



Commissariat  
à la protection de  
la vie privée du Canada

# Réputation en ligne

Que dit-on à mon sujet?

*Document de travail préparé par le Groupe des politiques et de la recherche du Commissariat à la protection de la vie privée du Canada*



# Table des matières

Résumé .....	1
Introduction .....	1
Réputation et respect de la vie privée .....	2
Quelques caractéristiques de la réputation en ligne .....	2
Risques d'atteinte à la réputation dans le monde réel .....	3
Publication de renseignements au sujet des autres .....	4
Un mot à propos des enfants.....	5
Le droit à l'oubli .....	5
Recours en vertu de la LPRPDE .....	6
Autres formes de recours en place ou possibles .....	8
Organisations .....	8
Législateurs .....	10
Tribunaux .....	11
Organismes de réglementation.....	12
Technologues .....	12
Individus .....	13
Éducateurs .....	13
Conclusion.....	14
Ressources supplémentaires .....	16

# Résumé

Le présent document de travail se penche sur la question de la réputation en ligne dans le contexte de la protection de la vie privée et explique les difficultés auxquelles font face les personnes dont la réputation a été entachée par suite de la publication en ligne de renseignements à leur sujet. En examinant l'expérience du Commissariat à la protection de la vie privée du Canada (le Commissariat), nous espérons faire avancer la discussion sur la meilleure façon d'aider les personnes lorsque des renseignements à leur sujet qu'elles ont elles-mêmes mis en ligne ou que d'autres ont mis en ligne portent atteinte à leur réputation. Nous solliciterons les commentaires des intervenants, dans le but ultime de présenter une position quant aux solutions à adopter.

## Introduction

En 2015, le Commissariat a choisi la réputation et le respect de la vie privée parmi ses priorités en matière de protection de la vie privée pour les cinq prochaines années. Le Commissariat met l'accent sur les risques d'atteinte à la réputation qui découlent de la grande quantité de renseignements personnels publiés en ligne de même que sur les mécanismes dont on dispose ou que l'on pourrait mettre en place pour gérer ces risques. Au cours de l'exercice d'établissement des priorités entrepris par le Commissariat, les intervenants et la population canadienne ont indiqué qu'ils étaient conscients des avantages personnels et professionnels associés à leur participation au monde numérique, mais qu'ils étaient de plus en plus préoccupés par leur réputation en ligne.

D'une part, les gens veulent avoir une présence en ligne et sont convaincus que le fait de bien choisir ce qu'ils publient contribuera à forger leur réputation en ligne. D'autre part, ils n'ont que peu de contrôle sur ce que d'autres personnes publient à leur sujet et sur la façon dont leurs renseignements personnels peuvent être interprétés par d'autres personnes ou par des organisations.

Shakespeare a écrit « La réputation est un préjugé vain et fallacieux : souvent gagnée sans mérite et perdue sans justice! »<sup>1</sup>. Cette observation revêt tout son sens dans l'environnement numérique, où l'information n'est pas simplement publiée, mais aussi manipulée, sortie de son contexte et interprétée<sup>2</sup>. En outre, tout contenu présenté en ligne peut être consulté et communiqué par des millions de personnes, et peut refaire surface des mois, voire des années après la publication, dans divers contextes, à des fins intentionnelles ou non.

Depuis l'avènement des médias sociaux, la réputation en ligne et ses répercussions possibles sur la vie réelle et virtuelle des gens ont fait couler beaucoup d'encre. Les technologies d'Internet ont entraîné un changement de paradigme dans la façon dont les réputations se forment, et la société doit composer avec les effets qui se font sentir sur les relations sociales et les possibilités professionnelles. Il faudrait approfondir la discussion sur le type de recours dont disposent les personnes qui contestent les renseignements personnels publiés en ligne à leur sujet.

Le présent document vise à susciter la discussion sur les moyens qui pourraient permettre de régler les problèmes associés à la permanence des renseignements personnels en ligne et aux répercussions sur la réputation. Nous nous tournons vers les organisations, les universitaires, les groupes de défense des droits, les ingénieurs en logiciel et les autres parties intéressées pour trouver des idées relativement aux façons nouvelles et innovatrices de protéger la réputation et la vie privée et d'apporter des améliorations à cet égard. Afin d'orienter la discussion, nous avons présenté l'expérience et les réflexions du Commissariat en ce qui touche les limites et les difficultés associées à la capacité des individus à assurer le respect de leur vie privée en ligne. Nous invitons les parties intéressées à présenter un mémoire sur les réponses possibles à certaines questions posées à la fin du présent document, en vue d'élaborer une position pour le Commissariat sur la meilleure façon de s'attaquer aux enjeux relatifs à la réputation.

## Réputation et respect de la vie privée

Le Larousse définit comme suit le terme « réputation » : « Opinion favorable ou défavorable du public pour quelqu'un, quelque chose » et « Manière dont quelqu'un, quelque chose est connu, considéré dans un public »<sup>3</sup>. Ces opinions et croyances reposent sur l'information dont on dispose au sujet d'une personne, et sur la façon dont cette information est interprétée et évaluée par d'autres. La réputation est une forme de jugement que l'on porte sur le caractère, l'apparence et les compétences professionnelles d'une personne, ou sur tout attribut qui se prête à une opinion. La capacité d'une personne à modifier le jugement des autres et, par le fait même, à gérer sa réputation dépend de sa capacité de contrôler l'accès des autres à ses renseignements personnels de même que le contexte dans lequel ces renseignements sont consultés et utilisés.

Le type et la quantité de renseignements que les gens choisissent de communiquer à leur sujet varient généralement en fonction des circonstances. Il y a plus de 50 ans, le sociologue Erving Goffman<sup>4</sup> utilisait la métaphore de la représentation théâtrale pour décrire la façon dont les gens se présentent et la quantité de renseignements qu'ils choisissent de révéler à leur sujet, sur la scène publique par opposition à un contexte plus intime, dans les coulisses. En public, les échanges sociaux reposent sur la compréhension des normes de comportement propres à un groupe social donné. En privé, les gens se sentent plus à l'aise et plus libres de s'exprimer comme ils le désirent que de suivre un scénario.

Hors ligne, les gens ont davantage l'occasion d'exercer une influence sur la façon dont les autres les perçoivent, et ce, de diverses manières, notamment par leur comportement, leur apparence, leurs réalisations et leurs aptitudes à communiquer. Par ailleurs, l'information met plus de temps à circuler dans le monde réel. L'évolution d'une réputation en ligne est plus complexe, car dans l'environnement numérique, les gens portent généralement des jugements sur les autres en fonction de l'information qu'ils lisent ou des images qu'ils voient, souvent sans l'avantage d'un contact personnel et pas forcément dans le contexte pour lequel il était destiné. Qui plus est, une fois mise en ligne, l'information acquiert des caractéristiques ayant une incidence sur la réputation.

## Quelques caractéristiques de la réputation en ligne



danah boyd, experte dans le domaine des médias sociaux et chercheuse principale chez Microsoft, définit quatre caractéristiques propres à l'information publiée sur les sites de réseautage social<sup>5</sup>. Les idées de M<sup>me</sup> boyd se transposent facilement au monde numérique en général. D'abord, les renseignements en ligne sont de nature persistante, c'est-à-dire qu'ils sont enregistrés et qu'il est difficile, voire impossible, de les supprimer une fois qu'ils ont été téléchargés. Ensuite, ils peuvent être reproduits. Ils peuvent aussi être consultés par un vaste public auquel ils ne sont pas nécessairement destinés. Enfin, ils peuvent être consultés au moyen d'une fonction de recherche.

Une autre manière de conceptualiser la façon dont l'information est transformée en ligne et l'incidence de cette transformation sur la réputation nous est donnée par l'analogie de la maison aux miroirs décrite par Johnson, Regan et Wayland dans leur article<sup>6</sup> concernant l'incidence d'Internet sur l'accessibilité des documents publics. Selon les auteurs, il faut réexaminer le processus qui permet de donner accès à des documents publics, en accordant la priorité au respect de la vie privée, étant donné qu'Internet déforme l'information tout comme une maison aux miroirs déforme les images. L'extrait suivant est particulièrement pertinent aux fins de la discussion sur le respect de la vie privée et la réputation :

*Une maison aux miroirs est un complexe d'images réverbérées, mises en lumière et ombragées qui produisent une expérience étonnante. L'individu voit une image déformée de lui-même par rapport à la perception de soi qu'il a habituellement. [traduction]*

La réverbération fait référence à l'information qui a été publiée à une fin particulière et qui est par la suite utilisée à une autre fin. Le fait de récupérer une photo sur un site de médias sociaux et de la vendre à une agence de publicité – ce qui est arrivé à une famille américaine dont une photo personnelle s'est retrouvée sur un panneau d'affichage faisant de la publicité pour une épicerie tchèque<sup>7</sup> – est un bon exemple d'effet kaléidoscope. Dans un autre cas, particulièrement marquant, une entreprise biomédicale suisse a utilisé la photo d'une fillette canadienne pour faire la publicité de tests génétiques visant à dépister le syndrome de Down. La photo avait été prise sans autorisation sur le blogue de la mère<sup>8</sup>.

La mise en lumière et l'ombre renvoient à la notion selon laquelle l'information peut prendre de la valeur ou en perdre, selon le contexte. Par conséquent, l'information peut jouer un rôle déformé lorsqu'il s'agit de forger la réputation d'une personne. À titre d'exemple, l'information qui figure en tête d'une liste de résultats de recherche ou vers le haut de la liste est mise en évidence peu importe son importance, tandis que l'information qui pourrait être pertinente, si elle figure au bas de la liste des résultats, sera estompée. Des études<sup>9</sup> ont révélé que les gens qui parcourent les résultats de recherche tendent à se concentrer sur le haut de la page. Lorsqu'il s'agit de cliquer sur des liens, les résultats d'une étude sont encore plus frappants<sup>10</sup>, puisque la grande majorité des gens ne sélectionne que les liens figurant à la première page des résultats de recherche. Ce type de présélection de l'information peut avoir une incidence négative.

