traçabilité et auditabilité de toute la chaîne de transactions :** la publication dans l'espace public de toutes les transactions réalisées depuis l'origine de la blockchain (Bloc 0 ou « *Genesis Block* ») permet à chacun de vérifier l'intégrité de la chaîne, et de retracer tous les mouvements associés à un compte. Ainsi, la fraude est en théorie éliminée ; tout se voit, tout se sait, dans la limite des garanties offertes par le pseudonymat.

- **Transparence des algorithmes :** le code utilisé pour miner, afin de s'interfacer avec la blockchain, ou pour mettre en œuvre un *smart contract* est lisible par tous. L'avantage est de permettre aux experts de la communauté d'utilisateurs de scruter le code et d'alerter en cas de suspicion. La confiance repose donc sur les lanceurs d'alertes.

La sécurité informatique

Enfin, la blockchain permet d'assurer une bonne gestion du risque informatique (cf. Chapitre 4), et ce grâce aux caractéristiques suivantes :

- **Une chaîne rigide et inaltérable :** les blocs contenus dans la blockchain ainsi que l'enchaînement de ces blocs sont rigidifiés pour éviter toute altération ultérieure de la chaîne. Pour cela, la sécurité s'appuie sur le caractère distribué de l'architecture, et sur un mécanisme de consensus fort. À cela s'ajoute éventuellement un mécanisme d'incitation à adopter un bon comportement, un mécanisme de dissuasion des mauvais comportements, et du matériel cryptographique pour apporter des garanties techniques fortes. Le PoW s'appuie sur un consensus et une preuve cryptographique coûteuse en calculs, tandis que le PoS s'appuie sur un consensus et des mécanismes d'incitation et de dissuasion qui n'ont pas encore totalement fait leurs preuves sur un système réel.

- **L'authenticité des transactions protégées par pseudonyme :** le besoin d'agir en toute discrétion mais aussi l'assurance que des moyens de sécurité adaptés sont mis en œuvre pour garantir la validité des transactions et donc des gains acquis sont gages de confiance pour les usagers de la blockchain.

- **Un niveau de sécurité adaptatif :** les avancées technologiques rendent vulnérables au fil des années des procédés de sécurité réputés résistants à une époque. Pour maintenir la confiance dans les outils techniques, plusieurs blockchains prévoient des mécanismes dont le niveau de sécurité est évolutif.

Cependant, la confiance dans la blockchain est loin d'être absolue. Plusieurs éléments peuvent en effet la remettre en cause suite aux déconvenues suivantes :

- **Des erreurs de programmation :** pour les blockchains programmables (ou non), un risque fort est lié à des erreurs humaines de programmation, comme ce fut le cas en 2016 pour l'attaque de détournement de fonds réalisée sur Ethereum. En quatre semaines, la plateforme *Decentralized Autonomous Organisation*

(*The DAO*)[5], qui permet à sa communauté d'investir en capital-risque, a procédé à une levée de fonds spectaculaire de 150 millions de dollars pour alimenter des projets de startups souhaitant utiliser Ethereum. *The DAO* a ensuite été piratée à hauteur de 50 millions de dollars par des attaquants qui ont exploité une vulnérabilité dans le code des *smart contracts*. Cette erreur a permis à ces derniers d'appeler à de multiples reprises la fonction du programme autorisant une sortie de fonds à partir d'un compte. Comme l'a rappelé dans un post de blog le co-fondateur d'Ethereum Vitalik Buterin, « *le problème affecte seulement DAO, la blockchain Ethereum reste parfaitement sûr*e». En 2017, une autre attaque a mis en cause une erreur dans le logiciel de porte-monnaie *Parity Wallet*, et a conduit au vol de 30 millions de dollars en ethers.

- **Double dépense :** la double dépense consiste à émettre deux transactions portant sur le même objet et qui devraient normalement s'exclure l'une l'autre. Il s'agit d'un acte volontaire malveillant d'un participant qui est normalement arbitré lors du minage. Cependant, il peut arriver que dans un processus de dédoublement de chaîne, chaque transaction soit validée indépendamment par chaque chaîne. À ce moment-là, le bénéficiaire sait s'il dispose ou non des gains qu'une fois la chaîne la plus courte abandonnée. Pour Bitcoin, le délai raisonnable considéré est d'environ une heure, soit le temps équivalent à la constitution de six blocs.

- **Rétention de transactions :** un mineur peut avoir intérêt à ne pas partager une transaction dont les frais de transaction sont élevés. En gardant cette transaction pour lui jusqu'au succès du minage d'un bloc, il s'assure qu'elle sera incluse dans un de ses blocs et qu'il bénéficiera de la récompense. Il peut donc s'écouler un certain laps de temps avant que cette transaction ne soit inclue dans la blockchain. Cette attaque de rétention sera de plus en plus crédible à l'avenir car le modèle de paiement reposera de plus en plus sur les frais de transaction à mesure que les récompenses de bloc diminueront. De la même façon, un mineur bien connecté peut retenir un bloc avant de le diffuser pour bénéficier d'un délai supplémentaire dans l'opération de minage. Ce n'est que lorsqu'il recevra un bloc concurrent qu'il

5 Blockchain France fournit la définition suivante d'une DAO : « *Une DAO (*Decentralized Autonomous Organization*) est une organisation fonctionnant grâce à un programme informatique qui fournit des règles de gouvernance à une communauté. Ces règles sont transparentes et immuables car inscrites dans la blockchain.* »

pourra alors diffuser massivement son propre bloc. Ces attaques forcent à réfléchir à l'amélioration des mécanismes d'incitation.

- **Blanchiment d'argent :** le problème de blanchiment d'argent se pose dès qu'un nouveau moyen d'échange d'argent est à disposition. Contrairement à ce qu'on pourrait croire, la transparence des transactions passées dans la blockchain n'empêche pas le blanchiment d'argent ; elle le rend juste plus complexe. En effet, des techniques existent pour brouiller les pistes et la traçabilité. La première, très simple, consiste à détenir une multitude de comptes (certains pouvant même n'être utilisés qu'une seule fois) et à réaliser des transactions entre plusieurs de ces comptes. Une autre approche, appelée Coinjoin dans Bitcoin, consiste à fusionner plusieurs transactions en une seule. Plus le nombre de transactions fusionnées (entrantes et sortantes) est important, meilleure est la protection car plus il est difficile de relier un débiteur à un créditeur. Notons toutefois que l'approche Zerocash décrite dans la section suivante garantit la non traçabilité des transactions et rend donc impossible la détection de blanchiment d'argent sur la seule base des éléments fournis dans la blockchain.

