LES DONNÉES PERSONNELLES À L'ÉPREUVE DE L'*OPEN DATA* DES DÉCISIONS DE JUSTICE : ENTRE PRINCIPE DE TRANSPARENCE DE LA JUSTICE ET DROIT À LA VIE PRIVÉE

Flora DORNEL[1]

1 L'autrice est candidate à la Maîtrise avec mémoire à l'Université Laval, cheminement bi-diplômant avec l'Université Paris-Saclay, programme Propriété Intellectuelle Fondamentale et Technologies Numériques.. E-mail : floradornel@gmail.com

Résumé

Que ce soit en France ou au Canada, les données judiciaires font l'objet d'une législation en faveur de l'open data. Les données judiciaires (décisions de justice, plumitifs…) sont mises à la disposition des citoyens gratuitement et de manière électronique, sur Internet. Or, ces données judiciaires comportent une multitude de renseignements personnels. La question qui est au cœur du problème est alors l'affrontement de deux valeurs fondamentales : d'un côté, le droit du public à la transparence de l'administration de la justice, qui justifie que les données judiciaires soient consultables, et de l'autre, le droit de l'individu à la protection de sa vie privée, qui pourrait se retrouver en situation de vulnérabilité.

[1] Le mouvement global de l'open data prend de l'ampleur[2], sans épargner le domaine judiciaire : on constate aujourd'hui, que ce soit en France ou au Canada, que les données judiciaires font l'objet d'une législation en faveur de l'open data, c'est-à-dire de la donnée ouverte, publique, gratuite, accessible par tous, et réutilisable[3]. L'équilibre préexistant entre deux principes fondamentaux, à savoir le principe de transparence de la justice et le droit à la vie privée, s'en trouve bouleversé.

I - L'*OPEN DATA* AU SERVICE DU PRINCIPE FONDAMENTAL DE LA TRANSPARENCE DE LA JUSTICE

[2] Comme le dit l'adage, « justice is not only to be done, but to be seen to be done ». Non seulement la justice doit être rendue, mais en plus l'on doit voir qu'elle est rendue : une justice secrète ne permettrait pas un régime démocratique. Ce principe de la transparence de la justice est traduit par l'exigence de publicité des débats judiciaires : « là où il n'y a pas de publicité, il n'y a pas de justice »[4]. Et l'open data est présentée comme un bon moyen pour renforcer ce principe de transparence de la justice. En France, le sujet est particulièrement actuel : la Loi de 2016 *pour une République numérique*, puis la Loi de 2019 de *programmation et de réforme pour la justice,* viennent prévoir l'application de l'open data aux décisions de justice. Un projet de décret pour la mise en application a été rendu public en décembre 2019, mais a été source de vives contestations[5]. En effet, l'un des arguments principaux soulevé par les professionnels du droit concerne les risques d'atteinte au droit à la vie privée[6] qu'engendre l'électronique au vu du nombre de données personnelles contenues dans ce type de documents mis en ligne. Le décret a été publié le 30 juin dernier, sans modification des dispositions qui faisaient l'objet des contestations[7].

2 Partenariat Open Government Partnership, regroupant 78 pays dans le monde, en ligne : <https://www.opengovpartnership.org/about/>

3 Loïc CADIET, « l'open data des décisions de Justice », Rapport de la mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, novembre 2017.

4 *A.G. (Nova Scotia) c. MacIntyre*, 1982 CanLII 14 (CSC), [1982] 1 RCS 175, <http://canlii.ca/t/1lpbp>.

5 Communiqué commun des syndicats de la magistrature, 6 février 2020, en ligne : <https://www.usma.fr/communiques/communique-commun-aux-syndicats-de-magistrats-tendant-au-retrait-du-projet-de-decret-sur-l-open-data>

6 *Ibid*.

7 Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, en ligne : <https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000042055251>.

