Autorité de protection des données
Gegevensbeschermingsautoriteit

Avis n° 98/2022 du 13 mai 2022

Objet: Demande d'avis concernant un projet de loi portant création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements et arrêts (CO-A-2022-078)

Le Centre de Connaissances de l'Autorité de protection des données (ci-après « l'Autorité »),
Présent.e.s : Messieurs Yves-Alexandre de Montjoye et Bart Preneel;

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données*, en particulier les articles 23 et 26 (ci-après « LCA »);

Vu le 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* (ci-après « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après « LTD »);

Vu la demande d'avis de Monsieur Vincent Van Quickenborne, Vice-Premier Ministre, Ministre de la Justice et de la Mer du Nord, reçue le 22 mars 2022;

Émet, le 13 mai 2022, l'avis suivant :

I. OBJET ET CONTEXTE DE LA DEMANDE D'AVIS

1. Le Vice-Premier Ministre et Ministre du Gouvernement fédéral en charge de la Justice et de la Mer du Nord (ci-après « le demandeur ») a sollicité, le 22 mars 2022, l'avis de l'Autorité concernant un projet de loi portant création du Registre central pour les décisions de l'ordre judiciaire et relative à la publication des jugements et arrêts (ci-après « le projet »).

2. Une décision par laquelle un litige est réglé comporte un certain nombre de données à caractère personnel afin qu'il soit clair pour les personnes concernées que la décision porte sur leur affaire et que, par exemple, les tiers compétents chargés d'exécuter cette décision sachent en faveur et à charge de qui ils interviennent. Ces données à caractère personnel traitées par les juridictions ne sont pas directement visées par le projet[1].

3. La publication de ces décisions peut être qualifiée de traitement ultérieur compatible avec la finalité initiale (règlement des litiges) pour laquelle ces données ont été collectées.

4. L'article 149, al. 2, de la Constitution[2] laisse le législateur libre de déterminer la manière de « *rendre public* » un jugement[3]. La loi du 5 mai 2019 modifiant le Code d'instruction criminelle et le Code judiciaire en ce qui concerne la publication des jugements et des arrêts[4] visait notamment à donner effet à l'article 149 de la Constitution en limitant le prononcé public des jugements et arrêts à la lecture du dispositif, ainsi qu'à « *faire publier* » le texte intégral des décisions judiciaires dans une banque de données électronique des jugements et arrêts de l'ordre judiciaire accessible au public. L'entrée en vigueur de cette loi a été reportée à deux reprises en raison des lacunes relatives à l'absence de cadre légal précis[5], à la prise en compte des conséquences d'une accessibilité de masse, à l'archivage des

---

[1] La « déclaration de protection de vos données à caractère personnel » précise que les traitements effectués d'une part, par le Collège des cours et tribunaux et, d'autre part, par les juridictions représentées par le Collège, sont « *sont nécessaires soit :*

- *à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;*
- *à la constatation, à l'exercice ou à la défense d'un droit en justice (ou quand les cours et tribunaux agissent dans le cadre de leur fonction juridictionnelle) ;*
- *au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;*
- *aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale ;*
- *à des fins archivistiques dans l'intérêt public ou à des fins statistiques* » (https://www.rechtbanken-tribunaux.be/fr/declaration-de-protection-de-vos-donnees-a-caractere-personnel)

[2] Modifié par la loi du 22 avril 2019 portant révision de l'article 149 de la Constitution

[3] Sauf en matière pénale, où le dispositif doit encore être prononcé en audience publique.

[4] DOC 54 3489/001, https://www.lachambre.be/FLWB/PDF/54/3489/54K3489001.pdf

[5] L'exposé des motifs du présent projet parle de cadre légal « *efficace* »

décisions déjà prononcées et à l'anonymisation des décisions qu'elle comportait[6]. Le projet entend donc abroger et remplacer la loi du 5 mai 2019 précitée.

5. Le SPF Justice a publié un avis de marché concernant le développement, l'hébergement, la maintenance et le support de la base de données centrale des arrêts et jugements en date du 8 février 2022 au bulletin des adjudications et le 11 février 2022 au journal officiel de l'Union européenne[7]. La description des prestations qu'il contient est particulièrement éclairante concernant les traitements de données envisagés :

« L'adjudication est composée de 1 (un seul) et consiste en 6 postes.
Poste 1 :
La création, l'hébergement et la gestion d'une banque de données permettant d'enregistrer les jugements et arrêts des tribunaux belges. La structure et le modèle de données doivent permettre de stocker des jugements et des arrêts historiques ;
d'encoder de nouveaux jugements et arrêts ; de contribuer à des jugements et des arrêts plus structurés à l'avenir.
Cette banque de données des jugements et arrêts prévoit un cryptage suffisant offrir la possibilité tels que : la signature électronique ; la pseudonymisation, la validation de la pseudonymisation ; l'importation en masse ; l'importation de jugements et d'arrêts historiques à l'aide d'OCR.
Les processus de signature électronique, de pseudonymisation et de validation de la pseudonymisation doivent également être mis en place dans le cadre de la présente adjudication. Le prestataire de services crée également des rapports en ligne sur l'état du système. Il peut notamment s'agir de savoir quels éléments sont en ligne/hors ligne, du temps de réaction, du nombre d'interventions en prestation de services, etc.
Poste 2 :
La fourniture d'un moteur de pseudonymisation optimisé pour la pseudonymisation des jugements et arrêts en français, en néerlandais et en allemand.
Poste 3 :
Fournir un système capable de détecter automatiquement les mots clés des jugements et arrêts, ainsi que de relever les passages les plus importants d'un jugement ou d'un arrêt. Ce système doit pouvoir fonctionner tant sur les documents originaux que sur les versions pseudonymisées.
Poste 4 :
Fournir un mécanisme d'indexation pour les jugements et arrêts stockés dans une banque de données ou un système de gestion de documents.

