

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

RGDP

Mont, Julie

Published in:
Journal des Tribunaux

Publication date:
2019

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Mont, J 2019, 'RGDP: faut-il anonymiser la jurisprudence publiée ? ', *Journal des Tribunaux*, numéro 6776, pp. 442 - 449.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

RGPD : faut-il anonymiser la jurisprudence publiée ?

Les décisions de justice au sens large comportent bon nombre de données à caractère personnel, qu'elles soient relatives aux parties, à leurs avocats, aux magistrats chargés de rendre justice ou encore à des tiers. Au vu de la diffusion grandissante de ces décisions sur internet et à l'ère de l'adoption du Règlement européen relatif à la protection des données, l'opportunité de protéger ces données mérite d'être analysée afin d'éviter certaines dérives, comme le profilage d'individus.

Introduction

La publicité de la justice est consacrée par la Constitution belge. Les audiences des tribunaux belges et le prononcé des jugements sont en principe publics.

Si la jurisprudence belge, entendue en son sens large comme émanant des cours et tribunaux du pouvoir judiciaire ainsi que des juridictions administratives (Conseil d'État...) et de la Cour constitutionnelle, a initialement été publiée dans des revues spécialisées et sur support papier, l'ère numérique a engendré de nouveaux modes de diffusion de celle-ci. Même si la publication des décisions de jurisprudence sous format numérique en Belgique est encore parcellaire et aléatoire, ces décisions sont de plus en plus accessibles à tous, en ligne et gratuitement.

Or, celles-ci contiennent des données à caractère personnel, telles que le nom, l'adresse postale, la profession ou le numéro de registre national d'une partie. Ces informations sont nécessaires pour permettre aux juges de rendre correctement la justice, et pour rendre possible l'exécution des décisions prononcées.

Si la collecte de données à ces fins se justifie, d'autres enjeux apparaissent lorsque les décisions de justice sont diffusées via internet et sont donc potentiellement accessibles à tous. Dans ce cadre, nous nous intéresserons dans la présente contribution aux enjeux relatifs à la protection des données à caractère personnel, et proposerons des solutions susceptibles d'y répondre.

1 La jurisprudence publiée et les finalités de cette publication

Actuellement, seules certaines juridictions sont tenues de publier leurs décisions, en vertu d'obligations légales.

La publication des arrêts rendus par la Cour de cassation n'est pas organisée par la loi, sous réserve de l'article 136 du Code judiciaire, qui lui intègre un service de documentation. Le site internet de la Cour comporte des arrêts listés par année, de 1832 à 2015, qui sont sélectionnés par les magistrats, selon qu'ils jugent ou non opportun de les rendre publics¹.

L'article 114 de la loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle prévoit que les arrêts rendus par celle-ci sont publiés dans leur intégralité ou par extraits au *Moniteur belge*. Depuis l'adoption de cette loi, le mode de publication a évolué et, aujourd'hui, c'est le site

internet de la Cour qui comporte un moteur de recherche permettant d'accéder à un genre de recueil officiel de tous les arrêts rendus.

Les lois coordonnées sur le Conseil d'État du 12 janvier 1973 prévoient, quant à elles, à la suite de leur modification par la loi du 4 août 1996, que les arrêts et les ordonnances de non-admission du Conseil d'État sont accessibles au public et que le Conseil d'État en assure la publication dans les cas, les formes et les conditions déterminés par arrêté royal délibéré en Conseil des ministres².

L'arrêté royal du 7 juillet 1997 traite spécifiquement de la publication des arrêts du Conseil d'État et prévoit, en son article premier, une publication, sur un réseau d'informations accessible au public, des arrêts et des ordonnances de non-admission rendus (exceptés les arrêts relatifs à la loi sur l'accès au territoire)³. Les raisons qui sous-tendent cette publication obligatoire sont l'accès rapide et complet à la jurisprudence pour les praticiens (i), une diffusion rapide pour permettre les référés administratifs (ii) et l'accès, pour les justiciables, à cette jurisprudence (iii). Le rapport au Roi rédigé par le ministre de l'Intérieur après l'adoption de la loi du 4 août 1996 stipule notamment qu'au vu de la nomination à vie des magistrats et de l'absence, pour ceux-ci, d'obligation de rendre directement des comptes sur la manière dont ils rendent la justice, il est impératif que leurs décisions soient accessibles au public.

Le site internet du Conseil d'État reprend donc toutes les décisions, celles-ci étant généralement publiées rapidement⁴.

S'agissant des cours et tribunaux « ordinaires », il n'existe pas de texte légal obligeant les magistrats à rendre accessibles les décisions qu'ils prononcent. Il existe une base de données générale, publique et gratuite, *Juridat*, qui n'est alimentée que de manière aléatoire⁵. Plus précisément, l'article 9 de la loi du 10 août 2005 prévoit que cette banque de données comprend des décisions qui sont sélectionnées par chaque juridiction, qui les introduit de manière volontaire⁶. Une note de service propose des critères pouvant guider les magistrats lorsqu'ils envisagent la publication de leurs décisions (exemple : un jugement comprenant une motivation standard n'est pas propice à la publication)⁷. Compte-tenu du caractère aléatoire des publications, à la date du 11 août 2017, la base de données *Juridat* regroupait 158.509 décisions de justice, ce qui ne représente que 0,47 % des décisions prononcées en Belgique depuis la seconde guerre mondiale⁸.

Outre le respect des obligations légales précitées, les finalités recherchées par cette publication « numérique » de la source de droit qu'est la jurisprudence, sont diverses. On peut citer :

— le contrôle élargi du fonctionnement des juridictions (lutte contre l'arbitraire et veille au respect de l'exigence de motivation des décisions édictée à l'article 149 de la Constitution)⁹ (i) ;

(1) Commission de modernisation de l'ordre judiciaire, Rapport consacré à la question de la publication des décisions judiciaires, La plume, le Pélikan et le nuage, 30 juin 2014, p. 9, disponible à l'adresse : <https://justice.belgium.be/sites/default/files/download/Rapport%20publication%20des%20d%20c%20judiciaires.pdf>.

(2) Lois coordonnées du 12 janvier 1973 sur le Conseil d'État, *M.B.*, 21 mars 1973, article 28.

(3) Arrêté royal du 7 juillet 1997 relatif à la publication des arrêts et ordonnances de non-admission du Conseil d'État, *M.B.*, 8 août 1997, article 1.

(4) Commission de modernisation de l'ordre judiciaire, *op. cit.*, p. 10.

(5) *Ibidem*, p. 4.

(6) Loi du 10 août 2005 instituant le système d'information Phenix, *M.B.*, 1^{er} septembre 2005, article 9.

(7) Commission de modernisation de l'ordre judiciaire, *op. cit.*, p. 13.

(8) J.P. BUYLE et A. VAN DEN BRAN-

DEN, « La robotisation de la justice », in *L'intelligence artificielle et le droit*, Bruxelles, Larcier, 2017, p. 278.

(9) CPVP, recommandation n° 03/2012 du 8 février 2012 relative aux banques de données de jugements et/ou d'arrêts accessibles à des tiers gratuitement ou contre paiement, p. 3.

— l'efficacité des acteurs de la justice, qui ont accès à l'arsenal des décisions publiées sous un format numérique pratique, efficace et à portée de mains sur leur ordinateur, *smartphone*, tablette¹⁰... (ii) ;
— plus généralement, l'accès à la justice et aux sources du droit pour tous, passant par une connaissance plus étendue de la jurisprudence¹¹ (iii) ;

Il est aussi avancé que la diffusion de la jurisprudence augmente sa prévisibilité et permet d'éviter l'introduction de trop nombreuses procédures judiciaires ou administratives (iv)¹². Enfin, dans certains cas, la publication de la décision est une forme de sanction, imposée par la loi. Il s'agit notamment des décisions en matière de droit à l'honneur ou à la réputation, de faillite, d'exploitation de débauche et de prostitution¹³...

