The Legal Side of the Cloud

by Jean-François De Rico

LANGLOIS

AVOCATS - LAWYERS

The Legal Side of the Cloud

Studies confirming the financial and technical benefits of cloud computing just keep on coming. In 2013, for example, a study by the firm IDC indicated that 82% of Canadian businesses that implemented cloud computing solutions reported reductions in their IT costs. Equally significant, is the finding that businesses surveyed claimed better governance and management of their information[1].

The Technology

The term "cloud computing" does not designate a specific technology, but a relatively new way to access and use IT resources and services.

Cloud computing essentially consists of accessing and using remote IT resources by using the increased capacity, speed and reliability of today's networks. Propelled by the attractiveness of a business model that allows organizations to avoid bottlenecks and reduce the time and effort spent on managing, maintaining and supporting IT resources, the cloud computing industry has grown substantially in recent years.

While the nature, extent and scope of the services and resources now available in the cloud has developed significantly, the rationale for delocalizing IT resources and accessing centralized ones is not new. The possibility of interconnecting the computers of the US defence department in the 1960s and the desire to expand the computing capacity of some supercomputers for the benefit of American university researchers and research centres in the 1980s were two of the primary drivers of the development of the Internet[2].

Nevertheless, the possibility of using external equipment and resources for an entire range of IT services, such as web hosting, telephone servers, data storage, using applications in production mode, or the use of office-automation software, is a recent phenomenon[3].

The offers of cloud computing solutions providers can be categorized in terms of service models (SaaS; PaaS; IaaS) as well as in terms of types of deployment (public, private, hybrid, and community). The characterization of the services involved in these deployment categories becomes important when it comes to risk analysis and the adequacy of the proposed contractual undertakings, which must be reviewed by an organization considering the advisability of using cloud computing services.

The Legal Framework

From a legal standpoint, resorting to cloud computing for services involving communications, transfers or processing of data, or for the storage of documents of a confidential nature that may contain personal information, requires consideration of several legal issues pertaining to information management and security, including the protection of personal information.

In addition one must examine the conditions allowing organisations to meet the obligations imposed by the *Act to Establish a Legal Framework for Information Technology* regarding the maintenance of the integrity, availability and security of documents transmitted or stored through cloud computing services.

"The right to privacy, one of the components of which is the protection of one's personal information, is recognized as a fundamental right..."

The right to privacy, one of the components of which is the protection of one's personal information, is recognized as a fundamental right by the Canadian and Quebec charters of rights and freedoms[4].The principle of confidentiality of personal information and the responsibilities of persons who gather such information are provided for in statutes of general application as well as in other statutes and regulations specific to various sectors of activity, such as financial and health-care services.

The location of the equipment used for data processing and document storage is also a factor that must be considered by both public organizations and private-sector businesses, for the purpose of ensuring statutory and regulatory compliance with both the various protection-of-personal-information statutes as well as several other statutes that deal accessorily with access to and availability of an organization's documents.

The general legal framework is defined by the *Act to Establish a Legal Framework for Information Technology* ("**ELFIT**")[5] as well as by, depending on the context, the *Act respecting Access to Documents*

held by Public Bodies and the Protection of Personal Information (the "**ADPBPPI**")[6], the *Act respecting the Protection of Personal Information in the Private Sector* (the "**PPIPS**")[7] and the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**")[8]. Several other statutes that apply to specific areas of activity supplement this legal framework. Certain Professional associations also set forth obligations pertaining to confidential and privileged information.

Act to Establish a Legal Framework for Information Technology

The ELFIT statute has a section entitled "Maintenance of Integrity of Documents throughout Lifecycle" which imposes obligations on a party who uses the services of a third party for the storage, preservation or transmission of documents[9].

Section 25 of ELFIT specifies the obligation of the person responsible for access to a digital document containing confidential information to take appropriate security measures to protect its confidentiality. Section 26 provides that anyone who places such a document in the custody of a service provider must inform the latter of its confidential nature, the level of protection it requires, and the persons who are authorized to access it. That section also obliges the service provider to "see to it that the agreed technological means are in place to ensure its security and maintain its integrity and, if applicable, protect its confidentiality and prevent accessing by unauthorized persons" as well as to "ensure compliance with any other obligation provided for by law as regards the retention of the document".

