Moteurs de recherche, déréférencement, oubli et vie privée en droit québécois

Pierre Trudel*

Par leur activité, les moteurs de recherche tout comme d'autres fonctions d'Internet génèrent des risques pour les internautes.
Nous examinons ici la responsabilité des moteurs de recherche en droit québécois de même que les principaux enjeux que ceux-ci peuvent poser au regard du respect de la vie privée.
Le droit québécois organise la responsabilité du moteur de recherche en ce qui a trait aux résultats livrés par celui-ci. La responsabilité du moteur de recherche en droit québécois est conditionnelle à la connaissance du caractère illicite du document référencé.
Les moteurs de recherche soulèvent aussi des enjeux relatifs à la vie privée des personnes. Les personnes concernées par les renseignements que peut repérer le moteur de recherche sont en effet concernées par les résultats sous forme de liens hypertextes que peuvent livrer les moteurs de recherche. C'est sur cet aspect que s'est penchée la Cour de justice de l'Union européenne dans son arrêt de mai 2014.
Mais les moteurs de recherche impliquent aussi d'importants enjeux au regard de la compilation d'information relative aux faits et gestes de leurs usagers.

Through their activity, search engines, like other Internet functions, generate risks for internet users.
Here, we examine the responsibility of search engines in Québec law and the primary stakes that they can raise with respect to privacy.
Québec law structures the responsibility of search engines in accordance with the outcomes they deliver. The responsibility of a search engine in Québec law is conditional on knowledge of the illicit nature of the document linked.
Search engines also raise issues concerning people's privacy. People concerned by information that a search engine can find are in fact concerned by the results in the form of hypertext links that search engines can deliver. It is on this aspect that the European Union Court of Justice focussed in its May 2014 judgment.
However, search engines also involve major stakes with regard to compilation of information on users' deeds and actions. Given their role as the functional equivalent of librarians, it is proposed that they be recognized as having a duty of confidentiality with respect to all user-related information of which they are made aware.

* Professeur titulaire, Centre de recherche en droit public, Faculté de droit, Université de Montréal, < www.pierretrudel.net >.

Étant donné leur rôle d'équivalent fonctionnel des bibliothécaires, il est proposé de leur reconnaître un devoir de confidentialité à l'égard de toutes les informations émanant de leurs usagers qui sont portées à leur connaissance.

Moteurs de recherche, déréférencement, oubli et vie privée en droit québécois

Pierre Trudel

INTRODUCTION

Internet permet d'accéder à des ressources portant sur une multitude de sujets. Mais sans des outils performants afin de repérer les informations pertinentes aux questions que l'on se pose, le réseau demeure un amas d'informations pratiquement inaccessibles[1]. Le défi est de départager, dans l'immense masse d'informations en ligne, celles qui sont pertinentes pour chacun des internautes.

Compte tenu de l'ubiquité du réseau et du fait que la quasi-totalité des informations disponibles sont susceptibles de s'y retrouver, il est apparu très tôt que l'usage d'Internet n'est en pratique possible que moyennant la disponibilité d'outils capables d'identifier rapidement l'information qui intéresse l'internaute : les moteurs de recherche.

Mais les règles encadrant l'activité de ces acteurs pourtant cruciaux d'Internet demeurent incertaines. Compte tenu de leur rôle central dans le fonctionnement du réseau, les moteurs de recherche sont au cœur de plusieurs controverses.

Les moteurs de recherche agglomèrent des informations sur les personnes ou sur les diverses entités à propos desquelles on peut formuler une requête de recherche exprimée habituellement sous forme de mots-clés. Ils permettent de localiser l'in-

1. Frank A. pasquale III et Oren Bracha, Federal Search Commission ? : Access, Fairness and Accountability in the Law of Search, University of Texas, School of Law, Public and Legal Theory Research Paper no 123, July 2007, p. 4; Laurent Caron, « Protection des données personnelles et moteurs de recherche : quels sont les réels enjeux ? », Légipresse, no 244, septembre 2007, p. 111; Jayni Foley, « Are Google Searches Private ? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases », 22 Berkeley Tech L.J. 2007, 447-475; James Grimmelmann, « The Structure of Search Engine Law », 93 Iowa L. Rev. 1 (2007); Eric Goldman, « Search Engine Bias and the Demise of Search Engine Utopianism », (2005-2006) Yale Journal of Law & Technology 111-123.

formation en délivrant à l'utilisateur des documents ou des liens à des documents qui sont le plus pertinents possibles eu égard à sa requête.

Les informations sont repérées dans des espaces virtuels; elles sont en principe publiques. Par leur efficacité, les moteurs de recherche contribuent puissamment à réduire les phénomènes d'«obscurité pratique » qui rendent souvent difficiles l'accès et la compilation d'un ensemble de documents portant sur une personne ou sur un sujet déterminé.

Il n'en faut pas plus pour amener certains à les considérer comme des entités qui effectuent des traitements d'informations portant sur des personnes. Au nom d'une conception étendue de la vie privée, on réclame de censurer les moteurs de recherche en accordant aux personnes un droit de revendiquer l'effacement de résultats de recherche relatifs à des documents disponibles en ligne qui sont pourtant en conformité avec les lois.

Dans sa décision Google Spain,[2] la Cour de justice de l'Union européenne déclarait en mai 2014 que le moteur de recherche Google traite des informations personnelles lorsqu'il donne suite à une requête de recherche comportant des mots qui correspondent au nom d'une personne, les interrogations sur le statut de ces ressources majeures d'Internet prennent de l'importance. La Cour a décidé qu'un individu vivant en Europe peut exiger que Google (et les autres moteurs de recherche) suppriment des listes de résultats, ceux qui comportent son nom et qu'il estime préjudiciables[3].

Dans la plupart des pays de même que dans les discussions internationales, on constate des différences d'appréciation sur le statut des moteurs de recherche. Tous conviennent que les moteurs de recherche tiennent une place incontournable dans l'Internet actuel. Tous reconnaissent que les moteurs de recherche sont en position d'influer radicalement sur les choix qui sont faits par les internautes. Mais on ne s'entend pas sur la nature des moteurs de recherche et du coup, sur les encadrements réglementaires dont ils pourraient faire l'objet.

La qualification juridique des moteurs de recherche est controversée. Les auteurs ont exprimé des visions passablement différentes à cet égard[4]. Selon les points de vues et surtout les intérêts de ceux qui prennent position, on tend à qualifier les moteurs de recherche en insistant sur un aspect de leur activité. On peut identifier

2. Google Spain SL, Google Inc. c.Agencia Española de Protección de Datos (AEPD), Mario Costeja González, arrêt du 13 mai 2014, en ligne : <http://curia.europa.eu/juris/document/document.jsf?docid =152065&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=253040 >.

3. Geneviève saint-laurent, « Vie privée et 'droit à l'oubli' : que fait le Canada ? », [2015] 66 UNB L.J., 185-197; Saminda Pathmasiri, « L'Internet n'oublie jamais ! dit-on. Est-ce toujours vrai ? » Développements récents en droit du divertissement (2015), Service de la formation continue du Barreau du Québec, 2015.

4. James Grimmelman, « Speech Engines », (2014) 98 Minn. L. Rev. 868, p. 871.

au moins trois dimensions des activités des moteurs de recherche qui conduisent à des qualifications contrastées de leur activité et de leur statut.

D'abord, du point de vue des propriétaires de sites web, c'est un conduit qui doit être le plus «neutre possible ». Il faut éviter que les moteurs de recherche génèrent des résultats qui favoriseraient l'entreprise qui possède le moteur au détriment de ses concurrents[5]. Ce type de préoccupation s'exprime notamment en Europe à l'égard de Google que certains soupçonnent de favoriser ses propres sites dans l'agencement des résultats de recherche et autres services qu'il offre[6].

Puis examiné du point de vue du moteur de recherche lui-même, c'est une entreprise qui exprime une opinion sur la pertinence des liens eu égard à une requête de recherche. D'où la tendance à le traiter comme un éditeur, titulaire d'une faculté d'appréciation semblable à l'éditeur de presse[7].

Enfin, envisagé du point de vue des usagers, le moteur de recherche est un « aviseur » procurant une opinion sur la pertinence des sites comportant les mots-clés introduits par le chercheur[8]. Du point de vue d'un usager, la confiance de même que la qualité des résultats de recherche sont des enjeux très importants.

La décision Google Spain de la Cour de justice de l'Union européenne insiste sur l'une des dimensions de l'activité des moteurs de recherche : soit le fait qu'ils peuvent, selon les requêtes introduites par des usagers, avoir à générer des résultats de recherche portant sur une personne. Appliquant une interprétation très étendue de la notion de « traitement de données personnelles », la Cour a statué que dans de telles situations, les moteurs de recherche se trouvent à « traiter » des informations personnelles au sens de la réglementation européenne.

Ainsi, selon le raisonnement sous-jacent à cet arrêt, introduire une requête de recherche avec les mots « rose » et « petit » emporte un traitement de données personnelles par le moteur de recherche s'il se trouve à exister en ligne des documents relatifs à une personne ayant pour nom « Rose Petit ».

La régulation des moteurs de recherche peut s'envisager dans la perspective de la gestion en réseau de l'ensemble des risques associés aux activités de recherche sur Internet. Sur Internet, la régulation s'applique en réseau et selon un mode réseautique, elle est pensée et produite dans les nœuds de normativité d'Internet que sont

5. Jennifer A. Chandler, « A Right to Reach an Audience : An Approach to Intermediary Bias on the Internet », (2007) 35 Hofstra L. Rev., 1095; Frank Pasquale, « Rankings Reductionism, and Responsibility », (2006) 54 Clev. St. L. Rev., 115.

6. Lisa Mays, « The Consequences of Search Bias: How Application of the Essential Facilities Doctrine Remedies Google's Unrestricted Monopoly on Search in the United States and Europe », (2015) 83 George Washington Law Rev., 721.

7. Eric Goldman, « Search Engine Bias and the Demise of Search Engine Utopianism », Yale Journal of Law & Technology, (2005-2006); Eugeve Volokh & Donald M. Flak, « Google First Amendment Protection for Search Engine Search Results », (2012) 8 J. L. Econ. & Pol'y 883.

8. James Grimmelman, « Speech Engines », (2014) 98 Minn. L. Rev. 868, p. 874.

les instances étatiques, les lieux de conception des normes techniques de même que les différents acteurs. Ces derniers relaient à leurs partenaires les exigences et les risques qu'ils ont à gérer. Ainsi envisagée, la régulation des moteurs de recherche sur Internet est essentiellement une démarche continue de prise en compte et de gestion des risques perçus à l'égard des activités de recherche[9].

Par leur configuration, leurs pratiques et les technologies qu'ils utilisent, les moteurs de recherche génèrent des risques pour les utilisateurs de même que pour les personnes concernées par les informations repérées et communiquées. Ces risques se présentent comme une « normativité par défaut » : les activités mêmes génèrent des risques. Parmi les risques générés par les moteurs, certains emportent des conséquences juridiques. Par exemple, l'accumulation et le stockage de données relatives aux requêtes de recherche des usagers emportent la constitution de répertoires d'informations personnelles qui peuvent devenir disponibles aux forces de police désireuses d'y accéder dans le cadre de leurs enquêtes.

Dans ce texte, nous exposons l'état du droit applicable au Québec au regard de la responsabilité des moteurs de recherche pour les résultats livrés à la suite d'une requête de recherche. Dans la seconde partie, certaines revendications tendant à censurer les résultats de recherche sont exposées, notamment le droit au déréférencement tel que reconnu en droit européen suite à l'arrêt Google Spain.

Enfin, il est fait état des enjeux que posent les moteurs de recherche au regard de la vie privée du chercheur d'information lui-même. Il s'agit là d'enjeux de transparence et de libertés fondamentales qui paraissent infiniment plus évidents que le désir de certains de faire censurer des liens vers des documents publics. Au regard des moteurs de recherche, les véritables enjeux de transparence et de protection de la vie privée ne sont pas d'occulter des informations publiques licites, mais plutôt de protéger la vie privée et la dignité des personnes, notamment contre les fouilles abusives.

1. La responsabilité des moteurs de recherche en droit québécois

En droit québécois, la responsabilité des moteurs de recherche pour les résultats qu'ils livrent à l'usager en réponse à une requête de recherche découle des principes du droit commun et de l'article 22 de la Loi concernant le cadre juridique des technologies de l'information[10].

9. Pierre Trudel, « La régulation du web 2.0 », (2008) 32 RDTI 283-307.

10. RLRQ, chapitre C-1.1. Voir : Pierre Trudel, Introduction à la Loi concernant le cadre juridique des technologies de l'information, Cowansville, Éditions Yvon Blais, 2012.

1.1. Les moteurs de recherche en tant que générateurs de liens hypertextes

Lorsqu'ils génèrent des liens hypertextes, les moteurs de recherche, comme les autres sites, nede sont pas a priori responsables des informations vers lesquelles conduit un lien. Dans Crookes c. Newton[11], la Cour suprême du Canada a examiné la question de savoir si l'incorporation dans un texte d'hyperliens menant à des propos prétendument diffamatoires équivaut à la « diffusion » de ces derniers.