2 La jurisprudence, un nid de données à caractère personnel

Les décisions de justice qui sont prononcées comportent des informations au sujet de certaines personnes. Ces données sont collectées et traitées pour une finalité précise. Lorsque les décisions sont ensuite publiées sur internet, les données qu'elles contiennent sont également diffusées. Avant d'examiner l'opportunité de rendre ces données publiques, il convient d'analyser quelles sont celles qui sont collectées et diffusées et de déterminer si une protection y est attachée.

A. Les données collectées et diffusées

Les juridictions au sens large disposent de données au sujet de différentes personnes : les parties, leurs conseils, les juges et auxiliaires de justice ou même les tiers impliqués dans les dossiers qu'elles traitent. L'obtention de ces données est nécessaire en vue du traitement des litiges dont les juridictions sont saisies puisque la décision judiciaire doit comprendre les éléments d'identification des personnes concernées afin qu'il soit clair pour ces dernières que la décision porte sur leur dossier. Les tiers compétents chargés d'exécuter cette décision (exemple : les huissiers de justice) doivent également savoir en faveur et à charge de qui ils interviennent¹⁴.

L'article 780 du Code judiciaire prévoit d'ailleurs que le jugement doit contenir, à peine de nullité, les noms des membres du siège, du magistrat du ministère public qui a donné son avis et du greffier qui a assisté au prononcé, les nom, prénom et domicile sous l'indication desquels les parties ont comparu et conclu et, le cas échéant, l'indication du nom des avocats.

Une fois ces données collectées, les juridictions opèrent donc un traitement de celles-ci en les employant pour rendre leurs décisions¹⁵.

Lorsque les décisions sont ensuite publiées sur des moteurs de recherche en ligne, les données qu'elles contiennent le sont généralement aussi. Un tour d'horizon des bases de données publiques de jurisprudence belge permet d'apercevoir des informations qui permettent d'identifier directement une personne et qui sont accessibles au grand public.

La rubrique « Pasicrisie » du site de la *Cour de cassation* contient les arrêts rendus, contenant les initiales des parties, ainsi que des noms complets des présidents, des juges, des rapporteurs et des conseils des parties.

Les décisions publiées sur le site de la *Cour constitutionnelle* comportent, quant à elles, l'initiale et le nom complet des juges, les prénoms et noms des parties et l'initiale du prénom et le nom de leurs avocats, ainsi que le barreau auquel ils appartiennent. La loi spéciale sur la Cour constitutionnelle prévoit, en son article 30^{quater}, que le président, sur demande ou d'office, peut décider que les données identifiant des parties ou des tiers intéressés soient supprimées¹⁶. Le principe est donc la publication, *in extenso*, et sauf demande contraire, des données à caractère personnel susmentionnées.

Sur le site *web* du *Conseil d'État*, on peut lire des décisions dans lesquelles les parties sont identifiées soit via les lettres XXX, soit via leurs noms et prénoms complets. On peut également voir l'initiale du prénom et le nom de leurs avocats, ainsi que l'adresse de leurs cabinets. Les noms des magistrats, greffiers, auditeurs et rapporteurs sont également mentionnés.

Cela signifie qu'en faisant une recherche par le nom d'un justiciable ou par le nom d'un avocat, on peut retrouver la liste des affaires dans lesquelles cette personne est intervenue. L'arrêté royal du 7 juillet 1997 relatif à la publication des arrêts et des ordonnances de non-admission du Conseil d'État précise en effet que les décisions sont publiées intégralement, à moins qu'une partie exige la dépersonnalisation avant la clôture des débats¹⁷.

Les décisions publiées sur la plateforme *Juridat*, contiennent les dénominations complètes des entreprises et, pour les personnes physiques, soit uniquement des initiales, soit uniquement les termes « demandeur » et « défendeur », soit le prénom et l'initiale du nom des parties. En recoupant les informations, il est donc tout à fait possible d'en déduire l'identité complète du justiciable. Les noms des avocats sont également mentionnés, accompagnés de l'adresse de leur cabinet, ainsi que les noms des juges et greffiers. L'article 9, alinéa 2, de la loi du 10 août 2005 prévoit pourtant que les décisions publiées sur cette plateforme doivent être anonymisées, et que les modalités de cette anonymisation sont déterminées par le Roi, sur avis de la Commission de la protection de la vie privée (ci-après la « CPVP »)¹⁸. Cette disposition ne semble pas avoir été suivie d'effet au regard des exigences en matière d'anonymisation, comme nous le verrons *infra*, et simplement parce que l'avis de la CPVP n'a jamais été demandé, et que l'arrêté royal n'a pas été adopté.

B. Les données protégées

En amont de l'analyse de la pertinence de mettre ces données à la disposition du public (*cf. infra*), il y a lieu de déterminer si ces données sont toutes susceptibles d'être protégées au titre de « données à caractère personnel ». La « donnée à caractère personnel » est définie par le règlement général relatif à la protection des données (ci-après le « RGPD ») comme étant « toute information se rapportant à une personne physique identifiée ou identifiable », la « personne physique identifiable » étant 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 »²⁰.

1. Les données des justiciables et des tiers

Les informations à caractère personnel au sujet des justiciables et des éventuels tiers impliqués dans les dossiers qu'ils soumettent à la juridiction (exemple : conjoint dont les données personnelles et financières apparaissent sur un avertissement de rôle) et qui pourraient se

(10) Commission de modernisation de l'ordre judiciaire, *op. cit.*, p. 4.

(11) CPVP, recommandation n° 03/2012, *op. cit.*, p. 3.

(12) Commission de modernisation de l'ordre judiciaire, *op. cit.*, p. 9.

(13) J.-P. MASSON, « L'anonymisation des parties dans les décisions de justice publiées », *J.T.*, 2016, p. 10.

(14) CPVP, recommandation n° 03/2012, *op. cit.*, p.3.

(15) Un « traitement de donnée à caractère personnel » est défini à l'article 4, 2), du RGPD comme :

« toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation,

l'effacement ou la destruction ».

(16) Loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, *M.B.*, 7 janvier 1989, article 30^{quater}.

(17) Arrêté royal relatif à la publication des arrêts et ordonnances de non-admission du Conseil d'État du 7 juillet 1997, *op. cit.*, articles 1 et 2.

(18) Aujourd'hui dénommée « Autorité belge de protection des données ».

(19) Loi du 10 août 2005 instituant le système d'information Phenix, *op. cit.*, article 9, alinéa 2.

(20) 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 de données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données), *J.O.U.E.*, 4 mai 2016, article 4, 1). Ci-après référencé comme suit : « RGPD ».

retrouver dans des décisions de jurisprudence sont notamment des prénoms, noms, numéros de téléphone, numéros de sécurité sociale, identifiants bancaires, informations cadastrales, ou encore des informations liées au casier judiciaire... Plus encore, les décisions de justice peuvent contenir des données sensibles au sens de l'article 9 du RGPD, comme des informations sur l'état de santé (exemple : évaluation d'un dommage corporel devant être indemnisé) ou sur l'orientation sexuelle (exemple : décision en matière de discrimination).

Comme il s'agit de personnes physiques, il semble évident que ces informations répondent à la définition de données à caractère personnel puisqu'elles permettent d'identifier ou de rendre identifiables ces personnes physiques.

La question demeure controversée pour les personnes morales qui ne sont pas visées par la définition de « donnée à caractère personnel », soit « toute information se rapportant à une personne physique identifiée ou identifiable »²¹. Certains estiment toutefois que les personnes morales ne devraient pas subir un sort différent des personnes physiques car elles ont également une vie intérieure que les tiers n'ont pas à connaître et qu'en plus, elles peuvent se prévaloir du secret des affaires²².