---

[6] Voy. DOC 55 1295/001, https://www.lachambre.be/FLWB/PDF/55/1295/55K1295001.pdf, pp. 45 et sv. ; comp. Avec l'Exposé des motifs du projet actuel qui parle de « pseudonymisation » des décisions

[7] Numéro de référence: SE-ICT-CDC2022.0400-F02_0; https://ted.europa.eu/udl?uri=TED:NOTICE:076310-2022:TEXT:FR:HTML

Poste 5 :

Doter la banque de données visée au poste 1 d'un écran de recherche, en recourant au marquage prévu au poste 3 et à l'indexation prévue au poste 4 afin d'obtenir rapidement des résultats de recherche pertinents.

Poste 6 :

Fournir un écran de recherche accessible au public, en recourant au marquage prévu au poste 3 et à l'indexation prévue au poste 4 afin d'obten (sic)

Le prestataire des services doit être en mesure d'offrir le projet et le soutien opérationnel nécessaires en néerlandais et en français sur le territoire belge ».

6. L'Autorité rappelle que la question des banques de données de jugements et/ou d'arrêts accessibles à des tiers a fait l'objet de sa recommandation n°03/2012[8], mais qu'elle fait également l'objet de divers avis[9] ainsi que de délibérations d'autorités étrangères[10], d'importantes décisions de justice[11] et d'une abondante doctrine[12].

II. EXAMEN DU PROJET

1. Base juridique et principe de légalité

7. Le(s) traitement(s) de données à caractère personnel au(x)quel(s) le projet donne lieu repose(nt) sur l'article 6.1.c) du RGPD et engendre(nt) une importante ingérence dans les droits et libertés des personnes concernées. L'Autorité constate en effet que le traitement de données à caractère personnel porte sur un volume important de données ou touche un nombre important de personnes concernées (traitement *« à grande échelle* »), qu'il est susceptible de porter sur des « *catégories particulières de données* » au sens des articles 9 et 10 du RGPD ou sur des données relevant de la sphère intime de

---

[8] Recommandation du 8 février 2012, https://www.autoriteprotectiondonnees.be/publications/recommandation-n-03-2012.pdf

[9] Avis n°11/2004 du 4 octobre 2004 (https://www.autoriteprotectiondonnees.be/publications/avis-n-11-2004.pdf); Avis n° 01/2007 de la Commission du 17 janvier 2007 (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_01_2017.pdf) ; Avis n° 16/2007 de la Commission du 11 avril 2007 (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_16_2007_0.pdf) ; Avis n° 116/2019 du 5 juin 2019 (https://www.autoriteprotectiondonnees.be/publications/avis-n-116-2019.pdf)

[10] Voy. CNIL, Délibérations 01-057 du 29 novembre 2001, 2012-245 du 19 juillet 2012 et 2012-246 du 19 juillet 2012

[11] Voy. CEDH, C.C. c. Espagne, req. N° 1425/06, 6 octobre 2009 (https://hudoc.echr.coe.int/fre?i=001-94632) et EFTA Court, affaires E-11/19 et E-12/19, 10 décembre 2020 (https://eftacourt.int/download/11-19-12-19-judgment/?wpdmdl=6966)

[12] Voy. notamment J. MONT, *RGPD : faut-il anonymiser la jurisprudence publiée ?*, JT 2019, pp. 442 et sv. (http://www.crid.be/pdf/public/8448.pdf); C. de TERWANGNE, Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles (http://www.crid.be/pdf/public/5021.pdf); S. MARKIEWICZ, *Dissemination of Legal Information: Wedding or Divorce between Open Data Movement and Implementation of Personal Data Protection Law Principles*, Law via the Internet Conference 2018 (http://lvi2018.ittig.cnr.it/conference-program); S. VAN RAEPENBUSCH, "Anonymisation des décisions de la Cour Justice de l'Union Européenne: protection de la vie privée versus publicité des jugements", *in Libertés,, (l)égalité, humanité. Mélanges offerts à Jean Preutels*, Brussel, Bruylant, 2019, pp. 331-350; L'Autorité rappelle par ailleurs que l'annexe II à la Recommandation n°R(95) 11 du comité des Ministres du Conseil de l'Europe, adoptée le 11 septembre 1995, contient les lignes directrices concernant la sélection, le traitement, la présentation et l'archivage des décisions judiciaires dans les systèmes de documentation juridique automatisés ; Voy. également la Recommandation n°R(83)3 relative à la protection des utilisateurs des services informatique juridique.

la personne concernée ou encore de concerner des personnes vulnérables (mineurs, personnes handicapées, migrants, personne en situation financière précaire, …).

8. L'Autorité rappelle qu'aux termes de l'article 22 de la Constitution, lu en combinaison avec l'article 8 de la CEDH et 6.3 du RGPD, une norme de rang législatif doit déterminer dans quelles circonstances un traitement de données est autorisé. Conformément aux principes de légalité et de prévisibilité, cette norme législative doit ainsi, en tout cas, fixer les éléments essentiels du traitement. Lorsque le traitement de données constitue une ingérence importante dans les droits et libertés des personnes concernées, comme c'est le cas en l'espèce, il est nécessaire que les éléments essentiels suivants soient déterminés par le législateur : la (les) finalité(s) précise(s) et concrètes[13], l'identité du (des) responsable(s) du traitement (sauf si c'est évident), les (catégories) de données qui sont nécessaires à la réalisation de cette (ces) finalité(s), le délai de conservation des données[14], les catégories de personnes concernées dont les données seront traitées, les (catégories de) destinataires auxquels les données seront communiquées[15], les circonstances dans lesquelles elles seront communiquées ainsi que, le cas échéant si c'est nécessaire, la limitation des obligations et/ou des droits visé(e)s aux articles 5, 12 à 22 et 34 du RGPD.

9. Cependant, comme l'a rappelé la Cour constitutionnelle, une délégation au Roi « *n'est pas contraire au principe de légalité, pour autant que cette délégation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur* »[16].

10. En l'espèce, le chapitre 2 du projet prévoit la possibilité pour le juge d'ordonner la publication de sa décision dans le « *Registre central pour les décisions de l'ordre judiciaire* » visé au chapitre 5 du projet. L'article 782, §1er du Code judiciaire (tel que remplacé par l'article 12 du projet) impose l'établissement des jugements sous forme dématérialisée et habilite le Roi à déterminer les conditions techniques auxquelles le jugement établi sous forme dématérialisée doit satisfaire. Le §4 de l'article 782 institue une banque de données informatisée appelée « *Registre central pour les décisions de l'ordre judiciaire* » auprès du SPF Justice et en énonce les « *finalités* ». Les §§2 et 3 de l'article 782 prévoient l'enregistrement des jugements revêtus d'une signature électronique qualifiée dans cette banque de données. Le §5 énumère les données pouvant être enregistrées tout en habilitant le Roi à « *déterminer*

---

[13] Voir aussi l'article 6.3 du RGPD.