Selon les six juges majoritaires de la Cour, une personne ne peut en diffamer une autre simplement en publiant un hyperlien menant au site Web ou à un document d'un tiers qui contient des propos diffamatoires : la juge en chef McLachlin et le juge Fish expliquent qu'« […] un hyperlien, en lui-même, ne devrait jamais être assimilé à la "diffusion" du contenu auquel il renvoie »[12]. Ils souscrivent à l'analyse de la Juge Abella qui écrit que : « Le fait de mentionner l'existence d'un contenu et/ou l'endroit où il se trouve par le biais d'un hyperlien ou de toute autre façon, sans plus, ne revient pas à le diffuser »[13].

Les juges majoritaires estiment que les hyperliens s'apparentent aux notes de bas de page d'un document papier. Si l'hyperlien offre, contrairement aux notes de bas de page, un accès immédiat au site Web d'un tiers auquel il renvoie, les lecteurs n'en savent pas moins que ce lien les mènera à une source différente.

Par contre, la majorité des juges se sont expressément abstenus de déterminer si cette conclusion devait être différente dans le cas des liens imbriqués ou automatiques.

Or, les moteurs de recherche génèrent bien des liens hypertextes en appliquant des algorithmes. Ces algorithmes fonctionnent de façon hautement automatisée, en des temps s'exprimant en fractions de secondes. Pour y arriver, ces algorithmes[14] analysent des masses considérables de données incluant notamment des données sur le contexte dans lequel se trouve la personne qui introduit la requête de recherche, son historique de recherche, sa position géographique etc.

Par contre, du fait du caractère contextuel de ce traitement, il paraît impossible de postuler que l'introduction des mêmes mots dans des requêtes de recherche lancées en différents points du réseau va forcément générer les mêmes résultats.

On peut même se demander si le type de résultats qu'obtient un individu en introduisant son propre nom dans une requête de recherche sera identique à celui ob-

11. [2011] 3 RCS 269.

12. Au paragraphe 47 de la décision.

13. Au paragraphe 42 de la décision.

14. Un algorithme est un ensemble d'instructions donné à un ordinateur permettant d'obtenir un résultat en effectuant des calculs. Voir : Seema Ghatnekar, « Injury by Algorithm », (2012-2013) 33 Loy. L.A. Ent. L. Rev. 171.

tenu par une autre personne se trouvant dans un contexte donnant à penser qu'elle a des intérêts éloignés de ceux de la première personne.

Mais selon le droit québécois, qu'ils soient générés automatiquement ou mis en ligne par décision humaine spécifique, les hyperliens sont régis par les règles énoncées à l'article 22 de la Loi concernant le cadre juridique des technologies de l'information.

1.2. La responsabilité fondée sur la connaissance du caractère illicite du document vers lequel pointe l'hyperlien

En droit québécois, les moteurs de recherche sont régis par un régime de responsabilité fondé sur la connaissance du caractère illicite du document vers lequel ils pointent.

Le principe posé au troisième alinéa de l'article 22 de la Loi concernant le cadre juridique des technologies de l'information est que le moteur de recherche n'est pas responsable des activités accomplies par la personne utilisant le service. La disposition se lit comme suit :

> [...] le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services. Toutefois, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité.

Cette exonération de responsabilité tient jusqu'à ce que le prestataire ait de fait connaissance du caractère illicite et qu'il ne prend pas promptement les moyens pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.

L'article 22 de la Loi concernant le cadre juridique des technologies de l'information pose la règle de la non-responsabilité de ces prestataires de services, mais cette limitation de responsabilité cesse d'avoir effet si certains faits sont établis. Et une fois ces faits établis, s'ouvre la possibilité que la responsabilité de l'intermédiaire soit engagée. C'est donc bien d'une responsabilité secondaire qu'il s'agit puisque tant que la condition de la connaissance n'est pas accomplie, il n'y a pas de responsabilité du prestataire.

Ce régime de responsabilité reflète celui qui est appliqué dans les juridictions de Common law canadienne. Ainsi, dans Equustek Solutions Inc. v. Google Inc.[15], la

15. Equustek Solutions Inc. v. Google Inc., 2015 BCCA 265 (CanLII), en ligne : <http://canlii.ca/t/gjgwv> (consulté le 13 avril 2016). La Cour suprême du Canada a accepté d'entendre l'appel

Cour d'appel de Colombie-Britannique a reconnu le bien-fondé d'une ordonnance d'injonction enjoignant Google de supprimer des résultats de recherche les liens conduisant à des sites qui ont été jugés comme contrevenant à la loi canadienne.

Les éléments requis pour que la responsabilité du moteur de recherche soit engagée sont la connaissance du caractère illicite ou de circonstances le rendant apparent.

Lorsqu'ils acquièrent connaissance du caractère illicite de l'activité associée aux documents auxquels ils donnent accès, les prestataires offrant des services de moteurs de recherche ont l'obligation d'agir. Le facteur qui déclenche leur responsabilité est la connaissance qu'ils ont ou qu'ils acquièrent de la nature délictueuse de l'information. Ce n'est toutefois pas la seule situation où la responsabilité de ces prestataires peut être engagée. L'article 22 de la Loi concernant le cadre juridique des technologies de l'information ne constitue pas une liste exhaustive des situations dans lesquelles un prestataire qui y est visé peut engager sa responsabilité. L'article 22 al. 2 énonce que le prestataire « peut engager sa responsabilité », « notamment s'il a de fait connaissance ». La même formule est reprise au troisième alinéa lorsqu'il est question des prestataires offrant des outils de recherche[16].

L'article 22 précise que la responsabilité concerne les propos ou les documents ou activités illicites.

Dans le Robert, on définit le mot «illicite» comme étant « […] ce qui est défendu par la morale ou par la loi »[17]. Jean Deliyannis considère comme illicite « Tout acte contraire aux principes même de l'ordre juridique, à savoir tout acte injuste, ou

de cette décision : Google Inc. v. Equustek Solutions Inc., et al., 2016 CanLII 7602 (SCC), en ligne : <http://canlii.ca/t/gndmt> (consulté le 13 avril 2016).

16. Voir : Nicolas W. Vermeys, Droit codifié et nouvelles technologies : le Code civil, Cowansville Éditions Yvon Blais, 2015, pp. 129 et ss.; Patrick Gingras et Nicolas W. Vermeys, Actes illicites sur Internet : qui et comment poursuivre, Cowansville, Éditions Yvon Blais, 2011, p. 38; Nicolas W. Vermeys, La responsabilité civile des prestateurs de moteurs de recherches et des fournisseurs d'hyperliens en droit québécois, (2005) 10 /1 Lex Electronica, <http://www.lex-electronica.org/articles/vol10/num1/la-responsabilite-civile-des-prestateurs-de-moteurs-de-recherches-et-des-fournisseurs-dhyperliens-en-droit-quebecois/>; Pierre Trudel, « La responsabilité des acteurs du commerce électronique », dans Vincent Gautrais (dir.), Droit du commerce électronique, Montréal, Éditions Thémis, 2002, p. 607-649; Pierre TRUDEL, Introduction à la Loi concernant le cadre juridique des technologies de l'information, Cowansville Éditions Yvon Blais, 2012, c. 7; Pierre Trudel, « Les responsabilités dans le cyberespace », dans Les dimensions internationales du droit du cyberespace, collection Droit du cyberespace, Paris, Éditions UNESCO - Economica, 2000, 235-269; Pierre Trudel, « La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information », dans Formation permanente, Barreau du Québec, Développements récents en droit de l'Internet, n° 160, Cowansville, Éditions Yvon Blais, 2001, p. 107-141.

17. Paul Robert, Dictionnaire alphabétique et analogique de la langue française, Paris, Société du nouveau Littré, 2015.

simplement antisocial […] même s'il n'est pas interdit formellement par la loi »[18]. Mais cet auteur ajoute qu'en tant qu'élément de la faute (au sens de la loi), on ne peut donner à la notion d'illicite une telle ampleur que cela irait même jusqu'à viser des gestes qui ne suscitent pas de réprobation[19].

Or, la notion de réprobation doit s'apprécier dans un environnement dans lequel la liberté d'expression tient une place importante. Dans les sociétés démocratiques, la liberté d'expression protège même les propos qui peuvent susciter la réprobation. C'est pourquoi on en revient au critère du propos qui est contraire à la Loi. Comme c'est la loi et seulement la loi qui au Canada peut imposer des limites à la liberté d'expression[20], il faut se fonder sur celle-ci pour déterminer si un propos ou une information ou une activité est illicite au sens de l'article 22 de la Loi concernant le cadre juridique des technologies de l'information.

1.2.1. La connaissance de fait

En tant qu'intermédiaires visés à l'article 22 de la Loi concernant le cadre juridique des technologies de l'information, la responsabilité des moteurs de recherche peut être engagée s'il est établi qu'ils avaient connaissance de fait du caractère illicite des activités accomplies par l'utilisateur du service au moyen de documents technologiques.

En raison de la règle énoncée à l'article 27 de cette même loi, excluant l'obligation de surveillance active, on ne peut déduire une faute de leur part en raison d'une omission de surveiller. Par conséquent, on conçoit mal que ces intermédiaires soient considérés comme ayant connaissance de la teneur des documents du seul fait que ceux-ci sont identifiés comme pertinents dans le contexte d'une requête fondée sur des mots-clés. Ils n'acquièrent connaissance que lorsqu'on leur notifie l'existence d'une activité à caractère illicite ou encore qu'on leur fait part de circonstances rendant apparente une activité illicite.

En vertu de la législation québécoise, étant donné la disposition législative explicite ci-haut mentionnée[21] selon laquelle ils n'ont pas d'obligation de surveiller, il est logiquement impossible de considérer que les moteurs de recherche effectuent un « traitement » de données personnelles qui pourrait découler de l'introduction de

18. Jean Deliyannis, La notion d'acte illicite, considéré en sa qualité d'élément de la faute délictuelle, Paris, Paris, Librairie générale de droit et de jurisprudence, 1952, p. 328.

19. Ibid., p. 329.

20. Il faut rappeler que l'article premier de la Charte canadienne des droits et libertés énonce que : « La Charte canadienne des droits et libertés garantit les droits et libertés qui y sont énoncés. Ils ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique. » Charte canadienne des droits et libertés, Partie 1 de la Loi constitutionnelle de 1982, annexe B de la Loi de 1982 sur le Canada, 1982, ch. 11 (R.U.), (soulignés ajoutés).

21. Loi concernant le cadre juridique des technologies de l'information, art. 27.

mots qui s'avèreraient correspondre au nom d'une personne. Tout au plus, ils pourraient avoir une responsabilité suite à l'introduction de tels mots s'ils ont connaissance du caractère illicite du document référencé.

De plus, contrairement au droit européen, les lois canadiennes sur la protection des renseignements personnels ne retiennent pas la notion de « traitement ». Les lois canadiennes régissent la collecte, l'utilisation et la communication de renseignements personnels. Pour constituer une collecte au sens de ces lois, il faut que l'entité ait au minimum une connaissance de la teneur et du sens des renseignements sur lesquels il acquiert ainsi le contrôle[22].

La connaissance pourra être imputée dans certaines circonstances. Ainsi, elle est présumée dès lors que l'information émane de la personne elle-même ou que cette dernière a effectivement pris la décision de diffuser. Le moteur de recherche qui choisit expressément de diffuser de l'information qui émane de lui-même, répond évidemment de celle-ci.

Un moteur de recherche peut avoir connaissance de fait s'il exerce une surveillance, constante ou occasionnelle, des documents référencés et que cette surveillance donne lieu à l'identification d'un document illicite. Mais il n'y a pas d'obligation de surveiller afin d'acquérir connaissance aussitôt que se pointeront des documents illicites. Si une telle surveillance est effectuée et qu'elle permet d'acquérir la connaissance du caractère illicite de documents, alors la responsabilité du moteur de recherche pourra être engagée s'il n'agit pas.

La connaissance peut concerner les circonstances rendant apparente une activité illicite. Une telle connaissance peut découler d'indices venant à la connaissance du prestataire et donnant à conclure à l'existence d'une activité illicite.

La connaissance peut aussi être acquise à la suite d'une notification de la part d'un tiers. C'est la situation dans laquelle une personne porte à l'attention du prestataire de services de moteur de recherche le fait que des documents illicites sont conservés par lui.

Enfin, lorsque le caractère illicite du document visé est matière à controverse, l'obligation d'agir du prestataire d'outil de recherche ne commencera qu'à compter du moment où le caractère illicite du document vers lequel pointent les résultats de recherche aura été effectivement établi.

