CANADIAN REPORT

Delisting in the Digital Age – a hybrid approach to bridge the European and American visions of the "right to be forgotten".

Karen Eltis* and Pierre Trudel**

---

* Professor, Faculty of Law, University of Ottawa, Karen.Eltis@uOttawa.ca, affiliated with the CITP, Princeton University.

** Professor, Faculty of Law, Centre de recherche en droit public, Université de Montréal. www.pierretrudel.net .

The one thing [the victorious plaintiff] Costeja did not want us to know about him is now the only thing the entire world knows about him.[1]

Dis-moi ce que tu oublies, je te dirai qui tu es.[2]

Introduction

Technology plays an indisputably crucial role in our personal narratives, and this goes far beyond the borders contemplated by legal traditions, firmly anchored in territorial systems. Given the Internet's ubiquitous role, it became clear very early on that using it would be possible in practice only if there were search engines capable of rapidly identifying information likely to meet web user needs.

Search engines agglomerate information on individuals and various entities on which we submit search queries, usually in the form of key words. Such engines are essential to web users who have to find information. They provide users with documents and links to documents that must be as relevant as possible to the query. The information is found in virtual spaces, and it is in principle public.

Their efficiency makes search engines powerful means of reducing "practical obscurity" phenomena, which often make it difficult to have access to and compile a set of documents concerning a given individual or a specific topic. This is probably why they have been targeted as resources that could lead to violations of the "right to be forgotten".

The emergence of information technologies is part of a socio-cultural context calling for a living, evolving normative framework. This is why this report proposes to contribute to improving human rights protection by promoting greater consistency among the fundamental principles in the now borderless environments created by digital systems. In order to understand the law that is emerging out of the "technological revolution", which is

---

1 Comments by the comedian John Oliver concerning the unanticipated consequences of the 2014 *Costeja* judgment, online, *YouTube*, https://www.youtube.com/watch?v=r-ERajkMXw0 , at 5.00.

2 Augé 2001: 26 "Tell me what you forget and I will tell you who you are". [Our translation.]

also borderless, this report employs the Canadian bijural perspective and the comparative method. [3]

Given that its system encompasses both civil law and common law, Canada is especially well placed to "bridge" the European and American traditions, and shed light on the strengths and weaknesses, and nuts and bolts, of the "right to be forgotten".[4] This bijural, bilingual field of vision provides opportunities to transcend "orthodox conceptions" of law.[5]

This report focusses, therefore, on the "hybrid" notion of delisting in Canadian law. This law is certainly emerging, but it has real potential to secure the balances that seem necessary to guarantee both free circulation of information and human dignity.

To begin with, we will look at the special features of the Canadian and Québec normative frameworks (in response to Q1-5). Next, we will offer a few general and contextual observations to better describe the way the European Union Court of Justice *Costeja* judgment was received in Canada (Q6-11). Lastly, we suggest certain avenues to be considered to meet the challenges of protecting rights in virtual space (Q12).

1. Canadian protection of the right to be forgotten: protection provided under common law (Questions 1-5)

It is well established in Canada that the courts can, after having found that a document on the Internet violates the law, order that it be suppressed. Judges also order the suppression

---

[3] For analyses of the state of Canadian law on this subject, see: Eloïse Gratton and Jules Polonetsky, "Droit À l'oubli: Canadian Perspective on the Global 'Right to Be Forgotten' Debate", *Colorado Technology Law Journal*, Vol 15, Issue 2 (2017); Geneviève Saint-Laurent, "Vie privée et 'droit à l'oubli': que fait le Canada?", *Revue de droit de l'Université du. Nouveau-Brunswick*. Vol. 66 (2015), p. 185-197; Pierre Trudel, "Moteurs de recherche, déréférencement, oubli et vie privée en droit québécois", (2016) 21 *Lex electronica* 89. Online: http://www.lex-electronica.org/s/1535.

[4] Karen Eltis, "Breaking Through the 'Tower of Babel': A 'Right to be Forgotten' and How Trans-Systemic Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics", (2011) 22 *Fordham Intellectual Property, Media and Entertainment Law Journal*, 69-95; Karen Eltis, "The Anglo-American/Continental Privacy Divide? How Civilian Personality Rights Can Help Reconceptualize the 'Right to be Forgotten' Toward Greater Transnational Interoperability", [2016] 94 *Canadian Bar Review*, 355-380.

[5] As Professor Robert Leckey, Dean of the Faculty of Law at McGill University, would put it. See: <https://www.mcgill.ca/law/about/deans-welcome>.

of hyperlinks to documents that violate the law. There is thus a balance between the right to search for information freely and the right to protect privacy and reputation. As soon as it has been demonstrated that a document harms an individual's reputation or violates their privacy, a judge can order that it be suppressed, along with the hyperlinks pointing to it.

Under Québec civil law, the courts apply the general rules of civil responsibility. In that framework, they have considered that in certain circumstances a wrong can be committed through a failure to forget. From this, some authors have deduced that there is a right to be forgotten. For example, recalling past events was deemed to be wrong when the person who disclosed the information did not demonstrate that it was in the public interest to do so. The following examples are taken from Québec jurisprudence.

In 1889, the Québec Superior Court found that the *Le Violon* newspaper had been wrong to revive certain "allegations long since forgotten" concerning the plaintiff.[6] That decision was upheld in the Court of Revision. More recently, in *Lévesque*,[7] the Superior Court had to render judgment on a claim to the right to be forgotten. The plaintiff, Lévesque, was suing the *Journal de Québec* for having recalled the crime he had committed two years earlier in a "shooting gallery" in the city of Montréal. Lévesque had been involved in a fight between criminal groups. The judge found that the *Journal* had not committed a wrong because the information revealed was easily accessible to the public. Moreover, since the subject of the article was a fire in the "shooting gallery" where Lévesque had committed the crime, the information disclosed remained of public interest.

