



CJUE, 24 septembre 2019, C-507/17 - Google c. CNIL

Dans un arrêt C-507/17 Google c/ CNIL du 24 septembre 2019 la Cour de Justice de l'Union Européenne (CJUE) s'est prononcée sur la portée géographique des obligations de déréférencement des moteurs de recherche au sein ou au-delà du territoire des États membres de l'Union européenne.

En France, la CNIL a prononcé le 10 mars 2016 sur le fondement des articles 38 et 40 de la loi n°78-17 du 6 janvier 1978 une sanction publique de 100 000 euros à l'encontre de Google au motif que la mesure de filtrage proposée par Google reposant sur « *le critère de la localisation de l'adresse IP, qui fait varier la protection accordée à un résident européen en fonction de l'origine géographique de celui qui interroge le moteur de recherche, n'est par principe pas satisfaisant en ce que, d'une part, l'information déréférencée demeure consultable par tout internaute situé en dehors du territoire concerné par la mesure de filtrage et, d'autre part, qu'un contournement de cette mesure par les utilisateurs concernés demeure possible* ».

Il ressort de cette décision que si le traitement de données à caractère personnel opéré par Google à travers sa filiale Google France relève de la loi du 6 janvier 1978 relative aux fichiers et aux libertés, le moteur de recherche de Google est décliné en différents noms de domaine par des extensions géographiques rendant accessibles ces informations. C'est pourquoi La CNIL, en 2016, avait estimé que, d'une manière générale, seul un déréférencement mondial était de nature à permettre une protection effective des droits des personnes. En pratique, selon la CNIL, en cas de déréférencement d'un lien concernant une personne vivant en France, les informations devaient être rendues inaccessibles quel que soit le lieu dans le monde depuis lequel la recherche était effectuée.

La société Google a décidé de ne supprimer que les liens des résultats obtenus à partir des recherches effectuées depuis les noms de domaine correspondant aux déclinaisons de son moteur dans les États membres. Elle a saisi le Conseil d'État afin d'obtenir l'annulation de cette délibération.

Le Conseil d'État a décidé de surseoir à statuer afin d'interroger la CJUE au regard des difficultés soulevées par les arguments des parties, et notamment de Google qui fait valoir que le droit au déréférencement n'implique pas que les liens soient supprimés sans limitation géographique, ou alors cela contreviendrait au principe de droit international public de non-ingérence ainsi qu'à l'article 11 de la Charte qui dispose « *toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières* ».

La Cour de justice de l'union européenne n'a pas retenue entièrement cette approche.

Elle ne donne pas à ce déréférencement une portée mondiale, mais établit clairement que le déréférencement doit être effectif à l'échelle européenne, et non sur la seule version du pays de résidence du demandeur.

La Cour précise par ailleurs que, si le droit de l'Union n'impose pas le déréférencement mondial, il ne l'interdit pas non plus. Cette décision relève alors dans le respect du principe de proportionnalité et du droit international aux

autorités publiques nationales selon les latitudes qui leur ont été laissées par les législateurs nationaux des pays de l'Union.

1 | Faits et procédure

1.1. L'état du droit

La décision contestée a été prise sous l'empire de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données avant l'entrée en vigueur du règlement général sur la protection des données 2016/679 dit « RGPD » qui pose le principe à son article 17 d'un « droit à l'effacement – droit à l'oubli »¹.

Toutefois, depuis l'affaire C-131/12 Costeja dite « Google Spain » du 13 mai 2014, la CJUE a consacré le droit au déréférencement.

En application de ce principe, un moteur de recherche qui indexe, stocke et met à disposition des résultats, procède à un traitement de données personnelles et doit dès lors être considéré comme un responsable de traitement.

Ainsi en application de cette jurisprudence, ce droit permet à toute personne de demander à un moteur de recherche de supprimer certains résultats associés à ses noms et prénoms qui apparaissent à partir d'une requête faite sur son identité à condition de ne pas entraver la liberté du public d'accéder à des informations. Cette suppression ne signifie pas l'effacement de l'information sur le site internet source.

En l'espèce, la Cour a suivi sa jurisprudence.

Avant l'entrée en vigueur du règlement général sur la protection des données le 25 mai 2018, la loi du 6 janvier 1978 ne comportait aucune disposition relative au droit à l'oubli. Depuis, l'article 51 de la loi précise que :

« I. Le droit à l'effacement s'exerce dans les conditions prévues à l'article 17 du règlement (UE) 2016/679 du 27 avril 2016

II.- En particulier, sur demande de la personne concernée, le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte. Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en oeuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci.