Au surplus, le prestataire de pareils services est souvent dépourvu d'un motif légitime pour intervenir afin de supprimer des liens vers de l'information potentiellement dommageable. Hormis les cas absolument clairs d'illicéité, au nom de quoi et en vertu de quelle autorité doit-il juger du caractère illicite ou non de telle ou telle

22. Pour pouvoir collecter et conserver des documents contenant des renseignements personnels, il faut au minimum acquérir le contrôle sur ceux-ci. Sur cette question voir : Vincent Gautrais et Pierre Trudel, Circulation des renseignements personnels et Web 2.0, Montréal, Éditions Thémis, 2010, p. 59 et s.

information ? En vertu de quelle autorité devrait-il s'ériger en juge chargé de déterminer si un contenu est ou non fautif et dommageable ?

1.2.2. Le degré de connaissance requis pour engendrer la responsabilité

Les points de vue peuvent diverger quant au degré de connaissance nécessaire pour entraîner la responsabilité du prestataire de services. Strowel et Ide font observer que « toute la question est de savoir comment définir ce seuil de connaissance à partir duquel la responsabilité joue pleinement »[23]. Compte tenu des impératifs de la liberté d'expression, le seuil de connaissance à partir duquel la responsabilité de l'intermédiaire est engagée doit être plus que la seule plainte ou allégation. Pour qu'une personne soit justifiée d'intervenir à l'égard d'un contenu, elle doit avoir acquis la connaissance confirmée du caractère effectivement illicite du document. La connaissance à partir de laquelle est engendrée la responsabilité n'est pas celle qui résulte de la seule réception d'une plainte ou d'un simple soupçon, mais vise plutôt le moment où le caractère illicite devient manifeste. C'est ce qui permet de dire que lorsque le caractère illicite est, à sa face même, manifeste, la connaissance en est acquise dès le moment où l'on apprend l'existence du document.

Dans les cas clairs, s'il en est, la question trouve une réponse aisée : si le caractère illicite saute aux yeux, l'intermédiaire pourra devoir agir dès la réception d'une plainte. Mais que faire dans les situations où le caractère illicite n'est pas évident ? Par exemple, un moteur de recherche reçoit une notification à l'effet que tel document vers lequel pointent des résultats de recherche comporte des informations portant atteinte au droit à l'image d'une personne. Or, on sait qu'il y a plusieurs situations où la diffusion de l'image d'une personne est tout à fait licite. S'il obtempère et supprime le lien vers le document, il s'érige en juge mais en juge n'ayant pas agi moyennant l'élémentaire obligation d'entendre les prétentions de toutes les parties en cause. Il peut se faire reprocher par le maître de l'information référencée, de n'avoir pas pris les précautions élémentaires pour s'assurer du caractère sérieux de la notification. S'il ne fait rien, l'intermédiaire s'expose à voir sa responsabilité engagée et à devoir en répondre lors d'une poursuite de la part de la victime.

Le législateur québécois n'ayant rien précisé quant aux précautions à prendre consécutivement à la réception d'un avis à l'effet qu'un site référencé est illicite, faut-il en conclure qu'il n'y aurait pas d'obligation à cet égard ? Une réponse négative doit être apportée à cette question. La responsabilité du moteur de recherche pourra être engagée si celui-ci obtempère à une notification sans prendre des précautions minimales. La personne qui verrait des documents bannis d'un système d'indexation pourrait assurément subir des dommages du fait d'une allégation non fondée à l'effet

23. Alain Strowel et Nicolas Ide, « Responsabilités des intermédiaires : actualités législatives et jurisprudentielles », dans Droit Nouvelles technologies, en ligne : < http://www.droit-technologie. org/dossier-26/responsabilite-des-intermediaires-actualites-legislatives-et-jurispru.html >, visité le 14 avril 2016.

qu'un document est illicite. Se posera alors la question de déterminer si l'intermédiaire a agi avec la prudence et pris les précautions qu'une personne raisonnable aurait dû prendre en de telles circonstances. Si la notification se révèle futile ou mal fondée, on aurait supprimé sans motifs valables un lien vers un contenu, violé la liberté d'expression et fait prévaloir les désirs, voire les lubies d'un plaignant, au préjudice d'une application prudente d'une mesure qui constitue de la censure, donc qui a par essence un caractère exceptionnel. Gingras et Vermeys observent à juste titre que l'intermédiaire n'est pas contractuellement tenu de référencer ou même, dans certains cas, d'héberger[24]. Mais cela n'empêche pas de tenir pour acquis que ces intermédiaires ont un devoir de prudence lorsqu'il s'agit de supprimer des informations de leurs environnements.

L'enjeu est donc ici de déterminer ce qu'il faut établir afin de pouvoir considérer que l'intermédiaire a eu une attitude raisonnable. Il ne s'agit pas pour ce dernier de décider lui-même si le matériel visé par une notification est effectivement illicite, mais plutôt de déterminer si une personne raisonnable aurait pu considérer que ce matériel est ou n'est pas illicite.

Dans une telle situation, l'attitude appropriée pour l'intermédiaire est d'obtenir une confirmation d'un tiers, tel un expert neutre, et d'agir sur la foi d'une telle évaluation. Car la connaissance de fait ne peut commencer qu'à compter du moment où la plainte à l'égard d'un document est suffisamment documentée pour écarter les doutes raisonnables quant à son sérieux. Cette approche est compatible avec une conception respectueuse de la liberté d'expression et du droit du public à l'information. On voit mal en vertu de quel principe il faudrait prendre pour avéré en tout temps les prétentions d'une personne qui se plaint d'un document, sans prendre au moins la précaution de vérifier si le document serait considéré comme illicite par une personne raisonnable. La censure aurait alors lieu sans un examen sérieux des prétentions à l'effet qu'un document est illicite. Il serait étonnant que le législateur québécois ait opté pour une pratique se conciliant si mal avec les principes d'une société démocratique.

Par conséquent, tant que l'intermédiaire n'a pas obtenu une confirmation indépendante du caractère illicite d'un document, il n'a pas d'obligation d'agir de manière à censurer l'information. S'il le fait, il s'expose à commettre une faute à l'égard de celui qui a publié le document. Ainsi, l'intermédiaire n'a connaissance du caractère illicite de l'information ou du document qu'une fois qu'il a été en mesure d'établir le sérieux d'une plainte ou d'une notification. C'est uniquement à compter de ce moment qu'il a l'obligation d'agir promptement.

Raisonner autrement reviendrait à conférer à toute personne se croyant lésée par un document un pouvoir de censure préalable, sans intervention d'un tiers en mesure de faire le départage des prétentions.

24. Patrick Gingras et Nicolas Vermeys, Actes illicites sur Internet : qui et comment poursuivre ?, Cowansville, Éditions Yvon Blais, 2011, p. 39.

Un moteur de recherche est en droit de supprimer une information qu'une fois établi son caractère illicite. Il serait absurde que le législateur ait formulé une règle de droit permettant à n'importe qui d'obtenir, par simple plainte, le retrait d'une information qui lui déplaît ou qu'il juge nuisible. Ce qui est visé par la disposition de la Loi est l'information illicite. Pour qu'une plainte soit sérieuse, elle doit démontrer des motifs sérieux donnant à conclure au caractère illicite du document visé et non résulter d'une demande arbitraire, vengeresse ou futile. Pour conclure au sérieux de la plainte, l'intermédiaire qui entretient des doutes à cet égard sera avisé d'obtenir une confirmation indépendante.

L'objet de la confirmation indépendante, lorsqu'un intermédiaire demande à être éclairé sur le caractère illicite d'un document se trouvant dans ses installations, n'est pas de déterminer si le document est effectivement illicite, mais plutôt de déterminer s'il est raisonnablement possible qu'un tribunal, convenablement informé, en vienne à la conclusion que le document visé par une notification est effectivement illicite. En somme l'objet de l'analyse n'est pas de décider si le document est illicite. Il s'agit plutôt d'évaluer si le document peut être considéré comme illicite par une personne raisonnable qui, convenablement informée, en ferait l'évaluation dans un contexte judiciaire. Ainsi, l'évaluation devra notamment déterminer à quelle règle de droit le document pourrait contrevenir. Une telle solution évite une approche de censure préalable des liens vers des documents comportant des informations qui pourraient déplaire à certains.

1.2.3. L'obligation de cesser promptement de fournir ses services aux personnes qu'il sait être engagées dans une activité illicite

L'obligation de cesser promptement de fournir ses services aux personnes qu'il sait être engagées dans une activité illicite s'impose au prestataire lorsqu'est établie la connaissance du caractère illicite. Lorsqu'ils agissent de cette manière, les prestataires visés à l'article 22 n'ont pas de responsabilité.

Dès qu'il acquiert la connaissance du fait que des personnes sont engagées dans une activité illicite, le prestataire de services de moteur de recherche a l'obligation de cesser promptement de fournir ses services. Pour sa part, le prestataire de moteur de recherche doit rendre l'accès aux documents impossible ou empêcher la poursuite de l'activité illicite. La façon dont doit être accomplie cette obligation d'agir promptement s'apprécie à la lumière des circonstances dans lesquelles agit le prestataire de service.

Le prestataire doit intervenir d'une manière prompte, en peu de temps. L'obligation d'agir naît avec la connaissance; elle commence dès lors qu'est établi, de façon sérieuse et indépendante, le caractère illicite. C'est à compter du moment où il acquiert connaissance que l'on évaluera si le prestataire a agi avec célérité. Le caractère suffisamment prompt de l'action s'apprécie en fonction des circonstances, des moyens nécessaires et des efforts consentis afin de passer à l'action.

L'action du prestataire doit être menée pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de l'activité. Il doit prendre les moyens possibles, compte tenu des ressources dont il dispose et des circonstances dans lesquelles il agit. Il n'a pas de responsabilité si les gestes nécessaires afin de corriger la situation sont posés promptement.

1.3. Les limites constitutionnelles à un droit de suppression des liens hypertexte

En droit canadien, on ne peut postuler que le droit de la protection des renseignements personnels procure un droit au déréférencement des résultats de recherche[25].

Outre les règles découlant de l'article 22 de la Loi concernant le cadre juridique des technologies de l'information, la garantie constitutionnelle de la liberté d'expression, entendue comme protégeant la liberté de rechercher des informations ne contrevenant pas à la loi, s'oppose à une application d'un « droit au déréférencement » qui prétendrait se réclamer du droit à la protection des renseignements personnels.

Dans Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401[26], la Cour suprême du Canada, dans une décision unanime, a invalidé la loi albertaine sur la protection des renseignements personnels en ce qu'elle prohibait la prise d'images dans un lieu public.

La Loi attaquée interdisait de recueillir des renseignements, ici des images de personnes franchissant une ligne de piquetage et ne comportant aucune information intime, sans le consentement de celles-ci. Dans la situation présentée à la Cour, aucun détail concernant le mode de vie ou les choix personnels des intéressés n'avait été dévoilé. Or, la loi, à l'instar des autres lois sur la protection des renseignements personnels en vigueur au Canada (y compris la loi québécoise) ne fait aucune distinction : tout renseignement personnel y est traité de la même façon, même ceux qui ne relèvent pas de la vie privée. Il est interdit de le collecter et de le diffuser sans consentement sauf pour des motifs définis de manière très étroite. C'est cette absence de possibilité de laisser un espace à l'exercice des autres droits fondamentaux qui rend la loi sur la protection des renseignements personnels excessive. En somme, la Cour fait échos à une évidence : il existe des renseignements portant sur les personnes qui ne relèvent pas de la vie privée de celles-ci.

La Cour rappelle la nécessité de baliser les interdictions se trouvant dans les lois sur la protection des renseignements personnels. Telles que rédigées, ces lois interdisent de capter, conserver et diffuser toute information relative à une personne

25. C.L. c. BCF Avocats d'affaires, 2016 QCCAI 114 (CanLII), 14 avril 2016, en ligne : <http://canlii.ca/t/ gr5q0>.

26. [2013] 3 RCS 733.

identifiable sans sa permission et cela même lorsqu'elle se trouve dans des lieux publics. La Cour juge que de tels interdits limitent la liberté d'expression de façon déraisonnable.

La Cour explique que ces lois doivent comporter des balises afin de permettre l'exercice des activités expressives ne portant pas sur des matières relevant de l'intimité des personnes. La Cour a jugé que la loi albertaine sur la protection des renseignements personnels empêchait de recueillir des renseignements personnels, telles que des prises d'images ou des vidéos lors d'une manifestation au cours de laquelle le public pouvait facilement observer les personnes qui y prennent part.

Cette décision de la Cour suprême invalide l'approche qui a prévalu au Canada depuis plus de trois décennies en matière de protection des renseignements personnels. Portées par un mouvement qui semble postuler que la vie privée est le seul droit fondamental à devoir être protégé, ces lois ignorent pratiquement les impératifs de la libre circulation de l'information dans les espaces publics. En invalidant la loi albertaine, la Cour met fin à ce déséquilibre.

Bien sûr la Cour reconnaît la légitimité de protéger le droit à la vie privée et d'assurer que la collecte et la communication de renseignements personnels soient encadrées. Mais elle vient rappeler que tout renseignement personnel n'est pas automatiquement un renseignement sur la vie privée d'une personne, surtout s'il s'agit d'un renseignement se trouvant légitimement dans l'espace public. Il est donc excessif de considérer tout renseignement personnel comme étant assujetti au bon vouloir du sujet. Les libertés expressives imposent de baliser la faculté de l'individu à l'égard des informations le concernant en tenant compte des droits des autres et du public en général.

