Le droit d'accès à l'information confronté aux données personnelles : la délicate balance des droits et libertés fondamentales

Droit à l'oubli et au déréférencement, traitements de données à des fins journalistiques, open data et anonymisation des décisions de justice… autant de sujets au cœur de l'actualité judiciaire et législative, qui témoignent de la difficulté de placer le curseur entre le droit d'accès à l'information et la protection de la vie privée et des données personnelles des individus.

Les atteintes au respect de la vie privée en raison de l'information délivrée au public étaient auparavant sanctionnées sur le fondement de l'article 9 du code civil ou de la LCEN1. Désormais, les mesures instaurées par la réglementation sur les données personnelles, dont notamment le droit à l'oubli grâce au déréférencement et le droit à l'anonymisation des décisions de justice, tel qu'il résulte de la loi de réforme de la justice du 23 mars 20192, offrent des moyens d'action susceptibles de faire échec au droit d'accès à l'information. En pratique, la protection des données personnelles n'est toutefois pas absolue et cède face au droit à l'information du public lorsque l'individu, par son fait ou son comportement, se retrouve au cœur d'un sujet d'intérêt général (rôle dans la vie publique, infraction ou condamnation pénale relatée par des journalistes ou résultant de décisions de justice).**I - Données personnelles et droit au déréférencement : la primauté discutée de la vie privée sur le droit des moteurs de recherche dans la société de l'information**Le droit à l'oubli, d'origine prétorienne avant d'être consacré par le Règlement sur la protection des données personnelles (RGPD)3, est aujourd'hui effectif grâce aux mesures de déréférencement prises par les moteurs de recherche, sous le contrôle des autorités de contrôle et des juridictions. Toutefois, la portée territoriale de ce droit reste encore à définir aussi bien au regard de la directive que du RGPD.**A - Consécration du droit à l'oubli par l'arrêt***Google Spain***Par son arrêt rendu le 13 mai 20144, la Cour de justice de l'Union européenne (CJUE) a retenu par la lecture combinée des articles 12 et 14 de la directive européenne 95/46/CE5 (la « Directive ») qu'il existe un droit à l'oubli au profit de la personne concernée par un traitement de données personnelles. Cette personne peut exercer son droit à l'encontre d'un moteur de recherche afin d'obtenir le déréférencement, dans les résultats de recherche effectuée sur la base de son nom, d'articles contenant des données personnelles la concernant et dont le traitement n'est plus adéquat.**

La Cour retient en particulier que le moteur de recherche est seul responsable du traitement de données personnelles effectué dans le cadre du référencement et de l'affichage de liens renvoyant vers des pages de sites édités par des tiers. Ce traitement est autonome et distinct de celui effectué par l'éditeur de la page web indexée par Google.

En pratique, le droit à l'oubli prévaut systématiquement sur l'intérêt économique de l'exploitant du moteur de recherche. Il prime également sur l'intérêt des internautes à avoir

accès à l'information relative à une personne concernée, lors d'une recherche effectuée sur la base de son nom, en fonction d'une analyse*inconcreto*« de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment, en fonction du rôle joué par cette personne dans la vie publique »6.

La mise en œuvre du droit à l'oubli par le déréférencement suppose de la part du moteur de recherche qu'il cesse d'associer l'information figurant dans les pages web indexées aux résultats de recherche effectuées sur la base du nom, prénom ou d'autres données personnelles de la personne concernée. Toutefois, les pages litigieuses restent accessibles lorsqu'une recherche est effectuée avec d'autres mots-clés. De plus, la page web d'origine stockée sur les serveurs du site source ainsi que sa copie en cache stockée par Google ne sont pas non plus supprimées par l'effet du déréférencement. Cette suppression ne peut avoir lieu que si l'éditeur du site d'origine supprime l'article ou s'oppose à son indexation par l'exploitant du moteur de recherche.**B - Mise en œuvre du droit à l'oubli : Google et le contrôle juridictionnel**Le droit à l'oubli est devenu effectif, comme l'attestent les décisions prises par les moteurs de recherche et les juridictions, mais n'est pas automatique puisque les situations ne s'apprécient qu'au cas par cas.

À la suite de la décision de la Cour de justice, Google s'est doté d'un panel d'experts qui a déterminé les critères à prendre en compte pour faire prévaloir le droit à l'oubli ou non, dont notamment (i) le rôle de la personne concernée dans la vie publique, (ii) la nature de l'information objet du traitement, (iii) la source de l'information, et (iv) le temps écoulé depuis la première publication des informations7. Sur la base de ces règles, Google a indiqué que, depuis le 28 mai 2014, sur les 773 282 demandes de déréférencement reçues, elle a fait droit à 44,2 % des demandes tandis que 55,8 % ont été refusées8.

La CNIL, lorsqu'elle est saisie d'une plainte par une personne concernée n'ayant pas eu gain de cause dans l'exercice de ses droits, est également compétente pour contrôler l'effectivité du droit à l'oubli et enjoindre au moteur de recherche d'y faire droit ou le conforter dans sa position lorsque des exceptions peuvent faire échec au droit à l'oubli9.

Lorsque la jurisprudence prend le relais, par l'introduction d'une action pénale avec constitution de partie civile ou d'une action civile à l'initiative du requérant (à titre individuel ou dans le cadre d'une action collective) lorsque le moteur de recherche ne fait pas droit aux demandes d'exercice des droits, elle confirme également qu'elle se prête à l'exercice de la mise en balance concrète des intérêts en présence pour déterminer s'il y a lieu ou non d'accorder un droit à l'oubli. À cet égard, la Cour de cassation a réaffirmé le 14 février 2018 que les juridictions ne peuvent retenir une analyse*in abstracto*en vue de prononcer une mesure d'injonction générale de déréférencement mais qu'il leur appartient de procéder à une appréciation du bien-fondé de la demande et à la mise en balance concrète des intérêts en présence.

À titre d'exemple, le droit à l'oubli a été accordé à une personne concernant l'affichage dans la liste des résultats de Google d'une condamnation pénale n'ayant pas donné lieu à inscription sur le

bulletin no 3 du casier judiciaire aux motifs que ces résultats pénalisaient sa recherche d'emploi. De même, il a été fait droit à la demande de déréférencement d'un article contenant des données personnelles relatives à un individu prétendument associé à un scandale sexuel, la véracité des propos n'ayant pas été démontrée.