[14] La Cour constitutionnelle a déjà reconnu que "le législateur pouvait régler de manière générale les conditions de conservation des données à caractère personnel, ainsi que la durée de cette conservation", Arrêt n° 29/2018 du 15 mars 2018, point B. 23.

[15] Voir par exemple, Cour constitutionnelle, Arrêt n° 29/2018 du 15 mars 2018, point B.18, et Cour constitutionnelle, Arrêt n° 44/2015 du 23 avril 2015, points B.36.1 e.s.

[16] Voir Cour Constitutionnelle : arrêt n° 29/2010 du 18 mars 2010, point B.16.1 ; arrêt n° 39/2013 du 14 mars 2013, point B.8.1 ; arrêt n° 44/2015 du 23 avril 2015, point B.36.2 ; arrêt n° 107/2015 du 16 juillet 2015, point B.7 ; arrêt n° 108/2017 du 5 octobre 2017, point B.6.4 ; arrêt n° 29/2018 du 15 mars 2018, point B.13.1 ; arrêt n° 86/2018 du 5 juillet 2018, point B.7.2 ; avis du Conseil d'Etat n° 63.202/2 du 26 avril 2018, point 2.2.

les données exactes » pouvant être enregistrées et à déterminer les conditions techniques auxquelles la copie dématérialisée doit satisfaire. Le §6 consacre l'existence d'un comité de gestion, en détermine la composition et les missions tout en habilitant le Roi à déterminer ses modalités de composition et de fonctionnement. Le §7 prévoit que les entités représentées au sein de ce gestionnaire agissent en qualité de responsables conjoints du traitement. Le §8 identifie les catégories de personnes ayant accès au registre, en distinguant la consultation des autres traitements et en rappelant que ces traitements sont limités par leurs missions légales. Ce même paragraphe prévoit la détermination des modalités de publication par la juridiction l'ayant rendue et habilite le Roi à déterminer les modalités de l'accès au registre ainsi que les procédures relatives à cet accès. Il rend en outre la disposition du Code pénal relative au secret professionnel applicable à toute personne traitant les données du Registre. Le §9 vise la durée de conservation des données. Le §10 habilite le Roi à déterminer les modalités de mise en place et de fonctionnement du Registre. L'article 13 du projet modifie l'article 782 CJ remplacé par l'article 12 du même projet ajoute les finalités relatives à la publicité des jugements et à la recherche scientifique, prévoit la publication des jugements sous forme pseudonymisée et identifie les catégories de données devant faire l'objet d'une pseudonymisation (automatique mais soumise à un contrôle humain). Il prévoit la possibilité d'introduire une demande de pseudonymisation auprès d'une instance désignée par le Roi, prohibe et sanctionne le traitement ultérieur des données d'identité des magistrats, des membres du greffe et des avocats ne peuvent faire l'objet d'une réutilisation ayant pour objet ou pour effet d'évaluer, d'analyser, de comparer ou de prédire leurs pratiques professionnelles réelles ou supposées et habilite le Roi à déterminer les modalités de la pseudonymisation, du contrôle humain ainsi que la portée de la dérogation à l'absence de pseudonymisation des données d'identité des magistrats, des membres du greffe et des avocats dans les décisions relative à la criminalité organisée. Le chapitre 3 (essentiellement les articles 5 et 7) du projet modifie le Code d'instruction criminelle en y prévoyant la publication des décisions pseudonymisées via le registre en prévoyant l'omission facultative de certaines parties de la motivation en cas d'atteinte disproportionnée au droit à la protection de la vie privée des personnes concernées. Enfin, le chapitre 4 du projet modifie le Code pénal en vue de permettre aux juges d'ordonner la publication ou la diffusion des décisions non pseudonymisées par affichage, publication, enregistrement dans le registre ou par « *tout autre moyen de communication* ».

11. L'Autorité constate que, tout comme loi du 5 mai 2019, la portée du projet dépasse la seule modalité de publicité des décisions (visée à l'article 149 de la Constitution), mais semble s'inscrire dans un projet plus vaste de « *réalisation d'un dossier numérique complet* »[17] impliquant la création d'une source authentique des décisions et permettant la réutilisation des données pseudonymisées contenues dans ces décisions à des fins diverses (détaillées ci-après).

[17] Voy. DOC 1610/015, point 1.2.1. (https://www.dekamer.be/FLWB/PDF/55/1610/55K1610015.pdf)

2. Finalités

12. En vertu de l'article 5.1.b) du RGPD, un traitement de données à caractère personnel n'est autorisé que pour des finalités déterminées, explicites et légitimes.

13. Comme indiqué *supra* le traitement des données figurant dans les décisions de justice constitue un traitement ultérieur. A cet égard, l'article 5.1.b) du RGPD prévoit que les données collectées ne peuvent être traitées ultérieurement d'une manière incompatible avec ces finalités, tout en précisant que le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales.

14. La publication au sens strict peut certainement être considérée comme une finalité compatible avec la finalité initiale (règlement des litiges) pour laquelle ces données ont été collectées. Toutefois, comme indiqué *supra*, les finalités mentionnées dans le projet vont plus loin que la seule publication. L'article 12 du projet distingue les finalités « *du registre* » des finalités des traitements. L'Autorité est favorable à la détermination des finalités d'un registre. Néanmoins, le respect de l'article 5.1.b) du RGPD impose la détermination des finalités des traitements de données à caractère personnel en distinguant, en l'espèce, les finalités liées à la création d'une source authentique[18] et à l'enregistrement des données à caractère personnel dans le registre (appelées à figurer à l'art. 782, §4, 1° à 3°) des finalités des autres traitements relatifs à ces données (4° et sv.).

