L'Introduction de la certification dans le règlement général de la protection des données personnelles: quelle valeur ajoutée ?

Olivia Tambou

L'introduction de la certification dans le règlement général de la protection des données personnelles : quelle valeur ajoutée ?

Si l'introduction de la certification dans le prochain règlement général de la protection des données personnelles comporte des avancées certaines, il présente également des limites potentielles liées à la manière dont les différents acteurs vont mettre en œuvre le cadre qu'il fixe. Tel est le sens de la présente analyse (*)

Par Olivia TAMBOU(**)

Maître de conférences en droit
Université Paris-Dauphine
PSL Research University
Coordinatrice de l'axe de recherche sur l'effectivité de la protection des données personnelles
Centre Droit Dauphine, Cr2D

➔3986

Le futur règlement général de la protection des données personnelles (ci-après « RGPD »)(1) doit remplacer l'actuelle directive n° 95/46/CE en 2018. Le RGPD a pour ambition générale d'adapter le cadre législatif à l'évolution des nouvelles technologies en facilitant « *la libre circulation des données au sein de l'Union européenne et leurs transferts vers les pays tiers (...), tout en assurant un niveau élevé de protection des données à caractère personnel* »(2).

Le futur RGPD comporte deux nouveaux articles dédiés à la certification(3). Il s'agit d'attester « *de la conformité avec le règlement des opérations de traitement effectuées par les responsables de traitement et les sous-traitants* ».

L'introduction de la certification dans le RGPD repose sur trois des grandes caractéristiques de la solide expérience développée par l'Union européenne en matière de certification dans le cadre, notamment, du marché intérieur.

Premièrement, la certification est classiquement définie comme un mécanisme permettant d'attester la conformité à des obligations en se conformant à un référentiel. Trois voies sont explicitement envisagées pour formaliser cette certification : d'une part, le recours à des normes techniques, d'autre part, l'usage de marques et, enfin, l'utilisation de labels.

Deuxièmement, la certification repose sur une logique incitative(4). Les responsables de traitement peuvent choisir eux-mêmes la voie qui leur permettra de se conformer à leurs obligations. La certification doit alors être replacée dans le contexte global du RGPD. Ce dernier propose aux acteurs d'autres possibilités pour faciliter leur mise en conformité avec le RGPD telles que l'adoption de codes de conduite(5) ou la

(*) Le présent texte remplace la version publiée dans le n°125 (p. 51 à p.55) qui ne comprend pas les notes de bas de pages. Nous prions l'auteure et nos lecteurs de bien vouloir accepter nos excuses pour cette bien involontaire erreur.

(**) L'auteure tient à remercier Éric Lachaud ainsi que ses collègues les professeures Anne Penneau et Fabienne Leneuf pour avoir bien voulu lui transmettre certaines références et à exprimer sa gratitude à Fabienne Leneuf pour ses remarques constructives.

(1) Voir l'accord politique du 15 décembre 2015 qui doit encore faire l'objet d'une adoption définitive prévue au printemps 2016. Pour une traduction provisoire en français de cet accord, voir <http://data.consilium.europa.eu/doc/document/st-5455-2016-init/fr/pdf>. Pour une analyse globale de ce texte, voir Gola R., La proposition de règlement européen sur les données personnelles, enjeux et opportunités pour l'entreprise et les citoyens, RLDI 2015/121, n° 3891.

(2) Voir consid. 5.

(3) art. 39 et 39 *bis*. Dans sa globalité le texte de l'accord du 15 décembre 2015 comporte 70 références à la certification alors que ce terme n'était pas présent dans le texte de l'actuelle directive n° 95/46/CE.

(4) Le RGPD n'a pas repris la proposition de certification obligatoire en matière de traitement de données sensibles qui avait été proposé par le Conseil d'État. Voir Le numérique et les droits fondamentaux, Étude annuelle 2014, proposition 19.

(5) art. 38 et 38 *bis*.

mise en place d'un délégué à la protection des données personnelles[6], etc.

Troisièmement, la certification s'articule autour d'une procédure en deux volets. D'une part, la certification nécessite que des organismes tiers soient accrédités. D'autre part, les candidats à la certification doivent saisir ces organismes dans le cadre d'une procédure de certification.