Le droit à l'oubli n'est cependant pas systématiquement accordé. Les juridictions françaises veillent à ne pas entraver la liberté du public à accéder à l'information. Une demande de déréférencement a ainsi été rejetée, en l'absence de juste motif, s'agissant d'une condamnation pénale datant de 2015 alors même qu'elle avait fait l'objet d'une réduction de peine. Les juridictions parisiennes ont également rappelé le 28 novembre 2018 que le droit à l'oubli ne saurait être invoqué pour réparer un préjudice moral dès lors que celui-ci résulte non pas de l'indexation par Google des condamnations pénales mais de l'implication de la personne concernée dans la procédure pénale ayant donné lieu aux condamnations.

La charge laissée aux moteurs de recherche de procéder à la mise en balance des droits et intérêts en présence étant soumis à un contrôledes juridictions, il ne leur est pas laissé toute latitude.

Toutefois, dans le prolongement de l'arrêt, de nouvelles questions se posent concernant la portée territoriale du déréférencement ou les obligations pesant sur le moteur de recherche en qualité de responsable de traitement lorsque sont traitées des données relatives à des condamnations pénales.**C - Portée du déréférencement : des difficultés pratiques non tranchées1 - La question de la portée territoriale du droit à l'oubli**a - Portée territoriale au regard de la Directive

L'arrêtne se prononce pas sur la portée territoriale du droit à l'oubli, ce qui a donné lieu à des prises de position divergentes du G29 et de la CNIL, d'une part, et de Google, d'autre part, sans solution tranchée à l'heure actuelle.

Afin d'accorder une protection large et effective aux personnes concernées, le G29 préconise d'appliquer le déréférencement à l'ensemble des extensions du moteur de recherche (c'est-à-dire sur Google.com ainsi que tous les sous-domaines comportant les extensions territoriales comme Google.fr) et quel que soit le lieu à partir duquel la recherche est effectuée (que ce soit à partir du territoire européen ou du sol d'un État hors de l'UE). Google ne s'est pas rangée à cette position et a choisi de ne mettre en œuvre le déréférencement que sur les extensions européennes du service de moteur de recherche.

La CNIL, suivant l'avis du G29, l'a alors mise en demeure publiquement, le 21 mai 2015, de procéder au déréférencement au niveau mondial. Google n'ayant pas obtempéré, la CNIL a prononcé publiquement une sanction pécuniaire le 10 mars 2016. Dans sa décision de sanction, la CNIL relève que Google a mis en place, postérieurement à la mise en demeure, une solution de géoblocage, fondée sur l'adresse IP de l'internaute utilisant le service Google Search, afin de l'empêcher d'accéder aux résultats du moteur de recherche tels que figurant sur les extensions non européennes, mais ne considère pas la mesure comme satisfaisante pour pleinement mettre en œuvre le droit à l'oubli.

Google a interjeté appel devant le Conseil d'État qui a sursis à statuer et saisi la Cour de justice

d'une demande de décision préjudicielle en interprétation de la Directive pour apprécier la portée territoriale du déréférencement. Il invite la Cour à préciser si le déréférencement s'applique au niveau mondial ou au seul niveau des États membres de l'Union européenne. Dans la seconde hypothèse, il s'interroge sur le point de savoir si la limitation du déréférencement s'applique, pour un internaute situé dans l'Union, aux seules extensions européennes ou bien quelle que soit l'extension du moteur de recherche.

Dans ses conclusions rendues le 10 janvier 2019, l'avocat général invite la Cour de justice de l'Union européenne à adopter une solution proportionnée, comme la Cour l'a déjà fait dans son arrêt *Lindqvist*, pour rejeter un droit au déréférencement mondial. Selon lui, le droit de l'Union ne doit s'appliquer que dans les frontières de l'Union européenne afin de réglementer le fonctionnement du marché intérieur et non interférer au niveau du marché mondial. Le déréférencement ne devrait conduire qu'à restreindre la diffusion des données devenues inadéquates, quelle que soit l'extension du moteur de recherche, résultant d'une recherche effectuée par un internaute situé dans l'Union. Dans l'attente de l'arrêt de la Cour de justice, il convient d'être prudent car rien ne permet de présager que la Cour suive l'approche nuancée de l'avocat général.

En pratique, il nous semble justifié d'admettre que la balance entre les droits et intérêts en présence s'effectue au regard (i) des activités affectant le marché intérieur européen uniquement et (ii) des droits conférés au public européen exclusivement. Lorsque le droit à l'oubli doit primer, le déréférencement ne serait alors admis qu'au niveau européen. De plus, la solution de géoblocage mise en place par Google apporterait, d'une part, des garanties suffisantes afin de conférer une protection large et efficace puisqu'elle permet d'empêcher ou tout du moins de rendre difficilement réalisable la consultation de résultats d'une recherche effectuée à partir du nom d'une personne ayant exercé son droit à l'oubli depuis l'ensemble du territoire de l'Union. D'autre part, en instaurant un niveau de protection identique au sein de l'ensemble des États membres, le géoblocage répondrait à l'objectif d'harmonisation des législations de la Directive.

En tout état de cause, l'arrêt sera rendu à la lumière de la Directive, ce qui laisse présager que des questions similaires pourraient être soulevées au regard du RGPD.

b - Portée territoriale au regard du RGPD

Le RGPD a introduit, en plus des critères existants relatifs à l'existence de moyens de traitements ou d'établissements situés sur le territoire européen, un nouveau critère tiré du ciblage des personnes concernées sur le territoire européen. Ce critère s'applique lorsque le responsable de traitement ou son sous-traitant ne dispose pas d'un lien de rattachement matériel (établissement ou moyen de traitement) à l'Union.

Cette extension du champ d'application territorial ainsi que la précision apportée au considérant 14 du RGPD, au terme duquel la protection des données personnelles est accordée aux personnes physiques « indépendamment de leur nationalité ou de leur lieu de résidence », ont pu laisser présager d'un vif renforcement des droits des personnes au détriment des acteurs économiques situés hors Union européenne (UE) désormais soumis aux obligations européennes.

Cette extension reste à nuancer. Le considérant 14 ne bouscule pas les règles applicables puisque la Directive, interprétée à la lumière de la Charte des droits fondamentaux de l'UE, conférait déjà une protection à « toute personne ». La nationalité du requérant n'était donc pas un critère différenciant.

Par ailleurs, il s'infère des articles 3(1) et 3(2) du RGPD la même recherche d'un critère de rattachement territorial à l'Europe : l'existence d'un établissement européen ou l'existence d'une situation dans l'Union.