2. L'identité des acteurs publics

On l'a vu, les noms et prénoms des présidents, magistrats, juges, auditeurs, représentants du ministère public, greffiers... apparaissent dans les décisions de jurisprudence accessibles en ligne.

Ces données semblent *a priori* pouvoir répondre à la définition de « données à caractère personnel » telles que définies *supra*, dans la mesure où elles permettent d'identifier une personne physique.

Mais ces acteurs, lorsqu'ils rendent la justice ou participent à l'œuvre des juges, agissent sur la base de prérogatives qui leur sont données par l'État et exercent un mandat public. En outre, lorsque les décisions contiennent leurs identités sont publiées, les données sont révélées dans un cadre professionnel qui dépasse la stricte sphère privée. On pourrait donc considérer que leur identité (nom et prénom) n'est pas protégée par la législation relative à la protection des données.

Toutefois, et notamment compte tenu des risques liés à la publication de ces données (*cf infra*), nous prônons une interprétation large de la notion de « vie privée ». Ce type d'interprétation a déjà été recommandé par le Groupe 29 en ces termes : « l'expression "données à caractère personnel" englobe les informations touchant à la vie privée et familiale d'une personne physique, *stricto sensu*, mais également les informations relatives à ses activités, quelles qu'elles soient, tout comme celles concernant ses relations de travail ainsi que son comportement économique ou social. Il s'agit donc d'informations concernant des personnes physiques, indépendamment de leur situation ou de leur qualité »²³.

La Cour européenne des droits de l'homme a également interprété le concept de « vie privée » dans le même sens, considérant que : « (...) le terme "vie privée" ne doit pas être interprété de façon restrictive. En particulier, le respect de la vie privée englobe le droit pour l'individu de nouer et développer des relations avec ses semblables ; de surcroît, aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de "vie privée" »²⁴.

3. Les données concernant les avocats

Si un justiciable fait appel à un conseil, le nom de famille, l'initiale du prénom ou le prénom complet, voire parfois l'adresse du cabinet et le barreau de celui-ci sont mentionnés sur le jugement. Le fait que l'avocat exerce cette fonction, l'adresse de son cabinet, l'identification de son barreau sont des informations publiques et accessibles à tous, que ce soit sur internet (site internet du cabinet, site internet du barreau avec la liste des avocats...) ou par exemple via les annuaires des avocats, disponibles auprès du secrétariat de chaque barreau.

Il n'en reste pas moins que ces données, bien qu'utilisées dans un cadre professionnel, peuvent, au même titre que celles qui concernent les magistrats et autres auxiliaires de justice, être protégées par la législation en matière de données à caractère personnel.

3 Le RGPD et les principes de finalité et de proportionnalité

Le RGPD impose que les données à caractère personnel soient collectées pour des finalités déterminées et qu'elles ne soient pas traitées ultérieurement d'une manière incompatible avec ces finalités²⁵. Or, lorsque les décisions et les données personnelles protégées qu'elles contiennent sont mises en ligne, il existe un risque que lesdites données soient utilisées dans un but différent de celui pour lequel elles ont été collectées (rendre correctement la justice) et de celui pour lequel la publication a lieu (offrir notamment un meilleur accès à la justice pour les citoyens).

A. Le profilage : un enjeu grandissant

Internet offre des possibilités de recherche et d'utilisation d'informations beaucoup plus étendues que ce qui était envisageable dans un environnement papier, et en tous cas avec une efficacité qui ne cesse de croître. Dans ce cadre, il pourrait être tentant d'effectuer, à partir d'une base de données jurisprudentielle, une recherche axée sur une personne et non sur un cas précis²⁶.

Le danger réside en effet en ce que les bases de données de jurisprudence deviennent un outil de profilage des individus (qu'ils soient justiciables, avocats ou juges) en les reliant à une catégorie abstraite définie, à une « case » telle que le « mauvais payeur », l'avocat qui perd ses dossiers, le magistrat sévère..., ce pour en tirer des conséquences concrètes.

Le profilage est défini par le RGPD comme étant « toute forme de traitement automatisé de données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement de travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique »²⁷.

Les bases de données permettent potentiellement de créer un « casier juridique » lié à une personne, d'entrevoir son passé judiciaire ou d'engendrer des préjugés révélés par des informations judiciaires. Il a également déjà été avancé, à juste titre, que la publication des décisions rendues en matière pénale peut compromettre la réhabilitation des personnes condamnées²⁸.

Déjà en 1996, soit à un moment où l'ère numérique n'avait pas encore connu son plein essor, la CPVP avait souligné ceci : « les recherches automatisées habituelles dans du texte libre, disponibles dans les logiciels de consultation des CD-ROM ou des réseaux comme Internet permettent en effet d'opérer des sélections dans de vastes recueils de prononcés sur la base des noms des parties, en combinaison avec d'autres critères de recherche, dont on peut déduire de façon systématique des informations concernant la vie privée des personnes identifiées »²⁹. À l'occasion d'un avis rendu une année plus tard, la CPVP a réitéré ses craintes : « Ainsi, on peut imaginer la facilité avec laquelle un internaute averti recueillera l'ensemble de la jurisprudence relative à des licenciements pour motifs graves pour en extraire les nom et adresses des employés mis en cause, ou identifiera les médecins dont la responsabilité aurait été mise en cause devant les tribunaux. Le comportement d'un juge face à tel ou tel type de conflits

(21) RGPD, article 4, 1).

(22) J.-P. MASSON, *op. cit.*, p. 11.

(23) Groupe de travail « article 29 » sur la protection des données, avis 4/2007 sur le concept de données à caractère personnel, n° 01248/07/FR-WP136, p. 7, disponible à l'adresse : <https://cnpd.public.lu/content/dam/>

cnpd.fr/publications/groupe-art29/wp136_fr.pdf.

(24) C.E.D.H., 16 février 2000, *Amann c. Suisse*, disponible sur le site internet de la Cour européenne des droits de l'homme.

(25) RGPD, article 5.1.b).

(26) C. DE TERWANGNE, *Diffusion de*

la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles, coll. Petites affiches, 2005, n° 194, p. 12.

(27) RGPD, article 4. 4).

(28) J.-P. BUYLE et A. VAN DEN BRAN-DEN, *op. cit.*, p. 273.

(29) CPVP, avis 07/96 du 22 avril 1996, disponible à l'adresse : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_07_1996_0.pdf, pp. 2 et 3.

pourra être évalué statistiquement et le nom d'un avocat pourra être associé à un pourcentage d'issues favorables de procès »³⁰.

Selon la CPVP, le risque de profilage existe donc tant à l'égard des parties que des professionnels, comme les juges et les avocats.

Vingt ans plus tard, avec le développement des recherches automatisées, ce risque n'a pu qu'augmenter et l'on constate que le contenu des bases de données publiques ne permet pas toujours d'éviter un tel écueil, au vu des informations à caractère personnel qui y sont encore généralement contenues. En effet, la mise en ligne des jugements à grande échelle (qui n'est, en Belgique et à ce stade, que limitée et parcellaire) et, en conséquence, leur mise à disposition sous un format lisible par une machine augmentent de manière considérable les possibilités d'ingérence dans la vie privée des individus et le risque de voir, par exemple, des entreprises réaliser des profils comprenant le passé judiciaire d'une personne pour ensuite les vendre à des recruteurs ou à des agences actives dans la lutte contre le terrorisme³¹.