Pour l'heure, bien qu'il porte sur un phénomène passablement distinct de ceux qui sont concernés par les moteurs de recherche, ce prononcé de la Cour suprême laisse planer d'importants doutes sur la possibilité, en droit canadien, d'un droit au déréférencement qui se fonderait sur les principes issus des lois sur la protection des renseignements personnels.

2. La vie privée et les résultats de recherche

Les moteurs de recherche agglomèrent des informations sur les personnes ou sur les diverses entités à propos desquelles on peut formuler une requête de recherche exprimée habituellement sous forme de mots-clefs. Ils permettent de localiser l'information en délivrant à l'utilisateur des documents ou des liens à des documents qui sont les plus pertinents possibles eu égard à sa requête. Les informations sont repérées dans des espaces virtuels qui sont en principe publics.

Par leur efficacité, les moteurs de recherche contribuent puissamment à réduire les phénomènes « d'obscurité pratique » qui rendent souvent difficiles l'accès et la

compilation d'un ensemble de documents portant sur une personne ou sur un sujet déterminé.

Du coup, cela amène certains à considérer qu'ils constituent des dossiers sur des personnes ou sur des sujets définis au fil des requêtes des usagers. Il n'en faut pas plus aux décideurs appliquant les textes européens pour les considérer comme étant des entités qui effectuent des « traitements » d'informations portant sur des personnes. Pourtant, le respect de la vie privée doit forcément s'envisager en tenant compte des exigences de liberté et de fiabilité des activités de recherche. La protection de la vie privée dans l'espace public ne saurait être tributaire de la seule volonté du sujet sans égard au droit des autres à connaître. Ce qui peut conduire à de vaines tentatives d'imposer le maintien d'une obscurité qui jusqu'ici s'imposait par défaut.

2.1. L'impératif de fiabilité des résultats de recherche

L'activité des moteurs de recherche participe de l'exercice du droit fondamental de rechercher librement des informations. C'est une composante inhérente de la liberté d'expression. Les textes fondamentaux qui proclament cette liberté lui reconnaissent un aspect positif, celui axé sur le droit des personnes de rechercher librement des informations et d'en recevoir. Ainsi, le Pacte international relatif aux droits civils et politiques précise que le droit à la liberté d'expression « comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce ». Il y a donc, dans l'idée de libre circulation de l'information, la reconnaissance d'un droit de rechercher de l'information.

Urs Gasser relève trois valeurs qui seraient à la base de l'écosystème informationnel sur Internet[27] : l'autonomie informationnelle, la diversité de l'information, et la qualité de l'information. Trois libertés sont à la source de l'autonomie informationnelle : la liberté de choix entre plusieurs sources d'informations, d'idées et d'opinions; la liberté d'expression de ses croyances et de ses opinions; et finalement la liberté de création de contenu d'information, scientifique ou de divertissement. C'est surtout ce dernier type de liberté qui a grandement bénéficié de l'avènement d'Internet. La participation active des individus à l'économie de l'information permet aux citoyens d'aller au-delà de la simple consommation passive d'information. Gasser ajoute que la diversité de l'information est l'un des éléments clés de la santé démocratique d'un État. C'est un mécanisme qui permet d'atteindre la vérité en matière d'information, en plus de protéger le processus et le discours démocratique. La diversité de l'information bénéficie aux individus qui sont mieux aptes à choisir ce qui leur convient en matière d'information. La dépendance croissante des individus envers l'information qui se trouve sur Internet implique nécessairement que cette information doive être de qualité. La qualité de l'information peut être déterminée

27. Urs Gasser, « Regulating Search Engines : Taking Stock and Looking Ahead », (2006) 9 Yale Journal of Law & Technology 124, p. 127.

selon des critères fonctionnels et cognitifs, mais également esthétiques et éthiques. Une information de qualité permet aux individus d'agir selon leurs goûts et leurs besoins.

Les moteurs de recherche sont a priori régis par le principe de la liberté de rechercher librement des informations. Ils n'inventent pas des informations, ils répertorient et reflètent ce que d'autres ont publié ou autrement rendu public. Dans une analyse datant de 2008, le Groupe de travail de l'article 29 estimait que les moteurs de recherche ne devraient pas être considérés comme étant « the principal controller which regard to the content related processing of personal data that is taking place »[28]. Par contre, les ordonnancements des résultats s'assimilent à des opinions sur la pertinence des résultats compte tenu de la requête à laquelle ils apportent une réponse[29].

Les usagers recherchent du contenu pertinent à leurs interrogations. Pour répondre à cette demande, les moteurs de recherche livrent des résultats aux requêtes des usagers sous la forme d'hyperliens. Les moteurs de recherche qui se démarquent par la pertinence, la clarté et l'efficacité de leurs résultats obtiennent un avantage compétitif sur les moteurs concurrents.

C'est donc uniquement en présence de motifs sérieux – par opposition à des menaces ayant un caractère purement éventuel – que la restriction aux activités des moteurs de recherche sera justifiée dans le contexte d'une société démocratique. La réglementation fondée uniquement sur des craintes de périls éventuels emporte un effet inhibiteur. Pour limiter leurs risques, les moteurs de recherche pourraient être tentés de censurer les résultats au-delà des exigences de réglementations trop restrictives prises au nom de la protection de la vie privée envisagée de façon excessive. Le droit des internautes de rechercher librement des informations se trouverait alors compromis.

Envisagés du point de vue de l'utilisateur, les enjeux et risques des moteurs de recherche se situent au plan de la fiabilité des résultats. L'usager cherchera habituellement à être assuré que le moteur comporte le moins de biais possibles. L'usager utilise le moteur de recherche afin de trouver des informations sur un sujet ou sur une personne. La fiabilité est une qualité essentielle : le moteur de recherche doit être fiable et crédible à défaut de quoi les usagers vont se tourner vers d'autres moyens afin de repérer l'information recherchée. La censure de certains résultats affecte la fiabilité et peut miner la crédibilité des résultats.

28. Article 29, Data Protection Working Party, Opinion on data protection issues related to search engines, adopted on 4 April 2008, p. 14, en ligne : <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/ wpdocs/2008_fr.htm>.

29. Oren Bracha et Frank A Pasquale III, Federal Search Commission ? : Access, Fairness and Accountability in the Law of Search, Public Law and Legal Theory Research Paper no 12, July 2007, en ligne : <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1002453>; Search King v. Google Technology Inc, U.S. Distrct Court Western Oklahoma, 2003 U.S. Dist LEXIS 27193.

Les enjeux envisagés du point de vue du fournisseur de moteurs de recherche concernent la minimisation des coûts ainsi que le fardeau de gérer les risques découlant des législations sur la vie privée et la protection des données personnelles. Si le fournisseur d'outils de recherche est tenu de deviner la volonté des personnes concernées par une information par ailleurs accessible sur Internet, il est à craindre qu'il adopte une attitude de censure préventive de ses algorithmes afin de limiter les risques de sanctions au nom de l'application de législations trop restrictives.

Les enjeux envisagés du point de vue des tiers concernent la propriété intellectuelle des œuvres qui peuvent se trouver à être reproduites ou diffusées au-delà de ce qui aurait été initialement envisagé. Les tiers peuvent aussi craindre que leur réputation pâtisse du fait de la persistance de l'information sur le net et des capacités des moteurs de ramener au chercheur des informations préjudiciables sur leurs faits et gestes. Aussi, l'enjeu de la protection de la vie privée est l'un des plus fréquemment évoqués lorsqu'on s'interroge sur les enjeux posés par les moteurs de recherche. On craint que les moteurs facilitent la transgression des barrières pratiques et juridiques qui limitent la circulation de l'information sur une personne.

En somme, la fiabilité des résultats de recherche apparaît comme un corollaire de la liberté de rechercher des informations. Les protections supra-légales de la liberté d'expression dont ce droit est l'une des composantes empêchent de limiter la liberté de fonctionnement des moteurs de recherche en l'absence de motifs sérieux, concordants ou fondés sur la protection de droits fondamentaux qui sont effectivement garantis.

2.2. La protection de la vie privée dans l'espace public

Plusieurs enjeux des moteurs de recherche s'inscrivent dans une perspective de protection de ce que l'on présente comme étant le droit de l'individu de maîtriser l'information qui le concerne.

Invoquant un droit qui n'a pas, à ce jour, été consacré dans les textes fondamentaux, on en vient à revendiquer rien de moins qu'un droit de veto pour l'individu au regard des informations qui le concernent. Ce « droit à la protection aux données personnelles» s'étendrait même aux informations qui sont relatives à la vie publique des personnes. Une telle conception s'accorde mal avec les exigences de la vie démocratique. Si l'on convient d'emblée que l'individu doit avoir la pleine maîtrise de sa vie privée, il paraît tout aussi évident que ce droit se conçoit dans un espace social au sein duquel les autres peuvent avoir un intérêt légitime à connaître[30].

Étant donné que les moteurs de recherche traitent des informations qui sont a priori du domaine public, il est préoccupant de voir invoquer des droits aux fondements conceptuels aussi fragiles pour justifier la censure des moteurs de recherche.

30. Voir, parmi l'abondante littérature sur ce point : Miguel PEGUERA, « The Shaky Ground of the Right to Be Delisted », [2016] 18 Vand.J.Ent.& Tech. L, 507-560.

De tels fondements se concilient difficilement avec le caractère public des informations relevant de l'espace public.

2.2.1. Les informations personnelles à caractère public

Les informations à caractère public sont en principe de libre parcours[31]. Comme elles n'entrent pas dans le domaine de la vie privée, il devrait être en principe licite d'y accéder, de les traiter et de les diffuser. En contexte démocratique, seuls les abus spécifiquement avérés à l'égard d'informations publiques sont susceptibles de mesures de censure.

Invoquant l'efficacité des moteurs de recherche qui peut produire un effet d'amplification des effets inhérents au caractère public de l'information, on en vient à postuler que les moteurs de recherche compilent des données personnelles. Les risques hypothétiques que certains regroupements d'informations sur des personnes puissent engendrer des effets défavorables permettent de justifier des demandes pour un régime juridique qui nie pratiquement le caractère public des informations dès lors qu'un individu se met à penser que cela présente un risque de l'affecter.

Ainsi, le Groupe de l'article 29 estime que les moteurs de recherche compilent des données personnelles. Dans son opinion du 4 avril 2008, il observe que :

> [...] in their role as content providers, search engines help to make publications on the internet easily accessible to a worldwide audience. Some search engines republish data in a so-called 'cache'. By retrieving and grouping widespread information of various types about a single person, search engines can create a new picture, with a much higher risk to the data subject than if each item of data posted on the internet remained separate. The representation and aggregation capabilities of search engines can significantly affect individuals, both in their personal lives and within society, especially if the personal data in the search results are incorrect, incomplete or excessive.[32]

Dans certaines juridictions, agglomérer des informations relatives à une personne peut équivaloir à constituer un dossier sur celle-ci. Au Québec, l'article 37 du Code civil dispose que :

> Toute personne qui constitue un dossier sur une autre personne doit avoir un intérêt sérieux et légitime à le faire. Elle ne peut recueillir que les renseignements pertinents à l'objet déclaré du dossier et elle ne peut, sans

31. Par exemple, l'article 55 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, R.L.R.Q, c. A-2.1, dispose que : « Un renseignement personnel qui a un caractère public en vertu de la loi n'est pas soumis aux règles de protection des renseignements personnels prévues par le présent chapitre »

32. Article 29, Data Protection Working Party, Opinion on data protection issues related to search engines, adopted on 4 April 2008, p. 5, en ligne : <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/ wpdocs/2008_fr.htm>.

> le consentement de l'intéressé ou l'autorisation de la loi, les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution; elle ne peut non plus, dans la constitution ou l'utilisation du dossier, porter autrement atteinte à la vie privée de l'intéressé ni à sa réputation.

Est-ce qu'un moteur de recherche qui agglomère des informations ou qui autrement collectionne des informations relatives à une personne constitue un dossier sur cette personne au sens de l'article 37 du Code civil du Québec?

En droit européen, des juridictions ont assimilé le fait de constituer un dossier sur une personne à un « traitement » de données personnelles. Ainsi, au nom d'un droit de l'individu à la maîtrise des informations qui le concernent, celui-ci aurait le loisir de s'opposer à ce que les autres compilent des renseignements, même émanant du domaine public qui le concernent. Pour qu'une telle compilation soit licite, elle devrait nécessairement procéder d'un intérêt « sérieux » et « légitime ». Dans pareil schéma, il revient aux juridictions de juger du caractère sérieux et légitime de ces démarches de recherche et de compilation.

Une telle conception de la protection de la vie privée ouvre la porte à un contrôle de la légitimité des recherches effectuées avec des mots qui se trouvent à correspondre au nom d'une personne.