En cas de non-exécution de l'effacement des données à caractère personnel ou en cas d'absence de réponse du responsable du traitement dans un délai d'un mois à compter de la demande, la personne concernée peut saisir la Commission nationale de l'informatique et des libertés, qui se prononce sur cette demande dans un délai de trois semaines à compter de la date de réception de la réclamation ».

Par conséquent, depuis l'entrée en vigueur du règlement, si une personne souhaite obtenir l'effacement de ses données et que le responsable de traitement s'y refuse, elle peut saisir la Commission nationale de l'informatique et des libertés, qui peut mettre en demeure le responsable de traitement de se mettre en conformité avec ses obligations, prononcer une injonction de mise en conformité sous astreinte pouvant aller jusqu'à 100 000 euros par jour ou prononcer une amende administrative pouvant aller jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu².

La demande de décision préjudicielle étant antérieure à l'entrée en vigueur du RGPD qui a abrogé la directive 95/46, en prévision de son entrée en vigueur, les juges se sont fondés sur les dispositions des deux textes, dont l'objectif est de « garantir un niveau élevé de protection des données à caractère personnel dans l'ensemble de l'Union », afin que leurs réponses s'inscrivent dans la durée.

1.2. Les questions reformulées par la Cour

La Cour a choisi de regrouper les questions du conseil d'État comme suit :

« il y a lieu de comprendre les questions posées, qu'il convient de traiter conjointement, comme visant à savoir, en substance, si l'article 12, sous b), et l'article 14, premier alinéa, sous a), de la directive 95/46 ainsi que l'article 17, paragraphe 1, du règlement 2016/679 doivent être interprétés en ce sens que, lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application de ces dispositions, il est tenu d'opérer ce déréférencement sur l'ensemble des versions de son moteur ou si, au contraire, il n'est tenu de l'opérer que sur les versions de celui-ci correspondant à l'ensemble des États membres, voire, uniquement, sur celle correspondant à l'État membre dans lequel la demande de déréférencement a été introduite, le cas échéant, en combinaison avec le recours à la technique dite du « géoblocage » afin de garantir qu'un internaute ne puisse, quelle que soit la version nationale du moteur de recherche utilisée, accéder, dans le cadre d'une recherche effectuée à partir d'une adresse IP réputée localisée dans l'État membre de résidence du bénéficiaire du droit au déréférencement ou, plus largement, dans un État membre, aux liens concernés par le déréférencement ».

2 | Les apports de la décision

La difficulté à laquelle la Cour a été confrontée tient, d'une part, au fait qu'Internet est un « réseau mondial sans frontières » et comme le précise la Cour en s'appuyant sur la jurisprudence Google Spain, « les moteurs de recherche confèrent un caractère ubiquitaire aux informations et aux liens contenus dans une liste de résultats affichée à la suite d'une recherche effectuée à partir du nom d'une personne physique » et d'autre part, que « de nombreux États tiers ne connaissent pas le droit au déréférencement ou adoptent une approche différente de ce droit ».

2.1. Le droit au déréférencement peut s'appliquer à l'ensemble des pays de l'Union européenne, en application d'une législation harmonisée sur ces questions ...

Sur le point de savoir si le déréférencement doit s'opérer uniquement pour la version de Google correspondant à l'État membre dans lequel la demande de déréférencement a été introduite ou s'il doit s'opérer pour les versions de Google de tous les États membres, la Cour répond que l'objectif de la directive 95/46 et du RGPD est d'harmoniser la protection des données personnelles dans l'ensemble de l'Union et partant, « le déréférencement en cause est, en principe, censé être opéré pour l'ensemble des États membres »³.

La Cour conclut alors que « lorsque l'exploitant d'un moteur de recherche fait droit à une demande de déréférencement en application de ces dispositions, il est **tenu d'opérer ce déréférencement non pas sur l'ensemble des versions de son moteur, mais sur les versions de celui-ci correspondant à l'ensemble des États membres** »⁴.

En revanche, le législateur européen n'a pas choisi de conférer aux droits ainsi consacrés une portée excédant le territoire de l'Union⁵ et dès lors, « en l'état actuel, il n'existe [...] **pas d'obligation découlant du droit de l'Union de procéder à un tel déréférencement sur l'ensemble des versions [du] moteur [de Google]** »⁶.