15. L'Autorité constate que l'article 782, §4, 5° prévoit la finalité d'amélioration de la qualité des données enregistrées. L'exposé des motifs illustre cette finalité par la réparation « *des fichiers illisibles ou corrompus* ». Afin d'éviter tout risque de confusion, l'Autorité estime qu'il convient de préciser dans le commentaire de l'article 12 qu'il ne s'agit pas de mettre en œuvre le principe d'exactitude figurant à l'article 5.1.d) du RGPD et de permettre la modification des données figurant dans les décisions prononcées par les juridictions. Ces dernières étant en effet généralement seules compétentes pour ce faire.

16. Si la finalité liée à l'optimalisation de l'organisation de l'ordre judiciaire est appelée à justifier des traitements de données à caractère personnel, il convient de détailler – dans le projet - ce qui est visée par « *optimalisation de l'organisation* » (par exemple en indiquant qu'il s'agit de permettre la mesure de la charge de travail, des performances, etc…). La mention dans le commentaire de l'article 12 selon laquelle « *une approche axée sur les données doit permettre une gestion plus efficiente et une*

[18] Par exemple « *faciliter l'accès des autorités habilitées à accéder à ces décisions en vertu d'une loi et pour les besoins de leurs missions* »

meilleure affectation des moyens humains et logistiques au sein de l'ordre judiciaire » est, à cet égard, insuffisante. A l'inverse, s'il ne s'agit que d'optimaliser la structure de l'organisation et qu'aucun traitement de données à caractère personnel n'est nécessaire pour ce faire, il convient également de le préciser (cette fois, dans le commentaire de l'article 12).

17. Par ailleurs, l'Autorité relève qu'à l'occasion de l'introduction de la demande d'avis le fonctionnaire délégué indiquait par ailleurs que l'accès en ligne, du grand public, aux décisions publiées était l'un des critères d'évaluation du « *Justice Scoreboard* » de l'UE[19]. L'Autorité observe que, dans la même logique, les institutions européennes[20] « *encouragent* » régulièrement les Etats membres à mettre en œuvre des programmes de digitalisation de la justice pour des objectifs variés allant de l'accessibilité et l'efficacité à l'établissement de « *European justice data spaces* », en passant le respect du principe « *only once* »[21]. L'Autorité estime que ces finalités ne sont pas problématiques en soi, mais qu'elles doivent néanmoins nécessairement être identifiées. L'Autorité estime en effet qu'il convient de faire preuve d'une transparence au moins aussi étendue lorsque les normes adoptées mettent en œuvre une « *stratégie européenne* »[22] que lors de la transposition d'une directive dans une matière dans laquelle l'Union dispose d'une compétence normative en vertu du Traité sur le fonctionnement de l''Union européenne (TFUE).

18. L'Autorité observe en outre que le commentaire de l'article 12[23], mentionne l'accès aux données qui serait octroyée « *par exemple, à une legaltech chargée de développer un algorithme pour fournir un appui à la magistrature dans la préparation de ses décisions, comme un algorithme de case law enhancement* ». Une telle finalité doit être déterminée explicitement dans le projet et **le caractère nécessaire et proportionnel[24] de l'utilisation des données à des fins d'entraînement d'algorithmes doit être démontré** dans l'exposé des motifs. L'Autorité rappelle en effet l'arrêt n° 29/2018 dans lequel la Cour constitutionnelle affirmait que l'exigence d'un fondement légal précis et prévisible (et donc d'une finalité claire) "*s'applique d'autant plus lorsque les données à caractère personnel sont ensuite traitées par les services publics à d'autres fins que celles pour lesquelles elles ont initialement été obtenues*"[25].

19. L'Autorité relève encore que la détermination de la finalité revêtira une importance particulière dans la détermination public concerné par la publicité, elle constituera également un élément déterminant de

---

[19] Voy. https://ec.europa.eu/info/sites/default/files/eu_justice_scoreboard_2021.pdf, pp. 37-39

[20] Parfois avec d'autres institutions

[21] Voy. la communication intitulée "*Digitalisation of justice in the European Union A toolbox of opportunities*", https://ec.europa.eu/info/sites/default/files/communication_digitalisation_en.pdf, p. 14 ou les conclusions du Conseil intitulées « *Access to justice – seizing the opportunities of digitalisation* »

[22] Comme c'est également le cas en matière de (données de) santé

[23] Page 23

[24] Sur cette question voy. *infra*

[25] Cour constitutionnelle, 15 mars 2018, Arrêt n° 29/2018, B.18.

l'analyse des traitements ultérieurs permis au titre de l'article 6, 4. du RGPD, par les personnes susceptibles de les traiter. Une finalité claire et précise est en effet d'autant plus importante lorsque le public concerné est celui des utilisateurs d'internet, à savoir un public global quant à sa localisation (européenne ou non), indéterminé quant à son nombre et à sa qualité (de bonne foi, professionnel, malveillant, familial, en quête de profit, plus ou moins nombreux, etc.) et anonyme (sans la mise en place de mesures spécifiques). C'est-à-dire un public concrètement invisible pour l'autorité qui est à la source de la publicité concernée et dont les individus poursuivent tous types d'intérêts et finalités, y compris potentiellement malveillants. Une finalité trop ouverte, bien qu'assurant au maximum l'objectif de transparence administrative, pourrait excéder l'objectif initial poursuivi par le législateur tout en ouvrant la possibilité de traitements de données ultérieurs non souhaités, et créer de l'insécurité juridique à charge in fine, du responsable du traitement. Il en résulte la nécessité , de distinguer les finalités liées à la transparence de la justice/de publicité, des autres finalités, d'imposer des contraintes fortes sur les éventuelles finalités pour lesquelles il pourrait être justifié de traiter des données en vue de l'entrainement d'un algorithme (et donc de définir ces finalités de manière extrêmement précise) et de préciser les notions de « *fins scientifiques* » et d' « *analyse statistiques* ». En effet, l'interprétation large qui en est faite à l'heure actuelle, dans l'exposé des motifs, ne peut en aucun cas permettre que l'adoption ultérieure d'une norme[26] autorise la fourniture des données (qui ne seraient pas parfaitement anonymisées[27]) collectées dans le cadre du règlement des litiges, à titre gratuit ou onéreux, directement ou après centralisation au niveau européen, à des opérateurs actifs dans le développement d'algorithmes, à des fins purement commerciales[28].