Pourtant, les situations relationnelles dans lesquelles chacun est engagé peuvent engendrer des intérêts légitimes et différenciés à connaître certaines informations sur les personnes se trouvant dans son environnement. Par exemple, le conjoint a un intérêt légitime à connaître certains éléments de la vie de l'autre conjoint alors que cet intérêt pourrait n'être pas présent chez le voisin de palier. De même, l'employeur a intérêt à connaître certaines informations relatives à l'employé pour certaines fins mais pas pour d'autres. Ces intérêts différenciés à connaître constituent autant de facteurs de limitation de la vie privée. Lorsque de tels intérêts existent, c'est-à-dire lorsque sont réunies les conditions y donnant ouverture, le droit à la vie privée cède le pas puisqu'il existe un intérêt légitime à connaître.

Ce phénomène peut être illustré en représentant les informations protégées par le droit à la vie privée en cercles concentriques. De tels cercles délimitent les informations qui peuvent demeurer du domaine privé et par le fait même, celles qui peuvent licitement circuler. Ces informations ne coïncident pas nécessairement avec ce que nous consentons à rendre disponible. Par contre, l'on reconnaît l'existence d'un droit des autres à connaître certaines informations qui nous concernent.

Ainsi, le fait qu'un professeur exerce ses fonctions dans telle ou telle université constitue une information possédant a priori un caractère public : on ne peut revendiquer les privilèges et avantages rattachés à une fonction sans supporter ce qui vient avec son caractère public.

Mais dans la décision Note2b.com, le Tribunal de grande instance de Paris[33] a ordonné à un site de notation de suspendre l'utilisation et le traitement des données personnelles des professeurs notés par les élèves ainsi que leur affichage sur le site, y compris sur le forum de discussion. En vertu de l'article 7 de la loi française Informatique et libertés, le traitement des données personnelles, même publiques, est conditionnel au consentement de la personne concernée, sauf si le responsable du site poursuit un intérêt légitime qui n'est pas contraire aux droits et intérêts de la personne visée.

Le tribunal s'est attaché à déterminer s'il y avait en l'espèce un intérêt légitime au traitement de données personnelles par ce site, en l'occurrence, des opinions des élèves sur les professeurs œuvrant dans les lycées ou dans les universités. Il a examiné le site et s'est interrogé sur la méthode d'expression des opinions exprimées sur les professeurs établies en fonction d'une seule note chiffrée et de six qualificatifs. Selon le tribunal, cette approche partielle peut conduire à une appréciation biaisée, favorable ou défavorable, et peut donc provoquer un trouble. Le tribunal estime aussi que le site n'a pas pris des précautions suffisantes pour empêcher les risques de dérive polémique, notamment en organisant la modération de son forum de discussion. On conviendra que la liberté d'expression des personnes exprimant une opinion au sujet de faits publics ne pèse pas très lourd dans un pareil raisonnement.

Le site n'avait pas non plus prévu la mise en place de procédures efficaces pour que les enseignants concernés puissent faire valoir leurs droits. Enfin, l'aspect commercial du site a joué pour beaucoup dans l'appréciation du tribunal. Selon lui, les personnes y figurant ont le droit de ne pas voir leurs noms associés aux messages publicitaires qui sont insérés sur les pages.

De son côté, la Commission nationale de l'informatique et des libertés (CNIL) a également conclu à l'illégitimité du site au regard de la protection des données personnelles. Dans son communiqué résumant sa décision du 6 mars 2008, l'organisme constate que « le système de notation des enseignants de la société note2be.com poursuit une activité commerciale reposant sur l'audience d'un site internet qui ne lui confère pas la légitimité nécessaire, au sens de la loi, pour procéder ou faire procéder à une notation individuelle des enseignants susceptible de créer une confusion, dans l'esprit du public, avec un régime de notation officiel »[34].

Ainsi, le but commercial dans lequel est supposé s'inscrire le traitement de même que l'hypothétique confusion avec un système de notation officiel semblent suffire

33. SNES FSU et autres / Note2be.com, Tribunal de grande instance de Paris, Ordonnance de référé, 3 mars 2008, Legalis.net, en ligne : <http://www.legalis.net/jurisprudence-decision.php3?id_article=2234#>. Voir Agathe Lepage, « Informatique et libertés Les professeurs notés sur Internet », Communication commerce électronique, avril 2008, p. 36-40.

34. La CNIL se prononce : le site note2be.com est illégitime au regard de la loi informatique et libertés, communiqué du 6 mars 2008, en ligne : <http://www.cnil.fr/index.php?id=2405&news[uid]=528&c Hash=7c1cd2d002>.

à ruiner la légitimité de ce qu'on aurait pu croire n'être que l'expression d'opinions – possiblement déplaisantes – à l'égard des activités publiques de personnes exerçant un métier qui concerne le public.

Si la tendance que représente la décision note2b.com devait se confirmer, il est à craindre que cela réduise la portée du droit de discuter des faits et gestes publics des personnes. Rien ne s'opposerait à ce que l'on reconnaisse aux personnes un droit d'invoquer les lois sur la protection des données afin de réclamer des moteurs de recherche qu'ils censurent les informations du domaine public qui les concernent et ce, au fil de ce qu'ils trouvent déplaisant ou agaçant ou en invoquant quelque risque de désagrément. Si on suit le raisonnement des affaires note2b.com, les tribunaux auraient alors à évaluer la « légitimité » de ce qui est considéré comme un « traitement » de renseignements personnels.

En droit québécois, un très grand nombre d'usages d'informations personnelles ne constituent pas, en soi, une violation de la vie privée. Il est difficile de justifier, au nom de la vie privée, les mesures relatives à certaines informations dont la circulation est inhérente à la vie sociale comme celles qui sont susceptibles d'être traitées par les moteurs de recherche.

On peut s'inquiéter de voir s'installer une conception en vertu de laquelle, le simple inconfort ressenti par une personne à l'égard d'une information licitement dans l'espace public déclenche un processus qui contraint toute personne qui souhaite le maintien en ligne de cette information à devoir défendre le droit de la rechercher.

2.2.2. La revendication du maintien d'une « obscurité pratique »

Plus ils sont efficaces, plus les moteurs de recherche tendent à réduire le temps et les efforts nécessaires afin de trouver des informations sur une personne. Il existe depuis longtemps des banques de données qui compilent des renseignements à caractère public sur les personnes. Mais leur consultation peut demander du temps et des efforts. L'ubiquité d'Internet et l'efficacité des moteurs de recherche tendent à réduire le temps et les efforts requis pour retrouver une information.

Ces gains d'efficacité résultant des performances des moteurs de recherche sont porteurs de risques accrus. Les renseignements – même à caractère public – portant sur les personnes peuvent circuler plus vite et dans un espace beaucoup plus large.

Dans plusieurs situations, la disparition des efforts à consacrer pour trouver l'information affaiblit ce qui est perçu comme une protection par défaut pour la vie privée. Avec les moteurs de recherche, la diffusion se trouve banalisée : l'information peut aisément se trouver à être diffusée en dehors des cercles de circulation initialement envisagés, d'où l'accroissement des risques.

Dans le cyberespace, les repères permettant de délimiter le privé du public sont brouillés. Belgum rappelle que :

> Personal data, such as address, phone number, income, poperty value, and marital status have always been available to those willing to dig. The Internet can make it possible for a much wider class of persons – essentially all internet users – to gain access to similar types of personal information at little or no cost.[35]

Internet modifie l'échelle spatiale à partir de laquelle s'apprécient les risques pour la vie privée. En dehors du monde en réseaux, l'accessibilité à une information demande des ressources qui peuvent être importantes. Sur Internet, on a l'impression que beaucoup d'informations sont à portée d'une requête de moteur de recherche. Solove observe que :

> Until recently, public records were difficult to access. For a long time, public records were only available locally. Finding information about a person often involved a treasure hunt around the country to a series of local offices to dig up records. But with Internet revolution, public records can be easily obtained and searched from anywhere.[36]

La problématique de l'accès aux documents rendant compte du déroulement des processus judiciaires est emblématique des changements quantitatifs et qualitatifs générés par Internet. Natale M. Gome-Velez relève que :

> Providing Internet access to court records increases exponentially the availibility of court records, including any sensitive information they contain. Examples of sensitive information that might be found in court records include : social security numbers, home addresses, names of minor children financial account numbers, and medical information.[37]

Il y a aussi décentrage temporel : la persistance de l'information emporte que celle-ci traverse les cercles dans lesquels elle était tenue pour légitime. Par exemple, une information peut être légitimement disponible au public en raison de l'actualité de l'événement. L'archivage et la disponibilité virtuellement permanente sur Internet iraient au-delà de ce qui est nécessaire afin de rendre compte de l'actualité.

Les capacités d'agglomération d'information permettent la constitution de gisements d'informations sur les personnes qui peuvent du coup devenir disponibles pour des forces de police de même que devenir des enjeux pour des malfaiteurs. En somme la disparition des efforts à consacrer pour trouver l'information emporte la disparition d'une protection par défaut pour la vie privée. Cela peut porter à revoir

35. Karl D. Belgum, « Who leads at Half-time ? : Three Conflicting Visions of Internet Privacy Policy », (1999) 6 Rich. J.L. & Tech. 1.

36. Daniel J. Solove, « Access and Aggregation : Public Records, Privacy and the Constitution », (2002) 86 Minn. L. Rev. 1137-1218, p. 1139.

37. Natalie M. Gomez-Velez, « Internet Access to Court Reports- Balancing Public Access and Privacy », (2005) 51 Loyola L. Rev. 365-438, p. 371.

les raisonnements qui permettaient de déterminer si on se trouvait dans le domaine de la vie privée ou dans le domaine de l'espace public.

Tous ces changements dans les dimensions des enjeux relatifs à la vie privée indiquent des modifications dans les niveaux de risques causés par la circulation de l'information dans le réseau du fait notamment de l'activité des moteurs de recherche. Ces dimensionnements nouveaux des risques pour la vie privée induisent des mutations au niveau de la raison d'être des règles de droit. Là où l'on prenait pour acquis que le niveau de risques pour la vie privée demeurait faible ou aisément maîtrisé, les mutations dans l'échelle qualitative et temporelle qu'induit la généralisation d'Internet, conduisent à postuler que les risques sont accrus. D'où les revendications pour un renforcement de la protection de la vie privée des personnes lors de la mise en place des environnements de traitement de l'information.

Mais l'accroissement du niveau de risque pour la vie privée ne doit pas constamment se traduire par une restriction de la liberté de diffuser et d'accéder à des informations relatives aux personnes. Lorsque le moteur de recherche est envisagé comme un facteur de réduction de l' « obscurité pratique » (practical obscurity) est-ce une raison pour affecter la fiabilité des résultats de recherche ?

Certes, le fait que l'information traverse les cercles d'intimité présente des risques. Mais ce n'est que dans de rares circonstances que cela emportera des effets démontrables sur la vie privée d'individus identifiables. Il paraît donc excessif de préconiser la censure des liens hypertextes livrés par les moteurs de recherche au nom de dangers qui demeurent au pire essentiellement du domaine de l'éventualité. Les moteurs de recherche n'inventent pas l'information qu'ils repèrent. Si des dangers réels existent vraiment à la circulation de certaines informations, une intervention en amont, soit la suppression du document vers lequel pointent les liens générés par le moteur de recherche, apparait moins liberticide.

Mais ce souci de maintenir une « obscurité » pratique peut fonder la mise en place de régimes juridiques encadrant certaines fonctions de recherche étendues. Au Québec, cette tendance est illustrée par l'article 24 de la Loi concernant le cadre juridique des technologies de l'information.

2.2.3. L'article 24 de la Loi concernant le cadre juridique des technologies de l'information

En droit québécois, l'article 24 de la Loi concernant le cadre juridique des technologies de l'information[38] peut trouver application à l'égard de certains moteurs de recherche. Il se lit comme suit :

38. Loi concernant le cadre juridique des technologies de l'information, RLRQ, c. C-1.1. Voir : Pierre Trudel, Introduction à la Loi concernant le cadre juridique des technologies de l'information, Cowansville, Éditions Yvon Blais, 2012, p. 85 et s.

> L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des données personnelles et qui, pour une finalité particulière, est rendu public, doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés.

Cette disposition reflète une tendance à promouvoir l'occultation de documents ayant pourtant a priori un caractère public. L'article 24 vise des informations qui ont un caractère public; non les renseignements à caractère privé. Il permet de restreindre l'utilisation des fonctions de recherche extensive à l'égard des documents technologiques comportant des données personnelles et rendues publiques pour une finalité particulière. On veut ainsi éviter, par exemple, les consultations de banques de données à l'aide de moteurs de recherche afin de repérer des données personnelles pour des fins « autres » que celles pour lesquelles elles ont été diffusées au public.

On peut supposer que ce genre de mesure se justifie du fait que dans l'univers des documents sur papier, la recherche est souvent longue puisque les documents publics doivent être examinés un à un. Pour les documents technologiques, susceptibles de recherches automatisées, les possibilités de recherche sont démultipliées, ce qui peut porter certains à craindre des abus. Devant cette possibilité hypothétique d'abus, la solution retenue est d'imposer la mise en place de moyens technologiques pour assurer la protection des données personnelles contenues dans ces documents publics. Et cette protection est de limiter l'accès uniquement aux fins pour lesquelles un document est rendu public comme si ces fins étaient connues et spécifiées.

