ARTICLE

CERTIFICATION AU SENS DU RGPD – ACCESSIBILITÉ NE VEUT PAS DIRE GRATUITÉ !

IT et données personnelles Droit de la concurrence, consommation et distribution Contrats commerciaux et internationaux | 16/12/20 | Florence Chafiol

PROTECTION DES DONNÉES PERSONNELLES

Cette étude a été mandatée par Microsoft.

L'article 43 (6) du Règlement Général sur la Protection des Données (ci-après le « RGPD ») prévoit que les exigences liées à l'agrément et les critères de certification doivent être « *publiés par les autorités de contrôle sous une forme aisément accessible* ».

Une interrogation a pu être soulevée quant au critère « aisément accessible » : cela implique-t-il une publication gratuite des critères de certification approuvés par l'autorité de contrôle compétente ou par le comité européen sur la protection des données (« *CEPD* ») ?

Du point de vue des acteurs européens, le CEPD, notamment, souhaite et encourage une publication des critères de certification et d'agrément, tout en rappelant et respectant le droit d'auteur protégeant les normes. Dans une étude commandée par la Commission européenne, ses auteurs encouragent la publication complète des critères de certification au regard des exigences de transparence, tout en rappelant qu'un droit de propriété existe.

L'approche française quant à elle consiste à reconnaître un droit d'auteur sur les normes présentant un caractère original et à ce titre, confère au titulaire de ce droit la faculté de mettre ces normes à disposition du public sous un caractère onéreux. Toutefois, une « exception » au monopole du droit d'auteur s'applique, dès lors que la norme est d'application obligatoire, au regard du principe constitutionnel d'accessibilité au droit.

Il apparait aux auteurs du présent article que dès lors qu'une certification, conformément aux articles 42 et 43 du RGPD n'est pas obligatoire, les normes (ou critères de certification), fruits du travail d'acteurs privés et œuvres protégées par le droit d'auteur, n'ont pas vocation à être mises à disposition dans leur intégralité gratuitement.

1. Le droit français en matière de publication des normes

1.1. La protection des normes par le droit d'auteur et son « exception »

La jurisprudence l'a récemment rappelé : une norme, dès lors qu'elle présente un caractère original, peut être protégée par le droit d'auteur. Il est en effet possible de reconnaitre un droit d'auteur sur la norme technique si celle-ci présente l'originalité nécessaire à la protection d'une œuvre. Ainsi, l'a précisé une décision de la Cour d'appel d'Orléans à propos d'une série de formulaires[1] : « *il n'est pas nécessaire qu'une œuvre soit d'un niveau particulier d'originalité pour pouvoir être protégée par le droit d'auteur* ».

Ce principe est rappelé au sein du rapport d'information du Sénat au sujet de la normalisation :

> ● « *Les organismes de normalisation – qu'il s'agisse du niveau national, européen ou international, bénéficient en effet d'un droit de propriété intellectuelle, assimilable à un droit d'auteur, sur les normes qu'elles élaborent et les autorisent à en contrôler la diffusion.* »[2]

1.2. L'incidence du caractère volontaire de la norme sur son accessibilité et « exception » au droit d'auteur

D'après la jurisprudence administrative, il existe toutefois une exception au monopole de l'auteur trouvant son origine dans le caractère obligatoire du respect d'une norme. Ainsi, l'article 17 du décret du 16 juin 2009 prévoit :

> ● « *Les normes sont d'application volontaire. Toutefois, les normes peuvent être rendues d'application obligatoire par arrêté signé du ministre chargé de l'industrie et du ou des ministres intéressés.* ***Les normes rendues d'application obligatoire sont consultables gratuitement sur le site internet de l'Association française de normalisation***. »

Dans un premier arrêt de principe, le Conseil d'Etat précise que les dispositions de l'article 17 imposant que les normes obligatoires soient consultables gratuitement mettaient en œuvre un principe supérieur, en l'occurrence l'objectif de valeur constitutionnelle d'accessibilité de la règle de droit.

Or, constatant que les normes concernées dans cet arrêt n'avaient fait l'objet d'aucune mesure de publicité et n'étaient accessibles que par acquisition, à titre onéreux, auprès de l'Association française de normalisation, le Conseil d'État a considéré que l'arrêté imposant le respect de ces normes ne pouvait avoir rendu obligatoire une norme dont l'accessibilité libre et gratuite n'était pas garantie[3].

Dans un deuxième arrêt un an plus tard[4], le Conseil d'Etat confirme l'existence d'une exception au monopole en affirmant que l'existence de droits d'auteur sur une norme ne doit pas empêcher sa libre mise à disposition gratuite dès lors que cette norme est d'application obligatoire.