In contrast, in a similar case,[8] Gilbert Ouellet sued the *Photo-Police* newspaper for having published an article reporting the crime committed by his late spouse ten years before. She had killed their four children and then taken her own life. The Court of Québec judge found that the article that had been published was "sensationalist" and that it could not be

---

6 *Goyette v. Rodier* (1889) 20 R.L. 108,110 (C. Rev). [Our translation.]

7 *Lévesque v. Communications Quebecor inc.* (QC SC, 1999-06-21), SOQUIJ AZ-99021730, J.E. 99-1527, [1999] R.R.A. 681.

8 *Ouellet v. Pigeon*, REJB 1997-03106, 1997 (C.Q.)

justified with respect to public interest. In another Court of Québec case,[9] Barbe J. noted that it is difficult for an individual participating in "public activities of a public nature" to invoke a right to be forgotten. Referring to Piché J.'s comments in *Szabo v. Morissette*,[10] Barbe J. said: "the person who is at the origin of the story cannot blame anyone but himself if he does not like it when others talk about him".

The wrong of failing to forget as it is recognized in Québec law follows from publishing formerly known information in a manner that gives the information temporal and spatial scope different from that of its initial publication. What is found to be wrong and punished is re-disclosing information when doing so is considered unjustifiable in the context. In this respect, the legal legitimacy of claiming the right to be forgotten is determined by assessing the context in which the information is published. To be forgotten is thus a right for the person concerned when it is considered unreasonable to disseminate the information. In such a case, the publishing is found wrong, that is, it would not have been done by a reasonable person in analogous circumstances. The publication context is a very important factor in this process of determining whether or not the action was wrong.

1.1 The limits of the right to be forgotten

The "right to be forgotten", as described above, must be distinguished from the right to have search engine-generated links erased, which was created by a decision of the European Court of Justice. Under Canadian law, we cannot postulate that personal information protection rights procure a right to have search engine results delisted.[11]

The constitutional guarantee of freedom of expression, understood as protecting the freedom to seek information not violating the law, contrasts with an application of a "right to delisting" that arguably follows from the right to protection of personal information. In *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers,*

---

9 *Mathieu v. Presse ltée (La),* (C.Q., 1998-11-24), SOQUIJ AZ-99036093, B.E. 99BE-169. [Our translation.]

10 (1993) R.R.A. 554, J.E. 93-1385 (C.S.). [Our translation.]

11 *C.L. v. BCF Avocats d'affaires*, 2016 QCCAI 114 (CanLII), April 14, 2016, online: <http://canlii.ca/t/gr5q0>.

Local 401,[12] the Supreme Court of Canada unanimously declared the Alberta statute on protection of personal information invalid because it prohibited the collection of images in a public place.

The Act that was attacked prohibited the collection of information, in this case, images that showed people crossing a picket line but no other personal information, without the consent of those people. In the situation presented to the Court, no details concerning the lifestyles or personal choices of the stakeholders were revealed. However, the Act, like other personal information protection laws in effect in Canada, draws no distinctions. All personal information is treated in the same manner, even that which is not private. It is prohibited to collect it or publish it without consent, except for very narrowly defined reasons. It was this failure to leave a space for exercising other basic rights that made the personal information protection act excessive. In sum, the Court's judgment reflected something obvious: there is information about people that is not part of their private lives. The Court recalled the need to balance the prohibitions set out in the various laws on protection of personal information. As written, these laws prohibit collecting, keeping and publishing any information about an identifiable person without his or her consent, even when that person is in a public place. The Court judged that such prohibitions limited freedom of expression in an unreasonable manner.

The Court explained that these laws must contain balancing mechanisms to permit expressive activities that do not concern personal privacy matters. The Court judged that the Albertan statute on protection of personal information prevented the collection of personal information, such as images and videos taken during a demonstration in which the public could easily see the people taking part.

This Supreme Court decision invalidated the approach to personal information protection that had prevailed in Canada for over three decades. Carried by a movement that seems to postulate that privacy is the only fundamental right that must be protected, these laws

12 [2013] 3 SCR 733.

overlook, for all practical purposes, the imperatives of free circulation of information in public spaces. By invalidating the Albertan statute, the Court put an end to this imbalance.

Of course, the Court recognizes the legitimacy of protecting privacy and ensuring that personal information gathering and sharing is regulated. However, it provides a reminder that all personal information is not automatically information about an individual's private life, especially if it is information found legitimately in public. It is therefore excessive to consider all personal information as subject to individuals' consent. Freedom of expression must weigh individuals' hold over information about themselves against the rights of others and of the public in general.

For now, although it is about a phenomenon somewhat different from those concerned by search engines, this Supreme Court ruling leaves the way open to serious doubts about the possibility in Canadian law for there to be a right to delisting based on principles flowing from personal information protection legislation.

However, search engines generate hyperlinks. In *Crookes v. Newton*[13], the Supreme Court of Canada examined whether the incorporation into a text of hyperlinks leading to allegedly defamatory statements was equivalent to "publishing" those statements. According to the six justices of the majority, a person cannot defame another by simply publishing a hyperlink pointing to a third-party website or document that contains defamatory statements. Chief Justice McLachlin and Fish J. explained that a "hyperlink, by itself, should never be seen as 'publication' of the content to which it refers".[14] They agreed with Abella J. that "[m]aking reference to the existence and/or location of content by hyperlink or otherwise, without more, is not publication of that content"[15].