Prenons, par exemple, l'émergence de la sous-culture de l'humiliation<sup>11</sup>, où les gens sont dépréciés pour rire dans les médias populaires et où les incidents de dénigrement ou de cruauté en ligne peuvent être vus par des millions de personnes. Comme les algorithmes des moteurs de recherche produisent généralement les résultats les plus populaires, peu importe leur contenu, le contenu viral peut se voir accorder fortuitement la priorité au lieu, et souvent au détriment, de renseignements plus pertinents et représentatifs au sujet d'une personne. Pour donner un exemple extrême<sup>12</sup> du préjudice qui peut être subi, citons le cas de parents qui ont tenté pendant plusieurs années de mettre fin à la diffusion en ligne des photos du corps déformé de leur fille victime d'un accident en Californie. Les photos prises sur les lieux de l'accident auraient été communiquées par des employés d'une autorité chargée de l'application de la loi et publiées sur des milliers de sites Web, avec nombre de commentaires cruels. Bien que la famille ait fini par s'entendre avec l'autorité chargée de l'application de la loi, les images demeurent faciles à trouver au moyen de moteurs de recherche.

Les médias sociaux reposent par définition sur le principe de la participation individuelle et de la communication de contenu. Les utilisateurs sont invités à télécharger des renseignements sur eux-mêmes et sur les autres lorsqu'ils naviguent dans le monde numérique. Qu'il s'agisse de sections de commentaires, de sites de partage de photos, de blogues ou de réseaux sociaux, les utilisateurs ont une multitude d'occasions de fournir des renseignements personnels. En fait, certaines fonctions demandent expressément aux utilisateurs de communiquer de l'information au sujet de personnes qu'ils connaissent, notamment de télécharger des listes de contacts, d'étiqueter des photos et d'envoyer des invitations à s'inscrire au site. On pourrait faire valoir que nos expériences en ligne ont donné lieu à la normalisation de la publication de renseignements à notre sujet et au sujet des intéressés.

Compte tenu des propriétés uniques des renseignements une fois qu'ils sont publiés en ligne, les intéressés exercent peu de contrôle sur ceux qui peuvent voir ces renseignements, la façon dont ils sont interprétés et l'incidence qu'ils auront sur leur réputation. Pour compliquer encore les choses, les gens n'ont aucun moyen définitif de savoir ce que d'autres ont publié à leur sujet dans l'environnement numérique. Le téléchargement de renseignements et d'images en ligne concernant d'autres personnes est un processus qui nécessite un simple clic et n'exige généralement pas que celui qui publie l'information obtienne le consentement des intéressés.

## Risques d'atteinte à la réputation dans le monde réel

Une grande partie du discours actuel sur la réputation en ligne est axée sur la connaissance des risques et sur l'atténuation des effets néfastes qui pourraient se produire. Les risques d'atteinte à la réputation sont souvent contextuels, dans la mesure où l'information qui est appropriée dans un contexte peut être inappropriée dans un autre, où elle peut porter atteinte à la réputation. À cet égard, citons l'exemple classique des photos de personnes en état d'ébriété qui font la fête. Ces photos qui, au départ, ont été partagées entre amis, finissent par être vues par des employeurs actuels ou éventuels. C'est ainsi qu'une enseignante américaine a perdu son emploi à cause d'une photo de vacances publiée sur Facebook qui la présente tenant un verre de vin dans une main et un verre de bière dans l'autre<sup>13</sup>.



De plus en plus, la réputation en ligne est prise en compte dans des décisions du monde réel. Dans ce contexte, des décisions telles que celles concernant l'octroi de crédit ou l'admission à un programme d'études peuvent reposer sur des renseignements en ligne désuets, inexacts ou incomplets. Et pour couronner le tout, le gens ne savent généralement pas que l'information en ligne peut limiter leurs possibilités, car à l'heure actuelle, le processus décisionnel associé à nombre de ces décisions importantes n'est pas transparent<sup>14</sup>.

Les services de gestion de la réputation recommandent depuis longtemps aux personnes d'effectuer régulièrement des recherches sur leur nom afin d'être au courant des résultats de recherche préjudiciables et d'être en mesure d'atténuer les risques d'atteinte à la réputation. Diverses stratégies ont d'ailleurs été mises au point pour « optimiser » les résultats de recherche de sorte que les résultats favorables s'affichent en premier, mais la gestion de la réputation est un processus accaparant et coûteux exigeant des ressources techniques et financières qui peuvent être hors de portée du citoyen ordinaire. De plus, en raison de la personnalisation<sup>15</sup> accrue des recherches, deux personnes effectuant une recherche sur le même nom obtiendront probablement des résultats différents, ce qui complique encore davantage les efforts en vue d'exercer une influence sur les résultats de recherche.

Une fois qu'une réputation en ligne a été ternie par un contenu préjudiciable, il est difficile de renverser la situation. En raison de la permanence de l'information en ligne, le temps n'efface plus les erreurs ou les mauvaises décisions du passé. Dans la foulée des émeutes de la Coupe Stanley en 2011 à Vancouver, les services de police ont demandé au public de fournir des photos et des vidéos, qu'ils ont publiées en ligne, et ils ont fait appel à la population pour établir l'identité des suspects. Or, les personnes identifiées comme étant des émeutiers n'ont peut-être jamais été accusées ni reconnues coupables. Quant à celles qui ont effectivement été reconnues coupables, elles continueront d'être associées à cet événement longtemps après qu'elles auront payé leur dette à la société, ce qui pourrait avoir une incidence sur de nombreux aspects de leur vie, dont leur employabilité.

## Publication de renseignements au sujet des autres

Certains sites Web ont vocation à faire connaître les renseignements personnels que les gens affichent au sujet des autres. Au nombre de ces sites figurent ceux visant à faciliter l'échange de renseignements sur les professionnels, comme les médecins et les enseignants. D'autres types de sites plus sournois encouragent la publication de renseignements personnels de nature sensible par des gens qui cherchent à humilier les autres pour s'amuser ou pour se venger, notamment les soi-disant sites de dénonciation de ceux qui ne se comportent pas selon les normes sociales reconnues<sup>16</sup>.

Les sites Web et d'autres services en ligne sont structurés de façon à permettre, voire à encourager, la publication de renseignements personnels au sujet d'autres personnes, notamment au moyen de l'étiquetage de photos, du téléchargement de listes de contacts et de la publication de commentaires. L'obtention du consentement des amis avant de publier des renseignements les concernant est rarement prévue au programme. Les moteurs de recherche, qui permettent de trouver de l'information en quelques clics, ne font qu'amplifier le problème.

La fonction de saisie semi-automatique des moteurs de recherche est un autre exemple de l'incidence de l'architecture des services en ligne sur notre réputation. Il s'agit de l'algorithme qui prédit les mots que l'on pourrait entrer en saisissant une requête, et qui propose des combinaisons de mots possibles. Cette fonction a donné lieu à des litiges<sup>17</sup> dans divers pays où il est arrivé que des suggestions automatisées communiquent une caractéristique désobligeante ou fausse au sujet d'une personne. Pour régler ce problème, Google a mis en place un mécanisme<sup>18</sup> permettant aux utilisateurs de signaler les suggestions choquantes de la saisie semi-automatique en vue de leur suppression.

En vertu de la législation canadienne relative à la protection de la vie privée dans le secteur privé, les organisations doivent obtenir le consentement de la personne concernée afin de recueillir, d'utiliser et de communiquer ses renseignements personnels dans le cadre d'activités commerciales, sauf dans de rares exceptions. Les personnes qui publient de l'information à titre personnel ne sont pas visées par les lois relatives à la protection de la vie privée applicables au secteur privé.

## Un mot à propos des enfants

Les enfants et les adolescents sont particulièrement vulnérables lorsqu'il est question de leur réputation en ligne. Non seulement ils naviguent eux-mêmes sur Internet alors qu'ils sont encore très jeunes, mais aussi leurs parents téléchargent leurs photos et des anecdotes amusantes à leur propos dès leur plus tendre enfance. Les écoles exigent que les élèves utilisent les technologies numériques dans le cadre du programme scolaire, et l'utilisation des technologies par leurs pairs pousse les enfants à mener leur vie sociale en ligne. Des études<sup>19</sup> ont révélé que les enfants ne communiquent pas forcément leurs renseignements personnels de leur plein gré, mais choisissent plutôt de le faire afin de participer à des activités sociales en ligne.



Ces facteurs représentent un défi de taille en ce qui concerne la capacité des jeunes à contrôler les renseignements numériques à leur sujet et, ainsi, leur réputation. Dans leur ouvrage intitulé *Born Digital*, Palfrey et Gasser<sup>20</sup> font remarquer ce qui suit en ce qui concerne une adolescente fictive de 16 ans :

*À l'ère numérique, son identité sociale peut être forgée par des associations qui sont visibles au public à tout moment par l'intermédiaire de liens sur les réseaux sociaux [...]. Puis, les gestes posés par ses amis et la réputation changeante de ces derniers peuvent avoir une incidence sur son identité et sa réputation.* [traduction]

Un autre facteur de risque pour la réputation tient au fait que l'enfance est une période d'expérimentation au cours de laquelle l'enfant teste les limites. Or, en raison de la permanence de l'information numérique, les transgressions ou les extravagances de l'enfance demeureront faciles à trouver et peuvent avoir une incidence durable sur la réputation. À mesure que grandit la première génération numérique, il nous reste à voir si les modes de comportement des jeunes seront influencés par le fait de savoir que ce qu'ils font en tant qu'enfants les suivra pour le reste de leur vie. De façon générale, quelles seront les répercussions de ce dossier permanent conservé pendant toute notre vie? Un enfant qui a une réputation de tyran verra-t-il cette étiquette le suivre jusqu'à l'âge adulte? Sera-t-il possible d'oublier les erreurs du passé? Les risques accrus d'atteinte à la réputation en ligne qui caractérisent notre époque actuelle auront-ils à terme une incidence sur le comportement et les types de choix qui seront faits ou ne seront pas faits?

Pour essayer de résoudre ce problème, la Californie a adopté une loi intitulée *Privacy Rights for California Minors in the Digital World*<sup>21</sup>, qui oblige les entreprises, les sites Web et les concepteurs d'applications à donner aux enfants âgés de moins de 18 ans la possibilité de supprimer l'information qu'ils ont eux-mêmes publiée. Toutefois, cette loi ne vise pas les renseignements que d'autres ont publiés au sujet de mineurs.