11.4. La transparence de la chaîne et l'atteinte à la vie privée

Une blockchain repose sur le pseudonymat des membres participants. Il suffit donc que soit dévoilée l'identité réelle de la personne associée à un compte pour que toutes les transactions effectuées par cette personne depuis son compte soient révélées, et ce, depuis l'origine. Comme expliqué plus haut, plusieurs techniques visent à protéger l'identité réelle des usagers, à savoir posséder des comptes multiples, certains à usage unique, et effectuer plusieurs transactions simultanément sur le principe du Coinjoin de Bitcoin.

Le principe de transparence de la blockchain doit rendre prudents les concepteurs de services quant à la prise en compte de la protection des données personnelles. En effet, toute information de nature privée, qu'elle soit sous forme algorithmique ou de données statiques (données personnelles, clés cryptographiques…), ne doit pas être hébergée en clair dans la blockchain, par exemple au sein d'une transaction. En revanche, la blockchain, pour laquelle il est préférable de limiter la taille des informations stockées dans les transactions pour des raisons de coûts, peut s'appuyer sur une mémoire distribuée,

externalisée et illimitée, qui peut prendre la forme d'un réseau pair à pair fonctionnant à la manière d'un réseau BitTorrent, Gnutella, Napster ou Kademlia. Il s'agit véritablement d'une mémoire externalisée dans la mesure où cette mémoire est indexée grâce à des clés DHT (*Distributed Hash Table*) qui peuvent être référencées dans la blockchain. Cette mémoire peut héberger des données en clair ou des données chiffrées. Dans ce dernier cas, il convient d'assurer la gestion des clés cryptographiques.

En 2014, l'initiative Zerocash a proposé une solution très intéressante de paiement anonymisé et décentralisé[6]. Cette solution assure le transfert de Bitcoins via une blockchain en toute transparence mais sans traçabilité possible des flux monétaires, c'est-à-dire sans révéler ni la source, ni la destination, ni le montant transféré. La solution repose sur le principe du *zero-knowledge* (schémas dits « à apport nulle de connaissance ») qui permet à un utilisateur de prouver la connaissance d'un secret à un tiers sans avoir à en révéler sa valeur. Pour cela, elle s'appuie sur le schéma zk-SNARKs (*zero-knowledge Succinct Non-interactive ARguments of Knowledge*), qui est particulièrement performant avec une preuve établie en quelques millisecondes. L'analogie suivante est souvent reprise pour expliquer le principe du Zerocash : tous les utilisateurs accrochent leurs billets sur un mur, qu'ils décrochent au moment d'une dépense.

Enfin, l'initiative Enigma du *Massachusetts Institute of Technology* (MIT) développée en 2015 propose une plateforme *cloud* décentralisée garantissant la confidentialité des traitements opérés et des informations traitées[7]. Elle s'appuie sur la blockchain pour garantir la traçabilité des opérations effectuées et sur le réseau pair-à-pair Enigma pour effectuer les traitements et le stockage des informations sensibles. L'idée est que chaque nœud du réseau Enigma ne possède qu'une vue partielle et sans valeur de l'information sensible et qu'il effectue un traitement partiel sur cette information. Ainsi, les nœuds n'ont accès individuellement à aucune information sensible, et grâce à des techniques de type SMC (*Secure Multi-party Computing*), il leur est possible de produire de façon collaborative un résultat qui a du sens pour l'application.

---

6 Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014 IEEE Symposium on Security and Privacy.

7 Zyskind, G., Nathan, O., Pentland, A., (2015). Enigma: Enigma: Decentralized Computation Platform with Guaranteed Privacy, http://enigma.media.mit.edu/enigma_full.pdf

11.5. Des limites à prendre en considération

Nous avons pu voir que la technologie blockchain présente des limites structurelles. Elle ne peut pas être présentée comme une garantie de confiance absolue, même limitée à la confiance décidée. En effet, les considérations organisationnelles, de rapports de pouvoir entre les acteurs, d'appropriation par les utilisateurs ou même strictement techniques, complexifient considérablement l'examen de la portée réelle de cette technologie. Elles indiquent en tout cas, une fois de plus, que la simple transparence n'est pas un gage absolu de confiance et du respect des données personnelles.

Rappelons qu'en son temps l'infrastructure à clés publiques (*Public Key Infrastructures* – PKI) a été présentée comme une technologie « révolutionnaire » garantissant la confiance, avant que ses limites ne soient communément admises.

Ainsi, et comme pour les labels dans le sens large, le fait d'utiliser une blockchain apporte certaines garanties, mais il s'agit plus ici d'un moyen d'induire ou de suggérer la confiance de l'utilisateur en mettant l'accent sur les aspects bien choisis de cette technologie.

Conclusion

Armen Khatchatourov
Claire Levallois-Barth
Maryline Laurent
Patrick Waelbroeck

Dans cet ouvrage, nous avons abordé les questions soulevées par un signe de confiance particulier, le ***label en matière des données personnelles***, ainsi que certaines pistes et tendances dans le paysage en cours de construction.

Si la problématique des labels n'est pas nouvelle en soi, comme en atteste leur présence dans les domaines de l'énergie ou de l'alimentation, la spécificité des biens numériques et leur essor exponentiel ne semblent pas permettre de recourir à des solutions déjà éprouvées. La circulation croissante des informations amène donc à poser sous une forme nouvelle la question des modes de gouvernance des données personnelles.