[3] Dans l'optique de renforcer la confiance des citoyens dans les cours et tribunaux, M. le rapporteur Christophe-André Frassa dit à propos des articles 20 et 21 de la Loi du 7 octobre 2016 qu'ils « visent un même objectif extrêmement important : garantir l'ouverture, le partage et la réutilisation, autrement dit l'open data des décisions de justice. Ces décisions de justice sont toutes rendues au nom du peuple français et sont publiques. Il apparaît donc opportun de prévoir la mise à disposition de toutes les décisions, et pas seulement de celles publiées par la Cour de cassation ou le Conseil d'État, car elles feraient jurisprudence »[8]. Le principe est alors renversé : toutes les décisions de justice doivent avoir le mérite d'être rendues accessibles. Ainsi décidé, il serait intéressant de mener une étude analysant les conséquences sur la jurisprudence… Sur la confiance que doit entraîner l'open data vis-à-vis des citoyens, Mme Axelle Lemaire, ancienne secrétaire d'État au numérique et à l'innovation ayant porté les articles 20 et 21 de la Loi du 7 octobre 2016, justifie l'open data par le renforcement démocratique que cette technique peut permettre par la transparence dont elle fait preuve[9].

II- ACCÈS ÉLECTRONIQUE : UN FACTEUR DE BOULEVERSEMENT POUR LA VIE PRIVÉE

A. LA DISPARITION DE L'« OBSCURITÉ PRATIQUE »

[4] L'électronique vient chambouler l'équilibre préexistant entre le droit à la vie privée et la transparence de la justice : la facilité d'accès aux renseignements contenus dans les plumitifs et les décisions de justice n'a plus rien à voir avec la situation antérieure, où il fallait fournir l'effort de se rendre en personne au Palais de justice afin de consulter les documents. Cette démarche, qualifiée d'« obscurité pratique »[10], disparaît puisque la consultation des informations judiciaires est numérisée. Chacun pourra, en théorie, consulter les données judiciaires depuis son poste informatique. Et cette possibilité est confortée par le mouvement *open data*.

[5] On note ici une différence entre l'approche canadienne et l'approche française. Au Canada, face à la « friction » entre le droit à la vie privée et la

8 Séance du Sénat du 27 avril 2016, propos de M. Christophe-André Frassa.

9 Revue pratique de la prospective et de l'innovation, n° 2, oct. 2017, entretien n°4, p. 9, en ligne : <http://www.tendancedroit.fr/wp-content/uploads/2017/10/ITW-ppi1702-3.pdf>.

10 Lynn E. SUDBECK, « Placing Court Records Online: Balancing Judicial Accountability with Public Trust and Confidence: An Analysis of State Court Electronic Access Policies and A Proposal for South Dakota Court Records », 51 S.D. L. REV. 81, 83 (2006).

transparence de la justice, la position de la Cour suprême est plutôt claire : sauf cas exceptionnels prévus par les textes, la transparence de la justice prime sur la vie privée des individus[11]. Et l'introduction de l'électronique n'en change pas le principe. On peut d'ailleurs avoir accès aux plumitifs et aux décisions de justice à partir d'un simple site Internet[12]. Mais quels sont les risques pour les individus de voir leur identité divulguée de la sorte, notamment dans les plumitifs où des tiers peuvent également apparaître ?

[6] En France, il est prévu que la mise à disposition sous forme électronique - qui ne concerne que les décisions de justice - doit se faire en analysant le risque de « réidentification »[13]. Il faut donc comprendre que les décisions judiciaires feront l'objet d'une dépersonnalisation, avant leur mise en ligne, au nom du respect au droit à la vie privée des individus.

B. LES RISQUES DE RÉUTILISATION DES RENSEIGNEMENTS PERSONNELS

[7] L'électronique vient modifier la situation que l'on avait avant, endossant alors un rôle menaçant pour le respect du droit à la vie privée : on peut penser dans un premier temps aux « prédateurs potentiels » ou aux « voisins fouineurs »[14] qui iront chercher des informations sans aucune justification légitime. Mais ces comportements, bien que parfois dérangeants, sont souvent peu préjudiciables de manière sérieuse, et ne sont pas la raison de la principale inquiétude véhiculée par l'électronique. La source d'inquiétude plus importante est celle qui concerne les sociétés privées[15], telles que les banques, les courtiers de données, les compagnies d'assurance, etc. Ces organisations auraient alors accès à des données qu'elles n'auraient jamais eues avant, et pourraient être à

11 A.G. (Nova Scotia) c. MacIntyre, [1982] 1 RCS 175 ; Edmonton Journal c. Alberta (Procureur général), [1989] 2 RCS 1326, ; Vickery c. Cour suprême de la Nouvelle-Écosse (Protonotaire), [1991] 1 RCS 671 ; F.N. (Re), [2000] 1 RCS 880 ; Sierra Club du Canada c. Canada (Ministre des Finances), [2002] 2 RCS 522.