Cependant, le RGPD prend aussi en compte la spécificité de la certification dans le domaine de la protection des données personnelles[7]. Le droit à la protection de ces données à caractère personnel constitue un droit fondamental inscrit depuis le Traité de Lisbonne non seulement à l'article 16 du TUE, mais également à l'article 8 de la Charte des droits fondamentaux[8]. Le RGPD place ainsi les autorités de protection des données personnelles au cœur du processus de certification[9]. Ce sont ces autorités qui devront établir les critères d'encadrement de la certification. En outre, il laisse la possibilité aux États membres de renforcer le rôle joué par ces autorités en matière de certification. Les autorités de contrôle des données personnelles peuvent attribuer elles-mêmes les certifications et/ou décerner l'agrément des organismes de certification. Ainsi, la certification illustre la particularité de la méthode d'harmonisation complète au sein du RGPD. Le texte oscille entre l'adoption d'un cadre législatif extrêmement contraignant complété par le renforcement de mécanismes de régulation des acteurs privés sous le contrôle des autorités de protection des données à caractère personnel[10].

L'émergence d'une certification européenne en matière de protection des données personnelles répond à de fortes attentes[11]. Elle est plébiscitée par le monde économique. Elle semble incontournable pour permettre aux PME de répondre aux nombreuses exigences imposées par le RGPD. Elle est centrale pour redonner confiance aux utilisateurs soucieux du respect de leurs données personnelles. Elle a été placée au cœur des préoccupations des autorités de protection des données personnelles pour l'année 2016[12]. L'élaboration d'une politique européenne de certification nécessitera un important travail dans les deux années à venir qui séparent l'adoption du RGPD de son entrée en vigueur.

Dans ce contexte, l'introduction de la certification dans le RGPD comporte des avancées certaines (I), mais également des limites potentielles (II) liées à la manière dont les différents acteurs vont mettre en œuvre le cadre fixé par le règlement.

I. – LES AVANCÉES CERTAINES LIÉES À L'HARMONISATION PROPOSÉE PAR LE RGPD

A. – La prise en compte de la complexité des cycles d'exploitation des données

Aujourd'hui, les données personnelles sont rarement exploitées uniquement par les personnes qui les ont initialement collectées. Le développement du *Cloud*, du *big data*[13] et des réseaux sociaux implique que l'essentiel des données personnelles voyage vers des États tiers. L'encadrement de la certification a été adapté afin qu'elle puisse donner des garanties aux différents acteurs de l'économie numérique pour répondre à leurs nouveaux usages.

1°/ L'adoption d'un champ d'application personnel élargi pour la certification

L'article 39 du RGPD détermine les deux types possibles d'acteurs susceptibles de bénéficier d'une procédure de certification. Il s'agit du responsable de traitement et de ses sous-traitants. Le responsable de traitement est défini comme sous l'actuelle directive n° 95/46/CE comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, déterminent les finalités et les moyens du traitement de données à caractère personnel* ». Au-delà de ces critères, le responsable de traitement peut être désigné par la loi ou le droit de l'Union européenne. Le sous-traitant est défini à l'article 3 du RGPD comme étant « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement* ». La principale nouveauté introduite par le RGPD est de développer un régime de coresponsabilité entre le responsable de traitement et le sous-traitant. Cela implique qu'il doit être associé à la politique de certification du responsable de traitement. Autre particularité, la certification peut s'appliquer à des responsables de traitement et sous-traitants de pays tiers qui ne seraient pas soumis au règlement[14]. Cette hypothèse a pour but de faciliter le transfert de données personnelles vers un pays tiers qui ne ferait pas l'objet d'une décision de niveau de protection adéquat.

(6) art. 35-37. Notons que la désignation d'un délégué à la protection des données personnelles peut aussi être contrainte en raison du type de traitement envisagé (traitement à grande échelle de données personnelles sensibles, par exemple) ou de la nature particulière du responsable de traitement (autorité publique ou organisme public), voir article 35.

(7) Pour un aperçu de l'état de la certification, voir Rodrigues R., Barnard Wills D., Wright D., De Hert P., Papakonstantinou V., *EU Privacy Seals Project, Inventory and Analysis of Certification Shemes*, Final Report 2013, <www.vub.ac.be/LSTS/pub/Dehert/481.pdf>.