ELFIT also deals with the obligations applicable to the transmission of a confidential document[10]. Section 34 of the statute provides that confidentiality must be protected by means appropriate to the mode of transmission" and requires the retention of "documentation explaining the agreed mode of transmission, including the means used to protect the confidentiality of the transmitted document ...". Thus, in a contract for the provision of cloud-computing services, the mechanism used to protect the confidentiality of transmitted documents (e.g. encryption) must be specified.

Protection of Personal Information

Like the federal statute[11], the Quebec statutes applicable to the public and private sectors both refer to the possibility for an organization to use the services of a third party for managing documents containing personal information. Section 67.2 of the Quebec public sector statute provides that the organization must enter into a written agreement setting out the applicable statutory provisions and the measures that will be taken to ensure the confidentiality of personal information, and to obtain confidentiality undertakings.

Both Quebec statutes provide for the possibility of retaining the services of a provider whose facilities are located outside Quebec for the purposes of holding, using or processing personal information. Thus, when a public body considers the advisability of using cloud computing services, section 70.1 of the ADPBPPI provides that it "must ensure that the information receives protection equivalent to that afforded under this Act". The statute applicable to the private sector imposes a less onerous obligation, namely not to disclose the PI to third parties subject to certain exceptions (s. 17 of PPIPS).

The type of documents and information as well as the functions or activities that process or use them are determinative of the extent of an organization's obligations. If there is personal information involved, some due diligence is called for pursuant to section 70.1 of the ADPBPPI (public sector) or s. 17 of PPIPS (private sector).

The organization must, as the case may be, not only ensure that the contractual undertakings of the service provider are adequate, but also that the jurisdiction(s) where the latter's facilities are located are subject to a legal regime governing the protection of personal information that allows the organization to conclude that the "information receives protection equivalent to that afforded under [Quebec law]" or that the information will not be used for ulterior purposes or communicated to third parties without the consent of the individuals concerned.

In 2014, after noting the conclusions of a study on the legal implications of the use of cloud computing[12], the government of Quebec, through the chief information officer of the Treasury Board

Secretariat, published a cloud computing guide entitled *Guide de l'infonuagique*, one of the volumes of which deals with considerations regarding the protection of personal information, in which the Treasury Board Secretariat states that it is important for public bodies to understand the legal regime applicable to the protection of personal information, and under what circumstances the courts, government entities and even police authorities from other countries can access that information[13].

Such an exercise may thus require an examination of the legal framework for privacy rights and the protection of personal information in other jurisdictions. One of the first things that must be ascertained is the existence of a rule prohibiting communication of personal information without the consent of the person concerned. That step must be followed by a comparison of the exceptions to such a rule in order to determine if they are similar to those under Quebec legislation and compatible with the provisions thereof, particularly with respect to the exceptions pertaining to rights of access of governmental authorities. This is an issue of particular interest to us, and we have undertaken a comparative analysis of rights of access available respectively to Canadian and American government authorities.

"One of the first things that must be ascertained is the existence of a rule prohibiting communication of personal information without the consent of the person concerned."

In the context of a planned outsourcing to a cloud computing provider, the call-for-tenders document should include requirements regarding delocalization and impose that bidders provide information on the legal framework for the protection of privacy rights and personal information in the jurisdiction proposed.

The *Centre de services partagés du Québec* (a provincial government entity that facilitates the procurement of services by public bodies) recently adopted this approach in a call for interest regarding cloud computing services, by requiring potential suppliers whose offers involved storing, using or communicating information outside of Quebec to demonstrate that the foreign jurisdiction's legal framework affords equivalent protection to that afforded by Quebec's legal framework[14].

If no personal information is involved, the documents and information to be outsourced should be assessed from a business continuity standpoint in order to weigh the risks and identify the appropriate contractual requirements. Service models and deployment modes should also be considered in order to gauge the client's degree of control and the attendant risks, as the case may be.

In a policy paper published in 2015 that led to a general consultation by a Quebec National Assembly committee[15], the government of Quebec set out its policy directions for the purposes of the upcoming revision of the ADPBPPI. Among them is the intention to amend the statute in order to define the concept of "equivalent protection" and to create regulatory powers to establish criteria in that regard.