12 Site SOQUIJ <https://soquij.qc.ca/fr/services-aux-professionnels/catalogue/plumitifs>.

13 Article 21 al.2 de la Loi de 2016 *pour une République numérique* : « Cette mise à disposition du public est précédée d'une analyse du risque de ré-identification des personnes ».

14 Nicolas VERMEYS, « Privacy v. Transparency: How Remote Access to Court Records Forces Us to Re-examine Our Fundamental Values » dans Karim BENYEKHLEF et al, dir, *eAccess to Justice*, University of Ottawa Press, 2016, 123–154, en ligne : JSTOR <https://www.jstor.org/stable/j.ctt1wn0qx3.9>.

15 Kristin MAKAR, « Taming Technology in the Context of the Public Access Doctrine: New Jersey's Amended Rule 1:38 », *Seton Hall Law Review (2011),* Vol. 41 : Iss. 3 , Article 7, en ligne : <https://scholarship.shu.edu/shlr/vol41/iss3/7>.

l'origine d'un changement de comportement de leur part, en fonction des renseignements personnels qu'elles pourraient trouver[16].

[8] Bien évidemment, récupérer et utiliser des renseignements personnels sans le consentement des individus est interdit par la Loi *sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[17]. Mais surveiller le respect de ce principe de manière concrète semble difficile à concilier avec la mise à disposition publique des données judiciaires, et ne permet pas de prévenir de potentielles situations de vulnérabilité dans laquelle se retrouveront certains individus. Il existe une multitude d'illustrations de réutilisation des renseignements personnels qui peuvent être citées, en dehors du cadre exclusif des documents judiciaires[18]. L'accès électronique peut devenir une faille juridique permettant le traitement de renseignements personnels et dont la finalité est totalement détournée. Il faut alors s'interroger sur le cadre juridique existant actuellement. Il n'est plus à prouver que la présence des renseignements personnels trouvés en lignes sont nombreux et qu'il est relativement aisé, en pratique, de se les procurer pour s'en servir à d'autres fins que celles prévues initialement.

III- PUBLICITÉ ET OPEN DATA : DIFFÉRENCE D'APPROCHE ENTRE LE CANADA ET LA FRANCE

[9] La France et le Canada n'envisagent pas le principe de publicité et celui de la publication de la même manière (A). Ainsi, il y a divergence quant à la réutilisation des renseignements personnels trouvés dans les documents judiciaires mis à disposition du public (B).

A. DIVERGENCE ENTRE LE CANADA ET LA FRANCE QUANT À L'APPRÉCIATION DE LA PUBLICITÉ ET DE LA PUBLICATION

[10] Au Canada, il semblerait que la publicité va de pair avec la publication, ou plus précisément, que la publication renforce la publicité.

16 Daniel J. SOLOVE, « Access and Aggregation: Privacy, Public Records, and the Constitution », 86 Minn. L. Rev. 1137 (2002) p.1149 : ChoicePoint Inc a compilé et regroupé des données sur des millions de personnes à partir de divers documents publics, que le gouvernement et les employeurs utilisent pour filtrer et enquêter sur les salariés actuels et potentiel.

17 Annexe 1 de la Loi sur la protection des renseignements personnels et les documents électroniques, LC 2000, c5 : « Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire ».

18 Etude par Synovate, « Federal Trade Commission - Identity Theft Survey Report » (2003), en ligne : <http://www.ftc.gov/os/2003/09/synovatereport.pdf> ; voir aussi « Federal Trade Commission Overview of the Identity Theft Program - October 1998-September 2003 » (2003), en ligne : <http://www.ftc.gov/os/2003/09/timelinereport.pdf>, Daniel J. SOLOVE, préc., note 16, p. 1149.

En effet, le juge LaForest indique dans l'arrêt *SRC c. N.-B. (Procureur général)*[19] que l'accès aux tribunaux « se rattache intégralement au concept de démocratie représentative et à l'importance correspondante de la publicité des débats en justice ». Et pour veiller à l'efficacité de cette publicité, le juge reconnaît que les médias jouent, par la collecte et la diffusion d'informations sur les tribunaux, un rôle essentiel dans l'information du public, et plus largement, que « les médias ont un rôle primordial à jouer dans une société démocratique »[20]. Ainsi dit, la diffusion, donc la publication, vient bien soutenir l'exigence de publicité, et *in fine*, la transparence de la justice.