La jurisprudence française est donc claire : une norme obligatoire doit être mise à disposition de façon libre et gratuite. A contrario, une norme volontaire bénéficie bien de la protection du droit d'auteur et n'a pas vocation à revêtir un caractère gratuit.

La doctrine est également claire sur le caractère onéreux des normes :

> ● « *De plus, l'accès à la norme technique nationale privée n'est possible qu'à titre onéreux. Seule l'homologation ministérielle permet de lever cette barrière, et ce, au nom du respect de l'objectif constitutionnel d'accessibilité de la règle de droit* »[5] .

Il convient ici de rappeler que la certification au titre du RGPD est de nature volontaire. L'article 42 (3) du RGPD prévoit en effet que :

> ● « *La certification est volontaire et accessible via un processus transparent* ».

2. L'interprétation de la notion « aisement accessible » par des acteurs européens

Au titre de la certification, le RGPD prévoit en son article 43 (6) que « *Les exigences visées au paragraphe 3 du présent article et les critères visés à l'article 42, paragraphe 5, sont publiés par les autorités de contrôle sous une forme aisément accessible. Les autorités de contrôle transmettent aussi ces exigences et ces critères au comité. Le comité consigne dans un registre tous les mécanismes de certification et les labels en matière de protection des données et les met à la disposition du public par tout moyen approprié* ».

Par ailleurs, le RGPD se réfère plusieurs fois à la notion « aisément accessible » notamment lorsqu'il précise la notion de transparence du traitement, qui exige que « *toute information et communication relatives au traitement de ces données à caractère personnel soient aisément accessibles, faciles à comprendre, et formulées en des termes clairs et simples* »[6].

Le CEPD s'est prononcé sur la mise en place d'un mécanisme de certification par le RGPD à de nombreuses reprises en encourageant la plus grande transparence, sans toutefois nier la protection conférée par le droit d'auteur sur les normes.

2.1. La position du Comité Européen à la Protection des Données

Le Comité Européen des Données a publié de nombreuses lignes directrices sur le sujet de la certification et notamment des lignes directrices relatives à l'agrément des organismes de certification au titre de l'article 43 du RGPD[7] dans lesquelles la question de la publication prévue par l'article 43(6) est traitée.

Le CEPD reformule les termes du RGPD en précisant notamment que :

> ● « *L'ensemble des critères et des exigences approuvés par une autorité de contrôle doit dès lors être publié afin de garantir la transparence. En ce qui concerne la qualité et la confiance à l'égard des organismes de certification,* ***il serait souhaitable que le public puisse facilement accéder à toutes les exigences en matière d'agrément*** ».

Sans plus de précision quant à la notion de « publication », le CEPD reprend à nouveau cette expression lorsqu'il vient préciser les exigences générales relatives à l'agrément et précise notamment que :

> ● « *L'organisme d'accréditation, outre l'exigence visée au point 4.6 de la norme ISO/IEC 17065:2012, exige au minimum de l'organisme de certification :*
> ***1. que toutes les versions (actuelles et précédentes) des critères approuvés utilisés au sens de l'article 42, paragraphe 5, soient publiées et facilement accessibles au public****, ainsi que toutes les procédures de certification, en mentionnant de manière générale les périodes de validité respectives […]* ;

Le CEPD n'a pas saisi cette opportunité pour définir de manière concrète la notion « aisément accessible » mais, à tout le moins, a précisé que les critères de certification doivent faire l'objet d'une publication. La notion de publication n'étant elle-même pas précisée, elle peut tant faire référence à une publication gratuite qu'à une publication payante.

Toutefois, dans son avis 4/2020 relatif au projet de décision de l'autorité de contrôle compétente du Royaume-Uni concernant l'approbation des exigences relatives à l'agrément d'un organisme de certification, le CEPD relève que la norme ISO 17065 sera utilisée comme « critères d'agrément », accompagnée d'exigences supplémentaires établies par l'autorité de contrôle britannique.

A ce titre, le CEPD relève que **les normes ISO sont soumises à des droits de propriété intellectuelle** et par conséquent, le comité ne fait pas référence au texte de la norme dans son avis[8].

2.2. L'interprétation des articles 42 et 43 du RGPD au sein d'une étude commandée par la commission européenne

La Commission européenne a commandé une étude portant sur les articles 42 et 43 du RGPD, dont le rapport final a été publié en février 2019[9].

Si la notion « aisément accessible » n'est pas explicitement définie, le critère de transparence est un élément récurrent du rapport. En effet, les auteurs, tout en se gardant de dire que la publication des critères de certification est obligatoire, insistent sur le fait que cela est nécessaire et encourage la Commission Européenne dans cette voie.