20. L'adoption ultérieure d'une telle norme – alors qu'il n'est déjà plus possible d'invoquer l'ignorance[29] pour justifier de l'absence d'un cadre légal clair dès aujourd'hui - serait constitutive d'un détournement de finalité et le traitement de données qu'elle prévoirait ne pourrait être considéré comme licite[30] qu'à la condition de porter sur une nouvelle collecte de données à l'occasion de laquelle les personnes concernées auraient pu avoir la possibilité de s'opposer à un tel traitement ultérieur après avoir été dûment informées des finalités du traitement ultérieur envisagé. L'Autorité fera preuve de vigilance à cet égard.

---

[26] Dans cet exemple, l'intérêt légitime ne pourrait bien entendu pas non plus être valablement invoqué.

[27] Sur cette question voy. *infra*

[28] L'Autorité invite le demandeur à être particulièrement attentif à l'utilisation abusive de l'intérêt légitime dans le cadre d'un traitement ultérieur de catégories particulières de données, comme le démontre l'exemple des données de santé au Royaume-Uni (https://www.wired.co.uk/article/google-apple-amazon-nhs-health-data)

[29] Voy. en effet Study on the use of innovative technologies in the justice field (https://orbi.uliege.be/bitstream/2268/252237/1/DS0220605ENN.en.pdf)

[30] Voy. C. de Terwangne (« Les principes relatifs au traitement des données à caractère personnel et à sa licéité », *in* Le Règlement général sur la protection des données – analyse approfondie, Bruxelles, Larcier, p. 89), qui précise que « *l'exigence de licéité signifie que le traitement de données à caractère personnel doit se faire conformément à l'ensemble des règles légales applicables.*

21. Si des finalités de ce type devaient être envisagées (et que le caractère nécessaire et proportionnel de ces traitements devait pouvoir être démontré), l'Autorité invite le demandeur à tenir compte des dispositions de la proposition de Règlement européen concernant l'intelligence artificielle[31] lors de la détermination de ces finalités dans le projet.

22. L'Autorité observe par ailleurs que le commentaire de l'article 12[32], mentionne l'octroi d'un accès aux données à « *des tiers autorisés par écrit par le gestionnaire, pour la finalité ou les finalités pour laquelle ou lesquelles l'autorisation a été donnée et dans les conditions déterminées par le gestionnaire* ». Cette disposition est de nature à laisser sous-entendre qu'il serait possible, pour un responsable du traitement, de permettre conventionnellement à un sous-traitant de traiter des données pour des finalités excédant celles dont le responsable du traitement peut se prévaloir, alors qu'il n'en est rien. Ce passage de l'exposé des motifs sera donc reformulé.

23. L'Autorité précise en outre que - comme le prévoit le projet concernant le traitement des données d'identification des magistrats - lorsque des traitements de données sont susceptibles d'engendrer une ingérence particulièrement importante, comme c'est le cas en l'espèce, le fait de prévoir expressément des interdictions de traitements ultérieurs pour certaines finalités, constitue une bonne pratique. L'Autorité insiste toutefois sur le fait que, même en l'absence de toute interdiction expresse, seule la réutilisation des données des justiciables à des fins de recherche scientifique au sens strict (à savoir, par exemple, la recherche juridique) est admissible (dans le respect de conditions strictes dont celles liées à une réelle pseudonymisation). En revanche, il n'en irait pas de même d'une réutilisation à des fins commerciales. Un traitement de données (et a fortiori de catégories particulières de données) pour une telle finalité ne pourrait en aucun cas porter sur des données collectées, enregistrées et partagées sous l'égide d'une norme ancienne ne prévoyant pas la **possibilité pour les personnes concernées de s'opposer** à un tel traitement après avoir été dûment informées des finalités envisagées, dès le stade de la collecte de leurs données.

24. Pour assurer cette information, l'Autorité estime qu'un formulaire constitue un bon biais de communication pour informer les personnes dont un responsable du traitement souhaite traiter les données. Le cas échéant, les mentions suivantes devront y figurer : la possibilité de s'opposer au traitement de ses données pour certaines finalités déterminées, le nom et l'adresse du responsable du traitement, les coordonnées du délégué à la protection des données, les finalités[33] de la collecte de

---

[31] https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52021PC0206&from=FR

[32] Page 23

[33] Un consentement « *spécifique* » implique que le consentement de la personne concernée doit être donné en lien avec une ou plusieurs finalités spécifiques et que la personne a un choix concernant chacune de ces finalités (Des orientations complémentaires concernant la détermination des «finalités» peuvent être trouvées dans l'avis 3/2013 sur la limitation de la finalité (WP203)). A titre d'exemple de modalité permettant de respecter cette condition, la loi allemande du 3 juillet 2020 relative à la protection des données des patients prévoit que les patients auront la possibilité (à partir de 2023) de consentir explicitement au principe et aux modalités de l'accès de leurs données à des chercheurs (Voy.

données ainsi que la base juridique du traitement auquel les données sont destinées, les destinataires ou catégories de destinataires des données, l'existence des différents droits consacrés par le RGPD aux personnes concernées (y compris le droit d'accès et de rectification), le caractère facultatif de la communication de données ainsi que les conséquences éventuelles d'un défaut de communication, la durée de conservation des données à caractère personnel collectées ou les critères utilisés pour déterminer cette dernière, le droit d'introduire une réclamation auprès de l'APD et le cas échéant, l'existence d'une prise de décision automatisée (y compris un profilage, visées à l'article 22 du RGPD) et les informations concernant sa logique sous-jacente ainsi que l'importance et les conséquences prévues de cette prise de décision automatisée pour les personnes concernées.