## Le droit à l'oubli

Une atteinte à la réputation peut prendre de graves proportions lorsque les moteurs de recherche accordent de l'importance à des renseignements personnels qui autrement seraient restés dans l'ombre. En mai 2014, la Cour de justice de l'Union européenne (CJUE) a statué<sup>22</sup> que les moteurs de recherche devaient offrir à tous les Européens la possibilité de demander la suppression des résultats de recherche renvoyant à des informations à leur sujet qui sont « inadéquates, pas ou plus pertinentes ». L'arrêt a été rendu dans la foulée d'une affaire mettant en cause un Espagnol qui s'est insurgé de voir que les résultats d'une recherche de son nom sur Google comportaient des liens menant à des articles de journaux faisant état d'une dette dont il s'était acquitté depuis longtemps. Il estimait que ces détails sur sa vie, qui n'étaient plus pertinents, nuisaient à sa réputation.

L'arrêt de la CJUE est qualifié de « droit à l'oubli », mais en réalité, l'information en cause n'est pas supprimée. L'arrêt ne vise que les résultats des moteurs de recherche et permet que l'information originale demeure sur le site Web où elle a été publiée. Afin de tenir compte du fait que l'information en cause demeure en ligne, certains analystes<sup>23</sup> affirment que l'arrêt de la CJUE donne aux personnes un moyen de contrôler l'accès à leurs renseignements personnels, et non de les supprimer, en faisant en sorte qu'ils soient plus difficiles à trouver. Pour reprendre les propos d'Isabelle Falque-Pierrotin, présidente de la Commission nationale de l'informatique et des libertés (CNIL) de France ainsi que du groupe de travail Article 29, le droit à l'oubli donne à chacun de nous non pas la possibilité de changer le passé, mais plutôt de contrôler une partie de ce que nous avons fait dans le passé et son aspect numérique<sup>24</sup>.

Au moment de la rédaction du présent document, Google déclarait<sup>25</sup> avoir reçu plus de 351 000 demandes de suppression visant plus de 1,2 million d'adresses URL. L'entreprise a retiré des liens dans près de 42 % des cas. Selon son site Web, Google tient compte d'un certain nombre de facteurs pour décider s'il y a lieu de répondre favorablement à une demande de suppression :

*Nous devons établir un équilibre entre le droit à la vie privée de la personne et les intérêts en faveur de l'accès à l'information, y compris l'intérêt public de même que le droit du webmestre à diffuser des renseignements. Lorsqu'il s'agit d'évaluer les demandes, nous déterminerons si les résultats de recherche en question incluent des renseignements désuets ou non pertinents au sujet de la personne concernée et si ces renseignements présentent un intérêt public<sup>26</sup>. [traduction]*

Le processus décisionnel de Google s'est appuyé sur les lignes directrices du groupe de travail Article 29 relatives à la mise en œuvre de l'arrêt concernant le droit à l'oubli, qui comprend les questions suivantes :

- La personne concernée est-elle une personnalité?
- Le contenu a-t-il été volontairement rendu public par la personne concernée? La personne concernée pouvait-elle raisonnablement savoir que le contenu serait rendu public?
- Les données nuisent-elles de manière disproportionnée à la vie privée de la personne concernée?
- Le résultat de recherche renvoie-t-il à des renseignements présentant un risque pour la personne concernée?

Google a fait l'objet de critiques<sup>27</sup> et l'on a reproché à l'entreprise son manque de transparence sur la façon dont elle s'y prend pour établir un équilibre entre le respect de la vie privée et l'intérêt public, ainsi que l'absence de mécanisme de recours et de surveillance indépendante. Son rôle de décideur de fait relativement à ces questions sociétales empreintes de valeurs a été fortement critiqué. D'ailleurs, Google a elle-même reconnu<sup>28</sup> qu'elle avait de la difficulté à mettre en œuvre la décision et a mis sur pied le Comité consultatif de Google sur le droit à l'oubli<sup>29</sup> dans le but d'obtenir l'opinion d'experts concernant la meilleure façon d'établir un équilibre entre le droit à l'oubli, un droit individuel, et le droit du public à l'information.

Mais il ne faut pas confondre le droit à l'oubli avec le droit à l'effacement en vertu du règlement général sur la protection des données<sup>30</sup> de l'Union européenne. En effet, en vertu du droit à l'effacement, le responsable du traitement des données serait tenu de supprimer les données si elles ne sont plus requises à des fins de traitement, si la personne concernée a retiré son consentement ou si le traitement enfreint toute autre disposition du règlement. Contrairement au droit à l'oubli, qui ne touche que les moteurs de recherche, le droit à l'effacement tient pour responsable l'organisation qui recueille et traite les renseignements au premier chef et renforce les obligations de cette organisation en vertu de la législation sur la protection des données.

## Recours en vertu de la LRPDE

Au Canada, il n'existe pas de loi sur le droit à l'oubli ou le droit à l'effacement en soi. Les gens s'adressent au Commissariat pour obtenir de l'aide lorsqu'ils tombent sur des sites Web qui affichent leurs renseignements personnels sans leur consentement. Le Commissariat surveille la conformité à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LRPDE), qui établit les règles que doivent respecter les organisations du secteur privé lorsqu'elles traitent des renseignements personnels dans le cadre de leurs activités commerciales. De manière générale, les organisations ne peuvent pas recueillir, utiliser ou communiquer des renseignements personnels sans le consentement de l'intéressé à moins qu'une exception



au consentement obligatoire ne s'applique. De même, les dispositions législatives confèrent aux individus le droit d'avoir accès aux renseignements personnels qu'une organisation peut avoir recueillis à leur sujet et de demander que des corrections y soient apportées. Les personnes qui estiment qu'une organisation visée par la LPRPDE ne s'acquitte pas de ses responsabilités aux termes de la Loi peuvent déposer une plainte auprès du Commissariat.

Au nombre des sites Web mis en cause par des personnes qui communiquent avec le Commissariat pour faire état d'atteintes à la réputation, mentionnons les sites de rencontres, les sites où sont reproduites les décisions judiciaires et, en tête de liste, les soi-disant sites de vengeance et de dénonciation<sup>31</sup>. L'une des plus grandes difficultés pour le Commissariat lorsqu'il est saisi d'une plainte pour atteinte à la réputation en ligne consiste à faire valoir sa compétence sur les sites mis en cause, surtout lorsqu'il s'agit de sites étrangers. En pareil cas, il arrive qu'il n'y ait pas de lien réel et substantiel avec le Canada, alors que ce lien est indispensable pour qu'un organisme étranger soit visé par la LPRPDE. De plus, pour que la LPRPDE s'applique, le site Web doit être impliqué dans le cadre d'activités commerciales. Or, il n'est pas rare que des renseignements personnels soient publiés sans le consentement de l'intéressé sur des sites Web destinés à un usage strictement personnel sans but commercial.

Dans les dossiers où la compétence du Commissariat a été établie, ce dernier a réussi, de manière générale, à faire retirer l'information du site Web de l'organisation en cause. Cependant, il convient de noter qu'une fois que l'information a été publiée en ligne, il n'y a jamais de garantie qu'elle n'a pas été reproduite ailleurs sur Internet. Malgré le retrait des renseignements d'un site, ces renseignements peuvent donc demeurer sur plusieurs autres sites inconnus.

Une plainte digne de mention a été déposée en vertu de la LPRPDE contre Globe24h, un site Web roumain qui reproduit les décisions judiciaires, y compris celles du Canada. Globe24h a obtenu les décisions canadiennes en récupérant les données d'un dépôt en ligne légitime de dossiers judiciaires qui limite l'indexation de ses décisions par nom par les moteurs de recherche afin de réduire le plus possible l'incidence sur la vie privée des gens. Or, Globe24h permet au contraire aux moteurs de recherche d'indexer les décisions reproduites et de communiquer des renseignements personnels par suite de recherches de nom de personnes. Le site impose ensuite des frais à ces personnes pour faire retirer leurs renseignements personnels.

Le Commissariat a conclu que Globe24h a enfreint la LPRPDE du fait qu'il a recueilli des renseignements personnels sans consentement (et sans qu'une exception ne s'applique) et à des fins inappropriées. Le commissaire a conclu ce qui suit<sup>32</sup> :

*À notre avis, il existe une différence importante entre le fait de rendre les décisions des cours et des tribunaux disponibles en ligne pour qu'elles soient accessibles à ceux qui veulent consulter les décisions antérieures et tenir les décideurs responsables, et le fait de rendre ces décisions – et leur contenu – indexables à l'aide d'outils de recherche populaires et accessibles à quiconque effectue une simple recherche sur quelqu'un d'autre. Comme les plaignants l'ont souligné en l'espèce, l'indexation de décisions de cours et de tribunaux par des moteurs de recherche peut causer une importante atteinte à la réputation et un profond embarras aux personnes en exposant inutilement leurs renseignements personnels sensibles à la découverte fortuite.*

Le commissaire a recommandé que Globe24h efface de ses serveurs les décisions de cours et de tribunaux canadiens qui renferment des renseignements personnels et qu'il prenne les mesures nécessaires pour supprimer ces décisions des mémoires caches des moteurs de recherche. Malheureusement, Globe24h a refusé de donner suite à ces recommandations.

Au moment de la rédaction du présent document, une requête a été présentée devant la Cour fédérale en vertu de l'article 14 de la LPRPDE à l'égard de Globe24h. Dans le but de réduire le plus possible les préjudices qui pourraient en découler, le Commissariat a communiqué avec les responsables de certains des principaux moteurs de recherche pour leur demander de retirer volontairement les liens menant au site Web de Globe24h ou de prendre d'autres mesures pour en réduire l'importance dans les résultats de recherche. Nous avons obtenu un certain succès à cet égard.