Contractual Framework

The contractual framework for the supply of cloud computing services is ultimately of great importance for any organization. It is not only a statutory legal obligation, but the mechanism whereby the client is able to stipulate provisions aimed at mitigating the identified risks, ensuring respect of the service provider's obligations and its own regarding retention of documents and protection of personal information, and obtaining service levels undertakings aligned with the degree of sensitivity or strategic nature of the functions or activities concerned.

Our approach is based on an analysis of the issues on two levels, i.e. governance and operations. The degree of control it exercises is a subject of concern for any organization concerned with the management and preservation of its informational assets. A loss of or reduction in control will have an automatic impact on governance in respect of informational management and must be accompanied by contractual undertakings of the cloud service provider with respect to confidentiality, security, availability and integrity.

The governance and operational issues that must be considered are numerous:

- Ownership rights and status of holder
- Business continuity
- Portability – Interoperability
- Transition at end of contract

- Location
- Internal controls
- Employees and subcontractors
- Legal access
- Audit / Retention of certifications
- Physical and electronic security
- Confidentiality / Protection of personal information
- Service levels
- Incident management and security
- Logs
- Return – destruction

In some cases, reference to a checklist or grid, such as the Cloud Controls Matrix published by the Cloud Security Alliance (CSA), or to the sections of such a grid, may prove useful.

Reference to norms or matrices based on standards such as ISO 27001, ISO 27018, ISO 17788 and ISO 17789 may also prove useful when reviewing the contractual undertakings and policies of the service provider.

The advisability of opting for cloud computing can only be determined pursuant to an examination of the legal framework applicable to the documents and information involved, which will allow the organization to adequately assess the risks associated with the type and model of the services considered. This review, and the negotiation of contractual undertakings and mechanisms aimed at reducing and managing residual risks, will also allow an organization to benefit from the financial advantages and efficiency gains resulting from cloud computing.

Our Services

Our team, headed by Jean-François De Rico, has developed exceptional expertise in Information Technology law. Our professionals provide services and advice in the following areas:

- IT governance;
- legal, regulatory and normative compliance;
- protection of personal information;
- negotiating and drafting service contracts, licences (free and commercial), development and implementation agreements;
- management of intellectual property rights, including IT-related copyrights,

in connection with projects for the development of software applications, the outsourcing of IT services, the provision of IT equipment and services, the implementation of e-business processing systems and the migration of IT systems.

Written by

Jean-François De Rico
Lawyer, Partner
+1 418 650 7923 | +1 514 842-9512
jean-francois.derico@langlois.ca

Notes

[1] IDC, Cloud Study
[2] INTERNET SOCIETY, Brief History of the Internet [http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet], consulted on January 2, 2014
[3] The emergence of this type of commercial service offering, such as Amazon Web Services – EC2, dates to the mid 2000s.
[4] The *Canadian Charter of Rights and Freedoms* (s. 8); the Quebec *Charter of Human Rights and Freedoms* (ss. 4, 5, 6, 7) and the *Civil Code of Québec* (art. 35) recognize the fundamental nature of the right to privacy.
[5] CQLR, c. C-1.1
[6] CQLR, c. A-2.1
[7] CQLR, c. P-39.1
[8] SC 2000, c. 5
[9] On the ELFIT statute, see in particular the website www.lccjti.ca as well as P. Trudel, *Introduction à la Loi concernant le cadre juridique des technologies de l'information* [Introduction to the *Act to Establish a Legal Framework for Information Technology*] Cowansville, Yvon Blais, 2012.
[10] For an exhaustive analysis of the provisions pertaining to transmission, see P. Gingras and J.-F. De Rico, "*La transmission des documents technologiques*" [The transmission of electronic documents] in *Actes de la XX^e conférence des juristes de l'État*, Cowansville, Yvon Blais, 2013, p. 409.
[11] Supra, note 8
[12] N. VERMEYS, J. M. GAUTHIER, S. MIZRAHI, *Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec*, Centre de recherche en droit public, 2014
[13] Sous-secrétariat du dirigeant principal de l'information du Secrétariat du Conseil du trésor, *Guide de l'infonuagique, volume 2 – Considérations en protection des -renseignements personnels,* November 2014 pp.13-14.
[14] Centre de services partagés du Québec, Call for Interest AI-20151202, Mise en place d'offres infonuagiques - volet courriel, December 2, 2015
[15] Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques, *Orientations gouvernementales pour un gouvernement plus transparent, dans le respect du droit à la vie privée et la protection des renseignements personnels*, 2015