B. Les finalités poursuivies par la publication des données - L'examen de proportionnalité

Les finalités visées par la publication en ligne des décisions de jurisprudence ont été exposées *supra* et sous-tendent un meilleur accès pour les citoyens à la source de droit qu'est la jurisprudence. Mais, au vu du risque de profilage exposé, est-il vraiment pertinent et proportionnel de divulguer les données à caractère personnel contenues dans la jurisprudence ? Ces données participent-elle réellement à une meilleure transparence de la justice et un accès plus étendu à celle-ci pour les citoyens ?

Quand elle a été saisie de la question en 2012, la CPVP a confirmé la position exprimée quelques années plus tôt³² et a estimé que le critère de proportionnalité n'était pas rencontré. Selon la Commission, le contrôle et l'apport de la jurisprudence portent sur le contenu et sur l'aspect juridique des décisions et la publication de données à caractère personnel n'est pas pertinente, qu'il s'agisse de données des parties, des avocats, des tiers, des juges ou encore des greffiers³³.

1. Les données des justiciables

A priori, il ne semble pas que les prénom et nom d'une partie soient des données publiées dans un but spécifique, excepté peut-être le fait, comme il a déjà été avancé par certains auteurs, que ces données pourraient permettre une meilleure mémorisation du contenu des décisions par les étudiants et praticiens du droit³⁴. Ces données ne nous semblent donc pas nécessaires ni pertinentes pour assurer, notamment, une meilleure transparence de la justice ou un accès plus étendu à celle-ci. La plus-value qui pourrait être retirée de la publication de ces données ne peut dès lors, selon nous, pas prévaloir sur les droits des personnes concernées.

Le défaut de proportionnalité entre le droit du public à être informé de la jurisprudence et à avoir accès aux noms des parties pour favoriser une mémorisation éventuelle et la protection des données des parties ne disparaît pas si l'une des parties est une personne morale. Celle-ci est susceptible également d'être profilée, éventuellement par un concurrent qui voudrait se renseigner sur les litiges dans lesquels cette personne morale a été impliquée, pour quel(s) motif(s)...

La publication de ce type de données ne semble donc ni pertinente par rapport à la finalité poursuivie, ni proportionnelle au regard des droits des personnes concernées. Si, à l'époque, certains ont considéré qu'une possibilité de refus, pour un justiciable, de voir ses données publiées suffisait ou à tout le moins que le consentement de celui-ci de-

vait être obtenu pour diffuser la décision³⁵, les points de vue tant des autorités de protection des données que celles des auteurs ou comités de recherche semblent aujourd'hui défendre l'effacement du nom des parties³⁶.

2. L'identité des acteurs publics (magistrats, membres du ministère public, greffiers...)

Comme exposé *supra*, les informations qui concernent les juges au sens large sont des données à caractère personnel. Les positions demeurent toutefois controversées sur la question de savoir s'il est justifié de les diffuser sur internet au regard du droit du public de connaître l'identité de ceux qui rendent la justice.

D'aucuns avancent que le maintien de celle-ci contribue à lutter contre l'arbitraire des juges et à la transparence de la justice³⁷. Le fait que l'identité des juges soit publiée permettrait de garantir la confiance du public dans la probité du système judiciaire et de vérifier que tel ou tel magistrat respecte les principes qui lui sont imposés. Nous pouvons également imaginer qu'un magistrat consciencieux, dont la décision a fait l'objet d'une réflexion poussée amenant à une motivation pointue, est enclin à ce que cette dernière fasse l'objet d'une publication intégrale dans un moteur de recherche jurisprudentiel et dès lors, n'est pas dérangé par le fait que son nom apparaisse en marge de celle-ci.

On l'a vu, la CPVP a estimé, en 2012, qu'il n'était pas proportionnel de publier les données concernant les juges et les greffiers pour assurer un contrôle et une connaissance plus étendus de la jurisprudence³⁸. En France, la Commission nationale de l'informatique et des libertés (la CNIL), a estimé qu'il n'y avait pas lieu, au motif de la vie privée de ces professionnels, d'occulter l'identité des magistrats ou membres des juridictions, ni celle des auxiliaires de justice ou d'experts, « même si le risque de constitutions de "profils" de juges ou d'avocats à partir des décisions de justice publiées ne peut être exclu »³⁹.

Une étude française répertorie les arguments pour et contre le maintien des noms des professionnels de la justice. Les partisans du maintien de l'identité des juges affirment qu'il participe au droit à un procès équitable, à la connaissance des décisions rendues, à l'amélioration de la prévisibilité de la justice, à l'information du citoyen (« consommateur de droit ») sur l'institution judiciaire en lui donnant également la possibilité de « noter » les juges sur des plateformes et systèmes de notation⁴⁰. Ils estiment que même si les noms des magistrats sont occultés des décisions, la puissance et la capacité croissante des algorithmes permettront, par croisement de données, de réidentifier les magistrats dont les noms auraient été retirés des décisions et que le retrait du nom des magistrats pourrait toucher à la crédibilité du droit français sur la scène internationale, le nom des magistrats étant un gage de sérieux et de fiabilité.

Les arguments en faveur du retrait du nom des magistrats sont notamment qu'il faut éviter de permettre d'imputer à chaque magistrat des pratiques juridictionnelles et orientations jurisprudentielles, que la publicité des audiences et du prononcé garantissent déjà tant aux parties qu'au public de connaître l'identité des magistrats qui composent la juridiction, qu'au regard de la finalité « connaissance du droit », l'intérêt de publier l'identité du magistrat est, à la différence de la mention de la juridiction auteure de la décision très limitée, voire nul⁴¹. Le retrait de ces données est également nécessaire pour éviter l'émergence d'une « justice prédictive » qui, sur la base d'analyses souvent erronées des décisions, prévoirait les résultats des litiges, les tentatives de déstabilisation (exemple : récusation) des magistrats dont les noms peuvent fournir des indications d'ordre personnel (sexe, origine...) mais aussi les problèmes de sécurité (ex. menaces, agressions)⁴².

(30) CPVP, avis n° 42/97 du 23 décembre 1997 sur la diffusion des décisions juridictionnelles par le recours aux technologies de l'information et de la communication, disponible à l'adresse : https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/avis_42_1997_0.pdf.

(31) J.-P. BUYLE et A. VAN DEN BRANDEN, *op. cit.*, p. 273.

(32) CPVP, avis n° 42/97, *op. cit.*

(33) CPVP, recommandation n° 03/2012, *op. cit.*, p. 3.

(34) C. DE TERWANGNE, *op. cit.*, p. 10.

(35) Y. POULLET, « Autour de l'arrêt royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'État : les technologies de l'information et de la communication, une solution à la pathologie législative », in J.M. VAN BOL (dir.) *La pathologie législative : comment en sortir ?*, Bruxelles, la Charte, 1998, p. 77.

(36) CPVP, recommandation n° 03/2012, *op. cit.*, p. 4 ; CNIL, Délibération n° 01-057 du 29 novembre

2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence, disponible à l'adresse : <https://www.legi-france.gouv.fr/affichCnil.do?id=CNILTEXT000017653503> ; C. DE TERWANGNE, *op. cit.*, p. 10 ; J.-P. MASSON, *op. cit.*, p. 11.

(37) J.-P. MASSON, *op. cit.*, p. 10.

(38) CPVP, recommandation n° 03/2012, *op. cit.*, p. 4.

(39) CNIL, délibération n° 01-057 du 29 novembre 2001, *op. cit.*

(40) L. CADIET, « L'open data des décisions de justice : mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice », Rapport remis à Madame la garde des Sceaux, ministre de la justice, novembre 2017, disponible à l'adresse : <http://www.justice.gouv.fr/publications-10047/rapports-thematiques-10049/remise-du-rapport-sur-lopen-data-des-decisions-de-justice-31165.html>, p. 44.