En ce sens, il faut sans doute concevoir les labels et l'intervention des experts qu'ils impliquent comme un outil d'accompagnement pour permettre aux responsables de traitements de données personnelles d'augmenter progressivement le niveau de protection des données qu'ils collectent et utilisent. La question reste ici ouverte quant aux modalités concrètes de cet accompagnement. Dans quelle mesure faut-il laisser les entreprises ou les associations professionnelles élaborer leurs propres référentiels et procédures d'audit ? Il nous semble ici essentiel d'impliquer l'ensemble des parties prenantes au processus de construction en reconfigurant le rôle aussi bien des régulateurs que des régulés, sans oublier les citoyens. En particulier, l'intervention de l'État nous semble incontournable au moins sur trois points : l'établissement des référentiels, l'accréditation des certificateurs en faisant intervenir des organismes existants et spécialisés tels que le COFRAC, et l'imposition de sanctions véritablement dissuasives afin d'assainir le marché. Car, au vu des abus potentiels, une forme de pression sur les entreprises semble ici nécessaire, ne serait-ce qu'à travers une menace de perte de réputation, et donc de confiance.

Mais, nous l'avons également constaté au cours de cet ouvrage (dans les chapitres 5 et 6), une intervention étatique trop stricte, ou entraînant des coûts trop importants, pourrait inciter les acteurs à se tourner vers des labels privés, lesquels peuvent comporter un effet potentiellement trompeur, en présentant une image embellie de la protection des données. À n'en pas douter, ce risque est réel compte tenu, d'une part, de la tendance actuelle de transfert vers le domaine du privé de ce qui relevait jadis, à tort ou à raison, du domaine de l'État et, d'autre part, du fait que les modalités d'élaboration et de délivrance des labels privés ne sont pas suffisamment encadrées sur l'ensemble de leur cycle de vie. La question qui est ainsi posée par ces signes de confiance est celle de la délégation des politiques de gestion des données personnelles des citoyens au secteur privé.

D'un point de vue plus restreint, on peut supposer que les labels présentent une utilité économique à la fois pour le consommateur et l'entreprise. « Rassurer » le client ou prospect, lui fournir des indices quant au bon fonctionnement des services numériques, peut sans doute lever certaines barrières. Ce constat est confirmé par l'enquête menée par la ***Chaire Valeurs et Politique des Informations Personnelles*** auprès de 2000 internautes en mars 2017, et qui montre que les utilisateurs avertis sont aussi ceux qui sont enclins à consommer le plus[1].

Cependant, aujourd'hui, force est de constater qu'il n'existe pas de modèle d'affaires en la matière. Le label en tant que signe de confiance fait nécessairement partie de la stratégie de communication de l'entreprise (cf. Chapitres 3 et 9), communication qui doit permettre aux consommateurs d'évaluer la fiabilité du signal envoyé. Comme nous l'avons souligné, les signaux envoyés sont trop nombreux et trop faibles pour être perçus par le public et les entreprises. De plus, les coûts associés au processus de labellisation varient de quelques centaines à plusieurs milliers d'euros en fonction notamment des exigences imposées, de la durée de validité du label et du processus d'audit retenu (cf. Chapitres 6 et 7). La question du coût à la fois financier et temporel, est ici importante. Il est nécessaire que l'obtention d'un label soit relativement onéreuse pour les entreprises, afin que le label puisse jouer pleinement son rôle de signal de bonnes pratiques en matière de protection des données personnelles. Pour autant, il ne doit pas être trop élevé afin de ne pas dissuader les entreprises, ou de ne pas leur faire augmenter excessivement les prix des services concernés (cf. Chapitre 9). Si ce coût est uniquement à la charge des entreprises, comment les inciter à se faire labelliser alors même que le retour sur investissement est difficile à déterminer ? La prise en charge de ce financement du côté des organismes labellisateurs publics se pose également : comment faire en sorte qu'ils puissent supporter financièrement le coût de l'audit ?

Face à ces interrogations, la tentation est grande d'asseoir la labellisation sur des éléments techniques dont on suppose qu'ils sont à même d'établir la confiance. Mais les solutions techniques peuvent-elles répondre à elles seules à la problématique de la confiance et envoyer un signal de qualité ? Ne se réduisent-elles pas à une évaluation du risque et, au mieux, à l'établissement d'un type particulier de confiance que nous avons

1 Waelbroeck, P., Khatchatourov, A., Levallois-Barth, C. (2017) Synthèse du Rapport « Données personnelles et confiance : quelles stratégies pour les citoyens-consommateurs en 2017 ? », Chaire Valeurs et Politiques des Informations Personnelles, 23 juin 2017.

qualifié de « ***confiance décidée*** » (cf. Chapitre 1) ? Cette évaluation du risque ne s'opère-t-elle pas selon les critères qui sont eux-mêmes établis dans un jeu de prises de position entre les acteurs concurrents ? En effet, les processus de gouvernance ne se réduisent pas à des signes extérieurs de transparence et à l'implémentation de telle ou telle technologie fut-elle qualifiée, de manière plus ou moins déclarative, de *data protection by design* à un moment donné. C'est l'articulation entre les technologies, leur évolution, et les mécanismes de gouvernance qu'il faut ici considérer, ainsi que le démontre l'exemple de la blockchain (cf. Chapitre 11) : même si cette technologie apporte des preuves de fiabilité et de robustesse d'un point de vue technique et promet dans certains cas une meilleure protection à travers une gouvernance décentralisée, encore faut-il que les mineurs de la blockchain ne soient pas majoritairement contrôlés par quelques acteurs. La qualification d'une solution technologique apporte des preuves de fiabilité et de robustesse d'un point de vue technique, mais elle n'apporte aucune garantie quant à son bon usage et ne fournit que des réponses partielles quant à sa gouvernance. Loin d'une vision statique, et pour tout dire simplificatrice qui consisterait à pouvoir résoudre les problématiques de gouvernance par des procédés techniques, la question des labels met en lumière la dimension temporelle des projets économiques et politiques concurrents.