(8) González Fuster G., *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, 2014 Springer.

(9) Tant l'article 16 du TUE que l'article 8 de la Charte des droits fondamentaux consacrent l'importance du rôle des autorités de protection en rappelant que « *le respect de ces règles est soumis au contrôle des autorités d'une autorité indépendante* ».

(10) Sur ce point voir notre article, Les enseignements de la réforme de la protection des données personnelles au regard du concept d'harmonisation, *in* Harmonisation et Union européenne, à paraître chez Bruylant en 2016.

(11) Voir Bonnet Fl., Les labels de protection des données personnelles sont source de valeur ajoutée, Banque 2014, n° 769.

(12) Voir <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf>.

(13) Voir Bensamoum A. et Zolynski C., *Cloud Computing* et *big data* : quel encadrement pour ces nouveaux usages des données personnelles ?, Réseaux La Découverte 2015/1, n° 189, p. 103-121.

(14) Voir art. 39, § 1 *bis*.

2°/ L'incitation explicite au recours à la certification pour garantir des technologies protectrices

La possibilité d'utiliser la certification est explicitement envisagée pour servir à attester du respect de deux types d'exigences fixés par le RGPD. La première est nouvelle. Il s'agit de pouvoir garantir que la protection des données soit assurée dès la conception (*privacy by design*) ou par défaut (*privacy by default*)[15]. La *privacy by design* a pour objectif de garantir que la protection de la vie privée soit intégrée dans les nouvelles applications technologiques et commerciales dès leur conception. Selon le concept de *privacy by default* chaque entreprise traitant des données personnelles doit garantir ***par défaut*** le plus haut niveau possible de protection des données.

Le recours à la certification est aussi encouragé pour assurer le respect de l'obligation de sécurité des données. Cette seconde obligation est ancienne mais son contenu a été renforcé dans le RGPD[16]. Actuellement, la Commission européenne a adopté un mandat chargeant les organismes européens de normalisations d'élaborer « *des normes européennes et des publications en matière de normalisation européenne pour la gestion de la vie privée et la protection des données à caractère personnel* »[17]. Les trois points évoqués précédemment : respect de la protection des données par défaut et dès la conception, respect des obligations de sécurité sont au cœur du texte du mandat[18]. En 2014, un comité de travail joint au CEN/Cenelec a été créé. Le JWG 8 « *Privacy Management in Products and Services* »[19] est chargé de répondre au mandat de normalisation de la Commission. Il devrait adopter son programme de travail d'ici à l'été 2016. Les normes voire les publications qu'il proposera pourraient être utilisées dès l'entrée en vigueur du RGPD prévue pour 2018.

Il faut rappeler qu'une norme technique est « *une spécification technique*[20] *approuvée par un organisme reconnu à activité normative pour application répétée ou continue, dont l'observation n'est pas obligatoire* »[21]. Il peut s'agir d'une norme internationale (ISO)[22], d'une norme européenne (EN) ou d'une norme nationale (NF, par exemple).

C'est donc la voie classique de la normalisation qui a été choisie par la Commission afin d'anticiper l'entrée en vigueur du RGPD. Il s'agit de donner les moyens aux acteurs économiques et notamment aux PME d'établir une présomption de conformité à certaines de leurs nouvelles obligations. La priorité accordée au respect des principes de *privacy by design* et de *privacy by default* prend en compte deux éléments. D'une part, l'absence de certification internationale sur ce point et, d'autre part, la volonté européenne d'en faire un élément fort de son modèle en matière de protection des données personnelles. Une telle normalisation devrait permettre aux responsables de traitement de s'assurer que les produits ou services qu'ils achètent et qui traitent de données personnelles leur permettent de se conformer au RGPD. Autrement dit, l'utilisation de la normalisation comme procédé de certification a pour but de faire évoluer la responsabilisation des responsables de traitement vers le concepteur de technologie.

Cela dit, la normalisation n'est qu'une des formes envisagées pour la certification. Elle est complétée par d'autres formes plus visibles[23], comme les labels et les marques.