Au regard du critère tiré de l'article 3(1) du RGPD, si la solution proposée par l'avocat général devait être retenue sous l'empire de la Directive, elle ne devrait pas souffrir de tempérament sous le RGPD. C'est d'ailleurs le parti pris par l'avocat général lorsqu'il constate que « la question [*dela portée du déréférencement*] ne se poserait même pas » au regard du Règlement.

Dans l'hypothèse où un moteur de recherche ne disposerait pas d'un établissement européen, les obligations de déréférencement lui incombant s'appliqueraient tout autant sur le fondement de l'article 3(2) du RGPD dès lors que (i) le moteur de recherche offre un service de la société de l'information par la mise à disposition d'informations au public situé dans l'UE, ou (ii) le moteur de recherche utilise des cookies lors de la fourniture de son service à l'internaute présumé situé dans l'UE en vue de personnaliser l'affichage, l'ordre des résultats et/ou les annonces publicitaires figurant sur la page de recherches. Quant à la portée du déréférencement, l'article 3(2) du RGPD vient conforter l'interprétation d'un champ d'application territorial du déréférencement limité. En effet, le traitement des données personnelles d'un citoyen américain ou espagnol qui s'affiche sur une extension, quelle qu'elle soit, du moteur de recherche accessible depuis un territoire européen relève du champ d'application du RGPD en vertu du critère de l'accessibilité de l'offre. En revanche, le traitement des données personnelles d'un citoyen américain ou espagnol qui s'affiche sur une extension internationale du moteur de recherche, ne relève pas du champ d'application du RGPD car l'offre n'est pas dirigée vers une personne située dans l'UE, de même que le suivi du comportement ne concerne pas un comportement situé au sein de ce territoire.

On peut en conclure que, bien que le champ d'application du RGPD puisse apparaître large, la protection conférée est raisonnable et proportionnée en ce qu'elle sanctionne un trouble rattaché à l'UE en raison de la localisation de la personne concernée ou de la localisation des données au sein du territoire européen.

Cette approche rappelle les règles en matière de compétence judiciaire et de reconnaissance et d'exécution des décisions en matière civile et commerciale aux termes desquelles les juridictions sont tenues de rechercher un lien de connexité entre les faits et la personne concernée et fondent leur compétence au regard du lieu où celle-ci a le centre de ses intérêts.**B - Portée du déréférencement en matière de traitement de données sensibles effectué initialement aux fins de journalisme**Dans le prolongement de l'arrêt, la Cour de justice de l'Union européenne a également été saisie par le Conseil d'État de questions préjudicielles portant sur l'interprétation des obligations pesant sur les moteurs de recherche en matière de traitement de données sensibles et

de déréférencement de liens menant vers des pages web qui comportent des données sensibles traitées à des fins de journalisme.
Les faits concernent des refus de déréférencement, opposés par Google, de liens, affichés à la suite d'une recherche effectuée à partir du nom et renvoyant vers des articles principalement de presse faisant état de procédures pénales ayant abouti ou non à des condamnations pénales. Les requérants déboutés ont individuellement saisi la CNIL d'une plainte en vue d'obtenir une injonction de déréférencement. Toutefois, l'autorité de contrôle a, dans chacun des cas d'espèce, fait primer la liberté d'information et a donné gain de cause à Google en clôturant les plaintes. Les personnes concernées ont par la suite introduit un recours devant le Conseil d'État en vue d'obtenir l'annulation de la décision de la CNIL et d'enjoindre à Google de procéder aux déréférencements litigieux.
La haute juridiction ayant considéré que les requêtes soulevaient des questions d'interprétation de la Directive, elle a décidé de sursoir à statuer et de s'adresser à la Cour de justice. Aux termes de ses conclusions rendues le 10 janvier 2019, l'avocat général rappelle à juste titre que le référencement par le moteur de recherche d'une page web comportant des données faisant état de la commission d'une infraction pénale ou d'une condamnation pénale constitue un traitement de données sensibles qui est interdit au sens de l'article 8.5 de la Directive sauf à pouvoir se prévaloir de l'une des exceptions (purement théoriques pour un moteur de recherche) prévues à l'article 8.2 de la Directive. Toutefois, il considère que la responsabilité de l'exploitant du moteur de recherche ne peut être engagée*ex ante* et d'office, car celui-ci n'est pas en mesure de contrôler *a priori* le contenu de chaque page indexée en vue de s'assurer de sa conformité aux lois applicables. Cette interprétation, qui s'inscrit dans le prolongement du régime de responsabilité allégé applicable aux hébergeurs, justifierait que c'est seulement à compter du moment où Google est informé du traitement de données sensibles illicite, par une demande de déréférencement, qu'il devrait procéder à la suppression du référencement des liens associés au nom de la personne afin de mettre un terme au traitement non conforme. L'avocat général en conclut que le moteur de recherche doit systématiquement faire droit à une demande de déréférencement portant sur des pages comportant des données sensibles sans rechercher si les données concernées demeurent pertinentes ou non.
Cependant, comme l'y invitaient déjà les lignes directrices du G29 et désormais le RGPD, l'avocat général note que la circonstance que le traitement initial effectué par l'éditeur de la page web ait pour base légale l'exception de traitement aux fins de journalisme doit être prise en compte dans la balance entre les droits à la vie privée du requérant au déréférencement et les droits du public à accéder à l'information ainsi que la liberté d'expression de celui dont émane l'information. Cette circonstance est susceptible de permettre le rejet d'une demande de déréférencement de données sensibles (même illicitement traitées par le moteur de recherche) lorsqu'il est justifié que les droits à l'information et la liberté d'expression doivent primer.
Il revient donc aux moteurs de recherche puis éventuellement à l'autorité de contrôle compétente et/ou aux juridictions nationales saisies d'apprécier, au cas par cas, lequel des droits fondamentaux

doit primer.**II - Traitements journalistiques : la primauté encadrée du droit à l'information dans une société démocratique**Le régime dérogatoire applicable aux traitements de données personnelles à des fins journalistiques a connu une évolution constante vers le renforcement de la primauté du droit à l'information. Le RGPD a confirmé la tendance en laissant aux États membres une marge de manœuvre pour déterminer les règles applicables aux traitements effectués par les journalistes dans le but de concilier la vie privée avec les droits à la liberté d'expression et l'accès du public à l'information. Toutefois, le périmètre de cette exception varie suivant la qualification des activités de journalisme retenue à l'échelon national. En droit interne, on peut s'étonner du choix du législateur français, opéré en novembre 2018, de maintenir une conception stricte du traitement journalistique, entendu comme celui applicable au bénéfice des personnes exerçant la profession de journaliste alors que la jurisprudence européenne invite à interpréter de façon large la notion de journaliste.**A - Un régime dérogatoire pour faire prévaloir la liberté d'expression**Dans sa version en vigueur en 1978, la loi Informatique et libertés instaurait un régime dérogatoire aux traitements effectués par les organismes de presse écrite ou audiovisuelle afin d'assurer un juste équilibre avec la liberté d'expression. La doctrine de la CNIL reconnaissait également que les droits d'accès et de rectification des personnes devaient être aménagés compte tenu de l'existence d'autres garanties procédurales (droit de réponse, règles de déontologie, rectifications et mises à jour des articles, etc.).

