PORTOLANO
CAVALLO
studio legale

Cross-Border Discovery and Cloud Computing: potential use of the cross border discovery before Italian Courts

March 29 2012

By Micael Montinari, Marco Bellezza and Matteo Magistrelli

The aim of this article is to outline the ever-increasing importance of discovery for civil law proceedings due to recent, favorable developments in law cases and judicial decisions within the EU.
In particular, we intend to consider the potential scenarios under which the result of discovery, a common law institution, could be introduced in civil-law based Italian proceedings. After a short description of the institution and of the way it may fit into civil law proceedings, we will focus our attention on litigation issues that can arise from a cloud computing relationship, and particularly on the potential conflicts between discovery and the European data protection rules, and on the possible solutions.

Pre-trial discovery

"Pre-trial discovery" is a common law procedural device to obtain evidence from the parties of a case, possibly through court orders issued for such purpose, on the assumption that an extensive exchange of information before the trial is the best way to define the matter of the litigation and can lead to a settlement between the parties. Similar obligations in the civil law experience derive under a court order to produce certain, specific documents held by the parties.
Other types of orders show major differences from the civil law in structuring evidence production. The most important is the "sub-poena duces tecum", a writ commanding a party to produce all documentation and evidence it possesses in relation to the dispute. Possession means that the party has the availability of such documentation at the moment that it is reached by the order.
In order better to understand the real scope of the order, it is important to notice that in the US the showing relates not only to documentation constituting evidence in itself, but also to documents liable to reveal the presence of further relevant information contained or stored elsewhere. In other words, it concerns all documentation which, either directly or indirectly, discloses information that may be useful for the trial. Similarly, Canada applies a broad "semblance of relevance" test to determine whether information ought to be subject to discovery. In the UK, the discovery obligation is limited to

reasonableness, assessed in light of a range of factors such as the number of documents, the complexity of the proceedings and the ease, accessibility and expense of retrieving documents. Nonetheless, the effort required may be massive.
Another important stipulation related to discovery is the so called “litigation hold”, requiring a party not to delete or destroy any documentation in its possession that could be subject to a future litigation or to a sub-poena order in a second stage of the proceeding. Because so much information is stored electronically nowadays, e-mails, stored files and even deleted electronic documents can be seen as documents. Thus, e-discovery has developed as a new form of discovery related to any kind of document and information stored in personal computers and servers.
In code-based systems, the powers of Judges in civil proceedings are quite different. An order of discovery may only be granted if certain specific requirements are met, which makes discovery rare in Italy. Indeed, the request from a party must indicate specific, well-identified documents held by the counterparty. A discovery order is granted if: (i) it is proved that this is the only way to obtain such documents and (ii) the applicant describes the facts the documents would be able to prove. In this conflicting scenario, what is clear is that discovery could play an important role for reaching a judgment in civil-law proceedings as well. When a party incorporated or based in a common law country is involved in a civil-law proceeding, for example, the counterparty may ask the common law Court to issue a discovery order.
The introduction of discovery into civil-law proceedings therefore clearly depends on whether one of the parties involved is subject to a jurisdiction where Judges have powers in relation to discovery, as is the case for cloud computing service providers.

Cloud computing

The development of cloud computing services in recent years has been and will be suggesting new questions and solutions related to the production in court of documents kept in the cloud[1]. Generally speaking, the Cloud is an information processing model that allows access to a broad range of on-request hardware and software services. Such services can be used on-line and made available to many clients at a time, allowing a very efficient storage of information.
We can identify two main players in the cloud service: the buyer, that is the recipient of the service, and the cloud provider. When the latter operates worldwide, it comes into contact with buyers from many different countries. Clearly, therefore, the probability that one of the parties to a Cloud agreement is subject to a common law jurisdiction is very high, also because the most important public providers are established in the US, which is a common-law country. Courts could thus be involved in a potential claim between two parties that store documentation in the Cloud, or between a buyer and a cloud service provider, whenever either of them is established in a common-law country.