25. L'Autorité attire l'attention du demandeur sur les possibilités techniques existantes et les modalités de mise à disposition des décisions qui ne seraient pas parfaitement anonymisées, mais dont les caractéristiques ne rendent pas une publication pure et simple du document simplement pseudonymisé, nécessaire, applicables en **fonction de la finalité envisagée**. En ce qui concerne la finalité liée à la publicité des décisions, l'Autorité estime que le recours à l'authentification, l'utilisation d'un *captcha*, le *rate limiting*, et la mise en œuvre de solutions prohibant par exemple techniquement le « *bulk downloading* », constitue une bonne pratique[34]. En ce qui concerne les finalités pour lesquelles il serait justifié de traiter des données dans le cadre de l'entraînement d'algorithmes, des solutions plus créatives, comme par exemple le recours à certains services[35], l'exigence de mise en place d'un comité d'éthique ou la réalisation d'un audit auprès du destinataire appelé à effectuer un traitement ultérieur sur ces données, pourraient minimiser les risques inhérents à la réutilisation des données concernées. A toutes fins utiles, l'Autorité attire cependant l'attention du demandeur sur les questions de droits intellectuels (propriété/restriction des droits d'utilisation à titre gratuit par les autorités publiques ayant mis les données à disposition des acteurs économiques), éthiques (type d'algorithme, usages autorisés), de droit de la concurrence (distorsion de concurrence liée au droit d'utilisation des données par certains acteurs), etc., qui sont susceptibles de se poser lorsque des données à caractère personnel collectées sur base de l'intérêt légitime d'une autorité publique sont communiquées en vue d'un traitement à des fins commerciales.

3. Proportionnalité/minimisation des données

26. L'article 5.1.c) du RGPD prévoit que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités visées (principe de "minimisation des données").

---

https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/P/PDSG-Bundestag_Drs-18793.pdf)

[34] L'Autorité précise en revanche qu'une limitation de l'accès aux seules personnes se situant sur le territoire de l'Union sera extrêmement facile à contourner, par exemple par le recours à un VPN.

[35] Voy. par exemple https://www.casd.eu/

27. L'article 782, §5 CJ (introduit par l'article 12 du projet) prévoit le traitement des métadonnées nécessaires pour atteindre les finalités du registre, lesquelles seront déterminées par le Roi. Au regard de l'importance de l'ingérence dans les droits et libertés des personnes concernées engendrée par les traitements prévus par le projet, les catégories de données à caractère personnel doivent nécessairement être déterminées dans le projet. Le Roi pouvant tout au plus être habilité à les préciser par voie d'arrêté. Le projet sera donc modifié en ce sens.

28. Le même paragraphe de l'article 782 CJ (modifié par l'article 13 du projet) prévoit la pseudonymisation des données d'identité des justiciables ainsi que « *de tout élément du jugement ou de l'arrêt permettant d'identifier directement ou indirectement les personnes physiques mentionnées dans le jugement ou l'arrêt,* (…) *dans les limites de la lisibilité et de la compréhension du jugement ou de l'arrêt* ».

29. L'Autorité attire l'attention du demandeur sur le fait que toute ingérence dans le droit au respect de la protection des données à caractère personnel, n'est admissible que si elle est nécessaire et proportionnée à l'objectif (aux objectifs) qu'elle poursuit[36]. Il en résulte la nécessité de distinguer en fonction des finalités visées et des personnes concernées (parties, témoins, experts, mineurs, etc.), quels traitements doivent porter sur des données anonymisées[37], quels traitements ne peuvent porter que sur des données pseudonymisées[38] et quels traitements peuvent être réalisés sur des données à caractère personnel non pseudonymisées[39].

30. A ce sujet, l'Autorité renvoie à l'avis 05/2014 du Groupe de travail "Article 29" sur la protection des données, prédécesseur sur Comité européen de la protection des données, sur les techniques

---

[36] un traitement de données à caractère personnel est considéré comme étant nécessaire s'il constitue la mesure la moins attentatoire pour atteindre l'objectif (d'intérêt général) qu'il poursuit. Il faut donc :

- Premièrement, que le traitement de données permette effectivement d'atteindre l'objectif poursuivi. Il faut donc démontrer, sur base d'éléments factuels et objectifs, l'efficacité du traitement de données à caractère personnel envisagé pour atteindre l'objectif recherché ;
- Deuxièmement, que ce traitement de données à caractère personnel constitue la mesure la moins intrusive au regard du droit à la protection de la vie privée. Cela signifie que s'il est possible d'atteindre l'objectif recherché au moyen d'une mesure moins intrusive pour le droit au respect de la vie privée ou le droit à la protection des données à caractère personnel, le traitement de données initialement envisagé ne pourra pas être mis en place. Il faut, à cette fin, détailler et être en mesure de démontrer, à l'aide d'éléments de preuve factuels et objectifs, les raisons pour lesquelles les autres mesures moins intrusives ne sont pas suffisantes pour atteindre l'objectif recherché.

Si la nécessité du traitement de données à caractère personnel est démontrée, il faut encore démontrer que celui-ci est proportionné (au sens strict) à l'objectif qu'il poursuit, c'est-à-dire qu'il faut démontrer qu'il existe un juste équilibre entre les différents intérêts en présence, droits et libertés des personnes concernées. En d'autres termes, il faut qu'il y ait un équilibre entre l'ingérence dans le droit au respect de la vie privée et à la protection des données à caractère personnel et l'objectif que poursuit – et permet effectivement d'atteindre – ce traitement. Les avantages qui découlent du traitement de données en question doivent donc être plus importants que les inconvénients qu'il génère pour les personnes concernées. À nouveau, il faut être en mesure de démontrer que cette analyse a bien été réalisée avant la mise en œuvre du traitement.

[37] Par exemple l'entrainement d'algorithmes

[38] Par exemple la publication des décisions à des fins de transparence ou de recherche scientifique au sens strict.

[39] Par exemple la conservation de la minute originale des décisions.

d'anonymisation[40], mais attire l'attention du demandeur sur le fait que l'EDPB procède actuellement à la révision de ces guidelines (qui devraient être soumise à consultation publique vers la fin de l'année 2022). Ces guidelines pourraient influencer fortement les caractéristiques minimales requises pour que des données puissent être considérées comme valablement pseudonymisées ou anonymisées.