3°/ La possibilité de création d'un label européen de protection des données

La valeur ajoutée du RGPD est de proposer la création d'un « *label de la protection des données* » à l'échelle européenne. Cette « *certification commune* » pourra être créée sur la base de critères adoptés par le Comité européen des données personnelles (ci-après « CEPD ») selon l'article 39, § 2 *bis*. Ce comité qui réunit l'ensemble des autorités de protection nationale remplacera l'actuel G29. L'intégration de la certification dans le plan de travail du G29 pourrait attester de sa volonté de mettre en place les éléments de ce label afin qu'il puisse être rapidement adopté au moment de l'entrée en vigueur du RGPD. Il sera intéressant de voir si le CEPD prendra en compte l'expérience de l'Union européenne du marquage CE[24] pour mettre en place cette certification commune. L'absence de référence à cette possibilité dans le texte même du RGPD semble plutôt augurer de la possibilité d'un label distinct et spécifique. Deux arguments pourraient être invoqués à l'appui de la pertinence d'une telle solution. D'une part, le marquage CE fait l'objet de certaines critiques. La plus importante est qu'il introduit la confusion dans l'esprit du consommateur qui ne sait pas très bien s'il atteste que le produit est fabriqué dans l'Union européenne ou s'il est présumé conforme à une norme européenne. D'autre part, le marquage CE est sans doute approprié

(15) Voir RGPD, art. 23.

(16) Voir RGPD, art. 30.

(17) Voir Décision d'exécution de la Commission, 20 janv. 2015, n° C(2015) 102 final <http://ec.europa.eu/transparency/regdoc/rep/3/2015/FR/3-2015-102-FR-F1-1.PDF>.

(18) Voir Annexe de la décision précitée, <http://ec.europa.eu/transparency/regdoc/rep/3/2015/FR/3-2015-102-FR-F1-1-ANNEX-1.PDF>.

(19) Voir <www.cencenelec.eu/standards/Sectors/DefenceSecurityPrivacy/Privacy/Pages/default.aspx>.

(20) Il s'agit d'« *une spécification qui figure dans un document définissant les caractéristiques requises d'un produit, telles que les niveaux de qualité ou de propriété d'emploi, la sécurité, les dimensions, y compris les prescriptions applicables au produit en ce qui concerne la dénomination de vente, la terminologie, les symboles, les essais et méthodes d'essai, l'emballage, le marquage et l'étiquetage ainsi que les procédures d'évaluation de la conformité* ».

(21) Voir directive n° 98/34/CE, 28 juin 1998.

(22) À l'échelle internationale, une première norme spécifique à la protection des données pour le *Cloud* a été adoptée : la norme ISO/IEC 27018:2014. Voir De Hert P., Papakonstantinou V., Kamara I., *The New Cloud Computing ISO/IEC 27018 Standard Through the Lens of the EU Legislation on Data Protection* <http://dx.doi.org/10.2139/ssrn.254212>. Il existe aussi deux normes en matière de sécurité de l'information : ISO 27001 et ISO 27002.

(23) Sur ce point, voir Viguri Cordero J., *Los mecanismos de certificación (códigos de conducta, sellos y marcas)*, *in* Rallo Lombarte A., Del Rosario García Mahamut M., *Hacia un nuevo derecho europeo de protección de datos*, 2015, Valencia, Tirant Lo Blanch, p. 901, spéc. p. 928.

(24) Éric Lachaud propose, par exemple, d'adapter le marquage CE dans le domaine de la protection des données, *Could the CE Marking Be Relevant to Enforce Privacy by Design in the Internet of Things? In Data Protection on the Move Current Developments in ICT and Privacy/Data Protection*, éditeurs Serge Gutwirth, Ronald Leenes, Paul De Hert, p. 135-162.

pour les produits, mais ne concerne pas les services ou les procédures. Or, le label européen de protection des données a vocation à couvrir l'ensemble de ces objets.