The majority justices considered that hyperlinks are like footnotes in a paper document. While hyperlinks, unlike footnotes, provide immediate access to the third-party websites to

---

13 [2011] 3 SCR 269.

14 [2011] 3 SCR 269, para. 47.

15 [2011] 3 SCR 269, para. 42.

which they point, readers are nonetheless aware that such links take them to a different source.

1.2 Recourses, implementation and effectiveness

Civil responsibility actions are the most effective means of punishing untimely and wrongful publication of past facts that cannot be demonstrated to be in the public interest. The right to delisting is possible, under the principles of common law, when it is shown that the document to which a hyperlink points is against the law.

If it has been judicially established that a wrongful document is online, the courts can render decisions and make orders to protect individuals' rights. In Canada, the right to be forgotten is understood as the right to have wrongful information suppressed when it brings past facts into the present. It is rarely invoked, except in situations in which recalling past facts is not in the public interest.

2. A contextual view of the right to be forgotten: how the Costeja decision was received in Canada (Questions 6-11)

The most telling example of the qualitative changes brought by the digital era seems to be the phenomenon of what the British daily newspaper *The Guardian* calls "the Internet's 'law of unintended consequences'"[16].

Mr. Costeja's case (see above) is now well known. Less so is that of his predecessor, which in fact unleashed the debate around the "right to be forgotten". It concerned a Spanish doctor named Hugo Guidotti Russo. The facts in the matter, which never made it to court, are however very striking and seem to summarize the problem much better than those in Mr. Costeja's case.[17]

---

[16] http://www.theguardian.com/world/blog/2014/may/14/mario-costeja-gonzalez-fight-right-forgotten

[17] Karen Eltis, *Courts, Litigants and the Digital age*, 2nd ed. (Irwin Law, 2016).

In short, they are as follows. Over 25 years prior, a female patient of Dr. Rossi had alleged malpractice.[18] The dispute, which had been reported in a local newspaper, had been settled and Dr. Rossi had practiced since then without incident. However, and given the very nature of the Internet, any time his name was queried, it always returned the allegations published in the shocking report, in a raw, decontextualized manner. Inevitably, the result was that the amicable (out-of-court) settlement of the case was eclipsed and 20 years of respectable professional practice were stained.

Search engines generate hyperlinks by applying algorithms.[19] Such algorithms function automatically, in fractions of seconds. This involves analyzing considerable masses of data, including, in particular, data on the context of the person who initiates the search, and his or her search history, geographical location, etc.

Owing to the contextual nature of algorithmic processing, it seems impossible to postulate that entering the same words in search queries made in different locations in the network by people who certainly have different search histories will necessarily generate the same results.

The question can even be raised of whether the type of results that an individual obtains by entering his or her own name into a search query will be the same as those that will come up for another person in a context that could lead to the belief that his or her interests are distant from those of the first individual.

However, the European Union Court of Justice seems to have overlooked this nonetheless fundamental aspect. It seems to have been concerned by a perception about another type of decontextualization. In the end, its decision required that search engines (referred to as

---

18 Paul Sonne, Max Colchester, & David Roman, "Plastic Surgeon and Net's Memory Figure in Google Face-Off in Spain" *The Wall Street Journal* (7 March 2011).

19 An algorithm is a set of instructions given to a computer to obtain a result by doing calculations. See: Seema GHATNEKAR, "Injury by Algorithm", (2012-2013) 33 *Loy. L.A. Ent. L. Rev*. 171.

"data controllers") delist results that were claimed to be decontextualized[20] under the "right to be forgotten" that it inferred from Article 12 of European Directive 95/46/EC.

As shown elsewhere in this text, Canadian courts are careful to respect freedom of expression, a constitutional value enshrined in the Canadian (and Québec) charter. Most of the groups that took part in a Privacy Commissioner's consultation on the right to delisting considered that such a right would be difficult to reconcile with the imperatives of freedom of expression as it is understood in Canadian law.

Out of the same concerns, the decision was also attacked in the United States and later in the United Kingdom[21], and denounced as "the biggest threat to free speech".[22] This criticism reveals a major divergence between the continental vision of privacy, focussing on procedural protection of data, and the United States' absolutist approach, based on the First Amendment. This division extends beyond the United States and seems to characterize the common law approach, which, for all practical ends, rejects a right to delisting based on protection of data, despite the Internet's particularities.[23]

The British Minister of Justice, Simon Hughes, expressed strong opposition to *Costeja*,[24] about which he said: "we are going to argue the case both in terms of the wrongness of the

---

[20] *Ibid*. As Bernal explains, only search results arising from a search under a particular name are suppressed. Neither the underlying source material itself, nor the same (contentious) search results obtained when searched for in any other way are required to be suppressed. See e.g. Paul Bernal, "Is Google Undermining the 'right to be forgotten'?", *CNN Opinion* (7 July 2014), online: CNN <http://www.cnn.com/2014/07/07/opinion/bernal-google-undermining-privacy-ruling/>.

[21] European Union Committee, Second Report EU Data Protection Law: a 'right to be forgotten'?, <https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/4002.htm>.

[22] See Jeffrey Rosen, "The Right to be Forgotten" (2012) 64 *Stan. L. Rev Online* 88, online: Stanford Law Review <http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten>. Many American scholars view this topic as the biggest threat to free speech on the Internet in the coming decade.

