

VIRTUALISING DATA IN THE CLOUD REQUIRES ACTUAL RISK MAPPING

Ever since its creation, the Internet has evolved hugely. However tautological this assertion may sound, the evolution of the Internet has clearly brought new legal issues that are increasingly raising concern.

Traditionally, Internet raises various legal questions such as piracy, legality of contents and online activities, safety of online payments, jurisdictional issues, intellectual property, confidentiality and privacy, taxation, export and import controls, etc.

Dealing with all those issues is a constant challenge because of the cultural differences from one country to another and the impossibility to reach an international consensus over a uniform set of rules. In addition, the constant evolution of techniques is forcing IT security providers to adapt their defence systems to the new attacks perpetrated, the violations of privacy, the identity thefts etc.

And the difficulty is about to move several steps forward as companies and organisations will increasingly use cloud-based services, following an outsourcing approach. Information technology services have continuously boomed over the past fifteen years and will keep on following the same pattern of development. The range of cloud-based services is absolutely enormous and the incredible development of storage and data transmission capacities will enable to offer more and more valuable services from all over the world.

Generally speaking, cloud computing refers to any service involving information technology services hosted online. The cloud describes the virtual space where data is being conveyed from one server to another. The underlying idea of cloud computing is that client-users should no longer have to deal with the technical aspects of hosting their data, thus allowing them to save money and focus on their business activities. A global survey

published this year shows that 60% of US companies and 48% of European companies are pursuing a cloud computing approach.

According to the same survey, the main benefits of cloud computing are:

- Obtaining greater flexibility for the organisations;
- Reducing costs;
- Increasing operational efficiency; and
- Using a cloud computing approach as a strategy for pursuing new technology developments.

Some of the major applications of cloud computing:

Software as a Service (SaaS) is the supply of a single software application through the browser to a large number of customers using a multitenant architecture. For the customer, this means no prior investment in servers or software licensing; for the provider, with just one application to operate, costs are low compared to conventional hosting.

Platform as a Service (PaaS) is a form of cloud computing that delivers development environment as a service. Customers build their own applications that run on the provider's infrastructure and are delivered to the users via the provider's platform.

Infrastructure as a Service (IaaS) delivers a computer infrastructure to the clients. Instead of purchasing servers, software, data-centre space or network equipment, clients buy a fully outsourced service.

Managed service provision (MSP) is the provision of an application to IT providers rather than to end-users. Those providers deliver for instance security services such as virus scanning or anti-spam devices for e-mail or applications monitoring the services.

Today, the advantages of cloud computing in terms of costs and efficiency have been fully acknowledged and the debate is no longer focused on the relevance of using cloud-based services but rather on how to use such services confidently and securely. The main problematic issues of cloud computing are relating to the security of storage and transmission of the data. A cloud-computing strategy must be thought of rigorously and carefully with a reliable and skilled expert. Therefore, the key question is how should companies contract and prepare for outsourced cloud-based services to ensure a viable and sustainable business case, reduce operational and legal risks and deliver improved business performance?

Dealing with security in the cloud involves strictly defining the **terms** of the contractual relationship as regards confidentiality, integrity, availability, reliability, resilience, and accountability.

Privacy refers to keeping data private and not only personal data relating to individuals, but also technical and transactional data that can disclose important details about the companies or organisations.

Integrity concerns the safety of the data in the cloud. It is a significant aspect to protect the data against unintentional or malicious alteration.

Availability is the ability for clients to use the cloud system at all time and as efficiently as if the data were stored in the companies' computers or servers.

Reliability is the need for a system to behave as expected and as specified by the client. Reliability may be secured by a robust computing architecture.

Resilience is the aptitude of maintaining an acceptable level of service in case of failure or security threats and can be safeguarded through back-ups and diversification.

Accountability means being able to identify who is liable at all time in view a conflict resolution by defining the processes of authorisation, access, operation and control.

There are indeed a number of actual risks that have to be taken into account when using cloud

computing services. Risks of security and privacy threats, such as malware are not totally avoidable. Contracts have to deal with these issues to ensure that the provider offers technical guarantees and a high level of security. Sometimes, electronic data may have stronger safeguards when stored on local rather than remote servers especially when data is stored in a country offering diminished legal guarantees. Furthermore, a provider cannot offer a risk-free guarantee against an unwanted outcome and adequate precautions must be taken together with the provider and extended to third parties contracted by the provider.

The significant issues that must be addressed in cloud-based service agreements are:

- Data protection and privacy;
- Security (integrity and reliability);
- Cross-border issues;
- Service levels (availability and resilience);
- Pricing;
- Acceptance;
- Tax;
- Liability and indemnification (accountability);
- Business and service continuity;
- Termination;
- Transition;
- Confidentiality;
- Intellectual property;
- Audit;
- Insurance;
- Governance.

Drafting cloud-based service agreements requires paying particular attention to data security, privacy and service level requirements. Cloud-based service agreements must contain details as to data storage and protection. In that respect, clauses must be

drafted so as to safeguard transparency and disclosure. Agreements must contain provisions on how and where the data is stored, what standards regarding data security are implemented and requirements for specific data security infrastructure and testing. Where appropriate, clients can even request details about the persons in charge of administering the system and how they are recruited when they are third party service providers. The issue of compliance with applicable laws and regulations pertaining to privacy and confidentiality must also be clearly addressed all the more since the contracting parties are often located in countries having different levels of privacy and confidentiality protection.

Furthermore, strong service-level agreements must be signed to define the rights and

obligations in case of a service failure and guarantee as far as possible the continuity of service.

Adopting a successful cloud-based strategy remains a challenging target. Cloud computing allows cost savings and increased efficiency of information technology services. The risks are high but a proper contractual and legal framework may considerably reduce the dangers of cloud computing and therefore increase the confidence of companies and organisations in those services. A cloud computing strategy may truly offer a lot of advantages provided that it is carried out through a concerted approach with technical and legal partners.

16th November 2010

By Diane Mullenex, Avocat à la Cour and Solicitor England & Wales, partner in charge of the TMT department, and Clément Gautier, legal counsel.

Ichay & Mullenex Avocats is a French law firm focusing on all legal issues related to the new technologies in France and abroad. They are considered experts in intellectual property and Internet law, e-commerce, online gaming, data protection. Ichay & Mullenex Avocats also assists its clients on all issues related to financing, mergers & acquisitions, restructuring, etc. and advises them on their litigation and arbitration procedures.

5, rue de Monceau 75008 Paris - France
Tel : +33 1 42 89 19 80
Fax : + 33 1 42 89 14 99
www.ichay-mullenex.fr