Dans un autre dossier d'enquête du Commissariat<sup>33</sup> mettant en cause une atteinte à la réputation, une mère a porté plainte, alléguant qu'une personne avait créé un compte Facebook au nom de sa fille adolescente qui n'était pas une utilisatrice de Facebook. L'imposteur aurait communiqué avec les amis de l'adolescente et formulé des commentaires inappropriés à leur sujet. La plaignante a contacté Facebook pour signaler l'usurpation d'identité et, après avoir confirmé que le compte était bel et bien faux, Facebook l'a supprimé ainsi que tout le contenu connexe (y compris les commentaires). La plaignante voulait que Facebook aille plus loin et qu'il communique avec tous ceux qui étaient devenus amis avec l'imposteur pour les informer de la supercherie, mais Facebook n'a pas jugé approprié d'intervenir dans les relations personnelles de ses utilisateurs. L'entreprise a néanmoins accepté de mettre en place des mesures susceptibles d'atténuer les conséquences de l'usurpation d'identité sur la réputation des non-utilisateurs de sites de réseautage social, comme l'adolescente en question. Dans le cas des non-utilisateurs, Facebook a accepté d'examiner au cas par cas les allégations d'usurpation d'identité portées à l'attention de l'administrateur du site lorsque la victime demande un type d'aide en particulier, et de faire enquête à cet égard. Une telle aide pourrait comprendre la mise en place, par Facebook, d'un processus permettant aux non-utilisateurs d'informer eux-mêmes les personnes devenues amies avec un imposteur.

## Autres formes de recours en place ou possibles

Lorsqu'il s'agit d'examiner les mécanismes permettant de supprimer ou de corriger des renseignements en ligne, il devient évident que les diverses parties concernées, dont les organisations, les législateurs, les technologues, les éducateurs et les individus eux-mêmes, exercent une influence sur la façon dont les réputations en ligne se font et se défont. Il est difficile de déterminer les niveaux relatifs de responsabilité à l'égard d'une question aussi vague que la réputation en ligne, et qui invoque d'autres valeurs sociétales comme la liberté d'expression, l'intérêt public et l'intégrité historique.

## Organisations

### a. Politiques de suppression

La façon la plus simple de gérer une situation où des renseignements personnels ont été publiés sans le consentement de l'intéressé consiste à demander aux responsables du site de les retirer. Les organisations peuvent accepter de le faire volontairement. De nombreux services en ligne ont, depuis longtemps, des politiques et des procédures en place permettant à une personne de supprimer ses propres publications (p. ex., Facebook et Twitter) lorsqu'elle ne souhaite plus les voir figurer sur sa page ou son compte personnel (mais les renseignements peuvent avoir été reproduits ailleurs ou partagés et être désormais hors de son contrôle). Il existe également des politiques en vue de retirer le contenu qui enfreint la loi ou les conditions de service. Depuis toujours, les renseignements constituant une violation du droit d'auteur, les renseignements diffamatoires et les renseignements financiers, tels que les numéros de carte de crédit, figurent au nombre des catégories de contenu pouvant être supprimé.

Récemment, en réponse au problème grandissant de la violence en ligne, des chefs de file de l'industrie ont mis en place des mécanismes permettant aux utilisateurs de demander la suppression d'un plus large éventail de contenu. Par exemple :

- Dans ses conditions d'utilisation, Twitter interdit aux utilisateurs de publier « les informations privées et confidentielles d'une tierce personne », dont « les photos ou vidéos intimes prises ou diffusées sans le consentement du sujet »<sup>34</sup>.
- Reddit a modifié sa politique de confidentialité en vue d'interdire les images explicites. Comme on peut le lire sur son blogue, il est interdit à quiconque de publier sans autorisation sur Reddit une photographie, une vidéo ou une image numérique d'une personne nue, excitée sexuellement ou se livrant à une activité sexuelle, ou de publier un lien menant à celle-ci. De même, Reddit reconnaît que les images personnalisées violentes constituent une forme de harcèlement non tolérable et il s'engage à retirer ces images après en avoir été avisé<sup>35</sup>.

- Les lignes directrices prévues par les Standards de la communauté<sup>36</sup> de Facebook présentent les types de contenu interdit par le service, comme l'intimidation, le harcèlement et la nudité.

## **b. Intermédiaires**

Les moteurs de recherche sont parmi les principaux outils permettant de trouver de l'information en ligne. Trouver de l'information au moyen de moteurs de recherche relève un peu du heureux hasard. En effet, on ne sait pas ce que l'on pourrait trouver jusqu'à ce que les résultats de recherche s'affichent. Si l'information n'est pas indexée de manière à en permettre la recherche au moyen d'un moteur de recherche, il est beaucoup plus difficile de la trouver et il faut généralement consulter des sites Web précis susceptibles de présenter l'information ou cliquer sur des liens menant vers le site Web où se trouve cette information. Dans leur article intitulé « Obscurity and Privacy », Evan Selinger et Woodrow Hartzog précisent que lorsque l'information est difficile à trouver, seules les personnes qui sont suffisamment motivées pour y consacrer les efforts et les ressources nécessaires parviendront à leurs fins<sup>37</sup>. Autrement dit, la personne qui effectue la recherche déploie délibérément des efforts pour mettre au jour des données et a probablement formulé des hypothèses quant au type d'information susceptible d'exister.

Le concept du « respect de la vie privée par l'obscurité », c'est-à-dire l'idée de rendre l'information plus difficile à trouver au moyen de moteurs de recherche, occupe une place importante dans les conseils et les services en matière de gestion de la réputation en ligne. DeleteMe<sup>38</sup>, par exemple, permet aux résidents américains de faire retirer leur profil public des principaux sites de données. Les responsables de Reputation.com offrent pour leur part un service de défense de la réputation aux termes duquel ils parcourent régulièrement Internet et avertissent les personnes concernées lorsqu'ils trouvent leurs renseignements personnels.

Certains services de gestion de la réputation appliquent les principes de l'optimisation des moteurs de recherche afin de gérer les résultats de recherche de sorte que les résultats favorables apparaissent en premier. Les méthodes utilisées consistent notamment à inonder Internet de nouveau contenu au sujet d'une personne afin de déplacer les liens indésirables plus loin dans les résultats de recherche. (Ironiquement, cette approche crée le paradoxe selon lequel on renonce à sa vie privée en vue de la protéger.)

Pour leur part, les responsables des moteurs de recherche protègent avec beaucoup de soin les algorithmes qu'ils utilisent pour indexer l'information en ligne. On sait que les sites peuvent être désindexés, que les liens menant à du contenu peuvent être supprimés et que le classement du contenu dans les listes de recherche peut être bouleversé, voire inversé. À titre d'exemple, Google a indiqué sur son blogue<sup>39</sup> que ses algorithmes relatifs à la qualité des sites visent à aider les gens à trouver des sites de grande qualité en reléguant à un rang inférieur le contenu de mauvaise qualité. L'utilité de tels mécanismes pour protéger la réputation en ligne mérite un examen plus approfondi.

Pour ce qui est du débat sur le « droit à l'oubli », si un tel mécanisme était pris en considération au Canada<sup>40</sup>, il faudrait établir soigneusement un équilibre avec les autres valeurs sociétales, telles que le droit à la liberté d'expression garanti par la *Charte canadienne des droits et libertés*. Bien que la liberté d'expression soit déjà restreinte au Canada par les lois relatives aux propos haineux, à l'obscénité et à la diffamation, elle demeure un des piliers du système démocratique du pays et permet aux gens d'exprimer leurs opinions et leurs idées sans ingérence ou contrainte de la part du gouvernement. Dans le monde numérique, nombre des mesures visant à lutter contre les risques d'atteinte à la vie privée et à la réputation peuvent également restreindre la liberté d'expression. Or, les risques d'entrave à liberté d'expression en ligne ont un effet paralysant sur la volonté et la capacité de s'exprimer pleinement. Parallèlement, toutefois, l'intérêt public penche fortement en faveur d'une limitation de la publication de renseignements personnels qui nuisent et portent atteinte à la réputation des gens, plus particulièrement sur un « Internet qui n'oublie jamais ».

La décision controversée prise par Twitter de bloquer les comptes de Politwoops illustre la complexité des enjeux. Politwoops est un service en ligne qui archive les tweets supprimés de politiciens dans plus de 30 pays, dont le Canada, au nom d'une plus grande transparence et responsabilité gouvernementales. Après que Twitter eut suspendu les comptes de Politwoops pour avoir enfreint les modalités de son accord et de sa politique développeurs, on a assisté à une levée de boucliers<sup>41</sup>. D'importants organismes de défense des droits comme l'Electronic Frontier Foundation ont fait valoir que la façon dont s'expriment les hauts responsables du pays est du plus grand intérêt pour le public.

## Législateurs

Comme les cas d'atteinte à la réputation en ligne deviennent de plus en plus répandus, les législateurs s'emploient à adopter des lois visant à compléter les lois sur la diffamation et à régler des problèmes précis en ligne. En Russie, par exemple, une nouvelle loi sur le droit à l'oubli<sup>42</sup> entrera en vigueur en 2016. Au Royaume-Uni, la publication de pornographie de vengeance est récemment devenue une infraction criminelle<sup>43</sup>. Aux États-Unis, plusieurs États ont adopté des lois interdisant la publication en ligne de photos d'identité judiciaire.

De nombreuses mesures de lutte contre la cyberintimidation portent sur l'atteinte à la réputation découlant de la publication de photos et de commentaires choquants. Ainsi, le projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité*, a modifié le *Code criminel* en vue de sanctionner la publication non consensuelle d'images intimes et les communications harcelantes. La *Cyber-safety Act* de la Nouvelle-Écosse prévoit la poursuite des personnes qui communiquent par voie électronique dans le but de nuire ou de porter atteinte à la santé, au bien-être affectif, à l'estime de soi ou à la réputation d'une autre personne, de la terroriser, de l'intimider, de l'humilier ou de la bouleverser<sup>44</sup>. Au Manitoba, le projet de loi sur la protection des images intimes permettrait aux victimes d'intenter des poursuites en justice et d'introduire une action en dommages-intérêts devant un tribunal civil.

Les périodes de conservation imposées par la loi pourraient également offrir un certain redressement, quoique limité. En vertu de la LPRPDE, les organisations ne sont autorisées à conserver les renseignements personnels qu'aussi longtemps que nécessaire pour réaliser les fins déterminées. « On devrait détruire, effacer ou dépersonnaliser les renseignements<sup>45</sup> » qui ne sont plus nécessaires. Cette disposition n'est pas particulièrement pertinente pour les services qui ne comportent aucune transaction précise dans un délai prévu. Par exemple, sur un site de médias sociaux, le but de la collecte et du traitement de l'information continuera d'être respecté aussi longtemps que l'individu demeure un membre. Par conséquent, la disposition relative à la conservation pourrait bien ne jamais être invoquée.