[23] Walker, Robert, "The Right to be Forgotten", (November 20, 2012). 64 *Hastings Law Journal* 257, December 2012. https://ssrn.com/abstract=2017967 or http://dx.doi.org/10.2139/ssrn.2017967

[24] We have criticized the government of China… for closing down people's right to information. There are other countries with strict information access. It is not a good position for the EU to be in to look as if it is countenancing restrictions in the access of the citizen to access to information because it could be a very bad precedent". Stuart Lauchlan, "Britain pledges to fight Europe's Right to be Forgotten bad law" *diginomica* (10 July 2014), online: Diginomica <http://diginomica.com/2014/07/10/britain-pledges-fight-europes-forgotten-bad-law/>.

principle—because we believe in freedom of information, and transmission of it—and the impracticality of the practice"[25].

3. Give private parties a power to limit expression?

The mechanism established by the European Court of Justice is based on the idea that it is easier for a search engine to take action on delisting requests than to resist them. Making the effort to analyze and then explain that certain links lead to documents that are in the real public interest is an expense some search engines might not wish to incur.[26]

However, beyond the issue of censure as such, there is the question of whether it is compatible with the rule of law to entrust a private, American, company with a judicial power normally reserved for a state institution (such as a constitutional council or analogous body). Should such a company have the power to determine the reasonable limits of freedom of expression, particularly when there are no clear, known guidelines?

Google's Peter Barron himself seems to have confessed to BBC News that the company was "learning as we go", inevitably adopting an ad hoc approach to implementing the judgment. Another edifying remark seems to confirm this uncertainty: "no one really knows what the criteria is … So far, we're getting a lot of noes... It's a complete no man's land".[27]

---

25 Hughes said: "If politicians think they can delete findings about their expenses, that's not going to happen. If people think they can delete their criminal history, it won't occur. It looks to me as if it may be an unmanageable task. It will be a phenomenal task. It's not technically possible to remove all traces of data loaded on to the internet from other sources. You can't exercise the right to be forgotten. The information system could not be made to do it."

Owen Bowcott, "EU 'right to be forgotten' law unenforceable, says justice minister", The Guardian (9 July 2014), online: The Guardian. <http://www.theguardian.com/technology/2014/jul/09/eu-right-to-be-forgotten-law-unenforceable-justice-minister-simon-hughes>.

26 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.

27 Mr. Wadsworth of the U.K. ORM firm Igniyte, referring to the ECJ's recent decision (Mark Scott, "European Companies See Opportunity in the 'Right to Be Forgotten', *The New York Times* (8 July 2014), online: The New York Times <http://www.nytimes.com/2014/07/09/technology/european-companies-see-opportunity-in-the-right-to-be-forgotten.html?_r=0)>.

Transparency and accountability are not easy to cultivate when the weighing of sensitive constitutional values is left up to private foreign players, who may be reticent to start judging the appropriateness of keeping a hyperlink to a document online. The legal framework guaranteeing protection of human rights in Canada, as stated in the Charter of Rights and Freedoms, applies exclusively to government measures. Fundamental rights are enshrined in the Constitution–as a bulwark against government abuses.[28] However, in the digital era it goes without saying that the power to violate–even inadvertently–constitutional values, including freedom of expression, does not lie exclusively in the hands of state authorities. On the contrary, in a post-*Costeja* world, private parties, namely, "data controllers", have global influence, use artificial intelligence, and have become involuntary arbitrators of public discourse on the global scale, but are bound by no specific guidelines or transparency. This is the reality that the Supreme Court of Canada seems to acknowledge (even though it does so indirectly) in the landmark *Douez* and *Equustek* decisions.[29]

Facebook, Twitter and other platforms have been given discretion to determine what to suppress, which has inevitably led these companies to use ad hoc approaches to perform a task normally reserved for the legislator and the courts. The difficulty increases when the "balancers" are inexperienced corporate players with little economic incentive to arbitrate delisting requests. Moreover, such entities are mainly located in the United States, where the legal framework remains highly protective of Internet intermediaries. In the end, the dominant web companies control algorithms and solutions based on AI, which they increasingly use for this purpose.[30] This shows the scope of the stakes brought into play by the European Court if we are at all concerned with ensuring the rule of law.

---

[28] S. 32.

[29] *Douez* v. *Facebook Inc*., 2017 SCC 33 and *Google Inc.* v. *Equustek Solutions*, 2017 SCC 34.

[30] http://csrcl.huji.ac.il/people/inadvertently-appointing-digital-judges-canadian-perspective-restricting-speech-and?ref_tid=3718

4. The next steps (Question 12): Reviewing the notion of government action and platforms' responsibility beyond Costeja

4.1 Government action and the Charter

To chisel the contradictions down to discord between the regimes flowing out of civil and common law systems regarding the "right to delisting" on the transborder level, the notion of "government action" must be carefully reviewed. Otherwise, the ultimate arbitrators of the appropriate limits of fundamental rights could be algorithms or other forms of artificial intelligence deployed on platforms that do not have the democratic legitimacy that we usually accord to judges in democratic societies.

As we are struggling to define the limits of the discourse in a post-Charlottesville world,[31] we need to acknowledge the importance of maintaining court oversight of constitutional values and appropriate limits on freedom of expression, rather than allowing them to become unknown territory (determined by AI "bots").

Moreover, and secondly, intermediaries must be made responsible in accordance with the "**context test**" model described below, and this should be done on the transborder level.

4.2 Making intermediaries responsible

A few years ago, Professor Jonathan Zittrain christened the right to be forgotten as set out in *Costeja* a "bad solution to a very real problem".[32] Acknowledging that misleading and decontextualized information is a real problem but nonetheless rejecting the solution adopted in Europe, Professor Zittrain has more recently examined the need to rethink the

---

31 http://csrcl.huji.ac.il/people/inadvertently-appointing-digital-judges-canadian-perspective-restricting-speech-and?ref_tid=3718

32 Jonathan Zittrain "Don't Force Google to Forget", *New York Times* (14 May 2014), online: The New York Times http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html. See also: David Streitfeld, "European Court Lets Users Erase Records on Web", The New York Times (13 May 2014), online: The New York Times<http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html?_r=0>.