La Directive a rendu obligatoire l'introduction d'exemptions et de dérogations à l'égard des traitements effectués « aux fins de journalisme » sous la réserve que celles-ci soient « nécessaires pour concilier le droit à la vie privée avec la liberté d'expression ».

Le G29 réaffirmait, en 1997, que les dérogations fixées par les États membres devaient respecter un principe de proportionnalité et être justifiées au regard des autres garanties dont disposent les personnes concernées (formes spécifiques de réparation par le droit de réponse et la correction de fausses informations, obligations professionnelles et déontologiques de la profession, dispositions légales sur la protection de l'honneur).

La transposition de la Directive en droit interne, par la loi du 6 août 2004, a alors renforcé les exceptions aux règles de protection des données personnelles applicables aux traitements journalistiques en ce qui concerne notamment, l'information des personnes, la durée de conservation, les droits des personnes et les modalités d'exercice de ces droits ainsi que les formalités auprès de la CNIL.

Désormais, c'est à l'article 85 du RGPD que figure l'octroi d'une marge de manœuvre accordée aux États membres. La liste des exemptions ou dérogations autorisées par le RGPD est encore plus étendue que celle prévue par la Directive.C'est par l'ordonnance du 12 décembre 2018 que la France a modifié son régime dérogatoire, lequel n'entrera en vigueur qu'au 1er juin 2019.**B - Difficultés d'interprétation du régime dérogatoire1 - Le choix du législateur et les questionnements de la CNIL**La CNIL a, par avis du 15 novembre 2018, alerté le gouvernement sur des difficultés d'interprétation. D'une part, le champ d'application de l'exception restreint aux

traitements mis en œuvre « à titre professionnel, de l'activité de journalisme » est questionnable dès lors que l'article 85(1) du RGPD vise les traitements aux fins de « journalisme » de façon générale et que le considérant 153 invite à retenir une « interprétation large des notions liées à cette liberté, telles que le journalisme ».

Si, selon sa doctrine antérieure, la CNIL privilégiait une définition restreinte de la notion de journaliste qui excluait notamment les bloggeurs et le journalisme amateur, conformément à la qualification de journaliste telle qu'elle résulte des dispositions du code du travail et de la loi sur la presse, elle semble aujourd'hui se faire l'écho de la jurisprudence libérale de la Cour de justice. Selon la Cour, l'activité de journalisme s'entend de celle qui a « pour finalité la divulgation au public d'informations, d'opinions ou d'idées », que cette activité soit effectuée à des fins lucratives par une personne morale ou par une personne privée comme l'a consacré l'arrêt du 14 février 2019.

À opter pour une marge de manœuvre limitée, la France pourrait s'exposer à une sanction pour non-respect du droit à l'information. D'autre part, le choix de soumettre les dérogations au critère de « nécessité » pourrait rendre l'application des dérogations délicates. Ce critère ferait peser sur le responsable de traitement, sous le contrôle de la CNIL et des juridictions, l'appréciation de la proportionnalité entre la nécessité de faire primer le droit à l'information et les dérogations qui s'ensuivent. Selon l'avis de la CNIL, le critère de nécessité prévu par le RGPD s'entend du choix laissé à l'État membre de retenir tout ou partie des dérogations autorisées par le RGPD dans le respect du principe de proportionnalité.

Enfin, les dérogations prévues en droit interne reprennent majoritairement celles issues de la transposition de la Directive puisque figurent des exceptions en matière de durée de conservation, de traitement des données sensibles et des données relatives aux infractions, de droit à l'information, de droits des personnes (droit d'accès, droit de rectification, droit à la limitation du traitement) et de transferts des données. On notera, toutefois, que contrairement à l'article 85.2 du RGPD qui inclut une exception au droit à l'effacement (droit à l'oubli), celle-ci ne figure pas dans la loi française. L'équilibre entre les droits de la presse et le droit à la vie privée risque d'être remis en cause, notamment à l'encontre des moteurs de recherche qui seraient alors systématiquement tenus de supprimer les liens renvoyant vers des pages objets de traitements effectués à des fins de journalisme contrairement aux recommandations de l'avis de l'avocat général rendu dans l'affaire C-136/17. Les juges pourraient toutefois se fonder, au cas par cas, sur le dernier alinéa de l'article 80 de la loi Informatique et libertés pour reconnaître que les règles applicables en matière de presse « préviennent, limitent ou réparent » déjà les atteintes à la vie privée des personnes.

C - État de la jurisprudence : une balance qui penche en faveur de la liberté d'expression des journalistes

1 - Absence de suppression des publications et des archives des sites de presse

Dans une décision du 28 mai 2014, la cour d'appel de Paris a refusé de faire droit à la demande d'un magistrat du tribunal de commerce, condamné pour des faits de corruption, d'enjoindre à un éditeur de presse en ligne de désindexer ou d'anonymiser un article relatant l'affaire de corruption. La cour considère qu'il n'y a pas lieu de limiter la liberté d'expression compte tenu du sujet d'intérêt général que

présente l'affaire et de la nature particulière de l'information révélée relative au fonctionnement de la justice. De même, il n'y a pas lieu d'enjoindre à l'éditeur de solliciter la désindexation du contenu par les moteurs de recherche car cela constituerait une atteinte à la liberté d'expression.

Par un jugement du 15 mars 2016, le Tribunal de grande instance de Bobigny a refusé de faire droit à une demande de suppression de deux articles d'archives d'un site de presse, formée sur le fondement des droits de rectification et de suppression. La juridiction motive sa position par le fait que ces droits sont inapplicables aux traitements effectués à des fins journalistiques. Le tribunal sous-entend que la solution aurait pu être différente si la demande avait été effectuée au nom du droit d'opposition.