Dans certains secteurs, des limites définies sont imposées par la loi à la conservation de certains types de renseignements. Au Canada, par exemple, les agences d'évaluation du crédit ne peuvent conserver<sup>46</sup> les renseignements défavorables sur le crédit que pendant six ou sept ans, selon la province. Comme le propose Julie Brill de la Federal Trade Commission des États-Unis<sup>47</sup>, l'application de règles semblables à d'autres types de données permettrait de réduire la durée de vie de l'information en ligne. Cette mesure pourrait contribuer à limiter la portée de la mémoire numérique en ligne de même qu'à réduire la quantité de renseignements personnels pouvant porter atteinte à la réputation d'une personne.

Une autre solution proposée pour atténuer le préjudice causé par l'information en ligne consiste à refuser les décisions prises en fonction de l'information en ligne, à condition que cela ne nuise pas à d'autres membres de la société. Plusieurs États américains, dont le Montana et le Connecticut, ont ainsi adopté des lois<sup>48</sup> interdisant aux employeurs éventuels d'obliger les candidats à fournir leurs mots de passe liés aux médias sociaux. Au Canada, des autorités provinciales comme la Commission ontarienne des droits de la personne<sup>49</sup> et le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique<sup>50</sup> ont publié une directive à l'intention des employeurs indiquant que l'utilisation des médias sociaux pour effectuer la vérification des antécédents pourrait contrevenir aux lois provinciales interdisant la collecte et l'utilisation de certains types de renseignements personnels.

Dans le cadre de la série de conférences *Le point sur la vie privée* du Commissariat, le professeur Avner Levin de l'Université Ryerson a proposé<sup>51</sup> que l'information en ligne soit considérée comme étant hors limite. À son avis, « les renseignements électroniques seraient associés à un motif illicite, et il serait généralement interdit d'intenter une action fondée sur ceux-ci ou il faudrait démontrer par des renseignements supplémentaires à l'appui provenant d'autres sources que l'action est fondée sur d'autres motifs de fond ». Une telle approche empêcherait notamment les employeurs de congédier un employé en raison de photos inappropriées publiées en ligne.



## Tribunaux

Des personnes estimant avoir été victimes de diffamation en ligne ont intenté des poursuites en diffamation et demandé des dommages-intérêts. Certaines ont réussi à révéler l'identité des auteurs anonymes en assignant à comparaître les fournisseurs de services Internet, les obligeant à donner des renseignements sur les abonnés liés au contenu litigieux dans le contexte d'une poursuite en diffamation en instance ou à venir. À titre d'exemple, dans l'arrêt *A.B. c. Bragg Communications Inc.*<sup>52</sup>, une adolescente a pu obtenir une ordonnance de la cour relativement aux renseignements sur l'abonné associés à l'adresse IP qui avait été utilisée pour créer, en utilisant sa photo, un faux profil Facebook sur lequel ont été publiés par la suite des renseignements offensants à son sujet et au sujet de ses préférences sexuelles. Il est remarquable dans cette affaire que la jeune fille ait été en mesure d'obtenir une interdiction de publication partielle de l'issue de la procédure.

Au Canada, la diffamation peut parfois constituer une infraction criminelle. C'est le cas dans la décision *R. c. Simoes*<sup>53</sup> rendue par une cour ontarienne. Dans cette affaire, une cliente avait publié des évaluations défavorables au sujet d'un restaurant à Ottawa.

Par mesure de représailles, la propriétaire du restaurant a entrepris une campagne de harcèlement dans le cadre de laquelle elle a créé un faux profil de la cliente sur un site de rencontres et a envoyé des courriels obscènes à son employeur. La propriétaire du restaurant a été reconnue coupable de libelle diffamatoire en vertu de l'article 298 du *Code criminel* et a été condamnée à une peine d'emprisonnement.

Le harcèlement en ligne dans un contexte professionnel peut donner lieu à une plainte relative aux droits de la personne s'il est lié à un motif de distinction illicite, par exemple le harcèlement sexuel. Au Canada, le harcèlement peut aussi parfois constituer une infraction criminelle. Récemment, il y a eu un long procès mettant en cause un homme accusé de harcèlement criminel après avoir engagé un débat sur Twitter avec des militants politiques, à la suite d'un désaccord sur un jeu vidéo. S'il est reconnu coupable, il pourrait faire face à une peine d'emprisonnement<sup>54</sup>.

Le délit d'atteinte à la vie privée peut fournir un recours en vertu de la loi ou de la common law, par exemple au titre du nouveau délit d'intrusion dans l'intimité introduit en Ontario<sup>55</sup>. Récemment, la Cour supérieure du Québec a statué qu'un enregistrement vidéo de la plaignante se livrant à des activités sexuelles avec l'intimé, qui avait été réalisé sans le consentement de la plaignante et visionné par un auditoire limité, constituait une atteinte à son droit à la vie privée ainsi qu'à son honneur et à sa dignité, en violation de la *Charte des droits et libertés de la personne* du Québec et du *Code civil du Québec*, et lui a accordé d'importants dommages-intérêts<sup>56</sup>.

Toutefois, il y a des limites importantes aux recours judiciaires, car on ne saurait parler de diffamation dans les cas où les déclarations sont véridiques ou constituent des commentaires justes ou des communications responsables portant sur des questions d'intérêt public; les poursuites en diffamation se révèlent inutiles en cas d'atteinte à la réputation en ligne mettant en cause des opinions préjudiciables et des photos inappropriées, plutôt que des affirmations mensongères. En outre, en cas de poursuite en justice, on accordera davantage d'importance aux faits compromettants que le plaignant souhaite dissimuler ou oublier, et par conséquent, l'atteinte à la réputation n'en sera que plus grave, ce qui peut être dissuasif au départ. De plus, en raison des coûts associés à un litige, ce type de recours n'est pas forcément accessible à tous. Dans le contexte pénal, bien des dossiers ne donnent pas lieu à des accusations ou à des poursuites, et ceux qui intentent un procès doivent assumer le lourd fardeau de la preuve.

Enfin, la grande question que doivent trancher les tribunaux dans ces dossiers est liée à l'équilibre entre la liberté d'expression de la personne qui formule les commentaires en ligne, garantie par la Constitution, et les intérêts de celle qui se dit victime de diffamation ou de harcèlement, ce qui rend ces affaires très complexes sur le plan juridique.





## Organismes de réglementation

Depuis l'arrêt *Google Spain*, les organismes de réglementation sont de plus en plus souvent saisis de questions relatives à l'atteinte à la réputation touchant les moteurs de recherche. En juin 2015, le groupe de travail Article 29 a publié les résultats d'un sondage<sup>57</sup> visant à évaluer les pratiques des autorités de protection des données de l'Union européenne relativement aux demandes de révision des décisions de déréférencement. Le sondage a révélé que plus de 2 000 demandes en ce sens avaient été présentées aux autorités de protection des données de l'Union européenne au cours des 18 premiers mois suivant l'arrêt *Google Spain*.

La portée de l'application de l'arrêt *Google Spain* à l'extérieur de l'Union européenne fait actuellement l'objet d'un débat. En France, la CNIL maintient fermement sa position<sup>58</sup> selon laquelle l'arrêt oblige les moteurs de recherche à retirer les liens URL menant à tous les domaines, et non pas uniquement à ceux qui ont une extension géographique correspondant aux pays de l'Union européenne. Selon elle, si les renseignements demeurent accessibles pour d'autres domaines de Google, comme google.com, cela revient à contourner le but même du déréférencement et, en réalité, dépouille l'arrêt de tout son sens. Le CNIL estime également que les droits d'un individu ne devraient pas varier selon la façon dont une autre personne formule une requête dans le moteur de recherche. Pour sa part, Google adopte la position<sup>59</sup> selon laquelle l'arrêt ne concerne que l'Europe et ne s'applique pas au déréférencement des résultats de recherche dans le monde entier. Selon Google, une région ne devrait pas imposer ses valeurs et ses principes à d'autres États souverains qui peuvent avoir des points de vue divergents quant à l'équilibre approprié.

## Technologies



On ne saurait clore la discussion sur les mécanismes d'atténuation des risques d'atteinte à la réputation en ligne sans faire mention du rôle de l'industrie dans la protection de la vie privée et de la réputation des individus au moyen de la conception et de l'infrastructure des services en ligne. Les défenseurs du « principe de protection de la vie privée dès la conception » encouragent les technologues à intégrer à leurs produits des principes équitables en matière d'information, de sorte que la protection des renseignements personnels fasse partie intégrante de la prestation de services en ligne.

De plus en plus, on insiste auprès des concepteurs de la technologie pour qu'ils tiennent compte des répercussions sociétales à long terme de leur travail. Dans un discours prononcé devant des professionnels de la technologie, danah boyd a vivement recommandé aux membres de l'auditoire de tenir compte des effets généraux de leurs activités quotidiennes sur les questions touchant l'équité, la protection de la vie privée, la politique et la culture<sup>60</sup>. Christopher Parsons de l'Université de Toronto, dans un article concernant la façon dont les liens sociaux peuvent être sabotés par les réseaux sociaux en ligne, exhorte les technologues, les législateurs et les citoyens à promouvoir une transformation fondamentale de l'infrastructure technique du Web<sup>61</sup>. Dans leur article sur l'obscurité et la protection de la vie privée, les professeurs Evan Selinger et Woodrow Hartzog précisent que des solutions axées sur la conception pourraient également servir à préserver ou à favoriser l'obscurité, notamment des mesures comportementales incitatives qui privilégient les pratiques relatives à l'obscurité et ne tentent pas de manipuler l'utilisateur pour lui faire adopter des pratiques nuisant à l'obscurité<sup>62</sup>. Le professeur Viktor Mayer-Schönberger de l'Université d'Oxford, défenseur du « droit à l'oubli », préconise<sup>63</sup> pour sa part l'établissement de dates d'expiration pour les renseignements personnels de sorte que les individus puissent choisir les renseignements personnels qu'ils souhaitent conserver et ceux qu'ils préfèrent voir disparaître au fil du temps.