B. – L'encadrement des pratiques de la certification en matière de protection des données personnelles

1°/ L'encouragement généralisé au recours à la certification

L'article 39 attribue un rôle d'encouragement et de promotion de la certification à un ensemble d'acteurs clés : les États membres, les autorités de contrôle, le CEPD et la Commission. Deux exemples permettent d'attester de la prise en compte par anticipation de cette mission par le législateur français. La procédure d'agrément des hébergeurs de données de santé à caractère personnel a été récemment modifiée au bénéfice d'une procédure de certification[25]. L'actuel projet de loi pour une République numérique renforce les pouvoirs de labélisation de la Cnil en lui donnant expressément des pouvoirs de certification « *de processus d'anonymisation des données à caractère personnel notamment en vue de la réutilisation d'informations publiques* »[26].

2°/ L'harmonisation du rôle joué par les autorités de protection des données en matière de certification

La certification a été explicitement incluse dans le champ des missions des autorités nationales de protection des données permettant ainsi une harmonisation dans les 28 États membres. La diversité des autorités de protection des données a été considérée comme favorisant les divergences de protection entre les États membres sous le régime actuel de la directive n° 95/46[27]. Aussi, l'un des apports du RGDP est de mettre en place une harmonisation poussée des statuts, missions et pouvoirs des autorités de protection des données. Dans ce cadre, chaque autorité nationale de protection des données acquiert trois nouvelles missions en lien avec la certification. D'une part, elle « *approuve les critères de certification* (...) », d'autre part, elle procède « *le cas échéant à l'examen périodique des certifications délivrées* (...) ». Enfin, elle « *rédige et publie les critères d'agrément d'un organisme de certification* »[28].

En outre, les autorités de protection des données sont dotées de pouvoirs directement liés à la certification. L'article 53 classe les pouvoirs des autorités de protection en trois grandes catégories : les pouvoirs d'enquête, les pouvoirs de prendre des mesures correctrices et les pouvoirs d'autorisation. Les missions précitées ont été naturellement reliées à des pouvoirs d'enquête et d'autorisation. Mais les autorités de protection de données personnelles acquièrent aussi des pouvoirs pour prendre de mesures correctrices telles que celles « *de retirer une certification ou ordonner à un organisme de certification de retirer une certification* (...) *ou ordonner à l'organisme de certification de ne pas délivrer de certification si les exigences applicables à la certification ne sont pas ou plus respectées* »[29]. Enfin, l'article 79 du RGPD donne la possibilité pour les autorités de protection des données d'imposer des amendes administratives. D'une part, il prévoit que l'application de mécanismes de certification doit être dûment prise en compte tant dans la décision d'imposer ou non une amende que dans la fixation du montant de cette amende. Cette affirmation doit être mise en relation avec l'article 39, § 2, du RGPD qui rappelle l'une des caractéristiques classiques de la certification. La certification pose une présomption simple de conformité. « *Elle ne diminue pas la responsabilité du responsable de traitement ou du sous-traitant quant au respect du présent règlement.* » Autrement dit, l'application conforme d'une certification peut tout au plus constituer un élément d'atténuation de sanctions sans exonérer la responsabilité de l'acteur concerné. D'autre part, l'article 79 du RGPD permet aux autorités de protection des données de sanctionner un organisme de certification qui ne respecterait pas ses obligations. L'amende peut 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* ». Il s'agit du premier niveau de sanction envisagé par le RGPD, sachant que le renforcement du montant des amendes constitue une des nouveautés introduites dans le RGPD. Le montant maximal prévu est de 20 000 000 € ou 4 % du chiffre d'affaires annuel, tel que précédemment défini.

3°/ L'harmonisation des critères communs pour décerner l'accréditation des organismes de certification

Des critères communs ont été fixés pour l'accréditation des organismes de certification. Autrement dit, les pouvoirs d'autorisation des autorités de données de protection sont encadrés par le RGPD afin de renforcer la fiabilité du processus de certification[30]. Cette préoccupation constitue une concrétisation du principe selon lequel la certification « *doit être accessible via un processus transparent* »[31].

(25) Maisnier-Boché L., Hébergement des données de santé : bilan et perspectives de réforme, RLDI 2015, p. 37-43.

(26) Voir l'article 30 du projet de loi tel qu'adopté par l'Assemblée nationale. Le pouvoir de labélisation de la Cnil a été introduit par la loi n° 2009-526 et renforcé par la loi n° 2004-344 qui donne la possibilité à la Cnil de se prononcer sur la labélisation d'un produit de sa propre initiative. Voir L. n° 78-17, 6 janv. 1978 « *relative à l'informatique, aux fichiers et aux libertés* », art. 11, 3.

