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

Claire Levallois-Barth

Levallois-Barth, C.

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

dans **Signes de confiance – l'impact des labels sur la gestion des données personnelles** (Chapitre 8, pages 136 à 152).
Coordonné par Claire Levallois-Barth, Chaire Valeurs et Politiques des Informations Personnelles (France), Janvier 2018.

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

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

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/

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.* »

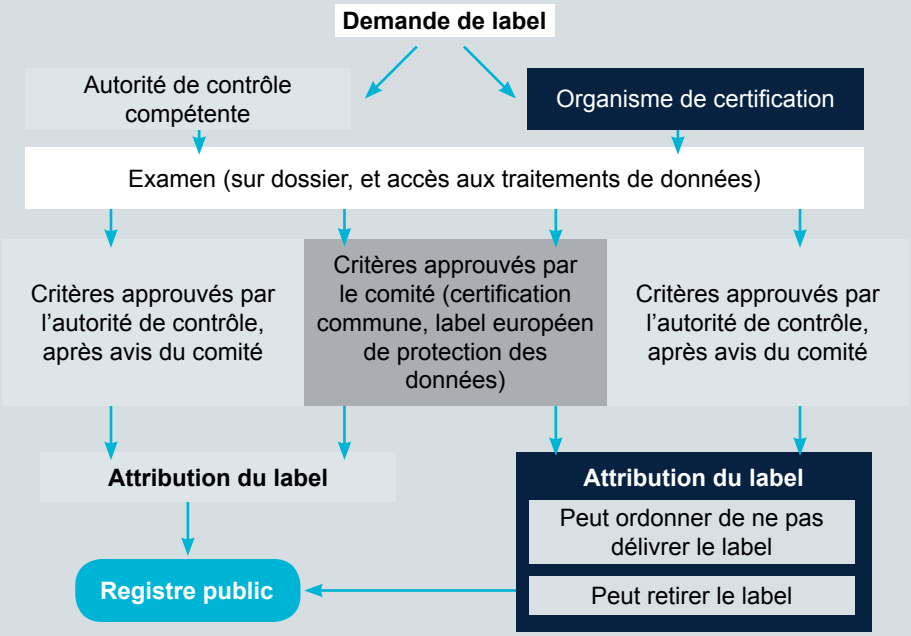

Figure 2. RGPD : délivrance d'une certification / d'un label

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.

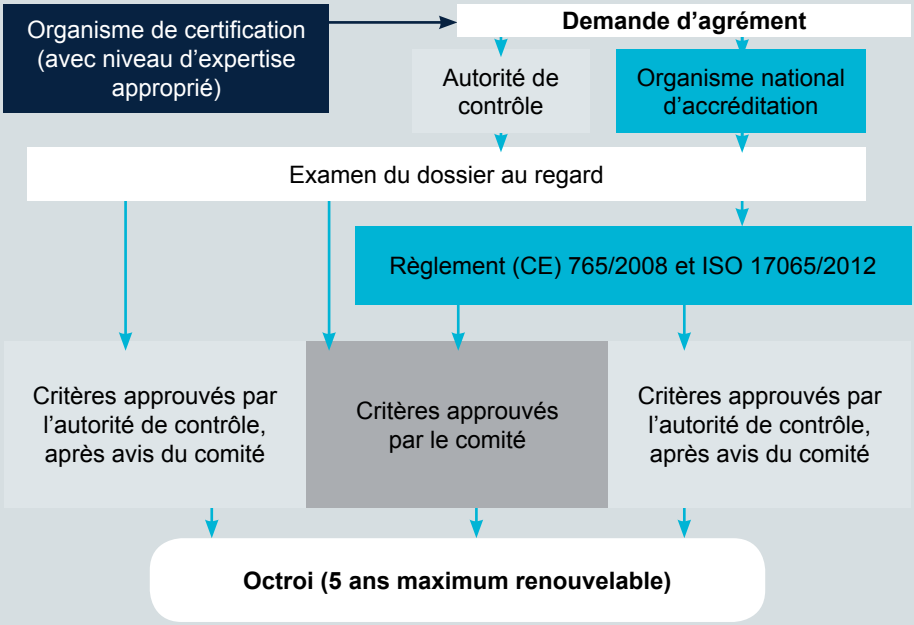

Figure 3. RGPD : agrément d'un organisme de certification

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.