Un arrêt de cassation rendu le 12 mai 2016 est également venu confirmer la décision de la cour d'appel de Paris qui a retenu qu'imposer à un organe de presse de supprimer de ses archives en ligne un article relatant une sanction judiciaire, ou de supprimer les noms et prénoms des personnes visées par la décision, ou encore d'en restreindre l'accès en modifiant le référencement habituel des articles, constituent des restrictions injustifiées à la liberté de la presse. La cour d'appel a pris soin de préciser que ces archives ne peuvent s'assimiler à une base de données de décisions de justice.

Enfin, plusieurs décisions européennes confortent la position des juridictions françaises. À plusieurs reprises, la prévalence du droit l'information sur la protection de la vie privée a été reconnue lorsqu'il s'agit d'archives de presse.**2 - La suppression des contenus sur les moteurs de recherche par le déréférencement**En retenant que le traitement effectué par l'éditeur de la page web et distinct de celui du moteur de recherche, l'arrêtsouligne qu'une demande de déréférencement peut échouer devant l'éditeur, lorsqu'il peut se prévaloir de l'exception de traitement journalistique, mais aboutir contre l'exploitant du moteur de recherche qui ne peut se prévaloir de cette même exception faute d'avoir la qualité de journaliste.

À titre d'exemple, en réponse à une action intentée par un administrateur de société à l'encontre d'un éditeur de presse en ligne, en vue d'obtenir la suppression de « tous les articles » le concernant, le tribunal a considéré que la conciliation entre le droit d'opposition et les dispositions du droit de la presse (loi des 29 juill. 1881 et 1982) ne justifiait pas de faire droit à la demande de suppression de « tout article ». En revanche, la juridiction ordonne à l'éditeur de presse de prendre les mesures adéquates afin que les moteurs de recherche cessent l'indexation des contenus litigieux. Il incombe alors à l'éditeur de modifier sa politique éditoriale et ses choix de diffusion par des protocoles d'exclusion comme « robot.txt » ou des codes comme « noindex » ou « noarchive ».

La différence de régime s'explique également par la portée moindre de la diffusion effectuée par l'organe de presse par rapport au moteur de recherche.

Toutefois, le déréférencement par le moteur de recherche n'est pas accordé systématiquement, dès lors que les circonstances justifient le maintien de l'accès au public à l'information et la liberté d'expression. C'est l'orientation préconisée par la CNIL, le G29 et récemment l'avocat général dans ses conclusions dans l'affaire C-136/17, précitée.

Enfin, les juridictions n'appliquent pas le même régime aux traitements effectués à des fins

journalistiques de décisions relatives aux infractions ou condamnations et aux traitements réalisés par les éditeurs de bases de données juridiques. La différence s'expliquerait par la nature différente des traitements : le premier vise à rendre compte au public de l'actualité sur des questions d'intérêt général tandis que le second vise à la délivrance d'informations juridiques à un lectorat distinct.**III -** *Open data*et anonymisation des décisions de justice : les étapes de la consécration légale du droit à l'anonymat**Initié par la CNIL, le mouvement de protection des données personnelles contenues dans les décisions de justice s'est construit pas à pas au rythme d'évolutions législatives. Si la protection accordée par les tribunaux au titre de la publicité des décisions de justice (ou***open data*) reste partielle, il est vraisemblable que le droit à l'anonymat a vocation à être reconnu lors de la réutilisation des décisions de justice par les autres acteurs (éditeurs de bases juridiques notamment) intervenant dans la diffusion du droit.**A - Anonymisation des décisions de justice : l'évolution de la doctrine de la CNIL1 - Position de la CNIL en 2001**Le caractère public des décisions de justice et leur libre communication à toute personne qui en fait la demande constituent des garanties fondamentales consacrées de longue date, notamment à travers l'article 6 de la Convention européenne des droits de l’homme. Ces droits ne sont cependant pas exclusifs et la législation française comporte de nombreux tempéraments qui visent à la protection de la vie privée des justiciables.

La CNIL s'est toujours préoccupée du caractère nominatif des décisions de justice et du risque que les bases de données juridiques soient détournées afin de créer des fichiers de renseignements. Elle rappelait, dès 1985, que ces bases constituent des traitements de données personnelles et que toute personne peut s'opposer au traitement de ses données pour des raisons légitimes. Cependant, à cette époque, elle n'avait pas jugé proportionné de requérir l'anonymisation des décisions en raison de leur diffusion restreinte à l'enceinte des juridictions ou aux professionnels du droit ayant souscrit un abonnement pour des fins strictement documentaires. Le développement d'internet et le risque de création de profils par les moteurs de recherche a renouvelé le débat et l'a conduite à émettre une recommandation.

En 2001, elle considère que la recherche d'un juste équilibre entre l'exigence de publicité des décisions de justice et le droit à la protection des données personnelles justifie d'accorder un niveau de protection différencié (et moins favorable) selon l'étendue de la diffusion : les adresses des parties et témoins mentionnées dans les décisions en accès restreint (par abonnement payant auprès de sites spécialisés) doivent être préalablement occultées, alors que les décisions en accès libre sur internet nécessitent de procéder à l'occultation préalable tant des noms que de l'adresse des parties et témoins mentionnés.

De façon générale, la CNIL considère qu'une anonymisation des décisions de justice, c'est-à-dire la mise en œuvre de mesures en vue d'ôter tout caractère identifiant aux données figurant dans les décisions, est disproportionnée et serait contraire aux exigences d'intelligibilité de la justice. La CNIL se contente donc d'une protection de faible niveau à l'égard des justiciables (parties et témoins) et exclut du champ de la protection les membres des juridictions (magistrats et auxiliaires de justice).