[11] En France, l'interprétation est différente. En effet, il faut distinguer entre accès et diffusion, c'est-à-dire entre publicité et publication. À ce propos, les dernières décisions des Cours de justice affirment que « l'open data n'a pas pour vocation de porter une nouvelle forme de publicité »[21]. Et d'après Yannick MENECEUR, la Loi 2018-2022 de programmation et de réforme pour la justice « ne remet pas en cause le régime de publicité des audiences et des décisions, et ne fait qu'organiser une nouvelle forme de délivrance au public des décisions de justice »[22]. Ainsi, un nouveau mode de diffusion est permis grâce à l'open data, c'est-à-dire une nouvelle forme de publication, mais cela n'est pas à confondre avec l'obligation de publicité, qui, elle, sera remplie par l'accès physique à la salle d'audience par exemple[23]. Il semble justifié qu'un nouveau moyen de publication ne devrait pas empiéter plus que nécessaire sur la vie privée des individus, et qu'il est alors évident que les décisions mises en ligne soient dépersonnalisées.

[12] On peut en effet se demander si l'accès à l'identification des individus dans les décisions en ligne permettrait de remplir davantage l'obligation de transparence de la justice.

19 *Société Radio-Canada c. Nouveau-Brunswick (Procureur général)*, 1991 CanLII 50 (CSC), [1991] 3 RCS 459, <http://canlii.ca/t/1fsh4>.

20 *Supra* note 19.

21 CA Paris, pôle 2 - ch. 1, 18 déc. 2018, n° 17/22211. Lire en ligne : <https://www.doctrine.fr/d/CA/Paris/2018/CBD628309EEBD087B10BA> et Cour d'appel de Paris, pôle 2, chambre 1, 25 juin 2019, n° 19/04407, en ligne : <https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2019/07/19-04407.pdf>.

22 Yannick MENECEUR, « Open data des décisions de justice - Pour une distinction affirmée entre les régimes de publicité et de publication », *JCP E*, n°37, 12 septembre 2019, 1415.

23 Article 6§1 de la Convention Européenne des Droits de l'Homme.

B. DIVERGENCE ENTRE LA FRANCE ET LE CANADA QUANT À LA RÉUTILISATION DES INFORMATIONS TROUVÉES DANS LES DOCUMENTS JUDICIAIRES MIS À DISPOSITION DU PUBLIC

[13] Concernant la réutilisation de l'identité des magistrats, cela fait l'objet, aux yeux d'une partie de pays étrangers, d'une « bizarrerie » française. En effet, si l'identité des magistrats reste publique à tous, la réutilisation de cette information est strictement interdite. Cela est expressément prévu à l'article 33 II. 1° alinéa 3 de la loi programmation 2018-2022 et de réforme pour la justice, qui dispose : « Les données d'identité des magistrats et des membres du greffe 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. La violation de cette interdiction est punie des peines prévues aux articles 226-18,226-24 et 226-31 du code pénal (…) ».

[14] Cette disposition peut surprendre à l'étranger : par exemple, aux États-Unis et au Royaume-Uni, les juges semblent avoir accepté la pratique consistant à analyser leurs décisions. Cela laisse le champ libre aux *legaltechs* pour essayer de trouver des modèles qui prévoiraient quel serait le comportement d'un juge donné[24], donc, en d'autres termes, le « profilage » est autorisé. La position française se démarque drastiquement en rendant cette éventualité tout simplement illégale. Cela peut s'expliquer en gardant en tête la finalité pour laquelle l'open data a été pensée et mise en œuvre : davantage de transparence et un accès aux décisions facilité. Mais sûrement pas dans l'idée de donner de la matière, non filtrée, aux *legaltechs*, qui pourraient en user de manière éthiquement discutable. Si l'on essaie de se projeter un tant soit peu, on peut en effet craindre que le jeu de profilage, de « prédiction » en fonction d'un litige donné, restreigne la liberté d'exercer du magistrat, et débouche sur un effet « moutonnier » des magistrats. Il faudra beaucoup de volonté et d'assurance de la part de ces derniers pour statuer différemment de ce que la technologie aurait prévu, et différemment de leurs collègues. Pourtant, on sait bien que chaque affaire peut être distincte, et qu'une décision d'un juge est également rendue *in concreto*, c'est-à-dire en prenant en compte le contexte dans lequel s'inscrit le litige. Et heureusement que les juges ont la liberté d'être à l'origine de revirement de jurisprudence en toute bonne conscience !