~

L'essentiel de cet ouvrage s'est employé à décrire cette conjonction entre la « ***confiance décidée*** » et un type nouveau de la confiance que nous sommes amenés à qualifier de « ***confiance suggérée*** » (cf. Chapitre 1). On entrevoit que, du moins en ce qui concerne le cadre de régulation que nous avons décrit (cf. Chapitres 2 et 9), les utilisateurs restent souvent cantonnés dans un rôle passif, ceux à qui les labels sont adressés ; ils n'accèdent que rarement à un rôle actif, qui consiste à participer au processus même d'élaboration des suggestions. Des mécanismes de labellisation (et de confiance) qui s'opéreraient de proche en proche, à l'instar des initiatives *peer-to-peer*, doivent donc être explorés dans le futur. Encore faut-il que les utilisateurs soient en mesure de procéder de façon décentralisée à l'évaluation des services numériques impliquant des données personnelles. Or, cette évaluation diffère fondamentalement de la notation « collaborative » d'une chambre d'hôtel ou d'une livraison par correspondance. Tout reste donc à construire pour parvenir à des formes d'audit et de labels citoyens. L'enjeu est ici de taille : il porte sur l'implication des citoyens et leur sentiment d'appartenance à la société numérique, et non seulement à l'économie numérique.

En définitive, la thématique des labels en matière de données personnelles soulève des enjeux qui nous semblent essentiels et pour tout dire ambivalents du point de vue sociétal. D'un côté, on déresponsabilise la personne, en mettant de fait à mal le projet initial des Lumières et de l'individu autonome : à se conformer sans réserve aux prescriptions et signes provenant des instances extérieures, l'individu risque de perdre la capacité critique nécessaire. Par exemple, la généralisation de la labellisation ne risque-t-elle pas de conduire à terme à la généralisation des conduites qui se donnent bonne conscience ou à une nouvelle forme de dépendance de l'utilisateur ?

D'un autre côté, on « responsabilise »[2] l'individu en l'obligeant à une « autogestion de soi » et de ses données personnelles, par exemple à travers un tableau de bord incorporé dans le logiciel. C'est dès lors l'individu qui risque d'en supporter le coût, dans la mesure où telle ou telle transaction via un service non-labellisé pourrait lui être désormais reprochée, ou en tout cas être perçue comme comportant un risque (économique, de sécurité, etc.) qu'il doit lui-même assumer. On considère donc que l'individu est responsable de ses choix, sans

2 Nous interprétons ici librement la thématique de responsabilisation telle que mise en place par Michel Foucault dans les Cours au Collège de France à la fin des années 1970, notamment Sécurité, territoire, population et Naissance de la biopolitique.

pour autant suffisamment le sensibiliser aux enjeux éthiques, économiques et politiques liés à la circulation mondiale des données personnelles. De même, on ne s'interroge pas sur les effets des choix ponctuels qu'il opère, en se conformant aux suggestions qui se mettent ainsi en place, sur la constitution de son identité vécue ou de sa capacité d'agir[3].

En un certain sens, il s'agit donc ici d'un nouveau paradigme de prescription des comportements des utilisateurs, d'une tendance profonde dans la société : il ne s'agit plus de formes de prescription ferme qui interdisent telle ou telle action, mais de formes de prescription souple qui suggèrent tel ou tel produit ou service (cf. Chapitres 1 et 2). Cette « confiance suggérée » dans le numérique constitue néanmoins bel et bien un instrument de gouvernance.

Il s'ensuit que, en matière de données personnelles, les labels sont un cas très particulier de « régulation » car ils seront amenés à reconfigurer non seulement les rôles des acteurs (régulés ou régulateurs) ou les mécanismes de concurrence, mais aussi et surtout la manière dont la société conçoit le vivre-ensemble à l'heure où toute action individuelle ou collective crée des données et est guidée par elles.

3 On consultera à ce sujet Khatchatourov, A. et Chardel, P.-A. (2016). La construction de l'identité dans la société contemporaine : enjeux théoriques. *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Annexes

Table des illustrations

Index

A

B

C

D

E

F

G

I

J

L

M

N

O

P

Q

R

S

T

U

V

Liste des abréviations

AFCDP	Association Française des Correspondants à la protection des Données Personnelles
AFNOR	Association française de Normalisation
Al.	Alinéa
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
Art.	Article
BBB	*Better Business Bureau*
CA	Cour d'Appel
Cass.	Cour de cassation
CCRA	*Common Criteria Recognition Arrangement*
CSPN	Certificat de Sécurité de Premier Niveau
CE	Communauté Européenne
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation en ÉLECtronique et en électrotechnique
CEPD	Comité Européen de Protection des Données
CESTI	Centre d'Évaluation de la Sécurité des Technologies de l'Information
Cf.	*Confer*
CIL	Corresponsant Informatique et Libertés
CISPE	*Cloud Infrastructure Service Providers in Europe*
CNIL	Commission Nationale de l'Information et des Libertés
COFRAC	COmité FRançais d'ACcréditation
coll.	collection
Crim.	Chambre criminelle
D.	Dalloz
DAO	*Decentralized Autonomous Organisation*
déc.	Décision
DHT	*Distributed Hash Table*
EAL	*Evaluation Assurance Level*
ECC	*Elliptic Curve Cryptography*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
eIDAS	*Electronic IDentification And trust Services*
ESRB	*Entertainment Software Rating Board*
FEVAD	FEdération du e-commerce et de la Vente A Distance
FNTC	Fédération des Tiers de Confiance du numérique
FTC	*Federal Trade Commission* – Commission fédérale américaine du commerce

G29	Groupe Article 29
ISO	*International Organization for Standardization*
J.O.C.E.	Journal Officiel de la Communauté Européenne
J.O.R.F.	Journal Officiel de la République Française
J.O.U.E.	Journal Officiel de l'Union européenne
LCEN	Loi pour la Confiance dans l'Economie Numérique
n°	numéro
p.	page
PASSI	Prestataire d'Audit de la Sécurité des Systèmes d'Information
PDIS	Prestataire de Détection d'Incidents de Sécurité
PFPDT	Préposé Fédéral à la Protection des Données et à la Transparence
PKI	*Public Key Infrastructure*
PoW	*Proof of Work*
PoS	*Proof of Stake*
PRIS	Prestataire de Réponse aux Incidents de Sécurité
PSCE	Prestataire de Service de Certification Électronique
PSHE	Prestataire de Service d'Horodatage Électronique
Règlement eIDAS	Règlement (UE) no 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
RGPD	Règlement Général sur la Protection des Données (Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), JOUE L 119/1 du 4 mai 2016).
RLDI	Revue Lamy Droit de l'Immatériel
RSA	Rivest Shamir Adleman
SHA	*Secure Hash Algorithm*
SOG-IS	*Senior Officials Group Information Systems Security*
SQS	Association suisse pour les Systèmes de Qualité et de Management
SSI	Sécurité des Systèmes d'Information
ToE	*Target of Evaluation* (périmètre de labellisation)
UBA	*User Behavior Analytics*
UE	Union européenne
ULD	*Unabhängiges Landeszentrum fuer Datenschutz* (Autorité de protection des données du Land allemand du Schleswig-Holstein)