31. L'Autorité estime par ailleurs qu'en ce qui concerne les décisions anonymisables, l'exposé des motifs du projet devrait contenir des informations quant à la stratégie d'anonymisation envisagée (le cas échéant, le demandeur gagnerait à se positionner à cet égard, afin de guider les responsables du traitements), à la manière dont procèdent certains responsables du traitement sur le plan international[41]. En effet, la transparence quant à la stratégie d'anonymisation retenue ainsi qu'une analyse des risques liés à la réidentification constituent des éléments qui contribuent à une approche réfléchie du processus d'anonymisation.

32. A toutes fins utiles, l'Autorité rappelle que les données pseudonymisées définies par l'article 4(5) du RGPD comme des données *« qui ne peuvent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires »* se distinguent des données anonymisées qui ne peuvent plus par aucun moyen raisonnable être attribuées à une personne précise et que seules ces dernières ne constituent plus des données personnelles et sont donc exclues du champs d'application du RGPD, conformément à son considérant 26[42].

33. Dès lors, eu égard à la définition de donnée à caractère personnel telle que figurant à l'article 4, 1) du RGPD[43], il convient de s'assurer que – lorsqu'un traitement ne peut porter que sur des données anonymisées - le standard élevé requis pour l'anonymisation est bien atteint[44] et que les données ne sont pas simplement pseudonymisées. En effet, le traitement de données, même pseudonymisées, doit être considérée comme un traitement de données à caractère personnel au sens du RGPD.

34. En revanche, lorsque le traitement de données pseudonymisées est pertinent :
- il conviendra de se référer au rapport de l'Agence de l'Union européenne pour la cybersécurité relatif aux techniques et meilleures pratiques de pseudonymisation[45] ;

---

[40] Cet avis est disponible à l'adresse suivante https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

[41] Voy. par exemple https://centre.humdata.org/guidance-note-responsible-approaches-to-data-sharing/

[42] Pour plus d'informations, voir l'avis 5/2014 (WP216) relative aux techniques d'anonymisation, 2.2.3, p. 11 du Groupe 29, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf

[43] A savoir : « *toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée») ; est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* ».

[44] L'identification d'une personne ne vise pas uniquement la possibilité de retrouver son nom et/ou son l'adresse mais également la possibilité de l'identifier par un processus d'individualisation, de corrélation ou d'inférence.

[45] ENISA : https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases et

- et ce traitement devra être encadré par toutes les garanties requises et répondre aux principes prévalant en la matière[46].

35. De plus, l'Autorité n'étant pas convaincue de la proportionnalité d'un éventuel traitement effectué à des fins d'analyse, elle invite (le cas échéant) la demandeur à procéder à une analyse stricte de proportionnalité. L'Autorité considère que le cadre de l'analyse d'impact relative à la protection des données qui est visé à l'article 35 du RGPD constitue une méthodologie adéquate pour examiner la proportionnalité du traitement de données à caractère personnel envisagé par le projet, par rapport à d'autres mesures présentant potentiellement un risque d'ingérence plus faible. L'Autorité rappelle, en outre, que dans la mesure où le traitement mis en place par le projet est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques au sens de l'article 35 du RGPD, le responsable du traitement devra réaliser une analyse d'impact spécifique avant la mise en œuvre concrète du traitement. En l'occurrence[47], l'Autorité estime préférable que cette analyse d'impact relative à la protection des données soit effectuée à ce stade du processus législatif. On ne peut en effet pas exclure que suite à cette analyse, des prescriptions spécifiques doivent être insérées dans la réglementation.

4. Responsable du traitement

36. Le projet prévoit que « *les entités représentées au sein du gestionnaire agissent, pour ce qui concerne le Registre central pour les décisions de l'ordre judiciaire, en qualité de responsables conjoints du traitement* ».

37. L'Autorité rappelle que les co-responsables du traitement sont susceptibles de voir leur responsabilité engagée le niveau de pseudonymisation n'atteint pas un niveau suffisant au regard de chacune des finalités pour lesquelles les données à caractère personnel sont traitées ou dans le cas où la publication d'une décision en vertu du chapitre 4 du projet venait à excéder la durée déterminée par le magistrat. Il importe donc que la désignation des responsables du traitement soit adéquate au regard des circonstances factuelles[48]. Il est nécessaire de vérifier pour chaque traitement de données à caractère

---

https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation;

[46] Il en va ainsi du principe de proportionnalité renvoyant à celui, plus spécifique, de « *minimisation* » des données impliquant que les données à caractère personnel doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard, des finalités pour lesquelles elles sont traitées, conformément à l'article 5, § 1er, c) du RGPD.

[47] Si des traitements de type profilage sont envisagés

[48] En effet, tant le Groupe de travail 29 – prédécesseur du Comité européen de la protection des données – que l'Autorité ont insisté sur la nécessité d'approcher le concept de responsable du traitement dans une perspective factuelle. Voir : Groupe de travail 29, Avis 1/2010 sur les notions de "responsable de traitement" et de "sous-traitant", 16 février 2010, p. 9 (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf) et Autorité de protection des données, *Le point sur les notions de responsable de traitement/sous-traitant au regard du au regard du Règlement EU 2016/679 sur la protection des données à caractère personnel (RGPD) et quelques applications spécifiques aux professions libérales telles que les avocats*, p.1. (https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Notions_RT_ST.pdf).

personnel qui poursuit la finalité pour laquelle elles sont traitées et dispose de la maîtrise des moyens utilisés pour atteindre cette finalité. Ceci permettra également d'éviter toute ambiguïté quant à l'identité de la personne ou de l'entité qui doit être considérée comme responsable du traitement et de faciliter ainsi l'exercice des droits de la personne concernée tels que prévus aux articles 12 à 22 du RGPD.