Il existe des difficultés évidentes à se tourner vers l'industrie pour mettre au point et adopter des mesures technologiques propres à limiter efficacement la quantité de renseignements personnels à l'appui des modèles opérationnels en ligne axés sur le monnayage des renseignements personnels. Cependant, lorsqu'on examine l'atténuation des risques d'atteinte à la réputation dans une optique de renforcement de la confiance des consommateurs et de l'avantage concurrentiel qui en découlera, les avantages de la mise en œuvre de solutions comme la dépersonnalisation et l'anonymisation deviennent plus convaincants.

## Individus

Dans le cadre des discussions du Commissariat sur [l'établissement des priorités en matière de protection de la vie privée](#), les membres des groupes de discussion à qui nous avons parlé étaient au courant des risques d'atteinte à la réputation auxquels ils s'exposent en ligne, plus particulièrement en ce qui a trait aux possibilités d'emploi et aux couvertures d'assurance. Selon leur dire, ils prennent soin de limiter leur empreinte numérique afin de protéger leur réputation, mais ils déplorent aussi un manque de contrôle sur leur réputation et ont exprimé des préoccupations face à l'absence de mécanismes permettant de supprimer des renseignements.

Selon une étude réalisée en 2012 par le Pew Research Center auprès des résidents américains<sup>64</sup>, 44 % des participants à l'enquête avaient supprimé les commentaires formulés par d'autres sur leur profil et 37 % avaient retiré leur nom de photos permettant de les identifier. Ces chiffres traduisent une préoccupation relativement à l'incidence des publications d'autres personnes sur notre propre réputation. Il convient de noter que ces chiffres ne prennent pas en compte le nombre de personnes qui auraient peut-être voulu supprimer l'information publiée par d'autres, mais n'ont pas été en mesure de le faire.

Au cours de l'exercice d'établissement des priorités entrepris par le Commissariat, certains nous ont affirmé que les gens doivent assumer la responsabilité de l'information qu'ils publient en ligne ainsi que les conséquences de leur publication sur la réputation en ligne. En ce qui concerne l'atteinte à la réputation causée délibérément, comme dans les cas de pornographie de vengeance, de cyberintimidation et de sites Web de dénonciation, les normes de comportement éthique qui s'appliquent dans le monde physique devraient également s'appliquer en ligne. Les utilisateurs de la technologie devraient être tenus de se comporter de façon éthique en ligne et de respecter la vie privée des autres.

Comme nous l'avons déjà mentionné, le monde numérique présente des difficultés particulières en ce qui concerne la protection de la réputation. Quiconque a une connexion Internet ou un plan de données est en mesure de créer et de distribuer un contenu à un auditoire instantané. Par suite de la démocratisation de l'information sur le Web, on peut devenir réalisateur, critique gastronomique ou journaliste sans que notre travail fasse l'objet d'un contrôle de la qualité ou d'un mécanisme de conformité à la loi, comme ce serait le cas s'il fallait passer par les canaux traditionnels hors ligne pour la publication et la diffusion. Les contenus offensants existent en ligne en partie parce qu'il est facile de les télécharger et difficile de les supprimer.

Ce que l'on appelle l'« effet de désinhibition en ligne »<sup>65</sup> contribue à assouplir les normes de comportement qui régissent les interactions dans le monde réel. En règle générale, l'absence d'interaction directe est propice au climat d'anonymat où les individus se sentent moins touchés parce que leur public est moins visible, tout comme eux-mêmes. Le téléchargement des données semble aussi coupé de la réalité et cette action ne donne pas la possibilité d'observer immédiatement la réaction des autres comme on le ferait dans le monde réel. Dans ce contexte, les individus sont plus enclins à donner libre cours à leurs impulsions lorsqu'ils publient des renseignements sur eux-mêmes ou sur d'autres personnes.

Enfin, dans le monde réel, les choses qui ne sont plus pertinentes s'effacent graduellement dans l'oubli, ce qui n'est pas le cas dans le monde virtuel. On peut facilement effectuer des recherches dans de vastes dépôts de données numérisées afin de mettre au jour des erreurs passées qui peuvent avoir une incidence que l'on n'avait pas envisagée sur la vie actuelle. Les gens ne peuvent plus compter sur le passage du temps pour effacer les moments embarrassants. En raison des difficultés associées à la protection et au maintien de la réputation en ligne, il est impératif de mettre en place une cyberéthique et de renforcer l'idée que les utilisateurs de la technologie devraient respecter la vie privée des autres.

## Éducateurs

La cyberéthique et l'empathie pour les autres en ligne font partie intégrante de l'enseignement de la littératie numérique que l'on intègre actuellement aux programmes scolaires. Ainsi, le tutoriel *Élever les enfants avec des principes éthiques pour un monde en réseau*<sup>66</sup> créé par HabiloMédias, le principal organisme canadien voué à l'éducation aux médias et à la littératie numérique, fait valoir l'importance de respecter les renseignements personnels des autres en évitant de communiquer trop d'information.

Selon la psychologue Sherry Turkle, la technologie tente de redéfinir les rapports humains, c'est-à-dire le souci des autres et le souci de nous-même, mais nous donne également l'occasion d'affirmer nos valeurs et notre orientation<sup>67</sup>. On peut espérer que l'enseignement de la littératie numérique contribuera à la création d'une culture de l'empathie où la pornographie de vengeance, la cyberintimidation et les sites de dénonciation ne seront pas tolérés et où la publication d'information sur les autres sans leur consentement sera un jour considérée comme étant non conforme à la norme sociale.



La littératie numérique est un domaine d'intérêt pour le Commissariat, plus particulièrement en ce qui touche les questions relatives à la protection de la vie privée des jeunes. Dans le cadre de notre Programme des contributions, nous avons financé des initiatives telles que la « Trousse pédagogique pour les enseignants et leurs élèves portant sur la protection des renseignements personnels »<sup>68</sup> et « Pirates de la vie privée : une application sur la protection des renseignements personnels en ligne »<sup>69</sup>. Dans le cadre de ses efforts de sensibilisation auprès des jeunes, le Commissariat s'emploie à mettre au point des outils et des ressources visant à aider les jeunes à mieux comprendre le processus de création des traces numériques ainsi que l'incidence éventuelle de ces traces sur leur réputation et la réputation des

autres. À ce jour, le Commissariat a créé une courte vidéo intitulée [L'information : quand elle est diffusée...](#), destinée à encourager les jeunes à réfléchir aux conséquences de la communication d'une trop grande quantité de renseignements en ligne. Le Commissariat élaborera un plan de cours qui accompagnera la vidéo et mettra l'accent sur les risques d'atteinte à la réputation et les stratégies pour les prévenir.

Dans le rapport de 2015 sur la cyberintimidation<sup>70</sup> qu'ils ont établi en collaboration, le Représentant des enfants et des jeunes de la Colombie-Britannique et le Commissariat à l'information et à la protection de la vie privée de la province indiquent que l'éducation numérique fait partie intégrante de la lutte contre la cyberintimidation. À leur avis, il faut enseigner aux jeunes la valeur du respect de la vie privée pour le civisme et la démocratie afin qu'ils soient en mesure de prendre des décisions responsables en tant que membres de la société dans son ensemble.

## Conclusion

Une section du *Rapport annuel au Parlement 2012* du Commissariat est consacrée à la sensibilisation de la population à la réputation en ligne. Le Commissariat a indiqué ce qui suit : « Dans le cyberspace, les informations sont particulièrement omniprésentes et accessibles. En règle générale, elles sont aussi persistantes; seuls les efforts les plus énergiques permettent de les purger ou de les maîtriser. Lorsque ces informations sont dommageables ou erronées, elles peuvent menacer grandement la vie privée et la réputation d'une personne, en ligne comme dans le monde réel. »

Pour ce qui est des effets potentiels des renseignements que nous publions et que les autres publient à notre sujet, il peut y avoir atteinte à la réputation et les recours efficaces à cet égard sont peu nombreux. Le fait que la plupart des lois aient été adoptées avant l'avènement des médias sociaux peut expliquer les lacunes sur le plan juridique, mais les autres moyens de régler ce problème, notamment par l'intermédiaire de codes de pratique de l'industrie ou de mesures technologiques, pourraient faire partie de la solution.

La recherche en vue de trouver des solutions et de transposer les règles d'éthique du monde réel au monde virtuel présente des défis de taille. Les commentaires relatifs à la contestation de l'arrêt rendu par la Cour de justice de l'Union européenne sur le droit à l'oubli ont fait ressortir le risque d'entrave à la liberté d'expression et d'autorisation de la censure. L'infrastructure Internet, et plus particulièrement la facilité avec laquelle on peut publier de l'information ainsi que la permanence de cette information en l'absence d'un mécanisme quelconque de gouvernance universelle, constitue également un obstacle à d'éventuelles solutions. En outre, il y a des questions d'ordre juridique à régler – par exemple, la LPRPDE sous sa forme actuelle reconnaît-elle certains aspects du droit à l'oubli au moyen de concepts tels que l'exactitude, fins acceptables ou le droit de retirer son

consentement? Ou ne faudrait-il pas plutôt modifier la LPRPDE afin de se pencher directement sur ces questions?

En publiant le présent rapport, notre but est d'attirer l'attention sur ce nouveau défi dans le domaine de la protection de la vie privée en vue de susciter des discussions sur les solutions. Au bout du compte, nous entendons présenter une position relativement aux recours. Pour ce faire, nous invitons les particuliers, les organisations, les universitaires, les groupes de défense des droits, les spécialistes des technologies d'information, les éducateurs et d'autres parties intéressées à donner suite au présent document, de même qu'à proposer des façons nouvelles et novatrices de protéger la vie privée et la réputation. Les articles présentés doivent nous permettre de répondre à au moins une des questions suivantes :

- Nous avons attiré l'attention sur certains écarts possibles concernant les mesures de protection entre le monde en ligne et le monde hors ligne. Quels sont les autres écarts?
- Quelles solutions pratiques, techniques, stratégiques ou juridiques faudrait-il envisager pour atténuer les risques d'atteinte à la réputation en ligne?
- Le droit à l'oubli peut-il s'appliquer dans le contexte canadien et, dans l'affirmative, comment?
- Faudrait-il prendre des mesures spéciales pour les groupes vulnérables?
- Qui sont les principaux acteurs et quels sont leurs rôles et leurs responsabilités?