(27) Voir les deux rapports de l'Agence des droits fondamentaux de l'Union européenne : La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données – Renforcement de l'architecture des droits fondamentaux au sein de l'UE II, 2010, <http://fra.europa.eu/sites/default/files/tk3109265frc_fr_web.pdf>, ou Accès aux voies de recours en matière de protection des données à caractère personnel dans les États membres de l'UE, 2015, <http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states>.

(28) Voir RGPD, art. 52.

(29) art. 53, § 1 *ter*, f *bis*.

(30) Sur les enjeux en cette matière, voir Penneau A., Standardisation et certification : les enjeux européens, *in* Bismuth R. (ss dir.), La standardisation internationale privée, Larcier, 2014.

(31) RGPD, art. 39, § 1 *ter*. Relèvent également de ce principe : l'information des autorités de protection des données des raisons de la délivrance ou du retrait de la certification demandée, par les organismes de certification, la publication sous une forme accessible des critères de certification des autorités de protection des données, et la publication des certifications dans un registre à l'échelle nationale et européenne.

Ces critères communs illustrent « *l'évolution du modèle actuel de la certification vers une posture interventionniste visant à écarter l'influence des organismes de certification insuffisamment compétents, indépendants ou impartiaux* (...) »[32].

Ces critères sont de type institutionnel : l'indépendance, l'expertise et l'absence de conflits d'intérêts de l'organisme de certification doivent être vérifiées. Ils sont aussi de type procédural. L'agrément nécessite, par exemple, la mise en place par le candidat de procédures de délivrance, d'examens périodiques et de retrait des certifications. L'établissement de procédures et de structures pour traiter de façon transparente les réclamations relatives à des violations de la certification doit être assuré.

4°/ L'harmonisation de l'encadrement de certification dans le temps

Le RGPD établit de simples durées maximales tant pour la validité de la certification (trois ans) que pour la durée de l'agrément (cinq ans). En outre, la certification est soumise à des mécanismes de contrôle réguliers. Le retrait ou un refus de renouvellement est envisagé en cas de non-conformité aux critères initiaux de la certification.

L'harmonisation introduite par le RGPD témoigne ainsi d'importantes libertés aux différents acteurs en matière de certification. Certaines d'entre elles peuvent constituer des limites potentielles à l'effectivité de l'introduction de la certification dans le RGPD.

II. – LES LIMITES POTENTIELLES LIÉES AUX LIBERTÉS LAISSÉES PAR LE RGPD

Le RGPD entre dans la catégorie des règlements incomplets[33] en ce qu'il ménage de nombreuses marges de manœuvre pour les États membres. Le RGPD ne propose pas un modèle unique de certification, ce qui serait susceptible de poser un problème au regard de l'effectivité de l'articulation entre les différentes certifications (A). Enfin, certaines garanties n'ont pas été introduites dans le RGPD (B).

A. – L'effectivité de l'articulation entre les certifications

Le RGPD ménage une marge de manœuvre pour les États membres dans le cadre de la procédure de certification à trois niveaux.

1°/ Les alternatives laissées aux États membres dans la procédure de certification

D'une part, le RGPD prévoit que l'attribution d'une certification peut se faire de deux manières. Premièrement, la certification peut être délivrée par l'autorité de contrôle compétente. Il pourra s'agir d'une autorité nationale ou du CEPD à l'échelle européenne. Deuxièmement, la certification peut être délivrée par des organismes de certification agréés. D'autre part, le RGPD laisse la possibilité que cet agrément soit décerné par l'autorité de contrôle compétente et/ou par un organisme national d'accréditation. Enfin, le RGPD établit de simples durées maximales tant pour la validité de la certification (trois ans) que pour la durée de l'agrément (cinq ans).

Ces alternatives prennent en compte les modèles existants ou en cours d'élaboration de certification en matière de protection des données. La France a opté jusqu'à présent pour une certification à travers des labels décernés par la Cnil sur la base de référentiels qu'elle élabore[34]. Elle pourrait continuer dans cette voie. Le développement des besoins en matière de certification pourrait néanmoins pousser la Cnil à faire appel à un organisme évaluateur extérieur rémunéré par le candidat à la certification. Mais l'État français pourrait aussi décider que le Comité français d'accréditation (Cofrac) joue un rôle pour agréer des organismes de certification en matière de protection des données personnelles. Des mécanismes de certification différents pourraient même être mis en place selon les produits ou les services visés.