24 Artificial Lawyer, « France Bans Judge Analytics », 4 juin 2019, en ligne : <https://www.artificiallawyer.com/2019/06/04/france-bans-judge-analytics-5-years-in-prison-for-rule-breakers/>..

[15] Concernant les parties au litige, leur identité est occultée. Nous avons déjà étudié les risques pour elles si leurs données à caractère personnel étaient rendues accessibles à tous facilement. Là encore, cette exigence d'occulter les noms des parties dans les décisions en France se démarque à l'étranger, et notamment au Canada. Pour ces derniers, la divulgation de l'identité des individus fait partie des obligations à accomplir pour le principe de publicité. Mais en France, tel n'est pas le cas. La conception française distingue là où le Canada ne le fait pas forcément : la mise à disposition est une publication, un moyen de diffusion de l'information. Ce n'est pas une des conditions à remplir pour respecter le principe de publicité. On l'a dit, ce principe sera rempli autrement. Alors faut-il considérer que le principe de publicité est davantage rempli lorsque la publication est totale, sans occultation aucune ? La transparence de la justice nécessite-elle que les individus soient identifiés, identifiables dans les décisions de justice ?

IV- UN NOUVEL ÉQUILIBRE ENTRE LA TRANSPARENCE DE LA JUSTICE ET LE DROIT À LA VIE PRIVÉE ?

[16] Quelles pourraient être les pistes de réflexion afin de trouver un équilibre entre le principe de la transparence de la justice et celui du droit à la vie privée, à l'ère du numérique ? La solution française réside dans la technique de la pseudonymisation (A). Elle est mentionnée comme technique de dépersonnalisation par le Règlement Général sur la Protection des Données. Ce règlement propose également d'autres instruments pour trouver un équilibre entre la diffusion d'informations judiciaires et le droit à la vie privée des individus (B).

A. LA SOLUTION FRANÇAISE ACTUELLE : LA PSEUDONYMISATION

[17] La pseudonymisation est la technique encouragée au sein de l'Union européenne, bien qu'elle puisse par certains aspects se retrouver limitée dans son efficacité (1). Comment pseudonymisation et open data évoluent-elles ensemble ? (2)

1. LA PSEUDONYMISATION ENCOURAGÉE MAIS LIMITÉE DANS SON EFFICACITÉ

[18] Le RGPD propose la pseudonymisation comme illustration de mesures techniques et organisationnelles appropriée pour la protection des données, et c'est la technique que la France a décidé de mettre en

œuvre pour diminuer le risque d'atteinte à la vie privée. Selon la Commission nationale de l'informatique et des libertés (CNIL), « c'est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires »[25]. Il ne faut pas confondre la technique de la pseudonymisation avec celle de *l'anonymisation*. Cette dernière est « un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible »[26]. C'est donc l'irréversibilité de l'opération qui caractérise l'anonymisation.

[19] La pseudonymisation semble être adéquate en théorie. Cependant, en pratique, il est souvent aisé de retrouver l'identité des individus grâce au croisement de données : dans le rapport Cadiet[27], il est bien spécifié que les décisions de justice « 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 »[28]. Pour illustrer cela, on peut faire référence à une étude[29] réalisée par des chercheurs du *Massachusetts Institute of Technology* : elle a mis en évidence, dans le cadre d'un travail réalisé sur les transactions des cartes bancaires d'1,1 million de personnes ne comportant aucun élément d'identification, que quatre données spatio-temporelles (coordonnées géographiques, dates, heures) permettaient à elles seules de réidentifier 90 % des individus. La pseudonymisation ne paraît donc pas la solution optimale pour garantir de manière absolue le respect au droit à la vie privée des individus.

25 CNIL, « L'anonymisation des données, un traitement clé pour l'open data », 17 octobre 2019, en ligne : <https://www.cnil.fr/fr/lanonymisation-des-donnees-un-traitement-cle-pour-lopen-data>.

26 *Ibid.*

27 Rapport sur « "l'open data" des décisions de Justice », dit *Rapport CADIET,* 9 mai 2018

28 *Ibid*.