(41) *Ibidem*, p. 47.

(42) *Ibidem*, p. 47.

Le fait d'individualiser certaines tendances juridictionnelles favorise selon nous une « justice prédictive », qui pourrait également se manifester par un *forum shopping*, où le justiciable, s'il en a l'occasion, porte son litige devant le juge supposé être le plus favorable à son dossier. On pourrait également imaginer qu'un délinquant pourrait être tenté d'accomplir ses actes délictueux là où les représentants du ministère public identifiés dans les décisions semblent les plus cléments.

Nous sommes d'avis que, pour toutes ces raisons, les noms des magistrats et auxiliaires de justice (et non l'identification de la juridiction) doivent être occultés des décisions de justice publiées en ligne.

Le principe de publicité de la justice n'en est, selon nous, pas amoindri, notamment parce que les audiences demeurent publiques, même s'il est vrai que les prononcés des jugements ne se font plus que très rarement lors des audiences. En outre, l'exemplaire original de la décision comportera toujours le nom du magistrat, puisque nous prôtons en effet l'enlèvement du nom du magistrat uniquement lors de la diffusion en ligne des décisions. Bien que l'original de la décision existe toujours au greffe, il n'engendre qu'un risque très minime de profilage ou *forum shopping* puisque dans les faits, il ne sera pas ou très rarement consulté.

À notre sens, la seule finalité liée au contrôle du pouvoir judiciaire (correcte application de la loi, respect de l'exigence de motivation, lutte contre l'arbitraire) ne peut pas affaiblir la protection des données à caractère personnel des juges et elle est garantie par le fait que les audiences sont, pour la plupart, publiques, et que les décisions originales sont consultables aux greffes des juridictions.

De même, s'il paraît légitime que les citoyens puissent avoir une vue sur le travail des juridictions, il ne nous semble pas que la possibilité pour ceux-ci de pouvoir noter ou classer les juges selon le résultat obtenu dans leur dossier — notation qui sera forcément subjective — puisse céder le pas à la protection des données à caractère personnel des professionnels concernés. En principe, il n'appartient pas aux citoyens de choisir le juge qui statuera sur leur demande.

Pour ce qui concerne le personnel des greffes, nous partageons le point de vue selon lequel le profilage peut mener à un manque de sécurité à leur égard, de même que celui-ci peut être, dans l'esprit des citoyens, intimement lié à l'œuvre du juge même s'il n'est pas à l'origine de la décision rendue⁴³. La CPVP s'est prononcée en faveur du retrait des données à caractère personnel au sujet des greffiers⁴⁴. Par conséquent, les données les concernant doivent à notre sens également être occultées.

3. Les informations relatives aux avocats

Tout comme pour les magistrats, on peut raisonnablement penser qu'un avocat qui a obtenu un bon résultat dans un dossier, peut-être au terme d'un travail long et fastidieux d'argumentation, est heureux que la décision obtenue soit publiée et qu'il soit identifié comme conseil de la partie triomphante. De même, il pourrait être utile pour un avocat à qui est confié un dossier similaire à un dossier dans lequel le litige a été tranché de faire appel au confrère mentionné sur la décision pour obtenir des conseils sur la stratégie et les arguments à développer.

Il s'agit, à notre sens, des objectifs qui pourraient être poursuivis par une publication des informations personnelles relatives à ces personnes.

Les avocats sont toutefois également susceptibles d'être profilés. En effet, un potentiel client pourrait être tenté, avant de faire choix d'un conseil, d'aller consulter les affaires dans lesquelles il est intervenu pour établir des statistiques de succès. La Cour de cassation française a d'ailleurs admis l'existence d'un site de notation des avocats par les internautes⁴⁵.

Or, aucun avocat ne remporte l'entièreté de ses dossiers et l'échec peut s'expliquer par d'autres raisons que son éventuelle incompétence. En outre, on l'a vu, des statistiques qui serait éventuellement réalisées à la suite d'un *scanning* des décisions dans lesquelles un avocat est inter-

venu ne seraient pas représentatives puisque toutes les décisions ne sont pas publiées et que la diffusion est parfois aléatoire.

La CPVP a prôné l'enlèvement des données à caractère personnel concernant les avocats⁴⁶. En France, le conseil national des barreaux (qui représente l'ensemble des avocats de France) s'est prononcé contre l'occultation du nom des avocats dans le cadre de l'*open data*, excepté lorsqu'ils sont parties au jugement⁴⁷.

Il convient dès lors d'opérer une balance d'intérêts entre le droit, pour le justiciable, de choisir librement son avocat et donc de se renseigner sur celui qui pourrait être « le meilleur » pour défendre son dossier, en consultant éventuellement les bases de données jurisprudentielles et le droit, pour l'avocat, de voir ses données à caractère personnel protégées et d'éviter ainsi, tant que faire se peut, d'être « catalogué ». À notre sens, et au vu du marché concurrentiel sur lequel exercent les avocats et du principe du libre de choix de l'avocat, la publication de leur identité en marge des décisions est moins problématique que la publication des données des parties ou des représentants du pouvoir judiciaire.

4 Anonymisation vs pseudonymisation : quelle solution ?

A. Les notions

Les « données anonymisées » sont les données qui concernaient auparavant une personne identifiable, mais qui ne permettent plus cette identification⁴⁸.

Les données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable, ne constituent plus des données à caractère personnel, ce pour autant que le processus d'anonymisation soit irréversible.

La pseudonymisation est, quant à elle, introduite dans le RGPD comme mesure de protection⁴⁹ et elle est définie comme « le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable »⁵⁰. Contrairement à l'anonymisation, la pseudonymisation permet donc de rétablir une identification, au moyen d'informations supplémentaires conservées séparément. Par conséquent, les données pseudonymisées retraçables peuvent être considérées comme des informations sur des personnes physiques « indirectement identifiables »⁵¹.

Lorsque sont évoquées les solutions à apporter pour veiller au respect des droits des personnes concernées par les décisions de justice publiées, ces deux notions ne sont généralement pas distinguées et laissent place à un concept général improprement nommé « anonymisation ». En tout état de cause, les auteurs et acteurs de terrains ne semblent pas d'accord sur la méthode exacte à prévoir pour protéger les données à caractère personnel contenues dans la jurisprudence.

B. Les méthodes envisagées

1. Pseudonymisation et anonymisation

Notre autorité de contrôle a, en 2012, estimé que « pour la lisibilité, les noms et prénoms des parties peuvent le cas échéant être remplacés par des pseudonymes ou initiales »⁵². La CNIL s'est, quant à elle, prononcée pour une anonymisation (des noms et adresses des parties et des témoins uniquement, *cf supra*)⁵³. D'autres auteurs sont partisans de l'anonymisation des données à caractère personnel⁵⁴.

(43) *Ibidem*, p. 51.

(44) CPVP, recommandation n° 03/2012, *op. cit.*, p. 4.

(45) Site www.alexia.fr ; Cass.fr., 11 mai 2017, n° 16-13669.

(46) CPVP, recommandation n° 03/2012, *op. cit.*, p. 4.

(47) L. CADIET, *op. cit.*, p. 52.

(48) Groupe de travail « article 29 » sur la protection des données, avis 4/

2007, *op. cit.*, p. 23.

(49) RGPD, considérant 28.

(50) RGPD, article 4. 5).

(51) Groupe de travail « article 29 » sur la protection des données, avis 4/

2007, *op. cit.*, p. 20.

(52) CPVP, recommandation n° 03/2012, *op. cit.*, p. 7.