Liste des entretiens effectués entre octobre 2015 et septembre 2017

Par Claire Levallois-Barth et Delphine Chauvet

Arnaud Belleil, Directeur transformation digitale, Cecurity.com

Maître Alain Bensoussan, Alain Benoussan Avocats

Jérome Beranger, co-fondateur et Chief Strategy Officer, ADEL

Florence Bonnet, CIL Consulting

Johanna Carvais, Responsable du pôle Labels, et **Valérie Bourriquen**, Juriste, pôle Labels, CNIL

Maître Etienne Drouard, avocat associée K&L Gates

Eric Lachaud, PhD candidate in Law and Technology, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Pays-Bas

Maître Denise Lebeau-Marianna, avocat associée DLA Piper France LLP

Xavier Leclerc, Président, Axil-Consulting

Maître Nathalie Metallinos, IDEA avocats

Laurent Midrier, Vice-Président Stratégie & Innovation, Bureau Veritas

Hervé Molina, Directeur de l'Audit Informatique et **Jean-Christophe Carbonel**, Chef de Mission, Direction de la sécurité globale, Groupe La Poste

Maître Fabrice Naftalski, avocat associé EY

Maître Yann Padova, avocat associé Baker & McKenzie (Paris), ancien membre (Commissaire) de la Commission de Régulation de l'Energie (CRE) en charge des questions relatives à la protection des données personnelles (2015-2017), ancien Secrétaire général de la CNIL (2006-2012)

Benoit Pellan, Chef de produit numérique, Département Innovation et Développement, AFNOR certification

Bruno Rasle, Délégué général, AFCDP (Association Française des Correspondants à la Protection des Données)

Frédéric Richter, Président, Stiftung Datenschutz, Allemagne

Stéphane Schmoll, Directeur général et **Laurent Cellier**, Directeur Expérience Utilisateur et Correspondant Informatique et Libertés, Deveryware

Maître Thibault Verbiest, avocat associé De Gaulle Fleurance & Associés

Cécile Wendling, Directrice de la prospective, Groupe AXA

Delphine Zeberro, Directeur - IT Advisory, Deloitte

Bibliographie

Acquisti, A. (2012). Nudging Privacy: The Behavioral Economics of Personal Information. *in Jacques Bus, Malcolm Crompton, Mireille Hildebrandt, George Metakides (eds), Digital Enlightenment Yearbook 2012*, IOS Press.

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.

Akerlof, G. A. (1970). The market for lemons : Quality uncertainty and the market mechanism. The quarterly journal of economics, 488-500.

Anton, A., Earp, J. B., Bolchini, D., He, Q., Jensen, C., Stufflebeam, W. (2003). The lack of clarity in financial privacy policies and the need for standardization. IEEE Security & Privacy, 2(2):36-45. DOI : 10.1109/MSECP.2004.1281243.

Bakos, Y., Marotta-Wurgler, F., Trossen, D. R. (2014). Does anyone read the fine print? Consumer attention to standard-form contracts. The Journal of Legal Studies, 43(1), 1-35. DOI : 10.1086/674424.

Barabàsi, AL. (2002). Linked: The New Science of Networks, Perseus, Cambridge, MA.

Becher, S. I., Zarsky, T. (2015). Online Consumer Contracts: No One Reads, But Does Anyone Care?

Ben-Sasson, E., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., (2014). Zerocash: Decentralized Anonymous Payments from Bitcoin, 2014 IEEE Symposium on Security and Privacy.

Bjørner, T. B., Hansen, L. G., & Russell, C. S. (2004). Environmental labeling and consumers' choice—an empirical analysis of the effect of the Nordic Swan. Journal of Environmental Economics and Management, 47(3), 411-434. DOI : 10.1016/j.jeem.2003.06.002.

Brounen, D., Kok, N. (2011). On the economics of energy labels in the housing market. Journal of Environmental Economics and Management 62(2):166-179. DOI : 10.1016/j.jeem.2010.11.006.

Cabral, L, Hortascu, A. (2010). Dynamics of Seller Reputation : Theory and Evidence from eBay, Journal of Industrial Economics, v. 58, no.1, March 2010, pp. 54-78

Carvais, J. (2015). Le label CNIL comme outil de conformité, *in AFCDP, Correspondant Informatique et Libertés, Bien plus qu'un métier*. pp. 497 à 510.

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

Chochois, M., Magnin, N., (2015). Qualité des produits de SSI, les labels français, Techniques de l'ingénieur, H5825 v2, octobre 2015.

Connolly, C. (2008). Trustmark Schemes Struggle to Protect Privacy, Working paper.

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.

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

Foucault, M. (2004). Naissance de la biopolitique, Paris, Gallimard/Le Seuil, coll. « Hautes Études ».

Fournier, P. (2015). La responsabilité comme mode de gouvernement néolibéral : l'exemple des programmes d'aide aux familles aux États-Unis de 1980 à nos jours. *in Les ateliers de l'éthique*, Volume 10, Numéro 1.

Gao, Z. (2007). Effects of additional quality attributes on consumer willingness-to-pay for food labels (Doctoral dissertation, Kansas State University).

Khatchatourov, A. (2016) Big Data entre archive et diagramme. Études Digitales n°2, Classiques Garnier, Paris.

Khatchatourov, A. (2016). Peut-on mettre la main sur les algorithmes? Note sur la «culture algorithmique» de Dourish. Études Digitales, n°2, Classiques Garnier, Paris.

Khatchatourov, A. et Chardel, P.-A. (2016). La construction de l'identité dans la société contemporaine : enjeux théoriques. *in «Identités numériques»*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Kiesel, K., Villas-Boas, S. B. (2007). Got organic milk? consumer valuations of milk labels after the implementation of the USDA organic seal. Journal of agricultural & food industrial organization 5(1). DOI : 10.2202/1542-0485.1152

Lachaud, E., (2016). Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things? *In Data Protection on the Move* (pp. 135-162). Springer Netherlands.