La disposition est difficile à appliquer car elle postule qu'il est possible de déterminer les finalités du caractère public d'une information. Il est difficile de concevoir comment une telle démarche est possible sans porter un jugement a priori sur la légitimité de certaines recherches. Il y a aussi la difficulté de déterminer, en l'absence de texte législatif, ce qui constitue la finalité du caractère public d'une information. Comment est-il possible, sans ajouter au texte de loi, de déduire une finalité au caractère public d'une information alors qu'il ne comporte aucune indication quant à la finalité que viserait le caractère public de l'information qui est en cause ?

Lorsqu'une information est à caractère public, elle est de libre parcours, sauf à démontrer qu'on en fait un usage fautif ou contraire à une loi. On ne peut présumer, sans nier le caractère public d'une information, qu'une information publique ne doit servir qu'à certaines fins et pas à d'autres. La seule limite légitime à l'usage d'une information à caractère public est le caractère abusif de l'usage : postuler a priori que des usages seraient abusifs laisse fort peu de place au droit à l'information[39].

De plus, il appert que cette censure d'informations à caractère public peut avoir lieu même sans avoir à justifier en quoi un usage spécifique d'informations à ca-

39. Voir toutefois Gyulai c. Cour du Québec, 2008 QCCS 1454 (CanLII) qui semble avoir confirmé la possibilité d'introduire de telles distinctions.

ractère public est illégitime. Dans R.D. c. Racine (Municipalité de)[40], le demandeur souhaitait obtenir de la municipalité de Racine (l'organisme public) communication d'une copie, « sur support informatisé, du registre des taxes de la municipalité pour l'année 2008 ». L'organisme refusa de communiquer le document demandé car il contenait des renseignements personnels concernant d'autres personnes physiques, lesquels sont inaccessibles à moins que celles-ci n'y consentent. Par la suite, l'organisme a changé de position et informé le demandeur que l'article 55, alinéa 2 de la Loi sur l'accès l'autorise à refuser la communication du « rôle 2009-2011 et/ou du rôle de perception en format PDF » au motif que le format PDF faciliterait le recoupement des données (nombre de propriétés détenues par un même propriétaire), ce qui serait contraire à l'esprit de la Loi sur l'accès. L'article 55, alinéa 2 prévoit que :

> Cependant, un organisme public qui détient un fichier de tels renseignements peut en refuser l'accès, en tout ou en partie, ou n'en permettre que la consultation sur place si le responsable a des motifs raisonnables de croire que les renseignements seront utilisés à des fins illégitimes.

La Commission d'accès a constaté que le rôle de perception de taxes foncières de l'organisme constitue un fichier de renseignements personnels à caractère public au sens de l'article 55, alinéa 2 de la Loi sur l'accès. Dans cette affaire, il a été mis en preuve que le demandeur souhaitait obtenir le format PDF du rôle de perception afin de profiter des fonctions de recherche contenues dans le document technologique et qui permettent de regrouper facilement les propriétés situées dans la Municipalité de Racine selon trois secteurs qu'il décrit comme étant « villageois », « rural » et « riverain ». Il souhaitait obtenir le rôle de perception afin de réaliser deux études permettant d'illustrer que le fardeau fiscal se déplace progressivement vers les propriétés riveraines alors que les services municipaux offerts à celles-ci n'augmentent pas. Sans indiquer en quoi l'utilisation projetée aurait eu un caractère illégitime, la Commission a décidé que l'utilisation que le demandeur projetait de faire du rôle de perception n'était pas conforme à la finalité pour laquelle ce fichier de renseignements personnels avait été rendu public, car elle n'est pas reliée aux fins de perception des taxes foncières. Le responsable de l'accès aux documents avait donc des motifs raisonnables de croire qu'en l'espèce, les renseignements seraient utilisés à des fins illégitimes. S'il faut en croire cette décision de la Commission d'accès à l'information, mener des analyses sur les évolutions du fardeau fiscal dans une municipalité serait une fin illégitime !

Une interprétation plus compatible avec le principe constitutionnel de la liberté de rechercher des informations[41] et du droit du public à l'information est d'appliquer

40. 2011 QCCAI 148 (CanLII).

41. La liberté d'expression comprend celle de rechercher librement des informations. Par conséquent, en l'absence de disposition limitant cette liberté, on doit donner à un texte de loi une interprétation en harmonie avec la liberté de rechercher des informations. Or, cette jurisprudence de la Commission d'accès va directement à l'encontre de ce principe.

l'article 24 uniquement dans les situations où la finalité du caractère public d'un document est mentionnée par le législateur. En l'absence de précision à cet égard dans un texte législatif ce serait ajouter à une disposition législative que d'y lire une finalité spécifique. Par exemple, de prétendre, comme le fait la Commission d'accès, que les informations faisant partie des rôles d'évaluation ne sont rendues publiques que pour permettre à une personne de s'enquérir de la valeur foncière d'une propriété à la fois, c'est d'ajouter à la Loi une disposition qui ne s'y trouve pas.

Au surplus, la lecture consistant à reconnaître qu'il est légitime de permettre à l'interprète de postuler, dans le cadre de l'exercice d'un pouvoir discrétionnaire, une finalité au caractère public donne ouverture à l'arbitraire. Par exemple, un bibliothécaire pourrait se mettre à spéculer sur les finalités du caractère public de certaines informations relatives aux auteurs répertoriés dans les fichiers de la bibliothèque. Donner un poids aussi important à un pouvoir discrétionnaire afin de cacher de l'information qui, faut-il le rappeler est a priori publique, constitue une interprétation difficilement conciliable avec le caractère supra-légal du droit de rechercher des informations.

C'est pourquoi l'application de l'article 24 de la Loi concernant le cadre juridique des technologies de l'information serait plus compatible avec les principes démocratiques si on en limitait la portée aux situations où la loi indique expressément une finalité au caractère public d'un document. Le libellé de l'article 24 donne d'ailleurs ouverture à une telle lecture puisqu'il lie le fait du caractère public du document et la finalité particulière.

En somme, rien ne justifie de censurer les moteurs de recherche en ce qui a trait aux résultats qu'ils délivrent à partir de documents publics au motif que cela pourrait porter atteinte à la vie privée.

Dans les situations où les impératifs de protection de la vie privée – non de vagues revendications pour une « maîtrise » sur des informations nous concernant - peuvent légitimement être invoqués pour exclure certaines informations des résultats délivrés par les moteurs de recherche, c'est via une intervention en amont qu'il faut procéder à ce genre d'exclusions. Lorsque cela est clairement justifié, une intervention au niveau des métadonnées peut être envisagée afin d'exclure un document portant sur la vie privée d'une personne de la portée des robots utilisés par les moteurs de recherche.

2.3. Le déréférencement des résultats de recherche : l'arrêt Google Spain

L'affaire Google Spain[42] vient couronner les revendications de censure des liens livrés à la suite de requêtes introduites dans les moteurs de recherche. L'arrêt a pour origine la demande d'un citoyen espagnol auprès de l'agence de protection de la vie privée d'ordonner à un journal de supprimer de ses archives des pages dans lesquelles était publié, en conformité avec la loi, un avis d'une vente aux enchères organisée à la suite d'une saisie destinée à recouvrer des dettes. La demande visait non seulement le site du journal mais aussi Google, à qui il était demandé de supprimer ou de rendre invisibles les liens vers ces documents publics. La demande réclamait de rendre les liens hypertextes inaccessibles à ceux qui font des recherches sur Internet en introduisant le nom du demandeur dans le moteur de recherche.

L'agence espagnole de protection des données a écarté la demande de suppression des archives du journal. Mais elle a ordonné à Google de retirer les liens hypertextes conduisant vers ces documents lorsqu'on utilise le moteur de recherche.

Dans sa décision, la Cour de justice de l'Union européenne conclut qu'un moteur de recherche comme Google « collecte » des données personnelles lorsqu'il applique ses algorithmes de recherche en vue de générer des listes de résultats. Contrairement à ce qui est généralement pris pour acquis en droit canadien, la Cour applique la notion très englobante de traitement qui prévaut en droit européen pour considérer que le moteur de recherche est responsable d'un « traitement » de données personnelles dès lors que le nom d'une personne est entré dans une requête du moteur de recherche et que se déclenche le processus par lequel le moteur délivrera à l'utilisateur la liste des documents comportant les mots qu'il recherche.

Autrement dit, introduire le mot « rose » et le mot « petit » dans une requête sur un moteur de recherche donne lieu à un traitement de données personnelles au sens des lois européennes dès lors qu'il s'avère que ces mots correspondent au nom d'une personne physique.

42. Google Spain SL, Google Inc. c.Agencia Española de Protección de Datos (AEPD), Mario Costeja González, arrêt du 13 mai 2014, en ligne : <http://curia.europa.eu/juris/document/document.jsf?docid =152065&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=253040 >. Voir sur cette décision : David Lindsay, « The 'Right to be Forgotten' by Search Engines under Data Privacy Law : A Legal Alaysis of the Costeja Ruling », (2014) 6 (2) Journal of Media Law 159-179; Orla Lynskey, « Control over Personal Data in a Digital Age : Google Spain v. AEPD and Mario Costeja Gonzalez, (2015) 78(3) Modern L.Rev. 522-548; Sarah M. Kalis, « Google Spain SL, Google Inc. v. Agencia Espanola de Protection de Datos Mrio Costeja Gonzalez : An Entitlement to Erasure and Its Endless Effects », (2015) 23 Tulane J. of Int'l 7 Comp. Law 589-605; Simon Wechsler, « The Right to Remember : The European Convention on Human Rights and the Right to Be Forgotten », [2015] 49 Columbia J. of Law and Social Problems 135-165.

La cour affirme que la responsabilité de l'exploitant du moteur de recherche fait en sorte que celui-ci est obligé de supprimer de la liste de résultats, affichée à la suite d'une recherche effectuée à partir du nom d'une personne, des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne. La Cour précise qu'une telle obligation peut exister également dans l'hypothèse où ce nom ou ces informations ne sont pas effacés préalablement ou simultanément de ces pages web, et ce, le cas échéant, même lorsque leur publication en elle-même sur lesdites pages est licite.

La Cour estime qu'un traitement de données à caractère personnel réalisé par un moteur de recherche permet à tout internaute, lorsqu'il effectue une recherche à partir du nom d'une personne physique, d'obtenir, par la liste de résultats, un aperçu structuré des informations publiques relatives à cette personne sur Internet. Elle relève que ces informations peuvent toucher à une multitude d'aspects de la vie privée.

Sans moteur de recherche, ces informations publiquement disponibles en ligne n'auraient pas pu être interconnectées ou n'auraient pu l'être que très difficilement. La Cour affirme que l'effet de l'ingérence dans les droits de la personne se trouve démultiplié en raison du rôle important que jouent Internet et les moteurs de recherche dans la société moderne, ces derniers conférant un caractère ubiquitaire aux informations contenues dans les listes de résultats. Compte tenu de sa gravité potentielle, une telle ingérence ne saurait, selon la Cour, être justifiée par le seul intérêt économique de l'exploitant du moteur dans le traitement des données.

La Cour ajoute que même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec les exigences de protection de la vie privée telles qu'édictées dans la Directive européenne. Elle explique que lorsque, eu égard à l'ensemble des circonstances caractérisant le cas d'espèce, ces données apparaissent inadéquates, pas ou plus pertinentes ou excessives au regard des finalités pour lesquelles elles ont été traitées et du temps qui s'est écoulé, elles peuvent être occultées des résultats de recherche.

Lorsqu'une demande de censurer les informations est introduite par la personne concernée à l'encontre du traitement réalisé par l'exploitant d'un moteur de recherche, il convient notamment d'examiner si cette personne a un droit à ce que les informations en question relatives à sa personne ne soient plus, au stade actuel, liées à son nom par une liste de résultats qui est affichée à la suite d'une recherche effectuée à partir de son nom. Si tel est le cas, les liens vers des pages web contenant ces informations doivent être supprimés de cette liste de résultats, à moins qu'il existe des raisons particulières, telles que le rôle joué par cette personne dans la vie publique, justifiant un intérêt prépondérant du public à avoir, dans le cadre d'une telle recherche, accès à ces informations.

Suite à ce précédent, des personnes qui souhaitent faire « oublier » des aspects de leurs faits et gestes publics ont introduit des demandes de purge des résultats de recherche.

2.3.1. La détermination du bien-fondé des demandes de déréférencement

La décision de la Cour de justice de l'Union européenne a ordonné au moteur de recherche Google de mettre en place une procédure afin de recevoir et traiter les demandes de déréférencement en application de la règle que venait d'instituer le jugement.

Le demandeur doit remplir un formulaire de demande de suppression de contenu mis à la disposition des internautes. Il doit y indiquer les informations personnelles permettant de confirmer son identité tel que nom, prénom de même qu'une adresse de courriel. Il faut ensuite indiquer l'URL que l'on souhaite voir supprimé des résultats de recherche et expliquer les raisons de cette demande de suppression.