Cross-border Discovery

When the disclosure order is issued by a country, other than where the relevant documents are stored, we are speaking of the so called cross-border discovery. In this case different territories and jurisdictions are involved and obviously not only material documents are included, but also information stored electronically. By way of example, assuming that a provider based in a common law country operates directly or through a branch in a civil law country within the EU, it is possible for its counterparty to ask for a sub-poena order from a US Federal Court although the case is set before a civil law Court.
On the other hand, during a trial set in a common law country, the Court may issue a sub-poena order in relation to information possessed by a party in a civil law country’s territory. As said, in fact, cross-border discovery is the situation in which documents stored in a civil law country may be transferred to a common law country, and vice-versa, pursuant to a sub-poena order. More specifically, this

bidirectional flow of information and documents occurs in the following situations:

• the trial is held in a common law country between a party established there and another established in a civil law country. The common law party may apply for the issue of a sub-poena order against the civil law party that possesses the documentation. Severe procedural sanctions may be imposed for failure to comply with the order. In Italy, for example, the party requiring the discovery can obtain a declaration of enforceability of the order by the competent Court of Appeal when the counterparty does not comply. Recently, the Italian Data Protection Authority stated that the presence of a server in a Member State implies that national Courts may enforce an order of disclosure if this is allowed by the national procedural rules;

• the trial is held in a civil law country but one of the parties is established in a common law country. The civil law party can file a petition for a sub-poena order with the common law Court of the country of the counterparty. If the order is issued, refusal to obey may lead to losing the case. In the US this is possible pursuant to section 28, U.S.C. § 1782 which authorizes the Federal Court "of the district in which a person resides or his found to order him, to produce a document or other thing for use in a proceeding in a foreign tribunal. The order may be made upon application of any interested person". The applicability of such rule to cross-border discovery has been confirmed by the U.S. Court of Appeal, Seventh Circuit in HeraeusKulzergmbh v. Biomet Inc. The judge expressly stated that "a party to litigation in a foreign country can seek discovery relating to that litigation in a federal district court, and, in the discretion of that court, can obtain as much discovery as it could if the lawsuit had been brought in that court rather than abroad".

Data protection

The main obstacle to cross-border discovery is represented by the rules set by [EU] Member States. These include national blocking laws, laws of confidentiality and banking secrecy, employment laws, wiretap laws and, most of all, data protection laws issued pursuant to Directive 95/46.
Cloud computing activities involve the processing of personal data of buyers, and the strict legislation of the EU regarding data protection applies even to third parties not resident in a Member State. The concept of "processing" incorporates all actions over the life-cycle of the data: collection, use, disclosure and destruction, therefore including recovery of data for discovery purposes. Although in the US the storage of personal data for "litigation hold" is not considered as processing, under Directive 95/46 any retention, preservation, or storage of data for such purposes would amount to processing. In practice, the flow of personal information between EU member States is not restricted. Export to a third-party State which might be considered to have inadequate privacy protection is generally prohibited, with limited exceptions. The Directive, and the relevant implementation provisions, imply the application of the data protection rules not only if the responsible for the processing is established in a Member State but also if it has some transmission or storage facilities in the European Economic Space (EES).
Pursuant to Directive 95/46, there are three important ways to justify data processing activities in relation to e-discovery: unambiguous consent by the data subject; need to comply with a legal obligation of the collector; achievement of legitimate interests of the data collector.
Under section 25 of the directive, transfer of data to a non-EU country is allowed only if the destination country grants adequate data protection standards. This creates particular difficulties for transfers to the US, since the EU has deemed data privacy protections in the US inadequate to support a transfer.
However there are two crucial exceptions to this roadblock: under Section 26, paragraph 1, letter d), a transfer may occur when in furtherance of "an important public interest" or the "exercise, establishment or defense of legal claims". For purposes of e-discovery, the legal claims exception probably carries more weight, but still has important limitations to consider. The Article 29 Working Party (a

representative body for European data protection regulators) has accepted the idea that the exception would most likely apply if the parent company of a multinational group were to be sued by employees of a European subsidiary. The litigation must already have commenced or be imminent, however, and the exception would not apply to large-scale prophylactic data transfers in preparation for the possibility of litigation sometime in the future.