Lachaud, E., (2016). Why the certification process defined in the General Data Protection Regulation cannot be successful. Computer Law & Security Review 32, 814–826.

Lachaud, E. (2017). The General Data Protection Regulation and the rise of certification as a regulatory instrument. Computer Law & Security Review.

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.

Laurent, M., et Kaâniche, N. (2016). Les preuves d'identités ou d'attributs préservant le pseudonymat. *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

Leire, C., Thidell, Å. (2005). Product-related environmental information to guide consumer purchases–a review and analysis of research on perceptions, understanding and use among Nordic consumers. Journal of Cleaner Production, 13(10), 1061-1070. DOI : 10.1016/j.jclepro.2004.12.004.

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.

Levallois-Barth, C., Meseguer, I. (2016). Privacy Shield : un bouclier à peine brandi déjà ébréché ?, Éditorial de la lettre d'information trimestrielle n° 5 de la **Chaire Valeurs et Politiques des Informations Personnellles**, décembre 2016.

Levallois, C. (2016). Identités numériques et gestion des données personnelles. *in « Identités numériques »*, Cahier n°1 de la **Chaire Valeurs et Politiques des Informations Personnelles**, coordonné par Claire Levallois-Barth.

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.

Levy, A. S., Mathews, O., Stephenson, M., Tenney, J. E., & Schucker, R. E. (1985). The impact of a nutrition information program on food purchases. Journal of Public Policy & Marketing, 1-13.

Li, Q., Curtis, K. R., McCluskey, J. J., & Wahl, T. I. (2003). Consumer attitudes toward genetically modified foods in Beijing, China.

Loureiro, M. L., McCluskey, J. J. (2000). Consumer preferences and willingness to pay for food labeling: A discussion of empirical studies. Journal of Food Distribution Research 34(3):95-102.

Luhmann, N. (2001). Confiance et familiarité: Problèmes et alternatives. Réseaux, no 108,(4), 15-35. doi:10.3917/res.108.0015. Traduction de Louis Quéré.

Luhmann, N. (2010). Le Pouvoir [« Macht »], Presses de l'Université Laval, 1975 / 2010.

Machina, M., (2007). Non-expected Utility, *in Darity (Ed), International Encyclopedia of the Social Sciences*, Macmilan Reference USA, 2nd Edition.

Mai B, Menon N M, Sarkar S (2010) No free lunch: Price premium for privacy seal-bearing vendors. Journal of Management Information Systems 27(2):189-212.

Mantelero, A. (2013). Competitive value of data protection: the impact of data protection regulation on online behavior, International Data Privacy Law 3(4): 229-238. DOI : 10.1093/idpl/ipt016.

McDonald, A. M., Cranor, L. F. (2009). The cost of reading privacy policies. ISJLP, 4, 543.

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

Melnik, M. I., & Alm, J. (2002). Does a seller's ecommerce reputation matter? Evidence from eBay auctions. The journal of industrial economics, 50(3), 337-349. DOI : 10.1111/1467-6451.00180.

Miyazaki, A. D., Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. The Journal of Consumer Affairs 28-49. DOI : 10.1111/j.1745-6606.2002.tb00419.x.

Moore, T., Anderson, R. (2012). Internet security. The Oxford Handbook of the Digital Economy'(Oxford University Press 2011).

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.

Naftalski, F. (2011). Label CNIL et conformité « informatique et libertés » : publication des premiers référentiels, Revue Lamy Droit de l'Immatériel.

Noussair, C., Robin, S., Ruffieux, B. (2002). Do consumers not care about bio-tech foods or do they just not read the labels? Economics letters, 75(1), 47-53. DOI : 10.1016/S0165-1765(01)00594-8.

Olurin, M., Adams, C., Logrippo, L. (2012). Platform for privacy preferences (p3p): Current status and future directions. IEEE, Tenth Annual International Conference on Privacy, Security and Trust (PST), pp 217-220. DOI : 10.1109/PST.2012.6297943.

O'Neil. (2014). Hacking Weber: Legitimacy, critique, and trust in peer production.

Parasuraman, R., Mouloua, M., & Molloy, R. (1996). Effects of adaptive task allocation on monitoring of automated systems. *in Human Factors: The Journal of the Human Factors and Ergonomics Society*.

Pasquale, F. (2015). The Black Box Society: The Secret Algorithms That Control Money and Information, Harvard University Press.

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.

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

Quéré, L. (2001). La structure cognitive et normative de la confiance.

Rodrigues, R., Wright, D. and Wadhwa, K. (2013). Developing a privacy seal scheme (that works), International Data Privacy Law Advance Access, published February 1, 2013, 17 pages,. p. 15.

Rodrigues, R., Barnard-Wills, D., Wright, D., De Hert, P., Papakonstantinou, E. (2013). EU Privacy seals project: Inventory and analysis of privacy certification schemes. Final Report. Publications Office of the European Union.

Rouvroy, A. & Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation. Réseaux 31.

Stiegler, B. (2015). La Société automatique. L'avenir du travail, Fayard.

Tambou, O., (2016). L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ?, Revue Lamy de Droit de l'Immatériel, avril 2016, pp. 51-54.

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.

Waelbroeck, P., Khatchatourov, A., Levallois-Barth, C. (2017) Synthèse du Rapport « Données personnelles et confiance : quelles stratégies pour les citoyens-consommateurs en 2017 ? », **Chaire Valeurs et Politiques des Informations Personnelles**, 23 juin 2017.

Zyskind, G., Nathan, O., Pentland, A., (2015). Enigma: Enigma: Decentralized Computation Platform with Guaranteed Privacy.