(53) CNIL, délibération n° 01-057 du 29 novembre 2001, *op. cit.*

Or, comme il a été relevé, à juste titre, dans le rapport français de L. Cadiet : « L'anonymisation d'une décision de justice suppose donc de garantir (...) que les personnes concernées par les décisions ne soient plus susceptibles d'être identifiées directement ou indirectement, selon un processus qui empêche cette identification de manière irréversible. Or, l'application de ces règles aux décisions de justice montre qu'il est quasiment impossible de satisfaire à ces conditions, sauf à retirer de la décision l'essentiel de son contenu et à porter atteinte à son intelligibilité et à sa motivation, exigences fondamentales du droit à un procès équitable. Les décisions de justice sont en effet des documents comportant des éléments de texte très construits. Elles contiennent un nombre très important de données réidentifiantes, particulièrement au sein de la motivation de la décision, qui comprend de nombreux éléments de contexte pouvant conduire, notamment par des croisements avec d'autres bases de données, à une réidentification des personnes »⁵⁵.

2. Selon un procédé systématique, aléatoire ou sur demande

S'agissant du caractère que doit revêtir l'effacement des données, il existe des divergences de points de vue entre une méthode systématique, sur demande, aléatoire ou encore sur le moment auquel cet effacement des données doit intervenir.

J.-P. Masson est partisan d'une anonymisation systématique, sauf exceptions⁵⁶. E. Lesueur de Givry, conseiller à la Cour de cassation française, critique quant à lui une telle anonymisation complète à la source et dite « sauf exceptions » car, même si elle présente l'avantage d'être plus aisée et moins coûteuse à mettre en œuvre, elle rendrait plus difficile la lisibilité des arrêts, notamment parce que les noms des parties permettent une meilleure mémorisation⁵⁷.

Pour d'autres, une anonymisation systématique ne se justifie pas et représente un obstacle insurmontable pour les éditeurs de sites gratuits⁵⁸. Il y aurait lieu d'ériger, selon ceux-ci, un droit à l'anonymisation sur demande de la personne concernée, pour motif légitime. C'est, pour rappel, la solution retenue par l'arrêté royal du 7 juillet 1997 relatif à la publication des arrêts et des ordonnances de non-admission du Conseil d'État et par la loi spéciale sur la Cour constitutionnelle⁵⁹.

Des critères sont également parfois avancés pour déterminer si une anonymisation doit être pratiquée, comme la nature du litige, le type de juridiction qui a rendu la décision et la qualité de la personne concernée⁶⁰.

Depuis le 1^{er} juillet 2018, dans toutes les publications relatives aux affaires préjudicielles soumises à la Cour de justice de l'Union européenne, les noms des personnes physiques impliquées dans l'affaire sont remplacés par des initiales. Il en est de même de la dénomination des affaires. De plus, tous les éléments complémentaires susceptibles de permettre l'identification des personnes concernées sont supprimés de toutes les publications⁶¹.

En Belgique, deux membres d'Avocats.be, parmi lesquels son président, ont présenté deux types d'anonymisation : l'anonymisation de *minimis*, qui consiste à effacer uniquement les noms des parties, et l'anonymisation large qui recouvre toutes les données permettant d'identifier directement ou indirectement les parties au litige et qui rend donc le processus de réidentification plus complexe⁶². Ces acteurs sont bien conscients qu'il est illusoire de prévenir tous les risques de réidentification des parties au litige et qu'il faut également se pencher sur une éventuelle anonymisation des données d'identification des plaideurs ou des magistrats⁶³.

S'agissant du moment auquel l'anonymisation doit intervenir, ils sont d'avis que lorsque l'anonymisation intervient *ex-post*, c'est-à-dire

après que la décision ait été prononcée et communiquée aux parties, au moyen d'un logiciel d'analyse qui retire les éléments d'identification, elle présente des risques de réidentification élevés, notamment parce que ce n'est pas le juge, le greffier ou un membre du personnel judiciaire qui a procédé à l'anonymisation⁶⁴. L'anonymisation *ab initio* (c'est-à-dire avant l'élaboration du jugement) proposée consiste en un modèle de jugement conçu spécialement pour garantir qu'il ne contiendra pas d'éléments d'identification des parties au litige : les noms et coordonnées des parties sont mentionnés sur un en-tête et remplacés dans le corps de texte par des pseudonymes, des initiales ou une définition. Deux versions du jugement sont ensuite préparées, celle contenant l'en-tête communiquée aux parties et l'autre publiée sur internet sans l'en-tête⁶⁵. Les auteurs relèvent que si cette technique est facile à mettre en place, elle peut nuire à la lisibilité des décisions. Pour y pallier, ceux-ci proposent que le hachurage (du type « XXX ») soit évité, mais que les parties soient identifiées par des pseudonymes ou des définitions qui rendent compte du contexte (du type « le conjoint », « la banque », « l'hôpital ») plutôt que des termes génériques ou procéduraux (du type « la requérante »)⁶⁶. Enfin, une troisième méthode vise une anonymisation « durante », réalisée par le juge lorsqu'il rédige sa décision. Celui-ci doit veiller à n'inclure dans le texte que les éléments d'identification des parties pertinents pour la solution du litige, étant le mieux placé pour savoir quelles données sont accessoires à la bonne compréhension de sa motivation⁶⁷.

Ces auteurs reconnaissent que « l'anonymisation *ex post* des jugements, telle que pratiquée aujourd'hui par les cours et tribunaux belges, constitue un écueil à la mise en ligne systématique des décisions de justice. Le processus est chronophage et contre-productif »⁶⁸.

J.-P. Buyle et A. Van den Branden recommandent donc de mettre en œuvre une anonymisation *ab initio* et « durante » généralisée des décisions, par la mise en place d'un modèle de jugement à en-tête détachable contenant les données d'identification des parties au litige, et la conscientisation des magistrats pour qu'ils n'incluent dans leurs décisions que les données à caractère personnel pertinentes pour la résolution du litige. Cette recommandation n'a, pour l'heure et à notre connaissance, pas été suivie d'effets.

C. La méthode préconisée

1. La pseudonymisation

Comme annoncé, il nous semble impossible d'anonymiser une décision de jurisprudence publiée en ligne puisque l'exemplaire original de celle-ci demeure au greffe, à disposition de qui en ferait la demande, et que les données à caractère personnel qui y figurent sont intactes.

La copie de la décision originale est également communiquée aux parties et aux huissiers éventuellement chargés des procédures d'exécution, voire à des tiers comme par exemple à l'employeur à qui est notifiée une décision emportant saisie-arrêt, entre ses mains, du salaire de son employé.

Défendre une anonymisation des décisions de jurisprudence publiées, c'est-à-dire une absence de possibilité de réidentifier les personnes concernées par les données à caractère personnel y contenues, n'est pas réaliste. D'autres auteurs partagent cette opinion⁶⁹.