Dans ce rapport, les auteurs proposent un certain nombre de possibilités pour encourager le développement de la certification, en visant toutes les étapes successives, de la rédaction des critères de certification à la certification de l'organisme elle-même.

Toutefois, les auteurs rappellent au sein de leur rapport – et suite à une analyse des certifications existantes – que la plupart de ces critères de certification ne sont pas toujours disponibles. Si le rapport prône une publication intégrale des critères de certification en faveur de la transparence et afin de préserver la confiance envers les mécanismes de certification, les auteurs rappellent la problématique de droits de propriété qui existent sur les méthodes d'évaluation[10] et envisagent comme solution la publication et l'accès sans entrave uniquement de la partie « fondamentale » de la méthode d'évaluation concernée[11]. L'exemple d'un résumé est également cité comme alternative par les auteurs[12].

Il semble ici que la recommandation formulée par les auteurs du rapport à destination de la Commission européenne consiste à ce qu'une partie seulement du mécanisme de certification soit publiée : ici est visée la partie fondamentale de la méthode d'évaluation, sans plus de précision quant à sa nature ou son contenu.

Dès lors, il est raisonnable de penser que la publication gratuite des critères de certification en tant que tels ne soit pour l'instant aucunement obligatoire.

A ce titre, le rapport cite en exemple une certification existante appelée « Ryerson Privacy by Design » qui ne publie qu'une liste exhaustive de points de contrôle[13], que les auditeurs utilisent pour évaluer les exigences de certification.

En conclusion, et à titre de possible recommandation, le rapport explique que l'une des options à envisager serait que la Commission publie des lignes directrices ou un guide, à l'attention du CEPD, fournissant un modèle de publication des critères de certification et la méthodologie d'évaluation ou bien un résumé de ceux-ci.

Il est intéressant de noter que le rapport continue sa démonstration en excluant clairement les critères de certification de la publication des mécanismes de certification par le CEPD au sein d'un registre public tel que prévu par l'article 42(8). [14]

Ce rapport permet ainsi d'établir un état des lieux de la législation européenne sur la problématique de la publication des critères de certification : il n'existe aucune obligation de publier ces critères, et un droit de propriété existe concernant lesdits critères. La recommandation des auteurs d'imposer la publication gratuite des critères n'étant qu'une simple recommandation.

Article rédigé par Florence Chafiol, Alice Hourquebie et Ariane Seyed-Movaghar

[1] Cour d'appel d'Orléans, chambre commerciale, 15 juin 2006, n°05/02452

[2] Rapport d'information de Mme Élisabeth Lamure, sénateur du Rhône - Rapport n° 627 (2016-2017) Où va la normalisation ? - En quête d'une stratégie de compétitivité respectueuse de l'intérêt général

[3] Conseil d'Etat, 10 février 2016, n° 383756, Fédération nationale des mines et de l'énergie

[4] Conseil d'Etat, 6e chambre, 28 juillet 2017, n°402752

[5] Du standard international à la norme technique nationale : l'exemple du Codex Alimentarius – RFDA 2019 p.985

[6] RGPD, considérant 39

[7] « Lignes directrices 4/2018 relatives à l'agrément des organismes de certification au titre de l'article 43 du règlement général sur la protection des données (2016/679) » – Dernière mise à jour le 4 juin 2019

[8] Avis 4/2020 relatif au projet de décision de l'autorité de contrôle compétente du Royaume-Uni concernant l'approbat ion des exigences relatives à l'agrément d'un organisme de certification conformément à l'article 43, paragraphe 3, du R GPD

[9] « Data Protection Certification Mechanisms Study on Articles 42 and 43 of the Regulation (EU) 2016/679 Final report » – Février 2019

[10]« *While we hold that the certification criteria should in their entirety be published to ensure transparency and safeguard the reliability of the certification, seal, and mark, it is true that there are proprietary rights over assessment methodologies which feed concerns over sharing publicly the methodologies.* »

[11]« *Another solution would be publication and unhindered access to the main rationale of the assessment methodology.* »

[12]« *Other certifications use other methodologies such as Protection Goals or Control Goals, which they summarise on their websites.* »

[13] Voir notamment : https://www.ryerson.ca/content/dam/pbdce/certification/PbD-Brochure.pdf

[14] « *In addition, if a data protection certification mechanism is interpreted to include the assessment methodology, apart from the certification criteria and other organisational or procedural issues, then such methodology should be included in the register of the EDPB (Art. 42(8) GDPR).* »