Interventions effectuées par les membres de la Chaire en lien avec la thématique des signes de confiance et des labels (évènements externes)

8 décembre 2017 • Participation au panel d'**Armen Khatchatourov**, **« Les approches pour la définition et la gestion des risques liés aux données personnelles dans les systèmes d'information »**, Journée d'étude «Vie privée, données personnelles et risques. Quels paramètres pour leur cohabitation à venir ? », ENS, Paris

8 novembre 2017 • **« La confiance en action : confiance, numérique et design »**, organisée par la Fondation Mines-Télécom, à Paris : intervention de **Claire Levallois-Barth** portant sur « Les signes de confiance »

5 octobre 2017 • **Journée Objets connectés de Santé** organisée par l'IMT à Paris. Animation de la table ronde « Mesure et qualité des données » par **Armen Khatchatourov** et de la table ronde « Sécurité et confiance » par **Maryline Laurent**, avec la participation de **Claire Levallois-Barth**.

10 mai 2017 • Participation de **Maryline Laurent** à la **table ronde « Que reste-t-il de la confiance à l'ère du numérique ? »**, sur « Les preuves de confiance en informatique », petit-déjeuner de la Fondation Mines-Télécom, NUMA, Paris, France.

28 avril 2017 • **Journée d'étude « Le cadre juridique applicable aux traitements de données à caractère personnel »** organisée par le CERAPS (UMR 8026) et l'Université de Lille dans le cadre du projet de recherche ANR « APPEL », Lille : intervention de **Claire Levallois-Barth** sur le thème « Le rôle des labels pour renforcer l'effectivité du cadre juridique applicable aux traitements de données à caractère personnel »

29 mars 2017 • **« La confiance distribuée à l'ère du numérique »** organisée par la Fondation Mines-Télécom, au WAI BNP Paribas, Paris. Présentation d'**Armen Khatchatourov** « La confiance dans le numérique » et de **Claire Levallois-Barth** « La confiance régulée : l'exemple des labels en matière de protection des données personnelles » .

Évènements internes organisés par la Chaire en lien avec la thématique des signes de confiance (réservés aux partenaires)

20 novembre 2017 • **Présentation à Orange labs, Chatillon**

Lors de cette réunion, **Claire Levallois-Barth**, **Armen Khatchatourov**, **Maryline Laurent** et **Patrick Waelbroeck** ont exposé leurs réflexions sur les signes de confiance en fonction de leur discipline de recherche.

15 mars 2017 • **Présentation au Comité de Labellisation de la CNIL**

Lors de cette réunion, **Claire Levallois-Barth** a exposé les résultats de la recherche sur les labels en matière de données personnelles. Les différentes modalités d'intervention des autorités de contrôle en la matière ont été discutées avec les Commissaires de la CNIL et l'équipe pluridisciplinaire de la Chaire.

14 mars 2017 • **Groupe de travail interne Règlement Données personnelles (RGPD)**

Clément Chevauché de l'AFNOR Normalisation a présenté et discuté le document intitulé « L'apport des normes volontaires dans le numérique ».

15 décembre 2016 • **Atelier interne « Labels en matière de protection des données personnelles : de quel type de confiance parlons-nous ? »**

Cet atelier visait à définir la notion de confiance, tant dans sa signification que dans sa fonction sociale. **Claire Levallois-Barth** a montré que ce concept, situé entre le savoir complet et le manque de savoir, visait à combler le vide entre l'expert et le profane. Elle a également exposé les dispositions du RGPD relatives à la certification et aux labels. **Armen Khatchatourov** a, quant à lui, présenté une critique du modèle de la confiance comme gestion des risques.

16 décembre 2015 • **Atelier interne « Labels en matière de protection des données personnelles : état de l'art juridique et économique »**

Lors de cet atelier, **Delphine Chauvet** et **Claire Levallois-Barth** ont tenté de cerner les notions de label, certification, marque de confiance et homologation en droit français et européen. Elles ont présenté un premier état de l'art sur les labels existants en matière de données personnelles et se sont interrogées sur les raisons pour lesquelles la centaine de labels répertoriés n'avaient pas acquis de visibilité du point de vue de l'opinion publique. **Patrick Waelbroeck** et **Antoine Dubus** ont, pour leur part, traité la question de la faisabilité économique des labels en matière de protection des données personnelles.

30 avril 2014 • **Atelier interne « Enjeux et problématiques posés par la labellisation en matière de données personnelles »**

Animé par **Claire Levallois-Barth**, cet atelier a fourni un premier aperçu de la labellisation en matière de données personnelles à travers deux présentations : la première d'**Arnaud Belleil**, Directeur Associé de Cecurity.com, sur les enjeux et problématiques ; la seconde, de **Matthieu Grall**, chef du service de l'expertise technologique, à la direction des technologies et de l'innovation de la CNIL intitulée « La labellisation vue par la CNIL, l'ANSSI et l'ISO ».

La chaire de recherche Valeurs et Politiques des Informations Personnelles

Créée par l'Institut Mines-Télécom en mars 2013, la Chaire regroupe une équipe pluridisciplinaire de chercheurs travaillant à la fois sur les aspects juridiques de régulation et de conformité, techniques de sécurité des systèmes et des données, économiques de partage des informations personnelles et philosophiques de responsabilisation et d'anticipation des conséquences sociétales.

Elle bénéficie du soutien de sept mécènes : le Groupe Imprimerie Nationale, BNP Paribas, Orange, LVMH, QWANT, SOPRA STERIA (mécènes fondateurs), Dassault Systèmes (mécène associé), de la collaboration de la Commission nationale de l'informatique et des libertés (CNIL) et de la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC), et du support de la Fondation Mines-Télécom.

La Chaire est coordonnée par Claire Levallois-Barth, maître de conférences en droit à Télécom ParisTech, et a été cofondée avec Ivan Meseguer, Affaires Européennes, Direction Recherche et Innovation de l'IMT, Maryline Laurent, professeur en sciences de l'informatique à Télécom SudParis, Patrick Waelbroeck, professeur en sciences économiques à Télécom ParisTech et Pierre-Antoine Chardel, professeur en philosophie à Télécom École de Management.

La Chaire Valeurs et Politiques des Informations Personnelles se propose d'aider les entreprises, les citoyens et les pouvoirs publics dans leurs réflexions sur la collecte, l'utilisation et le partage des informations personnelles, à savoir les informations concernant les individus (leurs vies privées, leurs activités professionnelles, leurs identités numériques, leurs contributions sur les réseaux sociaux, etc.), incluant celles collectées par les objets communicants qui les entourent. Ces informations fournies par les personnes, ou traces de leurs activités et interactions, posent en effet de nombreuses questions en termes de valeur sociale, valeur économique, politique de contrôle et politique de régulation.