Le risque de réidentification est un risque latent, qu'on ne peut complètement annihiler mais qu'on peut, à tout le moins, tenter d'amoin-drir. C'est dans cette perspective que le sujet doit, selon nous, être envisagé. Il nous semble donc, premièrement, que la solution à mettre en

(54) J.-P. MASSON, *op. cit.*, p. 11 ; F. LEPLAT, « Décisions de justice publiées sur Internet : pour le droit à l'anonymisation sur simple demande », disponible à l'adresse : <https://www.droit-technologie.org/actualites/decisions-de-justice-publiees-sur-internet-pour-le-droit-a-l-anonymisation-sur-simple-demande/> ; E. LESUEUR DE GIVRY, « La question de l'anonymisation des décisions de justice », rapport annuel de la Cour de cassation française, La documen-

tation française, 2000, disponible à l'adresse : https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2000_98/deuxieme_partie_tudes_documents_100/tudes_theme_protection_personne_102/decisions_justice_5854.html.
(55) L. CADIET, *op. cit.*, p. 36.
(56) J.-P. MASSON, *op. cit.*, p. 11.
(57) E. LESUEUR DE GIVRY, *op. cit.*
(58) F. LEPLAT, *op. cit.*

(59) Arrêté royal relatif à la publication des arrêts et ordonnances de non-admission du Conseil d'État du 7 juillet 1997, *op. cit.*, articles 1 et 2 ; loi spéciale du 6 janvier 1989 sur la Cour constitutionnelle, *op. cit.*, article 30^{quater}.
(60) Y. POULLET, *op. cit.*, pp. 75-76.
(61) Cour de justice de l'Union européenne, communiqué de presse n° 96/18 du 29 juin 2018, disponible à l'adresse [https://curia.europa.eu/jcms/upload/docs/application/pdf/](https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180096en.pdf)

2018-06/cp180096en.pdf.
(62) J.-P. BUYLE et A. VAN DEN BRANDEN, *op. cit.*, p. 274.
(63) *Ibidem*, p. 274.
(64) *Ibidem*, p. 275.
(65) *Ibidem*, p. 276.
(66) *Ibidem*, p. 276.
(67) *Ibidem*, p. 276.
(68) *Ibidem*, p. 276.
(69) D. MOUGENOT et L. GÉRARD, « Justice robotisée et droits fondamentaux », à paraître ; L. CADIET, *op. cit.*, p. 36.

œuvre, pour respecter les exigences de protection des données à caractère personnel, est une pseudonymisation des données, ainsi que l'a d'ailleurs prôné la CPVP il y a quelques années.

Une fois le procédé consacré, reste à voir si celui-ci doit être systématique ou non, à quel moment il doit être pratiqué et sur quel type de données.

2. Systématique

Nous ne sommes pas d'avis que la pseudonymisation des données doive s'opérer sur demande de la personne concernée, en tous cas en l'état actuel de la législation. Le processus de demande doit en effet être encadré par une procédure claire et transparente pour les justiciables (qui n'ont probablement pas conscience du principe-même de la publication). De quelle manière la personne concernée pourra-t-elle s'opposer à la publication ? Auprès de qui ? Quels seront les motifs acceptés ? Qui va évaluer sa demande ? Dans quel délai ? Seul l'arrêté royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'État répond à certaines de ces questions⁷⁰. Pour le reste, les questions demeurent ouvertes et, à notre sens, difficilement à résoudre en pratique.

Une pseudonymisation « sauf exceptions » semble également difficile à mettre en œuvre puisque cela suppose que la loi définisse des critères prévisibles et transparents pour déterminer dans quels cas les données à caractère personnel doivent être effacées, et lesquelles exactement. Rien n'est prévu actuellement.

La solution d'une pseudonymisation systématique se dessine, ce afin de ne pas distinguer les sorts à réserver aux données à caractère personnel des personnes concernées. Si, certes, cette procédure peut s'avérer coûteuse, elle semble être, actuellement et compte tenu de l'état de la législation belge, l'unique gage d'une application uniforme aux données à caractère personnel visées.

3. Ex-post

La technique d'un effacement des données *ab initio*, de manière « durant », c'est-à-dire avant et pendant le prononcé de la décision, présente l'avantage de requérir peu de travail une fois que celle-ci arrive à l'étape de la diffusion sur internet. Toutefois, la création d'un jugement « pro forma », avec un en-tête détachable sur lequel figureraient les données à caractère personnel, semble peu pratique pour les magistrats.

Il nous semble en effet qu'il n'est pas de la fonction du pouvoir judiciaire de veiller à rendre sa jurisprudence exempte de données à caractère personnel. Lorsqu'un magistrat délibère, il doit être libre de pouvoir rédiger la motivation de sa décision comme bon lui semble, sans devoir veiller à ôter de celle-ci certaines informations. En outre, une telle technique suppose de guider les magistrats sur ce qui doit être considéré comme une « donnée à caractère personnel », de même que, dans ce cadre, il est probable que les juges adoptent des interprétations différentes de cette notion voire fassent une application plus ou moins poussée de ce qui leur est demandé.

À notre sens, il n'appartient pas aux magistrats, en tant qu'individualités chargées de rendre la justice, de se préoccuper de tels enjeux en matière de protection des données à caractère personnel. Cette technique ne doit pas non plus, selon nous, être pratiquée par des membres des greffes, pour les mêmes raisons.

Enfin, elle risquerait de nuire à la publication des décisions, les magistrats et greffiers pouvant être découragés par l'effort à fournir.

Si l'effacement des données après le prononcé du jugement est considéré par certains comme difficile à mettre en œuvre et imputant de la lisibilité à celui-ci, il nous semble qu'il s'agit toutefois de la meilleure solution. À l'heure du développement croissant des nouvelles technologies et de la réflexion autour d'une justice robotisée, il ne semble pas inimaginable qu'un logiciel puisse, *ex-post*, analyser les décisions rendues et effacer les données à caractère personnel, en les pseudonymisant.

4. Des données identifiantes relatives à certaines personnes concernées

On l'a vu, les données pouvant figurer dans les décisions de jurisprudence peuvent être directement (nom, prénom...) ou indirectement (numéro de compte, lieu de travail, plaque d'immatriculation...) identifiantes.

Il ne semble plus y avoir de doutes sur le fait que les données qui identifient directement une personne, doivent être supprimées. À notre sens, si l'on veut tendre à une conformité maximale aux règles régissant la protection de la vie privée, les données permettant d'identifier indirectement un individu doivent également être occultées. La Cour de justice de l'Union européenne a, on l'a dit, pris le pli de supprimer de ses publications, « tout élément complémentaire susceptible de permettre l'identification des personnes concernées »⁷¹. À notre avis, cela devra toutefois se faire dans la mesure du possible, compte tenu du fait que la motivation d'une décision, et les faits qu'elle contient, emporteront presque toujours des risques de réidentification. À nouveau, l'idée est de limiter ceux-ci.

Il n'est pas nécessaire de tout supprimer et d'uniquement laisser des espaces vides ou remplis par des « XXX » mais simplement d'identifier les parties en leur donnant un prénom aléatoire, sans nom, et d'éventuellement remplacer, tant que faire se peut, les données identifiantes, fut-ce indirectement, par d'autres données générées aléatoirement et rendant ainsi la liaison entre les données publiées et les données réelles plus difficilement réalisable. Il ne semble pas insurmontable de dresser une liste — qui ne sera jamais exhaustive — des données à caractère personnel identifiantes pouvant figurer dans la jurisprudence et de commander à un logiciel, dès qu'il repère le format de ces informations, de les occulter et de les remplacer par des pseudonymes. La décision pourrait rester dans ce cas tout à fait lisible et compréhensible.

Outre les données à caractère personnel relatives aux justiciables, le sort de celles des auxiliaires de justice et des avocats doit être pris au sérieux.

Nous ne pensons pas que la décision perd en qualité si les noms du magistrat et de son greffier sont tout simplement effacés de la décision publiée en ligne, et que seule la juridiction qui a rendu la décision, soit mentionnée, avec éventuellement le numéro de la chambre concernée. Nous avons vu que, quoi qu'il arrive, la réidentification du magistrat sera toujours possible, par exemple en se renseignant auprès du greffe pour savoir quel magistrat, quelle chambre, a rendu la décision à une date précise. Nous pensons en outre que le fait que les décisions publiées soient dépourvues de cette information réduit déjà considérablement le risque de profilage puisqu'une intervention humaine est nécessaire pour coupler les informations, en interrogeant le greffe ou toute autre personne qui détiendrait une copie de la décision originale. Le profilage des juges, via un *scanning* informatique des décisions, est ainsi considérablement diminué. Il pourra certes exister pour les chambres, mais la composition de celles-ci n'est pas immuable et elle a le mérite de ne pas identifier le juge en tant qu'individu.