U.S. *Communications Decency Act* and the complete immunity section 230 of that legislation gives to intermediaries in the United States[33]:

> Section 230 nearly entirely eliminated the liability of Internet content platforms under state common law for bad acts, such as defamation, occasioned by their users. The platforms were free to structure their moderation and editing of comments as they pleased, without a traditional newspaper's framework in which to undertake editing was to bear responsibility for what was published. If the New York Times included a letter to the editor that defamed someone, the Times would be vulnerable to a lawsuit (to be sure, so would the letter's author, whose wallet size would likely make for a less tempting target). Not so for online content portals that welcome comments from anywhere—including the online version of the New York Times.[34]

However, the rationale underlying that immunity is no longer appropriate for an industry that has left infancy behind (according to Professor Zittrain, "an infant industry has grown up")[35]. Therefore, for our purposes, even pre-eminent American commentators, always resistant to delisting as an answer to the evils of decontextualization, now seem to be considering that "data controllers" should be made responsible to a certain degree, given their exponentially growing power. This is thus a crucial point for honing the definition of the right to delisting by making search engines' responsibility context-dependent, now that we are starting to see the cracks in their immunity armour.

While delisting in its present state is not consistent with the American (or British) vision of freedom of expression, Canada seems especially well situated to propose a measured approach to it. According to this hybrid approach, emphasis is placed on protecting not data, but individuals. In other words, the idea is to allow existing protection (enshrined in the Québec and Canadian charters and the *Civil Code of Québec*, among other things) to "extend" to Canadians' interactions in "cyberspace", in line with the logic of *Douez v. Facebook* inter alia, which aims to mitigate the inequalities inherent to the digital world and its "automatic nature".

---

33 https://www.law.com/therecorder/sites/therecorder/2017/11/10/cda-230-then-and-now-does-intermediary-immunity-keep-the-rest-of-us-healthy/

34 *Id*

35 *Id.*

For the right to delisting to be operable on the transborder level, it would be prudent to gradually take distance from formal emphasis on the right-to-data-protection theories that some try to use as bases for the "right to be forgotten".[36] The reasoning that the European Court employs as a foundation for a delisting requirement has its source in the importing into common law of notions flowing from personal data protection law. Overlooking the differences between private personal data, which were the basis for the development of personal data protection laws in the 1970s, and public domain information, which was never meant to be covered by the personal data regime when the data protection laws were designed, the Court chose to import the model for ensuring protection of private data and apply it to public data. The conceptual slide is not explained by the European Court, and it is difficult to reconcile with the required balance between the rights and freedoms characteristic of reasoning by Canadian courts.

When it is shown that a statement violates a law or fundamental right, Canadian courts do not hesitate in the least to order delisting. In *Corriveau* v. *Canoe*,[37] a case in which the intermediary conceded that it was responsible for all of the statements published on a blog, a Québec court condemned the intermediary to withdraw the defamatory statements. Following this logic, based on human rights (instead of data protection), the Federal Court of Canada recognized, for all practical ends, a "Canadian" right to delisting in A.*T. v. Globe24H.com*,[38] and viewed that right as extending beyond the borders of Canada.[39] In both situations, the Court recognized the defamatory or illegal nature of the statements.

According to section 22 of the Québec *Act to establish a legal framework for information technology*[40], a "service provider, acting as an intermediary, that provides document storage services on a communication network is not responsible for the activities engaged in by a service

---

36 (Especially since the definition of personal data is very problematic.)

37 2010 QCCS 3396.

38 https://www.canlii.org/fr/ca/cfpi/doc/2017/2017cf114/2017cf114.html

39 Note that this case involved a Romanian site that had republished/re-indexed Canadian court decisions in order to extract payment in exchange for withdrawing information.

40 *Act to establish a legal framework for information technology*, CQLR, c. C.1.1. See Pierre Trudel, *Introduction à la Loi concernant le cadre juridique des technologies de l'information*, (Cowansville: Éditions Yvon Blais, 2012), pp. 189*ff*.

user with the use of documents stored by the service user or at the service user's request". However, a service provider can incur responsibility through knowledge of the fact that the services it provides are being used to carry out an illicit activity and if it does not cease, in a timely manner, providing its services to those it knows are engaging in such an activity.

Under Québec legislation, given there is an express legislative provision[41] according to which they are not required to monitor, it is logically impossible to consider that search engines "process" personal data when words are entered that could prove to correspond to the name of a person. At the very most, they could incur responsibility following the entering of such words if they have prior knowledge of the illicit nature of the document to which referral is made.

Moreover, unlike European legislation, Canadian laws on protection of personal information do not contain the notion of "processing". Canadian laws govern the collection, use and communication of personal information. For there to be collection under these laws, the body must at least have knowledge of the content and meaning of the information over which it acquires control.[42]

5. The context test: between civil and common law

In the end, this convergence between the two great legal traditions united in Canadian law is translated in the approach favoured by an Australian court, *Duffy v. Google*, which was inspired by a Supreme Court of Canada decision (obiter). The Australian court placed responsibility on a search engine. In that case, which explicitly borrows the logic employed by the Supreme Court of Canada in Crookes *v. Newton* (obiter) – and opens the possibility to intermediaries' responsibility when they go beyond providing hyperlinks – the Australian court held the search engine responsible for having failed to delist defamatory sites and for having offered those sources through its "autocomplete", among other things. This approach, inspired by Canadian law, is much more consistent with the logic

41 *Act to establish a legal framework for information technology*, s. 27.