29 Y.-A. de MONTJOYE, L. RADAELLI, V. Kumar SINGH et A. PENTLAND, « Unique in the shopping mall : on the reidentifiability of credit card metadata », *Science*, 30 janvier 2015, en ligne : <https://science.sciencemag.org/content/347/6221/536?sid=9b47355e-d1da-4f56-b745-c876999ea9e3>

2. PSEUDONYMISATION ET OPEN DATA

[20] Les craintes des syndicats[30] de la magistrature française, suite à la publication du projet de décret en décembre 2019[31], se trouvent fondées : en effet, ils exigeaient « le retrait du projet de décret relatif à la mise en œuvre de l'open data des décisions de justice » en raison du manque d'évaluation de la charge de travail additionnelle, alors même que la justice est déjà surchargée. Et pourtant, la publication de ce décret le 29 juin 2020[32] définit les conditions de la diffusion des décisions des juridictions judiciaires et administratives, en chargeant les magistrats d'occulter les éléments permettant l'identification des individus (autre que les noms et prénoms)[33].

B. L'APPROCHE *PRIVACY BY DESIGN* PRÉVUE PAR LE RGPD

[21] L'article 25 alinéa 2 du Règlement Général sur la Protection des Données[34] prévoit que « le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées ». Il peut sembler opportun de s'intéresser aux apports de cette approche, d'origine canadienne[35], et consacrée dans le droit européen : pourquoi ne pas envisager d'appliquer, dès la création des documents, un système pour évacuer le maximum de données personnelles qui ne participent pas davantage à la transparence de la justice, et qu'il ne serait pas nécessaire de trouver en ligne. Évidemment, le débat sur ce principe de finalité est constamment en évolution, et il s'agira de mener une analyse approfondie sur la limitation, en ligne, du principe de la transparence de la justice face à la vie privée des personnes.

30 Communiqué commun des syndicats de la magistrature, 6 février 2020 : https://www.usma.fr/communiques/communique-commun-aux-syndicats-de-magistrats-tendant-au-retrait-du-projet-de-decret-sur-l-open-data.

31 Projet de décret relatif à l'open data des décisions de justice relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives, 13 décembre 2019, en ligne : <http://www.justice.gouv.fr/le-ministere-de-la-justice-10017/projet-de-decret-relatif-a-lopen-data-des-decisions-de-justice-32835.html>.

32 Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives.

33 Nouvel article R111-12 du *Code de l'organisation judiciaire*.

34 Article 25 alinéa 1 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 (Règlement général sur la protection des données).

35 Ann CAVOUKIAN, « Privacy by Design : The 7 Foundational Principles », 2009 (Janvier 2011), *Information and Privacy Commissionner of Ontario,* en ligne : https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf.

[22] La privacy by design dans le cadre de l'*open data* peut être un mode de régulation séduisant puisqu'il intègre la protection des données à caractère personnel dès la conception des outils de collecte, de traitement ou d'exploitation des données. On peut comparer cette technique à une sorte de filtre, à la charge du fabriquant, ou même à la charge du diffuseur de la base de données. La PbD s'inscrit dans une logique d'analyse de risque, participant à la consécration de l'accountability. Cela signifie qu'il y a obligation de rendre des comptes et de justifier des garanties mises en œuvre pour prévenir tout risque ou y remédier en cas de survenance (par exemple en cas de faille de sécurité). Alors comment la PbD peut venir en soutien pour empêcher que les données transmises par les administrations aux exploitants puissent être réutilisées de manière préjudiciable pour les individus[36] ?

CONCLUSION

[23] L'*open data* a été pensée dans l'objectif d'améliorer la transparence au profit des citoyens, et de permettre l'innovation. En effet, pour entraîner un algorithme, plus on pourra le nourrir de données, plus il sera performant. L'*open data* semble alors être une technologie très pertinente. Cependant, bien que l'open data puisse être louable dans le domaine judiciaire, puisque cela permet, entre autres, de participer à la transparence de la justice, et *in fine* à la confiance du public dans la justice, il ne faudrait pas perdre de vue les éventuelles atteintes aux autres droits et libertés des personnes qu'elle pourrait engendrer. Un raisonnement davantage global semble approprié, car une fois les données mises en ligne, il ne sera plus question de frontières étatiques. Des acteurs du monde entier pourront y accéder, et il est alors important de cerner ces enjeux à temps pour pouvoir les appréhender. N'attendons pas que la vulnérabilité des personnes se cristallise pour agir.

36 Loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal modifiée par l'ordonnance n°2015-1341 du 23 octobre 2015 transposant la directive 2013/37, article 13.