Pour les avocats, les points de vue resteront partagés entre ceux qui ne sont pas opposés à ce que leur travail fasse l'objet d'analyses et de statistiques et ceux qui y voient un inconvénient. La question n'est probablement pas prête d'être tranchée, au vu de la balance d'intérêts à réaliser entre le droit du public de choisir son avocat en fonction de ses éventuels résultats affichés publiquement et le droit de ce dernier à la protection de ses données personnelles.

Conclusion

Les décisions prononcées par les juridictions belges, qu'elles soient administratives ou judiciaires, sont publiques. Cette publicité implique qu'elles puissent faire l'objet d'une diffusion en ligne, via les sites internet des juridictions ainsi que des moteurs de recherche accessibles à tout un chacun.

Cette publication à grande échelle sur la toile repose sur un objectif de surveillance du pouvoir judiciaire pour les citoyens et participe à la

(70) Arrêté royal relatif à la publication des arrêts et ordonnances de non-admission du Conseil d'État du

7 juillet 1997, *op. cit.*, article 5.

(71) Cour de justice de l'Union européenne, communiqué de presse

n° 96/18 du 29 juin 2018, disponible à l'adresse <https://curia.europa.eu/jcms/upload/docs/application/pdf/>

2018-06/cp180096en.pdf.

lutte contre une justice arbitraire qui échapperait à leur contrôle tout en permettant un accès pour tous à cette source de droit parfois opaque. La publication sera également vraisemblablement renforcée dans le cadre de l'*open data* touchant les décisions de justice.

Si ces objectifs sont louables, ils entrent en conflit avec le principe fondamental du droit au respect de la vie privée, étant donné que les décisions de jurisprudence au sens large comportent des données à caractère personnel au sujet des parties au litige, des auxiliaires de justice, et des conseils éventuels des justiciables. Ces données sont susceptibles de bénéficier d'une protection, en vertu des règles applicables en matière de protection des données, et notamment du RGPD récemment entré en vigueur, qui consacre les principes de finalité et de proportionnalité dans le traitement de celles-ci.

Lorsqu'une décision est publiée sur internet et qu'elle contient, *in extenso*, des données à caractère personnel, l'on peut considérer que la divulgation de ces données n'est pas pertinente au regard de la finalité poursuivie par la collecte initiale de celles-ci ni par la finalité guidant la publication, si l'on prend en compte le risque latent de profilage.

La solution résiderait en un processus de pseudonymisation et non d'anonymisation, puisque même si les données diffusées par le biais des décisions publiées sont occultées, les personnes concernées seront toujours ré-identifiables, notamment via la consultation de la décision originale ou de copies de celle-ci.

Il convient d'adopter une approche axée sur le risque de réidentification, en mettant en place un processus d'effacement des données à caractère personnel qui le réduit au maximum, en gardant à l'esprit que ce risque sera toujours latent.

Nous proposons, au vu de l'état de la législation, un processus de pseudonymisation systématique *ex-post* réalisé éventuellement au moyen d'un outil informatique, qui porte sur les données qui identi-

fient directement une personne (nom, prénom, adresse...) et également sur un maximum de données permettant d'identifier indirectement celle-ci. Le cœur de la motivation, à plus forte raison si elle est factuelle, risque en effet souvent de permettre cette réidentification.

En tout état de cause, et dans un futur proche, il conviendra que le législateur appréhende les enjeux qui ont été pointés, en mettant fin aux divergences des points de vue en la matière et en conciliant la mise à disposition des décisions de justice pour le public et les règles de protection des données à caractère personnel. Celui-ci devra mettre un terme aux interrogations sur la méthode à utiliser, les données visées et le moment auquel appliquer la méthode, ce afin que les décisions subissent toutes le même sort une fois publiées, peu importe les juridictions qui les ont prononcées.

Une balance d'intérêts entre la diffusion des décisions de justice et la législation protectrice de la vie privée devra être opérée, afin de les concilier au mieux.

L'article 86 du RGPD n'empêche pas qu'un tel équilibre soit trouvé, puisqu'il prévoit : « Les données à caractère personnel figurant dans des documents officiels détenus par une autorité publique ou par un organisme public ou un organisme privé pour l'exécution d'une mission d'intérêt public peuvent être communiquées par ladite autorité ou ledit organisme conformément au droit de l'Union ou au droit de l'État membre auquel est soumis l'autorité publique ou l'organisme public, afin de concilier le droit d'accès du public aux documents officiels et le droit à la protection des données à caractère personnel au titre du présent règlement »⁷².

Julie MONT*

Assistante à l'Université de Namur, chercheuse au CRIDS
Avocate au barreau de Namur

(72) RGPD, article 86.

(*) L'auteure remercie Elise Degrave

et Loïck Gérard pour leurs conseils et relectures attentives.

Quelques observations complémentaires sur la publication des décisions

1. Le problème de l'anonymisation des décisions de justice lors de leur publication retient de façon légitime l'attention des éditeurs comme de l'ensemble des praticiens. Faut-il anonymiser, que faut-il masquer, qui doit le faire et comment ? Ces interrogations naissent ou se renouvellent dans un contexte de numérisation des décisions et de mise à disposition de bases de données de jurisprudence en ligne : celles-ci offrent en effet des possibilités accrues de recherche et de profilage qui semblent porteuses de menaces. Le sujet de l'anonymisation pose aussi un certain nombre de questions qu'il importe, je crois, de distinguer. À mon humble avis, les règles de protection des données à caractère personnel apportent une réponse structurée et cohérente à l'ensemble de ces interrogations¹, au-delà d'une opposition quelque peu simpliste entre vie privée, protection des données personnelles et liberté d'expression². Ces règles, et singulièrement le fameux règlement européen dit « RGPD », ne sont-elles pas destinées à préserver l'ensemble

des droits et libertés individuelles face au « pouvoir de l'informatique »³ ? Le lecteur n'en trouvera toutefois pas ici un exposé systématique, mais quelques brèves observations.

Je saisis aussi l'occasion pour évoquer 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 arrêts⁴. Celle-ci adapte les modalités du prononcé des jugements, et prévoit l'enregistrement de toutes les décisions dans une base de données, après anonymisation selon des modalités que le Roi est chargé de déterminer. Elle devrait entrer en vigueur à une date fixée par le Roi, qui ne peut toutefois être postérieure au 1^{er} septembre 2020. Le texte délègue largement au Roi la tâche de définir la portée de l'anonymisation des décisions.

2. Mais commençons par distinguer entre la protection de la vie privée et la publicité des audiences et du jugement. La publication de déci-

(1) L'analyse porte sur les dispositions du 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, *J.O.U.E. L 119* du 4 mai 2016, pp. 1-88, ci-après « le règlement européen sur la protection des

données ».

(2) Sur les relations subtiles entre protection de la vie privée et protection des données à caractère personnel, voy. notamment, G. GONZALES FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, New York, Springer, 2014 ; O. LYNSKEY, *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press, 2015.

(3) Voy. B. DOCQUIR, *Droit du numérique - Contrats, innovation, données et sécurité*, coll. R.P.D.B., Bruxelles, Larcier, 2018, pp. 354-359, n^{os} 483-486.

(4) *M.B.*, 16 mai 2019, p. 47030. Proposition de loi modifiant le Code judiciaire et le Code d'instruction criminelle en ce qui concerne la publication des jugements et des arrêts, *Doc. parl., Chambre.*, sess. 2017-

2018, n^o 54-3489/001. Le résumé de la proposition précise que celle-ci doit être lue en parallèle avec la proposition de révision de l'article 149 de la Constitution en ce qui concerne la publicité des jugements et arrêts, *Doc. parl., Chambre*, sess. 2017-2018, n^o 54-2628/001.