42 To be able to collect and store documents containing personal information, one must at least acquire control over them. On this issue, see: Vincent Gautrais and Pierre Trudel, *Circulation des renseignements personnels et Web 2.0*, (Montréal: Éditions Thémis, 2010), p. 59*ff*.

underlying delisting in the digital era, and achieves a better balance between freedom of expression and the right to protection of privacy and reputation, values on which the right to be forgotten is claimed to be based.

Moreover, this context-based vision, anchored in human rights rather than in data protection, allows courts with jurisdiction, instead of inexperienced corporate players, to judge what is really decontextualized or even defamatory (rather than simply "irrelevant" according to Costeja) and must therefore be delisted.[43] The "context test"[44] illustrates the serious difficulties described above, which are characteristic of the digital era.

6. The return of *LICRA v. Yahoo*? – the future of extraterritorial jurisdiction over delisting

Contemporary legal systems postulate that each state applies its norms within its own borders.[45] Clearly, this presupposition, which underlies our normative frameworks, no longer corresponds to the reality of the digital era.

As Professor Yuval Shany, Director of the new Cyber Security Research Center in Jerusalem so eloquently explained, "current interactions do not occur principally on physical territory, but in cyberspace. The reality is very different from that in which our laws were created and are applied."[46]

In a very recent decision, presaging the future, the District Court for the Northern District of California issued an order enjoining a Canadian company (Equustek) to execute a worldwide delisting order that the Supreme Court of Canada had rendered against Google a

---

43 *BCF avocats C.L. c. BCF Avocats d'affaires* 2016 QCCAI 114, (right to rectification under the Québec Act respecting the Protection of Personal Information in the Private Sector) "the company must take all reasonable means to rectify the plaintiff's information internally (on its Internet site), which is not, however, equivalent to a duty to delist (externally, on the rest of the Web)". [Our translation.] The decision does not address intermediaries' duties.

44 "Duffy v Google: is this the end of the Internet as we know it?" *Defamation e-bulletin* (30 October 2015). Online: http://www.landers.com.au/publications/dispute-resolution/duffy-v-google-is-this-the-end-of-the-internet-as-we-know-it/.

45 See, for example, Yuval Shany, Jerusalem

46 *Id.* [Our translation.]

few months prior. The injunction granted in the context of an intellectual property/trade secrets dispute required Google to delist all websites selling products that infringed Equustek's copyright. Canada's highest court declared: "The Internet has no borders — its natural habitat is global."[47]

Despite this reality, the traditional presuppositions of law remain intimately tied to territory. The unthinkable "reversal" of the Supreme Court of Canada's decision by a lower court on the other side of the border is a telling illustration of the increasingly disturbing dissonance between the uncompromising roots of law anchored firmly in territory and the borderless nature of cyberspace. Reflecting the major change in circumstances flowing from the digital era with respect to the extraterritorial scope of judgments, Google turned to a court in its home state of California, which, as indicated, blocked the injunctive relief granted by the Canadian decision. It found (on the basis of section 23 of the *Communications Decency Act* (supra), even though Google pleaded the First Amendment) that the worldwide injunction would have no effect beyond Canada's strict borders, thereby authorizing Google to put the contested search results "back on sale". Google.ca, in spite of the Canadian decision.

There is no need to point out that such a decision not only does violence to the highest court in Canada, but renders its decision without force and effect. This is because, in a world where electronic commerce knows no borders, what is the practical effect of delisting results uniquely within given borders? It also confirms the Canadian court's clear fear in an earlier case, *Douez v. Facebook* (supra), that public order choices enshrined in Canadian law would end up being stripped of meaning (or at least unenforceable) in the Internet age. The difficulty is made worse when the norms at stake are constitutional values, such as freedom of expression, to which special attention was drawn in *Equustek*.

Equustek therefore highlights the state's inability to regulate behaviour that efficiently defies traditional brick-and-mortar borders. This inevitably creates a legal vacuum in

---

[47] *Google Inc. v. Equustek Solutions Inc*, 2017 SCC 34 at para. 41 (Abella J.).

which the most omnipresent form of behaviour (ecommerce) is, absurdly, governed by outdated standards maladapted to interactions in cyberspace.

Conclusion

The controversies concerning the "right to be forgotten" seen as procuring a right to force the suppression of links to documents that do not violate laws are emblematic of the obsolescence of personal data protection legislation based on the fiction of "consent". Reflecting the centralized informatics of the 1970s, such legislation no longer produces appropriate balances to guarantee that data generated by the community will be used in accordance with respect for fundamental rights and democratic values. This increasingly looks like a case of yesterday's regulatory system being used to govern future practices.

By failing to innovate with respect to regulatory mechanisms, we exhaust ourselves trying to apply laws that persist in postulating that data on individuals can be used only with their consent and uniquely for specific purposes. This individualistic approach clings to the fiction of "consent" that cybernauts and all users of related objects supposedly give in a fully informed manner.

With this type of law, the form of regulation that really counts is that imposed by the platforms of this world!

Today, the big data essential to creating value in connected environments are left in the hands of companies with no real obligation to guarantee they are protected. With the right to delisting as created in Europe, we are sinking deeper into a formalist vision based on "consent" and the hypothesis that is it still possible to determine the end uses of a piece of information circulating in cyberspace.

However, big data processing is based on systems that do not care about the purposes for which the data was initially collected. Once they have become "Big Data", the information no longer "belongs" to individuals. Used massively, data are a resource shared by all, like the air we breathe and the water we drink. Like water, air, and radio-electric frequencies, data are at the core of AI-based value creation. Their use must be conceived of as a

privilege governed by rules that States must have the courage to impose and enforce. However, to build new foundations for the legal framework for protecting freedom, we have to dare to question the certainties and dogmas that are too often used as the cornerstones of personal data protection law.