Alors que l'accès en ligne des décisions de justice relève d'une mission de service public prévue par les textes, l'accueil de ces recommandations par les éditeurs de bases de données d'initiatives publiques a été mitigé. Le site Légifrance s'est conformé à la recommandation de la CNIL tandis que le Conseil d'État s'y est d'abord opposé, sur le fondement du principe constitutionnel d'accessibilité du droit, avant d'anonymiser une partie de sa base en 2011.
On notera également que la CNIL a appliqué sa doctrine à l'encontre d'une association ayant constitué une base de données de décisions de justice librement accessible mais non anonymisée. Elle a ainsi mis en demeure puis sanctionné l'association pour non-respect du droit d'opposition des personnes qui sollicitaient l'occultation de leurs noms tout en rappelant qu'il s'agissait d'un manquement à sa recommandation de 2001. Le Conseil d'État a confirmé cette condamnation.**2 - Bilan de la CNIL en 2006**Le débat a par la suite été renouvelé en 2006 lorsque la CNIL a dressé un bilan du traitement des données personnelles par les bases de données juridiques. À cette occasion, elle a rejeté le principe d'anonymisation à la demande de la personne concernée en raison des conséquences économiques trop importantes que cela ferait peser sur les juridictions (gestion des demandes et mise en œuvre de l'anonymisation). Cependant, elle invite le législateur à s'inspirer de la réforme consacrant la libre réutilisation des informations publiques, qui requiert une anonymisation préalable des données personnelles qu'elles comportent, et préconise d'appliquer ces règles aux décisions de justice.**B -**et décisions de justice : les règles édictées par la loi pour une République numérique et leurs suites**Les décisions de justice ne sont pas des données publiques mais elles ont bénéficié de la dynamique française d'ouverture des données.1 - Qualification des décisions de justice en tant qu'informations publiques**En vertu du principe de séparation des pouvoirs et d'indépendance de la justice, les décisions de justice ne sont pas des documents administratifs communicables au sens de la loi. Toutefois, selon la jurisprudence de la Commission d'accès aux documents administratifs (CADA), les décisions de justice comportent des données de nature publique, au sens de la loi CADA par application de l'article 11-3 de la loi no 72-626 du 5 juillet 1972, et de nature privée. Cette qualification d'informations publiques des décisions de justice a été consacrée par la loi pour une République numérique du 7 octobre 2016 qui est venue modifier l'article 10 du code de la justice administrative et l'article L. 111-13 du code de l'organisation judiciaire. La recommandation de la CNIL de 2006 a donc été suivie mais peine à trouver application en l'absence du décret d'application devant préciser les conditions de ces textes.
2 - La loi de réforme de la justiceL'absence de décret tient notamment au fait que le projet de loi de programmation 2018-2022 et de réforme pour la justice a fait l'objet d'une navette parlementaire qui a mis en exergue les difficultés auxquelles s'exposent les deux chambres à concilier le principe de publicité des décisions de justice dans le cadre de l'et le droit au respect de la vie privée. Le rapport Cadiet rendu public en novembre 2017 s'était déjà fait l'écho du difficile équilibre en la matière.
Dans la version définitive de la loi promulguée le 23 mars 2019, l'article 33 est venu modifier les règles de conciliation entre le principe de publicité des décisions de justice et le droit au respect de

la vie privée issues de la loi République numérique.
En matière d', les règles de diffusion des décisions de justice et de protection des données personnelles s'articulent en deux étapes. D'une part, les noms et prénoms des personnes physiques, lorsqu'elles sont parties ou tiers, doivent systématiquement être occultées préalablement à la mise à disposition du public des décisions par l'administration. D'autre part, sous réserve d'une analyse de risque préalable, l'administration est tenue d'occulter tout élément permettant l'identification des parties, des tiers et/ou des magistrats lorsque la divulgation de leur identité est de nature à porter atteinte à la sécurité ou au respect de la vie privée de ces personnes.
Les conditions de délivrance des copies de jugements obéissent à des dérogations moins strictes, au motif que le traitement est de moindre portée et moins attentatoire à la vie privée qu'en matière d' . Il n'est pas prévu d'occultation systématique préalable des noms et prénoms des personnes mais seulement au cas par cas, si leur divulgation est susceptible de porter atteinte à la sécurité ou au respect de la vie privée des personnes ou de leur entourage dans des conditions à préciser par décret.
S'agissant des règles applicables aux personnes souhaitant réutiliser les informations publiques contenues dans une décision de justice préalablement rendue publique, le principe d'une anonymisation demeure, selon des règles à fixer par décret.
On rappellera que l'anonymisation consiste en une technique visant à rendre impossible toute identification ou ré-identification des personnes, par quelque moyen que ce soit et de manière irréversible. La CNIL est aujourd'hui dotée d'une compétence de certification lui permettant notamment de certifier les processus d'anonymisation. Il est également prévu qu'elle se prononce sur le projet de décret.
Enfin, une interdiction, sous peine de sanctions, est posée à la réutilisation des données d'identité des magistrats et des membres du greffe, figurant dans les décisions mises à disposition en vertu de l', afin de déceler leurs pratiques professionnelles. Cette disposition visant à éviter un profilage des professionnels de justice susceptible d'altérer le bon fonctionnement de la justice a été jugée conforme par le Conseil constitutionnel le 21 mars 2019.**C - Rôle des tribunaux et des éditeurs de bases de données juridiques**En attendant le décret, les initiatives (judiciaires) d'une start-up souhaitant concurrencer les éditeurs de base de données juridiques permettent de faire le point sur les règles applicables et les obligations incombant aux tribunaux émetteurs des décisions et des diffuseurs.
La CADA a, par deux avis, reconnu qu'il convenait de faire droit aux demandes du moteur de recherche « Doctrine.fr » de copie et de réutilisation des minutes civiles du Tribunal de grande instance de Paris rendues publiquement formées auprès du greffe du tribunal et des Archives de France. Cela a conduit la cour d'appel de Paris, le 18 décembre 2018, puis la Cour d'appel de Douai, le 21 janvier 2019, à abonder dans le même sens en autorisant la délivrance de copies de décisions en vue de leur mise à disposition sur Doctrine.fr. Ces mises à disposition de copies de jugements, qui répondent (i) au droit d'accès à la copie des jugements en vertu du Code de

l'organisation judiciaire et (ii) au principe de libre réutilisation des informations publiques, ne requièrent pas de mesure de pseudonymisation de la part des juridictions (il ne s'agit pas de l'car la demande émane d'un tiers) mais nécessite de la part de celui qui entend réutiliser les informations publiques de procéder à une anonymisation préalable dont les règles restent à définir par décret.*En la matière, la récente circulaire du ministère de la Justice du 19 décembre 2018 a devancé le législateur puisqu'elle invite les juridictions à ne faire droit aux demandes de copie que dans la mesure du raisonnable et entend permettre aux greffes de refuser les demandes en masse. Cette règle, consacrée à l'article 33 de la loi, a fait l'objet d'une saisine du Conseil constitutionnel en ce qu'elle donnait trop de latitude aux greffes pour refuser les demandes de copies délivrées aux tiers. La constitutionnalité de la disposition a été confirmée au regard des objectifs de protection des personnes et de respect de la vie privée. Les sages notent également que les décisions des greffes peuvent faire l'objet d'un recours juridictionnel et qu'en tout état de cause les tiers peuvent accéder aux décisions sur le fondement de l'*.Il convient de retenir que les évolutions législatives ont consacré la doctrine de la CNIL et la pratique des juridictions de pseudonymisation des décisions. Elles marquent également une volonté de renforcement des droits des personnes dont la portée ne pourra être appréciée qu'à l'issue de la publication des décrets.