Pour obtenir de plus amples renseignements, veuillez consulter l'appel au dépôt de mémoires ci-joint.

## Ressources supplémentaires

Voici une liste de ressources dans lesquelles sont examinés de façon plus approfondie les sujets soulevés dans le présent document.

Austin, L. « Privacy and Private Law: The Dilemma of Justification », *McGill Law Journal*, vol. 55, n° 2, 2010, p. 165-210. En ligne : [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2016969](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2016969).

Bazon, Emily. *Sticks and Stones: Defeating the Culture of Bullying and Rediscovering the Power of Character and Empathy*, Random House Trade Paperbacks, 2013.

Beasley, Berrin et Mitchell Haney (dir.). *Social Media and the Value of Truth*, Lexington Books, 2013.

Citron, Danielle. *Hate Crimes in Cyberspace*, Harvard University Press, 2014.

Dash, Anil. « What Is Public? », 24 juillet 2014. En ligne : <https://medium.com/message/what-is-public-f33b16d780f9>.

Woodrow Hartzog et Frederic Stutzman. « Obscurity by Design », *Washington Law Review*, juin 2013. En ligne : <http://privacylawson.com/wp-content/uploads/2014/01/Hartzog-Stutzman-Obscurity-by-Design.pdf>.

Woodrow Hartzog et Frederic Stutzman. « The Case for Online Obscurity », *California Law Review*, février 2013. En ligne : <http://www.californialawreview.org/wp-content/uploads/2014/10/01-HartzogStutzman.pdf>.

Ivester, Matt. *Lo!...OMG!* Serra Knight Publishing, 2011.

James, Carrie. *Disconnected: Youth, New Media, and the Ethics Gap*, Cambridge (MA), The MIT Press, 2014.

Levmore, S. et MC Nussbaum (dir.). *The Offensive Internet: Privacy, Speech and Reputation*, Harvard University Press, 2010. Plus particulièrement, les articles suivants :

« The Internet's Anonymity Problem », par Saul Levmore

« Believing False Rumours », par Cass R. Sunstein

« Reputation Regulation: Disclosure and the Challenge of Commensurating Computing », par Frank Pasquale

Lewinsky, Monica. « The Price of Shame », *TED Talk*, mars 2015. En ligne : [http://www.ted.com/talks/monica\\_lewinsky\\_the\\_price\\_of\\_shame?language=en](http://www.ted.com/talks/monica_lewinsky_the_price_of_shame?language=en).

Marwick, A. et R. Miller. *Online Harassment, Defamation, and Hateful Speech: A Primer of the Legal Landscape*, Centre for Law and Information Policy, Fordham Law School, 10 juin 2014. En ligne : [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2447904](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2447904).

Massum, Hassan et Mark Tovey (dir.). *The Reputation Society: How Online Opinions are Reshaping the Offline World*, The MIT Press, 2011.

Mayer-Shönberger, Viktor. *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009.

Morozov, Evgeny. *To Save Everything Click Here: The Folly of Technological Solutionism*, PublicAffairs, 2013.

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

Pasquale, Frank. *The Black Box Society: The Secret Algorithms That Control Money and Information*, Harvard University Press, 2015.

Potts, D.A. *Cyberlibel: Information Warfare in the 21<sup>st</sup> Century?* Irwin Law Inc., 2011.



Solove, Daniel J. *The future of reputation: gossip, rumor, and privacy on the internet*, Yale University Press, 2007.

Trottier, D. *Identity Problems in the Facebook Era*, Routledge, 2014.

Tunick, Mark. *Balancing Privacy and Free Speech: Unwanted attention in the age of social media*, Routledge, 2015.

West Coast LEAF. *#CyberMisogyny: Using and strengthening Canadian legal responses to gendered hate and harassment online*, juin 2014. En ligne :

<http://www.westcoastleaf.org/userfiles/file/Cyber%20Misogyny%20Report.pdf>.

## Notes

---

<sup>1</sup> [William Shakespeare](#), *Othello* (c. 1603), (Iago) acte 2, scène 3, ligne 296.

<sup>2</sup> Deborah G. Johnson, Priscilla M. Regan et Kent Wayland, « Campaign Disclosure, Privacy and Transparency », *William & Mary Bill of Rights Journal*, vol. 19, n<sup>o</sup> 4, article 7, 2011. En ligne : <http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1585&context=wmborj>.

<sup>3</sup> Dictionnaire Larousse. En ligne : <http://www.larousse.fr/dictionnaires/francais/r%C3%A9putation/68543>.

<sup>4</sup> Erving Goffman, *La présentation de soi*, Les Éditions de minuit, 2009.

<sup>5</sup> Danah boyd, « Social Network Sites as Networked Publics: Affordances, Dynamics, and Implications », *Networked Self: Identity, Community, and Culture on Social Network Sites* (sous la direction de Zizi Papacharissi), 2010, p. 39-58.

<sup>6</sup> Deborah G. Johnson, Priscilla M. Regan et Kent Wayland, *op. cit.*

<sup>7</sup> <http://www.theguardian.com/media/2009/jun/11/smith-family-photo-czech-advertisement>.

<sup>8</sup> « Genetic testing company's use of child's image outrages mother Christie Hoos », *The Citizen*, 18 juin 2015. En ligne : <http://www.cbc.ca/news/canada/british-columbia/genetic-testing-company-s-use-of-child-s-image-outrages-mother-christie-hoos-1.3118339>.

<sup>9</sup> Blogue officiel de Google, « Eye-tracking studies: more than meets the eye », 6 février 2009. En ligne : <http://googleblog.blogspot.ca/2009/02/eye-tracking-studies-more-than-meets.html>.

<sup>10</sup> Chitika Online Advertising Network, « The Value of Google Result Positioning », 7 juin 2013. En ligne : <http://chitika.com/google-positioning-value>.

<sup>11</sup> Traduction d'une expression utilisée par le professeur Nicolaus Mills dans un commentaire sur la télé réalité. « Television and the Politics of Humiliation », *Dissent* (00123846), vol. 51, n<sup>o</sup> 3, p. 79, été 2004.

<sup>12</sup> Étant donné la nature de cette affaire, nous avons décidé de ne pas fournir de référence précise.

<sup>13</sup> CBS News, « Did the Internet Kill Privacy? », 6 février 2011. En ligne : <http://www.cbsnews.com/news/did-the-internet-kill-privacy/>.

<sup>14</sup> Reconnaisant ce problème, le nouveau bureau de la technologie de la recherche du bureau de la protection du consommateur de la Federal Trade Commission met l'accent sur la transparence des algorithmes afin que ceux-ci n'aient pas d'incidence nuisible ou discriminatoire sur les consommateurs. En ligne : <https://www.ftc.gov/news-events/blogs/techftc/2014/12/hello-world>.

<sup>15</sup> Les résultats affichés par de nombreux moteurs de recherche sont personnalisés pour chaque utilisateur en fonction d'une gamme de facteurs, dont l'emplacement et l'historique de recherche.

<sup>16</sup> Nous avons choisi de ne pas nommer ces sites afin de ne pas leur donner un rayonnement injustifié.

<sup>17</sup> Stavroula Karapapa et Maurizio Borghi, « Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm », *International Journal of Law and Information Technology*, vol. 23, juillet 2015, p. 261-289. En ligne : <http://ijlit.oxfordjournals.org/content/23/3/261.full.pdf> +html.

<sup>18</sup> Centre d'aide Recherche Web : Saisie semi-automatique. En ligne : <https://support.google.com/websearch/answer/106230?hl=fr>.

<sup>19</sup> Jacquelyn Burkell, Valerie Steeves et Anca Micheti, *Broken Doors: Strategies for Drafting Privacy Policies Kids Can Understand*, mars 2007. En ligne : [www.idtrail.org/files/broken\\_doors\\_final\\_report.pdf](http://www.idtrail.org/files/broken_doors_final_report.pdf).

<sup>20</sup> J. Palfrey et U. Gasser, *Born Digital: Understanding the First Generation of Digital Natives*, Basic Books, 2008.

<sup>21</sup> *Privacy Rights for California Minors in the Digital World*. En ligne : [http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill\\_id=201320140SB568](http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568).