Cross-border Discovery in the practice

Going forward from principles to practical application, it could be useful to consider the common law Courts approach to cross-border discovery. Only knowing how a sub poena order is granted by a common law judge, in fact, an Italian lawyer can effectively evaluate whether applying for an order of disclosure could be useful and what the extent of their request should be.
As mentioned, the focus will be on the UK and US Courts' interpretation. English courts have adopted similar reasoning to the Article 29 Working Party in the recent case arisen out of the Madoff scandal. In the Madoff case[2] the UK liquidators of Madoff Securities International Limited applied to the Court for directions on the transfer of specified personal information to the US trustee in bankruptcy. The English court approved the application in a brief order, finding it was both:

- necessary for reasons of substantial public interest (schedule 4, paragraph 4 of the UK Data Protection Act 1998); and
- necessary for the purposes of, or in connection with, any legal proceedings and establishing, exercising or defending legal rights (schedule 4, paragraph 4 of the UK Data Protection Act 1998).
-

The court was not asked to consider whether the discovery would also satisfy a general processing condition, such as the legitimate interests test. However, the court refused a request to give the liquidators general discretion to disclose any other information to the US trustee in bankruptcy as was in the interests of the liquidation.
The US legal system contains specific provisions allowing the Court to order discovery of information not located in the US (see Restatement (Third) of Foreign Relations Law, Section 442 Id). Before doing so, the US Courts must consider whether the information is also subject to conflicting privacy laws and if so, a balancing exercise has to be undertaken: the significance of discovery, the degree of specificity of the request, the availability of alternative means to obtain the information are the main aspects to be checked along with the good-faith efforts of the required party to secure the necessary permissions to transfer data.

Conclusions: a way to introduce the outcome of discovery before Italian Courts

In light of the above-mentioned principles, what happens if a cloud provider is required to file information and documents before an Italian Court, for instance in a claim arisen from a merger or an acquisition in which a virtual data room held and managed by individuals in a common law jurisdiction has been used for carrying out the due diligence? This way, indeed, information and documents are available on-line or stored by means of the Cloud.
As seen above, the counterparty of the provider or of the buyer that has information stored by a Cloud provider may ask the Federal Court that has jurisdiction over the latter to issue a sub-poena order. However, provided that we do not have precedents in Italy, if the provider does not obey the aforementioned order, this should be subject to a procedure for recognizing and enforcing foreign decisions. More in particular, the party who has obtained the disclosure order by the foreign Court would need to apply to the Italian Courts for enforcement when the data collector has a branch located in Italy where the information is stored.
The enforcement proceeding is set by Law no. 218/1995 in relation to orders coming from US Courts

and by EU Regulation 44/2001 in relation to orders coming from UK Courts. Although the rules set by the aforementioned bill are similar, they differ in relation to the need for an exequatur by the competent Court of appeal in case of US orders' enforcement.
It cannot be predicted whether national Courts will admit the enforcement of such orders, although European authorities seem to have taken steps in that direction of recent. It will mostly depend on the evaluation given by Judges in relation to the compliance of such orders with the Italian public order. Indeed, enforcement should be denied if a disclosure order is not compliant with the Italian public order.
Generally speaking, provided that the latter is constantly evolving, it is possible that even a broad disclosure order might be deemed acceptable. Naturally, if the Cloud provider complies with the order or obeys an enforcement decision, all the information transmitted to the counterparty should be stored and used in observance of the data protection laws described above.
In the end, cross-border discovery related to the processing of personal and sensitive data puts Italian lawyers in front of new challenges, but surely grants them powers and opportunities unheard of in their procedural systems. These new powers are going to change the way to assist clients, from the drafting of a multinational agreement to litigation before a Court. The key could be to consider all documents held by a client as potential evidence and, as a consequence, provide assistance starting from the best way to safely store data.

[1]Pursuant to the NIST (National Institute of Standards and Technology) definition: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

[2]Re Madoff Investment Securities LLC [2009] EWHC 442

PORTOLA

PORTOLAN

VALLO PORTOLA

PO

PORTOLANO CAVALLO PORTOLANO CAVALLO PORT

PORTOLANO C