5. Délais de conservation

38. En vertu de l'article 5.1.e) du RGPD, les données à caractère personnel ne peuvent pas être conservées sous une forme permettant l'identification des personnes concernées pendant une durée excédant celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

39. L'Autorité constate que le projet prévoit une durée de conservation indéterminée. Ce choix est justifié comme suit dans le commentaire de l'article 12:

« *Vu, d'une part, les objectifs du Registre central et la valeur ajoutée que représente à cet égard une source authentique unique, la plus complète possible et mise à jour en permanence, de la jurisprudence de l'ordre judiciaire, en premier lieu pour les membres de cet ordre et, d'autre part, les limitations imposées en termes d'accès aux données du Registre central, un tel délai exceptionnel de conservation fixé pour une durée indéterminée semble, d'une part, nécessaire et, d'autre part, justifié. Deux exemples concrets : Pour les arrêts de la Cour de cassation, il est difficile, voire impossible, de savoir quand ils cesseront d'être pertinents. Parfois, des arrêts très anciens sont encore juridiquement pertinents aujourd'hui. Cela peut également s'appliquer à d'autres décisions judiciaires, notamment des cours d'appel. Le deuxième exemple concerne la possibilité de réhabilitation à la demande de proches de personnes condamnées par le passé. Dans ce contexte également, il peut s'avérer utile de pouvoir consulter aisément des jugements historiques* ».

40. Si cette justification est parfaitement admissible en ce qui concerne les décisions judiciaires, il n'en va cependant pas de même en ce qui concerne les données à caractère personnel qu'ils contiennent. À la lumière de l'article 6.3 du RGPD, il convient de déterminer et indiquer dans le projet les délais de conservation (maximaux) des données à caractère personnel qui feront l'objet du traitement, en tenant compte des différentes finalités et catégories de données, ou au moins de reprendre dans le projet les critères permettant de déterminer ces délais (maximaux) de conservation. Dans l'exemple mentionné dans le commentaire de l'article 12, cela revient à distinguer les décisions selon leur degré d'utilité potentiel et, sans préjudice de la réglementation relative aux archives, à supprimer ou à anonymiser (de manière effective) les décisions dès l'instant où elles ne présent plus d'intérêt pour les finalités pour lesquelles elles ont été conservées.

41. Sans pour autant suggérer qu'il soit envisageable de contourner ce principe par ce biais, l'Autorité rappelle que le RGPD ne s'applique pas au traitement des données à caractère personnel des personnes décédées.

42. Enfin, en ce qui concerne la publication d'une décision en vertu du chapitre 4 du projet, l'Autorité attire l'attention du demandeur sur le fait que, s'agissant d'une publication par voie électronique, la détermination d'une durée par un magistrat devient un concept théorique. Les documents n'étant plus réellement « *récupérables* » après publication. Il convient donc de prévoir, dans le projet, une obligation de motivation au regard de cet élément, lorsqu'une décision de justice imposera une telle publication ainsi qu'une possibilité pour le magistrat, au vus des risques de détournement de finalités évoqués *supra*, de prononcer une interdiction pure et simple de publication par voie électronique (mais éventuellement limitée dans le temps) de sa décision, même en version pseudonymisée.

PAR CES MOTIFS,

L'Autorité

estime que :

- les finalités des traitements de données à caractère personnel doivent être déterminées de manière claire et précise dans le projet, en distinguant, les finalités liées à la création d'une source authentique et à l'enregistrement des données à caractère personnel dans le registre, des finalités des autres traitements relatifs à ces données (points 14 à 23) ;
- des contraintes fortes doivent être imposées sur les éventuelles finalités pour lesquelles des données à caractère personnel pourraient être traitées dans le cadre de l'entrainement d'algorithmes (point 19) ;
- le commentaire de l'article 12 doit préciser que la finalité d'amélioration de la qualité des données ne vise pas à mettre en œuvre le principe d'exactitude figurant à l'article 5.1.d) du RGPD, ni à permettre la modification des données figurant dans les décisions prononcées par les juridictions (point 15) ;
- la notion d'« *optimalisation de l'organisation* » doit être précisée (point 16) ;
- le commentaire de l'article 12 doit être reformulé de manière à ne pas laisser sous-entendre qu'il serait possible, pour un responsable du traitement, de permettre conventionnellement à un sous-traitant de traiter des données pour des finalités plus étendues que celles qui lui sont légalement imposées ou qui sont reposent sur une autre base légale de l'article 6 du RGPD (point 22) ;
- un formulaire constitue un bon biais de communication pour informer les personnes concernées (point 24) ;
- les catégories de données à caractère personnel doivent nécessairement être déterminées dans le projet (point 27) ;

- le projet doit distinguer en fonction des finalités visées et des personnes concernées, les traitements devant porter que sur des données anonymisées, les traitements ne pouvant porter que sur des données pseudonymisées et les traitements pouvant être réalisés sur des données à caractère personnel non pseudonymisées (point 29) ;
- l'exposé des motifs du projet devrait contenir des informations quant à la stratégie d'anonymisation envisagée (point 31) ;
- si un traitement à des fins d'analyse statistique ou entrainement d'algorithmes devait être envisagé, il convient avoir égard au projet de règlement européen relatif à l'intelligence artificielle et de réaliser un DPIA au stade du processus législatif (points 21 et 35) ;
- il est nécessaire de vérifier pour chaque traitement de données à caractère personnel qui poursuit la finalité pour laquelle elles sont traitées et dispose de la maîtrise des moyens utilisés pour atteindre cette finalité (point 37) ;
- le projet doit déterminer des délais de conservations maximaux des données à caractère personnel à chaque fois que c'est possible (point 40) ;
- le projet doit contenir une obligation de motivation au regard du caractère « irrécupérable » d'une décision publiée par voir électronique, lorsqu'une décision de justice imposera une telle publication ainsi qu'une possibilité pour le magistrat, de prononcer une interdiction de publication de sa décision par voie électronique, même en version pseudonymisée. (point 42) ;

attire l'attention du demandeur sur :

- l'importance de faire preuve d'une transparence au moins aussi étendue lorsque les normes adoptées mettent en œuvre une « *stratégie européenne* » que lors de la transposition d'une directive dans une matière dans laquelle l'Union dispose d'une compétence normative en vertu du TUE (point 17) ;
- les possibilités techniques et les modalités de mise à disposition des décisions, applicables en fonction de la finalité envisagée (point 25) ;
- le fait que l'EDPB procède actuellement à la révision des guidelines relatives aux techniques de pseudonymisation et d'anonymisation (point 30) ;
- le caractère élevé du standard requis pour l'anonymisation (point 31).

Pour le Centre de Connaissances,
(sé) Jean-Michel Serna – Responsable *a.i.* du Centre de Connaissances