Les travaux de la Chaire sont conduits selon cinq axes de recherche transdisciplinaires :

- les identités numériques ;
- la gestion des informations personnelles ;
- les contributions et traces ;
- les informations personnelles dans l'internet des objets ;
- les politiques des informations personnelles.

En plus de la publication d'articles de recherche et la participation aux colloques et conférences, la Chaire organise régulièrement des évènements ouverts à tous, pour sensibiliser le grand public sur ces enjeux majeurs du monde numérique.

EN SAVOIR PLUS

www.informations-personnelles.org
youtube.informations-personnelles.org
@CVPIP

CONTACTS

CLAIRE LEVALLOIS-BARTH
Coordinatrice de la Chaire
claire.levallois@imt.fr

ANNE-CATHERINE AYE
Assistante de la Chaire
cvpip@imt.fr
+33 1 45 81 72 53

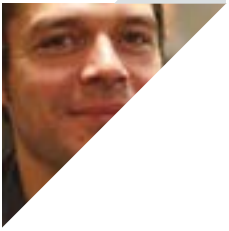
Télécom ParisTech - IMT
46 rue Barrault | F-75634 Paris Cedex 13

Auteurs

Claire Levallois-Barth

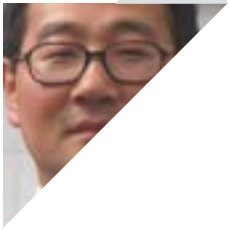
Maître de conférences en droit à Télécom ParisTech, coordinatrice de la Chaire. Elle s'intéresse à l'évolution de la protection des libertés et droits fondamentaux à l'ère numérique. Elle se concentre en particulier sur la question de la protection des données personnelles, notamment dans le contexte du *Big Data*, ainsi que sur la gestion des identités numériques.

Armen Khatchatourov



Ingénieur de recherche et docteur en philosophie de la technique à Télécom École de Management. En articulant l'approche théorique et l'ingénierie, il s'intéresse à la manière dont les technologies numériques affectent notre sentiment de soi et aux conséquences sociétales de ces technologies.

Patrick Waelbroeck

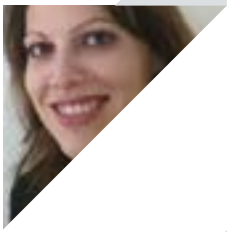


Professeur en sciences économiques à Télécom ParisTech, cofondateur de la Chaire. Ses travaux portent sur l'économie de l'innovation, l'économie de la propriété intellectuelle, l'économie de l'internet et des données personnelles. Il enseigne l'économie de l'internet et des données.

Maryline Laurent

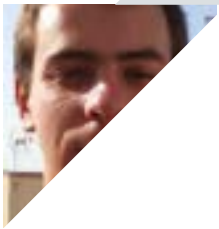
Professeur en sciences de l'informatique à Télécom SudParis, cofondatrice de la Chaire. Responsable de l'équipe R3S (Réseaux, Systèmes, Services, Sécurité) du laboratoire UMR 5157 SAMOVAR. Elle s'intéresse aux problématiques de sécurité et de vie privée dans les environnements de *cloud*, de systèmes miniaturisés et à la gestion des identités numériques.

Delphine Chauvet



Post-doctorante en droit à Télécom ParisTech, elle a soutenu sa thèse sur « La vie privée. Étude de droit privé. » à l'Université Paris-Sud et est chargée d'enseignement à l'Université Paris 2 Panthéon-Assas.

Antoine Dubus



Doctorant en sciences économiques au sein de la Chaire Valeurs et Politiques des Informations Personnelles, il travaille sur le thème « Protection des données personnelles et concurrence ». Ses recherches portent plus particulièrement sur la vente de données à des fins de ciblage publicitaire, de recommandations personnalisées en ligne, ou encore de ciblage par les prix.

Avec la contribution d'Ivan Meseguer, cofondateur de la Chaire, Affaires Européennes, Direction Recherche et Innovation de l'IMT, et les participations de Stéphane Ménégaldo, chargé de communication, Chantal Friedman et Anne-Catherine Aye, assistantes de la Chaire

Située au centre de la construction de toute société, la confiance questionne la possibilité même des échanges institutionnels et commerciaux, et le rôle que ces échanges peuvent avoir dans la structuration de notre vivre-ensemble. Or, nous assistons aujourd'hui à une crise de confiance manifeste, dont le numérique est l'un des vecteurs.

Tandis que les sciences économiques et informatiques se réfèrent à la notion de risques dans le cadre d'une transaction ou de la sécurité des systèmes techniques, le droit définit classiquement la confiance comme une croyance en la bonne foi d'autrui. D'un point de vue socio-philosophique, la confiance constitue un des principaux mécanismes de réduction d'incertitude dans une société contemporaine complexe. Deux aspects simultanément à l'œuvre permettent de diminuer cette complexité : la confiance assurée et la confiance décidée (*confidence* et *trust* en anglais).

Cet ouvrage propose d'aborder la question des labels en matière de données personnelles comme outil de confiance. Quel est leur impact sur la perception de l'utilisateur et ses actes de consommation ? Quelles réponses la technologie – dont la blockchain – peut-elle apporter ? Quel est ou quel doit être à cet égard le nouveau rôle de l'État ? L'omniprésence de labels ou de *trust by design* n'a-t-elle pas ses limites ? La sur-utilisation de labels ne risque t-elle pas parfois de déresponsabiliser les individus en les déchargeant de toute analyse critique ?

Les partenaires de la Chaire Valeurs et Politiques des Informations Personnelles (CVPIP)

MÉCÈNES FONDATEURS

GROUPE Imprimerie Nationale

BNP PARIBAS

orange

LVMH

sopra steria

Qwant

MÉCÈNE ASSOCIÉ

DASSAULT SYSTEMES

PARTENAIRES QUALIFIÉS

CNIL. Commission Nationale de l'Informatique et des Libertés

DINSIC*

**Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'État*

Nepeys – 06 62 12 15 25 – www.nepeys.fr – RCS 499 438505