La Cour interpelle toutefois Google sur le fait que si cela est nécessaire, au-delà du déréférencement, des mesures efficaces empêchant l'accès aux résultats de recherche ou de nature à « sérieusement décourager » les internautes effectuant la recherche sur la base du nom de la personne concernée doivent être mises en place.

2.2. ...mais la possibilité d'un déréférencement mondial reste envisageable *via* les autorités de contrôle nationales

La Cour précise cependant que « *si [...] le droit de l'Union n'impose pas, en l'état actuel, que le déréférencement auquel il serait fait droit porte sur l'ensemble des versions du moteur de recherche en cause, il ne l'interdit pas non plus* »⁷.

Conformément à l'article 9 de la directive 95/46 et à l'article 85 du RGPD, les juges européens renvoient aux autorités de contrôle ou aux autorités judiciaires des États membres le soin d'effectuer une mise en balance entre le droit de la personne demandant le déréférencement et le droit à la liberté d'information « *pour enjoindre, le cas échéant, à l'exploitant de ce moteur de recherche de procéder à un déréférencement portant sur l'ensemble des versions dudit moteur* »⁸.

Ainsi, la CNIL souligne, en réaction à cette décision, « une autorité de contrôle, et donc la CNIL, est compétente pour obliger un moteur de recherche à déréférencer les résultats sur toutes les versions de son moteur si cela est justifié, dans certains cas, pour garantir les droits de la personne concernée »⁹.

Il appartient désormais au Conseil d'État d'apprécier si les demandes de la Cnil étaient justifiées et proportionnées et si les modifications apportées par Google à son moteur de recherche depuis 2016 sont suffisantes.

¹ « 1. La personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:

- a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;
- b) la personne concernée retire le consentement sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement;
- c) la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;
- d) les données à caractère personnel ont fait l'objet d'un traitement illicite;
- e) les données à caractère personnel doivent être effacées pour respecter une obligation légale qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;
- f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.

2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre

d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou
e) à la constatation, à l'exercice ou à la défense de droits en justice. »

² Article 20 de la loi n°78-17 du 6 janvier 1978 : « I.- Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable de traitement ou son sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi.

II.- Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, si le manquement constaté est susceptible de faire l'objet d'une mise en conformité, prononcer à son égard une mise en demeure, dans le délai qu'il fixe :

1° De satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;

2° De mettre les opérations de traitement en conformité avec les dispositions applicables ;

3° A l'exception des traitements qui intéressent la sûreté de l'État ou la défense, de communiquer à la personne concernée une violation de données à caractère personnel ;

4° De rectifier ou d'effacer des données à caractère personnel, ou de limiter le traitement de ces données.

Dans le cas prévu au 4° du présent II, le président peut, dans les mêmes conditions, mettre en demeure le responsable de traitement ou son sous-traitant de notifier aux destinataires des données les mesures qu'il a prises.

Le délai de mise en conformité peut être fixé à vingt-quatre heures en cas d'extrême urgence.

Le président prononce, le cas échéant, la clôture de la procédure de mise en demeure.

Le président peut demander au bureau de rendre publique la mise en demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l'objet de la même publicité.

III.- Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes :

1° Un rappel à l'ordre ;

2° Une injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du 27 avril 2016 ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en oeuvre par l'État, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ;

3° A l'exception des traitements qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en oeuvre pour le compte de l'État, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du même règlement ou de la présente loi ;

4° Le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;

5° A l'exception des traitements qui intéressent la sûreté de l'État ou la défense ou de ceux relevant du titre III de la présente loi lorsqu'ils sont mis en oeuvre pour le compte de l'État, la suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;

6° La suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes ;

7° A l'exception des cas où le traitement est mis en oeuvre par l'État, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du 27 avril 2016, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

Le projet de mesure est, le cas échéant, soumis aux autres autorités de contrôle concernées selon les modalités définies à l'article 60 du même règlement.

³ Point 66 de l'arrêt.

⁴ Point 73 de l'arrêt.

⁵ Point 62 de l'arrêt.

⁶ Point 64 de l'arrêt.

⁷ Point 72 de l'arrêt.

⁸ Point 73 de l'arrêt.

⁹ <https://www.cnil.fr/fr/droit-au-dereferencement-la-cjue-rendu-ses-arrets>