ANNEX – Answers to the questionnaire

The Right to Be Forgotten – Questionnaire by Franz Werro

Question 1

How is the right to be forgotten protected under your law? Does your law specifically grant a right to be forgotten or does this right derive from a more general framework?

Under Québec civil law, the courts apply the general rules of civil responsibility. In that framework, they have considered that in certain circumstances a wrong can be committed through a failure to forget. From this, some authors have deduced that there is a right to be forgotten. For example, recalling past events was deemed to be wrong when the person who disclosed the information did not demonstrate that it was in the public interest to do so. The following examples are taken from Québec jurisprudence.

In 1889, the Québec Superior Court found that the *Le Violon* newspaper had been wrong to revive certain "allegations long since forgotten" concerning the plaintiff.[48] That decision was upheld in the Court of Revision. More recently, in *Lévesque*,[49] the Superior Court had to render judgment on a claim to the right to be forgotten. The plaintiff, Lévesque, was suing the *Journal de Québec* for having recalled the crime he had committed two years earlier in a "shooting gallery" in the city of Montréal. Lévesque had been involved in a fight between criminal groups. The judge found that the *Journal* had not committed a wrong because the information revealed was easily accessible to the public. Moreover, since the subject of the article was a fire in the "shooting gallery" where Lévesque had committed the crime, the information disclosed remained of public interest.

---

48 *Goyette v. Rodier* (1889) 20 R.L. 108,110 (C. Rev). [Our translation.]

49 *Lévesque v. Communications Quebecor inc.* (QC SC, 1999-06-21), SOQUIJ AZ-99021730, J.E. 99-1527, [1999] R.R.A. 681.

In contrast, in a similar case,[50] Gilbert Ouellet sued the *Photo-Police* newspaper for having published an article reporting the crime committed by his late spouse ten years before. She had killed their four children and then taken her own life. The Court of Québec judge found that the article that had been published was "sensationalist" and that it could not be justified with respect to public interest. In another Court of Québec case,[51] Barbe J. noted that it is difficult for an individual participating in "public activities of a public nature" to invoke a right to be forgotten. Referring to Piché J.'s comments in *Szabo v. Morissette*,[52] Barbe J. said: "the person who is at the origin of the story cannot blame anyone but himself if he does not like it when others talk about him".

The wrong of failing to forget as it is recognized in Québec law follows from publishing formerly known information in a manner that gives the information temporal and spatial scope different from that of its initial publication. What is found to be wrong and punished is re-disclosing information when doing so is considered unjustifiable in the context. In this respect, the legal legitimacy of claiming the right to be forgotten is determined by assessing the context in which the information is published. To be forgotten is thus a right for the person concerned when it is considered unreasonable to publish the information. In such a case, the publishing is found wrong, that is, it would not have been done by a reasonable person in analogous circumstances. The publication context is a very important factor in this process of determining whether or not the action was wrong.

Question 2

What are the limits to the right to be forgotten under your law?

The "right to be forgotten" must be distinguished from the right to have search engine-generated links erased, which was created by a decision of the European Court of Justice.

50 *Ouellet v. Pigeon*, REJB 1997-03106, 1997 (C.Q.)

51 *Mathieu v. Presse ltée (La),* (C.Q., 1998-11-24), SOQUIJ AZ-99036093, B.E. 99BE-169. [Our translation.]

52 (1993) R.R.A. 554, J.E. 93-1385 (C.S.). [Our translation.]

Under Canadian law, we cannot postulate that personal information protection rights procure a right to have search engine results delisted.[53]

The constitutional guarantee of freedom of expression, understood as protecting the freedom to seek information not violating the law, contrasts with an application of a "right to delisting" that arguably follows from the right to protection of personal information. In *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*,[54] the Supreme Court of Canada declared the Alberta statute on protection of personal information invalid because it prohibited the collection of images in a public place.

The Act that was attacked prohibited the collection of information, in this case, images that showed people crossing a picket line but no other personal information, without the consent of those people. In the situation presented to the Court, no details concerning the lifestyles or personal choices of the stakeholders were revealed. However, the Act, like other personal information protection laws in effect in Canada, draws no distinctions. All personal information is treated in the same manner, even that which is not private. It is prohibited to collect it or publish it without consent, except for very narrowly defined reasons. It was this failure to leave a space for exercising other basic rights that made the personal information protection act excessive. In sum, the Court's judgment reflected something obvious: there is information about people that is not part of their private lives. The Court recalled the need to balance the prohibitions set out in the various laws on protection of personal information. As written, these laws prohibit collecting, keeping and publishing any information about an identifiable person without his or her consent, even when that person is in a public place. The Court judged that such prohibitions limited freedom of expression in an unreasonable manner.

The Court explained that these laws must contain balancing mechanisms to permit expressive activities that do not concern personal privacy matters. The Court judged that

---

53 *C.L. v. BCF Avocats d'affaires*, 2016 QCCAI 114 (CanLII), April 14, 2016, online: <http://canlii.ca/t/gr5q0>.

54 [2013] 3 SCR 733.

the Albertan statute on protection of personal information prevented the collection of personal information, such as images and videos taken during a demonstration in which the public could easily see the people taking part.

This Supreme Court decision invalidated the approach to personal information protection that had prevailed in Canada for over three decades. Carried by a movement that seems to postulate that privacy is the only fundamental right that must be protected, these laws overlook, for all practical purposes, the imperatives of free circulation of information in public spaces. By invalidating the Albertan statute, the Court put an end to this imbalance.