On constate néanmoins aujourd'hui que la simple occultation des noms et prénoms n'est pas satisfaisante pour la personne concernée et que le droit à l'information judiciaire prime bien souvent sur les intérêts personnels des parties à l'affaire. Toutefois, au regard des mesures de pseudonymisation qui s'imposent aux juridictions ainsi que des exigences d'anonymisation qui pèsent sur les moteurs de recherche et les diffuseurs de jurisprudence, la diffusion des décisions de justice devrait avoir un impact moindre sur les personnes, ce qui participe au renforcement de la protection de la vie privée.

S. L et D. P.

Auteur(s) :

Sabine Lipovetsky - Avocat associé

Harlay Avocats

Domitille Philippe - Avocat à la Cour

Harlay Avocats

Notes de bas de page :

1. L'art. 6 de la loi no 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN) permet de solliciter le retrait ou la cessation de la diffusion de contenus manifestement illicites.

2. Loi no 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, JO 24 mars.

3. Règl. (UE) 2016/679 du 27 avr. 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.

4. CJUE, gde ch., 13 mai 2014, C-131/12, AJDA 2014. 1147, chron. M. Aubert, E. Broussy et H. Cassagnabère ; D. 2014. 1476, note V.-L. Benabou et J. Rochfeld ; ibid. 1481, note N. Martial-Braz et J. Rochfeld ; ibid. 2317, obs. J. Larrieu, C. Le Stanc et P. Tréfigny ; AJCT 2014. 502, obs. O. Tambou ; JAC 2014, n° 15, p. 6, obs. E. Scaramozzino ; Constitutions 2014. 218, chron. D. de Bellescize ; RTD eur. 2014. 283, édito. J.-P. Jacqué ; ibid. 879, étude B. Hardy ; ibid. 2016. 249, étude O. Tambou ; Rev. UE 2016. 597, étude R. Perray.

5. Dir. 95/46/CE du Parlement européen et du Conseil, du 24 oct. 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

6. CJUE 13 mai 2014, aff. C-131/12, préc., pt 81.

7. The advisory council to Google on the right to be forgotten, févr. 2015.

8. https://transparencyreport.google.com/eu-privacy/overview.

9. À titre d'exemple, dans le cadre de l'instruction de 4 plaintes pour refus de déréférencement, la CNIL a validé les refus opposés par Google. Les requérants ont cependant interjeté appel de la décision de la CNIL devant le Conseil d'État (CE 24 févr. 2017, nos 391000, 393769, 399999, 401258, Lebon ; AJDA 2017. 436 ; ibid. 740, chron. G. Odinet et S. Roussel ; D. 2017. 500, obs. M.-C. de Montecler ; ibid. 2018. 1033, obs. B. Fauvarque-Cosson et W. Maxwell ; Dalloz IP/IT 2017. 479, obs. O. Henrard ; RFDA 2017. 535, concl. A. Bretonneau ; RTD eur. 2017. 803, obs. A. Bouveresse) ce qui a donné lieu à des demandes de décisions préjudicielles pendantes devant la CJUE (aff. C-136/17).

10. Civ. 1re, 14 févr. 2018, no 17-10.499, D. 2018. 348 ; ibid. 1033, obs. B. Fauvarque-Cosson et W. Maxwell ; Dalloz IP/IT 2018. 250, obs. E. Derieux.

11. TGI Paris, ord. réf., 24 nov. et 19 déc. 2014, Marie-France c/ Google France et Google Inc.

12. TGI Paris, ord. réf., 13 mai 2016, M. X c/ Google France et Google Inc.

13. TGI Paris, ord. réf., 10 févr. 2017, M. X. c/ Google France et Google Inc.

14. Préc. note 11 et Paris, 28 nov. 2018, no 17/19759, Franck B. c/ Google France.

15. Lignes directrices du 26 nov. 2014 relatives à l'exécution de l'arrêt Google Spain C-131/12 (wp225), p. 9.

16. Décis. no 2015-047 du 21 mai 2015.

17. Délib. no 2016-054 du 10 mars 2016.

18. CE, 10e et 9e ch. réun., 19 juill. 2017, no 399922, Lebon ; AJDA 2017. 1479 ; D. 2018. 1033, obs. B. Fauvarque-Cosson et W. Maxwell ; RFDA 2017. 972, concl. A. Bretonneau ; RTD eur. 2018. 396, obs. A. Bouveresse.

19. CJUE, aff. C-507/17.

20. Concl. de l'avocat général, M. Maciej Szpunar, du 10 janv. 2019, aff. C-507/17.

21. CJUE 6 nov. 2003, aff. C-101/01, par lequel la CJUE a rejeté une interprétation large de l'article 25 de la Directive dans le contexte d'internet en ce qui concerne le transfert de données à caractère personnel vers des pays tiers, D. 2004. 1062, obs. L. Burgorgue-Larsen ; RSC 2004. 712, obs. L. Idot.

22. Art. 8 de la Charte des droits fondamentaux de l'Union européenne.

23. Pt 77 des concl. de l'avocat général dans l'affaire C-507/17, préc.

24. Le Comité européen de protection des données (CEPD) confirme, dans son avis du 16 nov. 2018 sur le champ d'application territorial du RGPD, p. 14, que la notion d'offre ou de service inclut tout service de la société de l'information au sens de l'article 1(1) point b, de la Directive (EU) 2015/1535.

25. Règl. (UE) no 1215/2012 du 12 déc. 2012.

26. Y. Padova, Le droit à l'oubli est-il un droit universel, régional ou « global » ? À la CJUE d'en décider, RLDI no 145, 1er févr. 2018.

27. Ibid. note 8.

28. Concl. de l'avocat général, M. Maciej Szpunar, du 10 janv. 2019, aff. C-136/17.

29. Lignes directrices du 26 nov. 2014 relatives à l'exécution de l'arrêt Google Spain C-131/12 (wp225), p. 23.

30. L'art. 17.3.a du RGPD reconnaît une limitation du droit au déréférencement, y compris pour des données sensibles, pour des raisons relatives à la liberté d'expression et d'information.

31. En matière de flux de données transfrontières, de traitements des infractions et condamnations ou mesures de sûreté et en matière de données sensibles.