Le demandeur doit joindre à sa demande une copie numérique d'un justificatif d'identité (carte d'identité, permis de conduire). La demande doit être signée électroniquement en écrivant son nom et en cliquant sur « envoyer ». Les demandes sont traitées une à une et peuvent requérir, selon les cas, une étude plus ou moins approfondie. Les délais de suppression peuvent donc être très variables. Le déréférencement ne concerne que les recherches Google mentionnant le nom d'une personne physique.

Google a reçu des milliers de demandes en provenance de personnes ayant autrefois fait la manchette et souhaitant se faire « oublier ». Ainsi, des personnes ayant été reconnues coupables de crimes, de fraudes auprès des consommateurs ont revendiqué que les liens vers les archives de journaux en ligne concernant ces faits soient censurés.

Certes, la décision de la Cour prévoit que les informations qui présentent un intérêt public pourraient être exclues de la faculté de déréférencement. Mais en Europe, contrairement au droit nord-américain, des interprétations souvent très étroites de ce qui est d'intérêt public prévalent très souvent[43].

De plus, le mécanisme institué par la Cour de justice européenne est ainsi conçu qu'il est plus facile pour un moteur de recherche de donner suite aux demandes de déréférencement que d'y résister. Pour chaque moteur de recherche, faire l'effort d'analyser et ensuite d'expliquer que certains liens conduisent à des documents qui présentent un réel intérêt pour le public représente un coût que certains d'entre eux pourraient ne pas souhaiter encourir[44].

43. James Whitman, « The Two Western Cultures of Privacy : Dignity vs. Liberty », (2004) 113 Yale L.J., 1151; Pierre Trudel, « Visions américaines et européennes de l'e-réputation », dans Christophe Alcantara, E-réputation regards croisés sur une notion émergente, Paris, Gualino lextenso éditions, 2015, 61-71.

44. Simon Wechsler, « The Right to Remember : The European Convention on Human Rights and the Right to be Forgotten », [2015] 49 Colum. J.L.& Soc. Probs. 135-165.

2.3.2. Les revendications des agences de protection des données quant à la portée du déréférencement

À la suite de l'arrêt Google Spain, le Groupe Article 29 (le G29) constitué des autorités européennes de protection des données personnelles a publié des lignes directrices sur la façon dont devrait s'appliquer le jugement de la Cour de justice européenne. Des lignes directrices qui poussent encore plus loin le déséquilibre à l'encontre du droit de rechercher librement des informations licites[45].

Le G29 s'appuie sur la décision de la Cour de justice prévoyant que les individus ont le droit de réclamer le déréférencement des documents licites qui apparaissent dans les résultats de recherche. Cela vise les résultats obtenus après une recherche effectuée sur la base du nom d'une personne. Comme l'information qu'il s'agit d'occulter ne contrevient à aucune loi, celle-ci demeure toujours accessible en ligne en effectuant une recherche sur d'autres termes ou en consultant directement le site source. En somme, la censure vise l'efficacité des recherches. L'application de la règle européenne vise à compliquer la tâche de ceux qui effectuent des recherches sur Internet avec des outils disponibles au grand public.

Ceux qui ont les moyens d'effectuer leurs recherches avec d'autres outils que les moteurs de recherche destinés au grand public demeurent libres de rechercher ce qu'ils veulent. Par exemple, les employeurs ou d'autres personnes qui souhaitent en savoir plus sur une personne peuvent continuer à utiliser des outils qui ne sont pas offerts au grand public afin de réunir des informations sur le passé des personnes qu'ils envisagent de recruter. Mais cette dimension, pourtant fondamentale dans les argumentaires en faveur du déréférencement, est ignorée par le G29.

Le G29 a estimé que le déréférencement ne doit pas se limiter aux versions européennes de Google. Lorsqu'il y a une désindexation, celle-ci doit aussi avoir lieu sur les autres déclinaisons du moteur de recherche, comme par exemple Google.com. Cela concerne aussi les déclinaisons internationales d'autres moteurs de recherche comme Bing ou Yahoo. En somme, tous les internautes de la planète devraient, si on suit la directive de ce groupe, être privés d'un accès à des documents par ailleurs licites.

Le G29 a également mis de l'avant une liste des critères communs que les autorités de protection des données appliqueront pour traiter les plaintes qu'elles reçoivent suite à des refus de déréférencement par les moteurs de recherche. La liste contient différents critères qui doivent être considérés comme des outils de travail flexibles

45. Article 29 Data Protection Working Paper, Guidelines on the Implementation of the Court of Justice of the European Union Judgment on « Google Spain and Inc v. Agencia Espanola de Proteccion De Datos (AEPD) and Mario Costeja Gonzalez », 26 novembre 2014, en ligne : <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf>, consulté le 16 mai 2016.

qui aideront les autorités dans la prise de décision. Les critères seront appliqués au cas par cas et en accord avec les dispositions nationales applicables.

Le document rappelle que selon la décision de la Cour, les moteurs de recherche sont réputés avoir le contrôle des données personnelles correspondant aux mots-clés qui sont introduits par les internautes menant des recherches.

Autre élément des lignes de conduite : les moteurs de recherche ne devraient pas afficher de notices aux chercheurs à l'effet que des liens vers des documents ont été supprimés pour faire suite à une demande d'un individu. Le Groupe va même jusqu'à réclamer que les notices soient publiées de façon à protéger ceux qui ont réclamé la suppression de liens contre des déductions « incorrectes » de la part des chercheurs.

Enfin, le Groupe estime qu'il n'y a pas de fondement à la pratique des moteurs de recherche d'informer les sites que leurs documents ont fait l'objet d'une désindexation.

On relèvera que ni dans la décision de la Cour de justice, ni dans l'interprétation que le G29 en fait au nom des autorités européennes de protection des données personnelles, il est fait mention du droit, pourtant partie intégrante de la liberté d'expression, de rechercher librement des informations licites.

3. Le caractère privé des traces générées par l'activité du chercheur

Par leur capacité d'accumuler et de compiler des informations découlant des requêtes effectuées par chacun des usagers, les moteurs de recherche soulèvent d'importants enjeux relatifs à la vie privée.

Afin d'optimiser la pertinence des résultats, un moteur de recherche peut compiler les mots-clés utilisés par un usager de même que d'autres données. Il y a alors constitution d'un « dossier » sur chacun des usagers. Le traitement réservé à ces requêtes est en effet susceptible d'accroître radicalement les risques pour la vie privée. Le risque induit par le moteur de recherche est un risque pour les usagers : ceux qui font confiance à cette ressource pour les aviser dans leurs recherches. Il existe une possibilité réelle de perte de confiance des usagers qui pourraient estimer que de telles pratiques sont trop risquées au regard des avantages qu'ils obtiennent de la fréquentation du moteur.

L'article 11 de la Charte des droits fondamentaux de l'Union européenne précise que la liberté d'expression « 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 ».

Le G29 infère de cette disposition que « information should be accessible without any surveillance by public authorities […] ». Dans certaines situations, il ne sera pas toujours possible de déterminer que le dossier concerne une personne : les données sont compilées à partir d'informations qui sont répertoriées habituellement par les ordinateurs ou les serveurs à partir desquels les usagers sont connectés.

Toutefois, en droit américain, dans Gonzales v. Google[46], le tribunal n'a pas eu d'hésitation à considérer que les moteurs de recherche collectent et conservent des données personnelles sur leurs usagers. Cette affaire s'inscrivait dans le contexte d'une demande par le gouvernement américain pour des données détenues par des moteurs de recherche afin de déterminer si certaines techniques de filtrage étaient moins restrictives à la liberté d'expression tout en produisant les résultats escomptés.

L'opinion du G29 relève à cet égard que :

> [...] in their role of service providers to the users, search engines collect and process vast amounts of user data, including data gathered by technical means, such as cookies. Data collected can range from the IP adress of individual users to extensive histories of past searching behaviour or data provided by users themselves when signing up to use personalised services. The collection of user data gives rise to many questions. After the AOL case a large audience was made aware of the sensitivity of personal information contained in search logs.[47]

Contrairement aux liens pointant vers des documents publics, les données sur les comportements des chercheurs sont des renseignements personnels qui en principe font partie de la vie privée ou du secret qui caractérise la discrétion professionnelle.

En droit canadien, dans les arrêts R. c. Cole[48] de même que dans R. c. Morelli[49] la Cour suprême a expressément reconnu que les Canadiens peuvent raisonnablement s'attendre à la protection de leur vie privée à l'égard des renseignements contenus dans leurs propres ordinateurs personnels de même que dans les ordinateurs de travail, lorsque leur utilisation à des fins personnelles est permise ou raisonnablement prévue. Dans R. c. Cole, le juge Fish, au nom de la majorité explique que :

> [...] les ordinateurs qui sont utilisés d'une manière raisonnable à des fins personnelles — qu'ils se trouvent au travail ou à la maison — contiennent des renseignements qui sont significatifs, intimes et qui ont trait à l'ensemble des renseignements biographiques de l'utilisateur. Au Canada, la Constitution accorde à chaque personne le droit de s'attendre à ce que

46. 234 F.R.D. 674, 687 (N.D. Cal. 2006).

47. Article 29, Data Protection Working Party, Opinion on data protection issues related to search engines, adopted on 4 April 2008, p. 4, en ligne : <http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/ wpdocs/2008_fr.htm >.

48. 2012 CSC 53, [2012] 3 R.C.S. 34.

49. 2010 CSC 8, [2010] 1 R.C.S. 253.

> l'État respecte sa vie privée à l'égard des renseignements personnels de ce genre.[50]

Les moteurs de recherche compilent les listes de mots-clés des requêtes introduites par l'usager. Ils peuvent accumuler des informations sur les faits et gestes de leurs usagers qui sont tout à fait comparables aux renseignements qui se retrouvent dans la plupart des ordinateurs utilisés couramment. Omer Tene explique à ce sujet que « Google keeps a record of all search queries linked to a specific Internet Protocol (IP) adress »[51]. Ces requêtes en forme de mots-clés peuvent être conservées en relation avec l'adresse IP de l'usager.

Cela pose la question de la mesure dans laquelle il peut être loisible au moteur de recherche de disposer des informations relatives à de telles requêtes des usagers. Deux hypothèses d'utilisation de ces données doivent être envisagées.

Premièrement, il y a l'usage des données par le moteur lui-même ou par ses partenaires commerciaux aux fins de faire du profilage ou du marketing ciblé. Il existe de bons arguments pour réclamer un encadrement des pratiques à cet égard.

Deuxièmement, l'existence de données permettant de rattacher une personne à des mots-clés ou autres renseignements sur une requête de recherche présente le risque de générer des données sur les habitudes ou les intérêts des chercheurs. La création d'un tel répertoire engendre en soi le risque qu'il puisse éventuellement être réclamé par les tiers et les autorités gouvernementales ou les forces de police.

S'agissant des données utilisées par le moteur lui-même ou par ses partenaires, d'aucuns pourraient estimer que les moteurs de recherche ont besoin de conserver et de traiter ces données afin de répondre efficacement aux requêtes des usagers. Les usagers attendent des moteurs de recherche qu'ils délivrent en quelques fractions de secondes une liste de liens pertinents à ce qu'ils cherchent. Pour y arriver, les moteurs de recherche doivent pratiquement « deviner » l'état d'esprit de l'usager qui introduit une requête de recherche. Omer Tene remarque que « Google faces the daunting task of having to guess what users intend, essentially 'read their minds' based on two or three words they enter as a search query »[52].

Or, les mêmes mots-clés peuvent prendre des significations passablement différentes selon les multiples contextes. Les moteurs de recherche peuvent donc avoir besoin d'informations qui renseignent à l'égard du contexte spécifique de chaque usager. L'information découlant de ses requêtes antérieures ou de ses habitudes peut

50. R. c. Coles 2012 CSC 53, [2012] 3 R.C.S. 34. par. 2.

51. Omer Tene, « What Google Knows : Privacy and Internet search engines », en ligne : <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021490>; MSNBC, Google Tightens Privacy Measures, Company promised to wrap a cloak of anonymity around search requests, en ligne : <http://www.msnbc.msn.com/id/17617234/>.

52. Omer Tene, « What Google Knows : Privacy and Internet search engines », p. 20, en ligne : <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1021490>.

fournir des informations contextuelles utiles pour accroître la pertinence des résultats qui seront délivrés à l'usager.

Tant que l'information sur les requêtes de recherche des usagers est conservée aux fins d'assurer un meilleur service aux usagers, il paraît légitime de postuler qu'elle est conservée et traitée aux fins d'assurer un service de qualité. La démarche procède donc d'un impératif d'assurer la qualité et la pertinence des résultats de recherche. Une réglementation qui limiterait ces capacités de conservation pourrait accroître les risques de biais ou de résultats mal ciblés.