De son côté, le Royaume-Uni s'oriente vers une certification à travers des organismes tiers privés qui seront accrédités par l'organisme national UK Accreditation Services (Ukas). L'autorité britannique de protection des données, l'Information Comissioner Office (ICO), élabore actuellement des critères pour l'adoption d'un label vie privée reposant sur un logo déposé sous forme de marque commerciale[35].

Enfin, la durée maximale de trois ans peut paraître assez longue étant donné l'évolution rapide des technologies. Elle correspond néanmoins à la durée de l'attribution des labels par la Cnil. Elle semble adaptée aux besoins des professionnels et conforme au principe de responsabilisation des responsables de traitement. L'important semble avant tout de garantir un examen périodique du respect de la certification par l'organisme concerné soit par un organisme évaluateur, soit par l'autorité nationale de protection des données.

À ce stade, la liberté laissée aux États membres n'est pas en soi critiquable. Elle interroge néanmoins sur la fiabilité des mécanismes futurs de certification malgré l'encadrement évoqué antérieurement.

2°/ Les conséquences néfastes que ces alternatives pourraient induire

Le maintien dans le RGPD de deux niveaux de certification, l'un à l'échelle nationale, l'autre à l'échelle de l'Union européenne, peut s'analyser comme un compromis provisoire. Toutefois cette solution pragmatique ménage avant tout les autorités nationales de protection et les marchés nationaux de la certification. Cela posera nécessairement trois types de difficultés.

D'une part, des difficultés de reconnaissance mutuelle des certifications nationales pourraient apparaître. L'article 39 *bis*, § 8, du RGPD se contente de donner compétence à la Commission

(32) Penneau A., Certification et codes de conduite privés : articles 38 et 39 (dans leur version originelle) prérapport, *in* Martial-Braz N. (ss dir.), La proposition de règlement européen relatif à la protection des données à caractère personnel : propositions du réseau Trans Europe Experts, Société de législation comparée, vol. 9, 2014, spéc. p. 353.

(33) Expression empruntée à Masclet J.-Cl., Règlement, *in* Répertoire de droit européen, Dalloz.

(34) Naftalski F., Label Cnil et conformité « informatique et libertés », publication des premiers référentiels, RLDI 2011.

(35) « *Trademarked privacy seal logo* », voir <https://iconewsblog.wordpress.com/2015/08/28/whats-the-latest-on-the-ico-privacy-seals/>.

pour fixer des mécanismes de reconnaissance de ces mécanismes de certification, labels et marques par le biais d'actes d'exécution. En outre, le CEDP joue un rôle de coordination des divergences entre les autorités de protection des données dans le cadre du mécanisme dit « *de cohérence* ».

D'autre part, la prolifération des labels et des marques risque d'être contre-productive. Elle ajoute plus de confusion qu'autre chose dans l'esprit du consommateur final. On peut d'ailleurs s'interroger sur la pertinence du périmètre de la labélisation. Faut-il créer un label exclusivement relatif à la protection des données au risque que son champ d'application trop limité ne soit pas adapté aux nécessités des acteurs de l'économie numérique ? Le respect de la protection des données ne constitue qu'un des aspects de leurs obligations. Aussi, la labélisation proposée par le RGPD devrait être articulée avec une labélisation plus globale. Cette dernière pourrait être envisagée lors de la révision annoncée de la directive n° 2002/58 dite « *vie privée et communications électroniques* » et de la directive n° 2001/31/CE sur le commerce électronique. L'objectif à terme de l'Union européenne doit être d'inclure la protection des données dans une approche globale et intégrée de certification à l'échelle européenne.