Of course, the Court recognizes the legitimacy of protecting privacy and ensuring that personal information gathering and sharing is regulated. However, it provides a reminder that all personal information is not automatically information about an individual's private life, especially if it is information found legitimately in public. It is therefore excessive to consider all personal information as subject to individuals' consent. Freedom of expression must weigh individuals' hold over information about themselves against the rights of others and of the public in general.

For now, although it is about a phenomenon somewhat different from those concerned by search engines, this Supreme Court ruling leaves the way open to serious doubts about the possibility in Canadian law for there to be a right to delisting based on principles flowing from personal information protection legislation.

Question 3

What are, in your law, the legal remedies available to enforce the right to be forgotten?

Civil responsibility actions are the most effective means of punishing untimely and wrongful publication of past facts that cannot be demonstrated to be in the public interest. The right to delisting is possible, under the principles of common law, when it is shown that the document to which a hyperlink points is against the law.

Question 4

As a follow-up to the previous question, does your law allow the plaintiff to receive material or immaterial damages? If yes, is such remedy realistic in practice?

If it has been judicially established that a wrongful document is online, the courts can render decisions and make orders to protect individuals' rights.

Question 5

In general, how do you assess the implementation of the right to be forgotten in your law? Is it effective? Is it used in practice? Are there particular obstacles in the implementation of this right?

In Canada, the right to be forgotten is understood as the right to have wrongful information suppressed when it brings past facts into the present. It is rarely invoked, except in situations in which recalling past facts is not in the public interest.

Question 6

How did courts and commentators in your country welcome the ECJ ruling on Google v González?

A large number of authors have pointed out the imbalance of the European ruling, which also says nothing about cybernauts' right to access information that is legally on line.

Question 7

For those who are from a country that is not part of the European Union, did your courts follow the ECJ ruling on the right to be forgotten? Is it likely Do that they will follow it?

It is to be hoped that Canadian courts will distance themselves from the approach taken in the ECJ decision.

Question 8

Did your law already grant a similar right to be forgotten than the one stated in the ECJ ruling?

In Canadian law, it is not possible to postulate that the right to protection of personal information procures a right to delisting of search results.[55] A right to delisting that would be based on the principles flowing from personal information protection laws seems to pose major problems of compatibility with freedom of expression.

Question 9

To implement the ECJ ruling, Google has created a form in which anyone interested can submit a request to have information about him-or herself be delisted. Based on this request, Google will weigh between the private interest of the petitioner and the public interest to be informed. Google does not disclose the ways in which it deals with requests. In particular, Google does fully not disclose, the category of requests that are excluded or accepted, the proportion of requests and successful de-listings and, among others, the reason for the denial of delisting. Do you think that Google should be more transparent about the ways it uses to implement the right to be forgotten?

In many democratic countries, we would begin by expressing surprise that a court supposedly attached to upholding the rule of law would have no problem entrusting a company with the responsibility for deciding the outcome of conflicts between the public's right to access documents that are legally online and the claims of those who would prefer information on things they did in public in the past to be made unobtainable. In this respect, the question of transparency would be pertinent only in so far as it is found to be consistent with the rule of law to entrust a private company with arbitrating between fundamental rights.

---

55 *C.L. v. BCF Avocats d'affaires*, 2016 QCCAI 114 (CanLII), 14 April 2016, online: <http://canlii.ca/t/ gr5q0>.

Question 10

Is the procedure prepared by Google used in your country?

Under Canadian law, the right to delisting is possible only once a court has recognized that the document to which the hyperlink points is against the law.

Question 11

Is there any upcoming legal reform in your country whose purpose is to reinforce or modify the right to be forgotten?

Generally, it is considered that there are more urgent priorities on the level of personal information protection than those consisting in censuring information that is in the public domain.

Question 12

In your opinion, what should be the next step in the protection of the right to be forgotten? Do you think that one must go further and strengthen the right to be forgotten? Do you think that the European Union should modify or adapt its legislation on the right to be forgotten?

The current personal data protection laws based on the "consent" fiction no longer provide the appropriate frameworks for guaranteeing that data generated by the community will be used in accordance with respect for fundamental rights and democratic values. In Europe, where reflection is sometimes more advanced on these issues, the regulation of data associated with individuals continues to be envisioned as it was in the last quarter of the twentieth century. The result of such an approach is that yesterday's regulatory system is used to regulate future practices.

By failing to innovate with respect to regulatory mechanisms, we exhaust ourselves trying to apply laws that persist in postulating that data on individuals can be used only with their consent and uniquely for specific purposes. This individualistic approach clings to the fiction of "consent" that cybernauts and all users of related objects supposedly give in a

fully informed manner. This approach produces a flawed outcome: practically most data uses by internet giants, even those that raise a great deal of concern, are authorized. We have all clicked on the ritual “I accept” when we have decided to use an application, site or object in this connected world!

Current laws on personal data simply manage the abandon of our freedoms under the conditions defined by the Internet giants. In this respect, the right to delisting is a mechanism that gives those with the means the ability to complicate the lives of those seeking a degree of transparency with respect to people in power, such as professionals and public figures.

Today, big data are essential to creating value in connected environments. For now, the laws persist in requiring that these masses of information be used only for defined “purposes”. With the right to delisting as created in Europe, we are sinking deeper into a formalist vision based on “consent” and the hypothesis that is it still possible to determine the end uses of a piece of information circulating in cyberspace.

However, big data processing is based on systems that exclude the purposes for which the data was initially collected. Once they have become “Big Data”, the information no longer “belongs” to individuals. Used massively, data are a resource shared by all, like the air we breathe and the water we drink. Like water, air, and radio-electric frequencies, data are at the core of AI-based value creation. Their use must be conceived of as a privilege governed by rules that States must have the courage to impose and enforce.