Quant aux informations mises à la disposition des partenaires commerciaux, l'on doit forcément observer qu'elles sont traitées avec le consentement à tout le moins implicite de l'usager. Les conditions d'utilisation des moteurs de recherche peuvent indiquer que ceux-ci se réservent la possibilité d'utiliser ces données avec des partenaires. Dans une large mesure, c'est en quelque sorte le prix que l'usager doit payer pour bénéficier du service. À l'instar des publications gratuites financées par la publicité, les moteurs de recherche fonctionnent selon un modèle commercial en vertu duquel on propose un auditoire à une entité désireuse de bénéficier de visibilité publicitaire.

Dans un tel modèle, il revient aux États, compte tenu de l'importance qu'ils reconnaissent au droit à la vie privée, de déterminer selon quelles balises les moteurs de recherche peuvent avoir le loisir de proposer des auditoires à des annonceurs en faisant usage de données personnelles à des fins de ciblage publicitaire.

L'autre type de risque paraissant inhérent aux moteurs de recherche est celui qui découle de la constitution de répertoires d'informations plus ou moins reliés aux personnes et qui pourraient intéresser les forces de police ou les tiers impliqués dans un processus judiciaire.

Les forces de l'ordre ne se privent pas pour réclamer l'accès à ce type de données. Omer Tene explique que tous les moteurs de recherche indiquent qu'ils vont forcément se conformer aux demandes des autorités gouvernementales et judiciaires pour de l'information qu'ils ont en leur possession. Par exemple, les Règles de confidentialités et conditions d'utilisation de Google prévoient que :

> Nous ne partagerons des données personnelles avec des entreprises, des organisations ou des personnes tierces que si nous pensons en toute bonne foi que l'accès, l'utilisation, la protection ou la divulgation de ces données est raisonnablement justifiée pour :
>
> se conformer à des obligations légales, réglementaires, judiciaires ou administratives;
>
> faire appliquer les conditions d'utilisation en vigueur, y compris pour constater d'éventuels manquements à celles-ci;
>
> déceler, éviter ou traiter des activités frauduleuses, les atteintes à la sécurité ou tout problème d'ordre technique;

> se prémunir contre toute atteinte aux droits, aux biens ou à la sécurité de Google, de ses utilisateurs ou du public, en application et dans le respect de la loi.[53]

En fin de compte, le risque de surveillance découlant de l'activité des moteurs de recherche découle principalement du fait que les répertoires qu'ils constituent peuvent devenir intéressants pour les forces de police. Ce ne sont pas les pratiques des moteurs de recherche avec des répertoires comme telles qui posent des risques. Dans la plupart des situations, les données personnelles sont recueillies, conservées et traitées afin de procurer un service fiable aux usagers.

Les véritables risques résultent de la possibilité que des tiers exigent d'accéder à des données qui ont été compilées et conservées aux fins d'assurer un meilleur service aux usagers. Face à ce genre de risques, il paraît intéressant d'envisager l'hypothèse d'une immunité qui pourrait être conférée à ces renseignements.

Les données conservées par les moteurs de recherche s'apparentent au savoir que peut avoir acquis un bibliothécaire auquel on fait appel pour nous aider dans nos recherches. Le bibliothécaire pourra connaître le contexte de nos recherches et sera du coup en mesure de répondre plus efficacement à nos besoins. En somme, la situation du moteur de recherche s'apparente à la relation de confiance qui existe entre un professionnel et un usager-client.

En termes d'équivalence fonctionnelle, le moteur de recherche présente plusieurs analogies avec les fonctions d'une bibliothèque de référence. Plusieurs des fonctions qu'il assure s'assimilent à celles qu'un bibliothécaire accomplit avec son savoir professionnel, les outils documentaires à sa disposition et la connaissance qu'il possède du chercheur. C'est pourquoi les obligations légales et déontologiques du bibliothécaire paraissent constituer un bon guide de départ aux fins de préciser les devoirs des moteurs de recherche dans le contexte d'Internet.

Conférer aux données conservées par les moteurs de recherche une immunité qui serait de la nature du secret professionnel permettrait de protéger les usagers aussi bien des tentations des entreprises de monnayer, sans précautions, les informations personnelles qu'elles possèdent sur les individus ayant logé des requêtes de recherche. De même une telle approche permettrait de fonder les balises pour encadrer les pratiques des forces de police en matière d'accès aux données de recherche des usagers. Une telle approche procurerait également de réelles protections à l'égard des risques fréquemment invoqués par ceux qui craignent les effets à long terme de l'accumulation de données sur les requêtes de recherche des usagers.

À l'instar de certains régimes juridiques du secret professionnel, ce ne serait que moyennant une démonstration claire que des activités illicites ont eu lieu qu'il serait

53. Google, Règles de confidentialités et conditions d'utilisation, 25 mars 2016, en ligne : <https://www. google.com/intl/fr/policies/privacy/>, consulté le 30 avril 2016.

possible d'accéder à des informations sur les utilisateurs de moteurs de recherche. Le tout devant se décider sous surveillance (supervision) judiciaire.

En somme, les meilleures garanties de la vie privée du chercheur-utilisateur de moteur de recherche supposent de considérer les moteurs de recherche comme des bibliothécaires professionnels. Dans une telle situation, le moteur de recherche se trouve dans une situation ressemblant à celle du bibliothécaire auquel l'usager demande assistance. À l'instar du bibliothécaire, le moteur de recherche accumule des connaissances à l'égard de l'usager, ses demandes, ses champs d'intérêts. Ces connaissances sont accumulées afin de mieux servir l'usager.

Le critère de « service à l'usager » peut contribuer à départager les pratiques de collecte d'informations sur les usagers qui sont acceptables de celles qui ne le sont pas ou qui posent problème.

Tant que le moteur de recherche se sert des connaissances accumulées sur l'usager afin de lui proposer des liens correspondant mieux à ses préférences, il est difficile d'y voir une atteinte à la vie privée. On pourrait postuler qu'il en est de même des liens publicitaires dans la mesure ou les services du moteur de recherche sont proposés sans coûts directs aux usagers. Par contre, les renseignements qui seraient remis à des tiers posent plus de difficultés.

C'est pourquoi le moteur de recherche devrait, à l'égard des renseignements personnels qu'il collecte sur les usagers, être tenu à une obligation de secret. Par exemple, le Code de déontologie de la corporation des bibliothécaires du Québec énonce la règle du secret professionnel. Il précise que « Le bibliothécaire doit respecter le secret de toute information de nature confidentielle obtenue dans l'exercice de sa profession »[54].

S'appuyant sur les règles d'associations de documentalistes et bibliothécaires, les Principes directeurs pour la gestion des associations professionnelles d'archivistes, de bibliothécaires et de documentalistes établis en 1989 par Russel Bowden pour le compte de l'UNESCO présentent un « exemple-modèle de code de déontologie » dans lequel on préconise la reconnaissance d'un devoir de secret professionnel. Le paragraphe (h) de la section 2 est ainsi libellé :

> (i) Le bibliothécaire ne doit pas communiquer ni permettre que soient communiqués à quiconque des documents, des informations ou des dossiers administratifs (sur support papier ou sur support électronique) qui lui ont été confiés à titre confidentiel, ni utiliser cette information à des fins autres que son objet inital sans le consentement préalable du client. Cette obligation demeure après la cessation de la relation entre le bibliothécaire et son client.

54. Code de déontologie de la Corporation des bibliothécaires professionnels du Québec, art. 33, en ligne : <http://www.cbpq.qc.ca/corporation/loi_et_regl/deonto.html>.

(ii) Le bibliothécaire est dégagé de l'obligation énoncée à l'alinéa (i) ci-dessus pour autant que la loi l'exige ou pour les besoins de sa défense devant la Commission de discipline si des accusations sont portées contre lui.[55]

Le document explique que le champ d'application du paragraphe est expressément limité aux documents et informations confiés « à titre confidentiel ». La question se pose de savoir si le bibliothécaire peut considérer, sans l'accord exprès du client, que l'information n'avait pas un caractère confidentiel. Le principe général est clair : aucun renseignement concernant un emprunteur ne doit être fourni à quiconque ne fait pas partie du personnel de la bibliothèque. Les exceptions ne sont admises que lorsqu'il est parfaitement clair pour le bibliothécaire que l'emprunteur ne s'y opposerait pas. L'interdiction faite dans le code vise la fourniture de l'information à des « tiers ».

Il en résulte que les autorités de police qui souhaiteraient accéder aux données détenues par les moteurs de recherche sur les usagers ne devraient pouvoir le faire que sur autorisation judiciaire et uniquement dans des circonstances strictement délimitées.

Si l'on est conséquent avec les impératifs de la protection des données personnelles, il faut avoir le courage d'aller jusqu'au bout et réclamer l'immunité pour ces données. Cette approche paraît à long terme plus viable que celle consistant à forcer les moteurs de recherche à une efficacité plafonnée (en raison de l'interdiction de faire usage d'indices découlant des patterns de recherche des usagers). Il n'y a pas de raison de protéger la vie privée au prix d'une dégradation généralisée de la qualité des recherches.

Ce qui constitue le risque de surveillance n'est pas en soi le fonctionnement des moteurs de recherche mais le caractère insuffisamment balisé du droit des tiers et des forces de police d'avoir accès aux données générées par les processus de recherche. Devant de tels enjeux, l'approche à privilégier est de rechercher un balisage des prérogatives des forces de police et autres entités publiques et privées.

55. Russel Bowden, Principes directeurs pour la gestion des associations professionnelles d'archivistes, de bibliothécaires et de documentalistes, Paris, UNESCO, 1989, 128 p., en ligne : <http://www.unesco.org/ webworld/ramp/html/r8911f/r8911f00.htm>.

CONCLUSION

Avec la brosse à dents, les moteurs de recherche sont assurément parmi les principaux objets de notre quotidien. Leur encadrement normatif est un enjeu crucial. Ces outils contribuent à nous relier avec les gisements d'information caractéristiques de la société numérique.

La technologie constitutive des moteurs de recherche est le premier ensemble de normes qui obligent, empêchent ou habilitent les personnes qui recherchent des informations ou qui sont concernées par celles-ci. Les moteurs de recherche sont des objets a priori normés par la technologie. Ils appliquent de puissants algorithmes afin de livrer en une fraction de secondes des résultats qui se veulent pertinents et ce, compte tenu d'une multitude de contextes.

Le droit étatique encadre évidemment les activités des moteurs de recherche sur Internet. Ceux-ci sont principalement encadrés par des régimes de responsabilité conditionnels à leur connaissance du caractère illicite du matériel vers lesquels pointent les liens hypertextes qu'ils livrent aux usagers.

Au nom d'une conception extensive d'un droit des individus à faire retirer des informations publiques, émerge une inquiétante réglementation visant à censurer les résultats livrés par les moteurs de recherche à l'égard de documents tout à fait licites.

Pourtant, les enjeux et risques des moteurs de recherche doivent être appréhendés en tenant compte aussi bien des impératifs de protection de la vie privée des personnes que de ceux de la liberté d'expression. La liberté d'expression est comprise dans les pays démocratiques comme incluant un droit de rechercher librement les informations licites.

En contraignant ceux qui souhaitent le maintien des liens hypertextes conduisant à des documents licitement publics à en défendre le bien-fondé, la décision Google Spain de la Cour de justice de l'Union européenne paraît incompatible avec le droit canadien. Elle privilégie une vision extrême du droit à la vie privée et ne tient pas compte que la liberté d'expression comprend le droit de rechercher librement des informations qui sont licites. Une pareille reconnaissance d'un droit des individus visés dans des documents licitement publics à les faire occulter est difficile à concilier avec une vision démocratique de la liberté d'expression.

Depuis l'arrêt Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401 de la Cour suprême du Canada, il est difficile de postuler qu'un droit au déréférencement tel que celui mis de l'avant en droit européen puisse être compatible avec la liberté d'expression.

Par contre, il existe des enjeux majeurs au plan de la protection de la vie privée. Des enjeux qui concernent effectivement ce qui est au cœur de ce droit. Les informations, les traces et les informations révélatrices des comportements des utilisa-

teurs de moteurs de recherche constituent des gisements d'information relevant du noyau dur de la vie privée.

La faculté des moteurs de recherche et des autorités d'accéder à ces informations et de les partager pose de réels défis au regard de la protection effective des droits fondamentaux.

Si elles ne sont pas adéquatement balisées, les pratiques de conservation de données sur les requêtes des usagers présentent des risques de constitution de répertoires de données qui pourraient être utilisées par les autorités publiques ou privées à des fins de surveillance des citoyens. À l'égard de ce type de risque, il faut préférer les solutions qui limitent le droit des autorités publiques et privées à accéder aux données relatives aux utilisateurs des moteurs de recherche.

Les enjeux relatifs à la vie privée du chercheur lui-même nécessitent de reconnaître aux moteurs de recherche une obligation s'apparentant au secret professionnel. Non seulement ces derniers devraient-ils être assujettis à un devoir strict de discrétion au sujet des données relatives aux usagers mais les forces de police ne devraient pouvoir accéder à ces données que dans des circonstances très exceptionnelles et moyennant un encadrement judiciaire.