Enfin, le RGPD ne pose pas clairement la question du périmètre de l'objet de la certification. La formulation très large de l'article 39 du RGPD laisse entendre que la certification peut porter sur l'ensemble des obligations imposées par le règlement aux responsables de traitements et sous-traitants. Une même généralité se retrouve à l'article 22 *ter* qui rappelle qu'un « *mécanisme de certification (...) peut servir à attester du respect des obligations incombant au responsable de traitement* ». Or, comme il a été rappelé récemment, la certification constitue « *une activité marchande ordinaire pleinement ouverte à la concurrence* »[36]. Deux risques ne peuvent être exclus. D'une part, la propension possible de certains acteurs à développer le champ de la certification au-delà de ce qui est nécessaire simplement par intérêt économique[37]. D'autre part, certains acteurs économiques pourraient chercher à s'installer dans les États membres leur permettant de bénéficier d'une certification n'existant pas dans d'autres États membres, ou plus globalement d'un modèle de certification qui leur semblerait plus avantageux. Il s'agit d'une forme particulière de *forum shopping*.

Enfin, le modèle proposé ne permet pas d'apporter certaines garanties nécessaires pour assurer tant l'effectivité que la légitimité du processus de certification.

B. – L'absence de certaines garanties

L'expérience acquise dans le domaine de la certification invite à s'interroger sur l'absence de deux types de garantie dans le RGPD.

Premièrement, le RGPD ne fait aucune référence à la nécessité de rendre abordable la certification. Cette préoccupation avait été relevée par le Parlement européen[38]. Il avait ainsi proposé d'introduire une telle exigence qui a disparu dans le compromis final. Pourtant, les distorsions de coûts en matière de certification entre les États membres ont déjà été dénoncées[39].

Deuxièmement, les critiques faites autour des implications démocratiques de la normalisation[40] peuvent pleinement s'appliquer au RGPD. La certification peut être analysée comme une méthode alternative à la réglementation, élément de la conception idéologique de la Commission européenne d'une meilleure législation.

Placer les autorités de régulation de protection au cœur du processus de certification ne suffit pas à garantir que l'élaboration des certifications se fera de façon légitime en associant tous les acteurs, en particulier la société civile et les utilisateurs. Ces préoccupations devraient pourtant être au cœur de la régulation du droit fondamental de la protection des données à caractère personnel.

Enfin, la certification dans le RGPD n'échappe pas à une réserve faite en général au modèle européen de protection des données personnelles. L'effectivité de ce modèle est profondément liée à la capacité qu'auront les autorités de protection des données à assumer le rôle qui leur a été attribué. Difficile de dire à l'heure actuelle si la coopération entre les autorités de protection des données personnelles permettra réellement de surmonter les différences culturelles d'approche de la protection des données entre les États membres. Même au-delà de ces difficultés, il n'est pas évident que l'harmonisation des statuts, missions et pouvoirs place réellement les différentes autorités de protection sur un pied d'égalité pour remplir correctement leurs rôles. Cela dépendra des moyens humains et financiers attribués aux autorités nationales de protection de données, mais aussi au futur CEPD. ■

(36) Voir Avis du Conseil de la concurrence n° 15-A-16, 16 nov. 2015, portant sur l'examen, au regard des règles de concurrence, des activités de normalisation et de certification, not. point 51.

(37) Sur ce point nous partageons pleinement la critique d'Anne Penneau sur la nécessité de se préoccuper du « *quoi normaliser et certifier* » ; voir article précité sur standardisation et certification : les enjeux européens, p. 118.

(38) Voir la résolution adoptée le 12 mars 2014 et notamment la formulation de l'article 39, § 1 *ter* <www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR>.

(39) Voir l'avis précité du Conseil de la concurrence, pts 63 et s.

(40) Voir les travaux de Fabienne Péraldi, en particulier La normalisation : une alternative à la réglementation, Revue Constructif, 2011 ; Vers une externalisation de la production du droit – la place des acteurs privés, *in* Péraldi-Leneuf F. et de La Rosa St. (ss dir.), L'Union européenne et l'idéal de la meilleure législation, éd. Pedone ; Burgorgue Larsen L. (ss dir.), À propos des normes juridiques et des normes techniques : observations sur l'interaction et la concurrence normative dans le droit de l'Union européenne, Cahiers de l'Iredies, juin 2013 ; Contribution aux Mélanges en l'honneur du professeur François Hervouët, éd. Université de Poitiers, 2016.