32. Art. 33 de la loi Informatique et libertés dans sa version alors en vigueur.

33. Délib. no 95-012 du 24 janv. 1995.

34. Des dérogations aux règles en matière de licéité des traitements, de transfert de données et d'étendue des pouvoirs de contrôles des autorités de protection pouvaient être prévues.

35. Recommandation 1/97 (wp1) du 25 févr. 1997.

36. Les dérogations supplémentaires portent sur les obligations des responsables de traitement et sous-traitants, la faculté de coopération des autorités de contrôle et les dispositions relatives aux situations particulières de traitement.

37. Ord. no 2018-1125 du 12 déc. 2018, art. 80 : à titre dérogatoire, les dispositions du 5° de l'article 4, celles des articles 6, 46, 48, 49, 50, 53, 118, 119 et celles du chapitre V du règlement (UE) 2016/679 du 27 avril 2016 ne s'appliquent pas, lorsqu'une telle dérogation est nécessaire pour concilier le droit à la protection des données à caractère personnel et la liberté d'expression et d'information, aux traitements mis en œuvre aux fins : « 1° D'expression universitaire, artistique ou littéraire ; « 2° D'exercice à titre professionnel, de l'activité de journaliste, dans le respect des règles déontologiques de cette profession ». Les dispositions des alinéas précédents ne font pas obstacle à l'application des dispositions du code civil, des lois relatives à la presse écrite ou audiovisuelle et du code pénal, qui prévoient les conditions d'exercice du droit de réponse et qui préviennent, limitent, réparent et, le cas échéant, répriment les atteintes à la vie privée et à la réputation des personnes.

38. Délib. no 2018-349 du 15 nov. 2018.

39. Délib. no 2005-285 du 22 nov. 2005.

40. C. trav., art. L. 7111-3 à L. 7111-5.

41. Art. 2 de la loi du 29 juill 1881.

42. CJCE 16 déc. 2008, aff. C-73/07, RSC 2009. 197, obs. L. Idot .

43. Ibid. note 43, § 59.

44. CJUE 14 févr. 2019, aff. C-345/17.

45. TGI Paris, ord. réf., 12 oct. 2009, qui note que la loi Informatique et libertés n'est pas une norme instituée pour limiter la liberté d'expression consacrée par l'art. 10 de la Conv. EDH.

46. Par renvoi à l'art. 17.3 du RGPD, v. note 30.

47. Préc., note 27.

48. Paris, 28 mai 2014, no 12/19857.

49. TGI Bobigny, 15 mars 2016, no 15/00870.

50. Paris, pôle 2, ch. 7, 26 févr. 2014, no 12/14813 et Civ. 1re, 12 mai 2016, no 15-17.729.

51. CEDH 16 juill. 2013, no 33846 (numéro incomplet) et CEDH 28 juin 2018, nos 60798/10 et 65599/10, AJ pénal 2018. 462, note L. François ; Dalloz IP/IT 2018. 704, obs. E. Derieux ; RSC 2018. 735, obs. J.-P. Marguénaud.

52. TGI Paris, ord. réf., 25 juin 2009, n° 09/55437 ??, C. Vernès c/ SAS Les Échos.

53. Il s'agit notamment des art. 39 et 39 quater de la loi sur la presse du 29 juill. 1881, des dispositions du code de la santé publique en matière de maladie vénériennes, de l'article 14 de l'ordonnance du 2 février 1945 relative à l'enfance délinquance ou de l'article R. 123-154 du code de commerce.

54. Premier rapport annuel d'activité de la CNIL, p. 96-97 et sixième rapport annuel d'activité, p. 200-2005.

55. Délib. no 01-057 du 29 nov. 2001 portant recommandation sur la diffusion de données personnelles sur internet par les banques de données de jurisprudence.

56. Décr. no 2002-1064 du 7 août 2002 relatif au service public de la diffusion du droit par l'internet.

57. Délibération no 2008-158 du 29 mai 2008.

58. Délib. no 2011-238 du 30 août 2011 prononçant une sanction pécuniaire et une injonction de cessation de traitement.

59. CE 23 mars 2015, no 353717, Lebon ; AJDA 2015. 1398.

60. Bilan de l'application de la recommandation de la CNIL du 29 nov. 2001, adopté le 19 nov. 2006.

61. Ord. no 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques et Décr. no 2005-1755 du 30 déc. 2005 relatif à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques, pris pour l'application de la loi no 78-753 du 17 juill. 1978.

62. Loi no 78-753 du 17 juill. 1978 modifiée portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal (dite « loi CADA ») ; désormais partiellement codifiée au sein du code des relations entre le public et l'administration (CRPA).

63. CADA, avis no 20053620 du 3 nov. 2005.

64. CADA, avis no 20103040 du 27 juill. 2010.

65. Loi no 2016-1321 du 7 oct. 2016.

66. Cet article renvoi désormais aux dispositions des art. L. 321-1 à L. 326-1 du CRPA qui encadrent les conditions de réutilisation des « informations publiques figurant dans les jugements » et imposent que la publication des informations ne peut intervenir qu'après anonymisation des données, sauf si une disposition législative ou réglementaire autorise une diffusion sans anonymisation préalable ou si la personne intéressée y a consenti.

67. Cet article exige que la mise à disposition du public des décisions de justice se fasse dans le respect de la vie privée des personnes concernées et entend fixer les conditions dans lesquelles elles peuvent être réutilisées.

68. Rapport rendu dans le cadre de la Mission d'étude et de préfiguration sur l'ouverture au public des décisions de justice, « L'open data des décisions de justice », nov. 2017.

69. Loi no 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice promulguée après décision du Conseil constitutionnel.

70. Décis. no 2019-778 DC du 21 mars 2019.

71. CADA, avis no 20171247 du 7 sept. 2017 et avis no 20174865 du 14 déc. 2017.

72. Paris, 18 déc. 2018, no 17/22211 et Douai, 21 janv. 2019. Chacune des deux cours semble faire application de la circulaire : à Paris il est constaté que « les difficultés d'ordre pratique » opposées par le greffe ne sont pas étayées et semblent surprenantes car « d'autres organismes tels que l'INPI, ou des éditeurs privés, ont un accès régulier aux décisions » alors qu'à Douai la demande est accordée avec plus de nuance en retenant que « s'agissant d'une demande isolée, il n'existe pas de raison juridique permettant de s'opposer à la communication de la décision sollicitée ».

73. Circ., 19 déc. 2018, relative à la communication de décisions judiciaires civiles et pénales aux tiers à l'instance.

74. Ibid. note 70.