- <sup>22</sup> Cour de justice de l'Union européenne, *Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González*, affaire C-131/132, 2014. En ligne : <http://curia.europa.eu/juris/document/document.jsf?docid=163494&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=111438>.
- <sup>23</sup> Eric Posner, « We all have the right to be forgotten », *Slate*, 14 mai 2014. En ligne : [http://www.slate.com/articles/news\\_and\\_politics/view\\_from\\_chicago/2014/05/the\\_european\\_right\\_to\\_be\\_forgotten\\_is\\_just\\_what\\_the\\_internet\\_needs.html](http://www.slate.com/articles/news_and_politics/view_from_chicago/2014/05/the_european_right_to_be_forgotten_is_just_what_the_internet_needs.html).
- <sup>24</sup> Mark Halper, « Isabelle Falque-Pierrotin: Privacy needs to be the default not an option », *Wired*, juin 2015. En ligne : <http://www.wired.com/2015/06/isabelle-falque-pierrotin-privacy-needs-default-not-option/>.
- <sup>25</sup> Google – Transparence des informations, 6 juillet 2015. Consulté le 6 juillet 2015 à l'adresse : <http://www.google.com/transparencyreport/removals/europeprivacy/?hl=fr>.
- <sup>26</sup> <https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/edit?pli=1>.
- <sup>27</sup> « Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data », 13 mai 2015. En ligne : <https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd>.
- <sup>28</sup> « This is how Google handles “Right to be forgotten” requests », *Computerworld*, 19 novembre 2014. En ligne : <http://www.computerworld.com/article/2849686/this-is-how-google-handles-right-to-be-forgotten-requests.html>.
- <sup>29</sup> En ligne : <https://www.google.com/advisorycouncil>.
- <sup>30</sup> Parlement européen, « Règlement général sur la protection des données », version du 12 mars 2014. En ligne : <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//FR>.
- <sup>31</sup> Ces sites représentent plus de la moitié des plaintes et enquêtes du Commissariat concernant l'affichage de renseignements personnels sans consentement.
- <sup>32</sup> Commissariat à la protection de la vie privée du Canada, *Un site Web générant des revenus en publiant des décisions judiciaires canadiennes et en permettant leur indexation par les moteurs de recherche a contrevenu à la LPRPDE*, rapport de conclusions d'enquête en vertu de la LPRPDE n° 2015-002, 5 juin 2015. En ligne : [https://www.priv.gc.ca/cf-dc/2015/2015\\_002\\_0605\\_f.asp](https://www.priv.gc.ca/cf-dc/2015/2015_002_0605_f.asp).
- <sup>33</sup> Commissariat à la protection de la vie privée du Canada, *À la suite d'un cas où une adolescente a été victime d'usurpation d'identité en ligne, le site de réseautage social Facebook accepte d'aider, au cas par cas, les non-utilisateurs à rétablir leur réputation en ligne*, rapport de conclusions en vertu de la LPRPDE n° 2013-010. En ligne : [https://www.priv.gc.ca/cf-dc/2013/2013\\_010\\_0711\\_f.asp](https://www.priv.gc.ca/cf-dc/2013/2013_010_0711_f.asp).
- <sup>34</sup> « Informations privées publiées sur Twitter ». Consulté le 6 juillet 2015 à l'adresse : <https://support.twitter.com/articles/20170168#>.
- <sup>35</sup> « Protecting your digital privacy », blogue de Reddit, 24 février 2015. Consulté le 6 juillet 2015 à l'adresse : [http://www.reddit.com/r/announcements/comments/2x0g9v/from\\_1\\_to\\_9000\\_communities\\_now\\_taking\\_steps\\_to](http://www.reddit.com/r/announcements/comments/2x0g9v/from_1_to_9000_communities_now_taking_steps_to).
- <sup>36</sup> Facebook – Standards de la communauté. Consulté le 6 juillet 2015 à l'adresse : <https://www.facebook.com/communitystandards>.
- <sup>37</sup> Evan Selinger et Woodrow Hartzog, « Obscurity and Privacy », *Routledge Companion to Philosophy of Technology*, 2014. En ligne : [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2439866](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2439866).
- <sup>38</sup> [www.abine.com/deleteme/landing.php](http://www.abine.com/deleteme/landing.php).
- <sup>39</sup> « More guidance on building high-quality sites », blogue central du webmestre de Google, 6 mai 2011. En ligne : <http://googlewebmastercentral.blogspot.ca/2011/05/more-guidance-on-building-high-quality.html>.

<sup>40</sup> Une certaine jurisprudence provinciale s'établit dans le domaine du déréférencement des résultats de recherche. Pour de plus amples renseignements, voir *Equustek Solution Inc. c. Jack* (2014 BCSC 1063) et *Niemela c. Malamas* (2015 BCSC 1024).

<sup>41</sup> « Open letter to Twitter to restore Politwoops access to API », Accessnow.org, septembre 2015. En ligne : <https://www.accessnow.org/pages/open-letter-twitter-restore-politwoops-access-api>.

<sup>42</sup> <http://www.natlawreview.com/article/right-to-be-forgotten-russian-data-protection-law-has-passed-all-stages-approval>.

<sup>43</sup> « Revenge porn: new offence comes into force », *The Telegraph*, 12 avril 2015. En ligne : <http://www.telegraph.co.uk/news/uknews/crime/11530889/Revenge-porn-New-offence-comes-into-force.html>.

<sup>44</sup> *Cyber-safety Act*, SNS 2013, chap. 2. En ligne : <http://www.canlii.org/en/ns/laws/stat/sns-2013-c-2/latest/sns-2013-c-2.html>.

<sup>45</sup> Principe 4.5.3 de la LPRPDE.

<sup>46</sup> Agence de la consommation en matière financière du Canada, *Comprendre votre dossier de crédit et votre pointage de crédit*. En ligne : <http://www.fcac-acfc.gc.ca/Fra/ressources/publications/creditPrets/Pages/Understa-Comprend-7.aspx>.

<sup>47</sup> Evan Selinger et Woodrow Hartzog, « Why you have the right to obscurity », *The Christian Science Monitor*, 15 avril 2015. En ligne : <http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0415/Why-you-have-the-right-to-obscurity>.

<sup>48</sup> National Conference of State Legislatures, « Access to Social Media Usernames and Passwords », 14 septembre 2015. En ligne : <http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx>.

<sup>49</sup> Publication du 23 mars 2012 sur la page Facebook de la Commission ontarienne des droits de la personne. En ligne : <https://www.facebook.com/the.ohrc/posts/320570581329371>.

<sup>50</sup> Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, *Guidelines for Social Media Background Checks*, octobre 2011. En ligne : <https://www.oipc.bc.ca/guidance-documents/1454>.

<sup>51</sup> Avner Levin, « Les renseignements électroniques devraient-ils être considérés comme un motif illicite? », série de conférences *Le point sur la vie privée* du Commissariat à la protection de la vie privée du Canada, mars 2011. En ligne : [https://www.priv.gc.ca/information/research-recherche/2011/levin\\_201103\\_f.asp](https://www.priv.gc.ca/information/research-recherche/2011/levin_201103_f.asp).

<sup>52</sup> Dans *A.B. c. Bragg Communications Inc.*, [2012] 2 SCR 567, 2012 SCC 46 (CanLII), la Cour suprême du Canada infirme la décision d'une cour inférieure et accorde à la plaignante le droit à l'anonymat. En ligne : [canlii.ca/t/fstvg](http://canlii.ca/t/fstvg).

<sup>53</sup> La décision du tribunal inférieur n'a pas été publiée. La Cour d'appel de l'Ontario a confirmé la déclaration de culpabilité, mais a réduit la durée de la peine d'emprisonnement. *R. c. Simoes*, 2014 ONCA 144 (CanLII). En ligne : [canlii.ca/t/g469m](http://canlii.ca/t/g469m).

<sup>54</sup> *R. c. Elliott, Gregory A.* (Cour de l'Ontario). Le verdict dans cette affaire est attendu en janvier 2016.

<sup>55</sup> *Jones c. Tsige*, 2012 ONCA 32.

<sup>56</sup> *L.D. c. J.V.* [2015] JQ n° 2563, 2015 QCCS 1224.

<sup>57</sup> Communiqué du groupe de travail Article 29, 18 juin 2015. En ligne : [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2015/20150618\\_wp29\\_press\\_release\\_on\\_delisting.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20150618_wp29_press_release_on_delisting.pdf).

<sup>58</sup> Commission nationale de l'informatique et des libertés, « Droit au déréférencement : rejet du recours gracieux formé par Google à l'encontre de la mise en demeure », 21 septembre 2015. En ligne : <http://www.cnil.fr/linstitution/actualite/article/article/droit-au-dereferencement-rejet-du-recours-gracieux-forme-par-google-a-lencontre-de-la-mis/>.

---

<sup>59</sup> Blogue européen de Google, « Implementing a European, not global, right to be forgotten », 30 juillet 2015. En ligne : <http://googlepolicyeurope.blogspot.ca/2015/07/implementing-european-not-global-right.html>.

<sup>60</sup> « Teens are waging a privacy war on the Internet – Why marketers should listen ». University of Pennsylvania: Wharton. 5 août 2014. En ligne <http://knowledge.wharton.upenn.edu/article/teens-privacy-online>.

<sup>61</sup> C. Parsons, « Sex, Lies and Digital Memory: How Social Surveillance Threatens Communities », *Communication in Question: Competing Perspectives on Controversial Issues in Communication Studies*, Nelson Education, 2013, p. 174-180.

<sup>62</sup> Evan Selinger et Woodrow Hartzog, « Obscurity and Privacy », *Routledge Companion to Philosophy of Technology*, op. cit.

<sup>63</sup> Viktor Mayer-Schönberger, « Why we need to let our online memories go », *The Washington Post*, 23 novembre 2012. En ligne : [https://www.washingtonpost.com/opinions/why-we-need-to-let-our-online-memories-go/2012/11/23/29d0e54e-33ec-11e2-bfd5-e202b6d7b501\\_story.html](https://www.washingtonpost.com/opinions/why-we-need-to-let-our-online-memories-go/2012/11/23/29d0e54e-33ec-11e2-bfd5-e202b6d7b501_story.html).

<sup>64</sup> Mary Madden, PEW Internet and American Life Project, « Privacy management on social media sites », 24 février 2012. En ligne : <http://www.pewinternet.org/2012/02/24/privacy-management-on-social-media-sites/>.

<sup>65</sup> John Suler, *CyberPsychology & Behavior*, vol. 7, n° 3, juin 2004, p. 321-326. En ligne à : <http://online.liebertpub.com/doi/abs/10.1089/1094931041291295>.

<sup>66</sup> En ligne : <http://habilomedias.ca/tutoriel/%C3%A9lever-enfants-avec-principes-%C3%A9thiques-monde-r%C3%A9seau>.

<sup>67</sup> Sherry Turkle, « Connected, but alone? », *TED Talk*, février 2012. En ligne : [http://www.ted.com/talks/sherry\\_turkle\\_alone\\_together](http://www.ted.com/talks/sherry_turkle_alone_together).

<sup>68</sup> Pour obtenir de plus amples renseignements, voir [https://www.priv.gc.ca/resource/cp/2013-2014/p\\_201314\\_05\\_f.asp](https://www.priv.gc.ca/resource/cp/2013-2014/p_201314_05_f.asp).

<sup>69</sup> Pour obtenir de plus amples renseignements, voir [https://www.priv.gc.ca/resource/cp/2014-2015/p\\_201415\\_05\\_f.asp](https://www.priv.gc.ca/resource/cp/2014-2015/p_201415_05_f.asp).

<sup>70</sup> Office of the Privacy Commissioner for British Columbia, Representative for Children and Youth. Cyberbullying : Empowering children and youth to be safe online and responsible digital citizens, novembre 2015. En ligne : [http://www.rcybc.ca/sites/default/files/documents/pdf/reports\\_publications/rcy\\_cyberbullying-web.pdf](http://www.rcybc.ca/sites/default/files/documents/pdf/reports_publications/rcy_cyberbullying-web.pdf).