Legal Issues in Grid and Cloud Computing

Abstract This chapter addresses the most relevant legal issues in Grid and Cloud computing scenarios. The main focus will be on the contractual relationship between technology provider and customer. In particular, it will be assessed which clauses should be inserted in a typical agreement (namely a Service Level Agreement) between a Grid/Cloud provider and a client. Furthermore, other issues like the law applicable to the contract, liabilities of the technology provider, security and privacy issues will be analysed, together with an overview of the relationship between Grid and Cloud computing from the tax point of view.

1 Introduction: the lawyer's perspective about Grid and Cloud computing

A business scenario based on the adoption and implementation of Grid and Cloud technology presents many legal issues that have to be taken into account by companies and individuals that plan to start a Grid/Cloud-based business. In general terms, in fact, Grid/Cloud technology is not 'neutral', in the sense that it brings several particularities as regards, mainly, contractual and security profiles (Parrilli et al. 2008). In other words, a contract between a Grid/Cloud provider and a customer is likely to be slightly different from an agreement between a provider of a different technology (not based on dispersed resources) and a client.

The legal issues that affect a Grid/Cloud-based business are many, and include, just to mention a few of them, contract law, intellectual property rights, privacy law, taxation etc. The aim of this chapter is precisely that of providing the reader with some clarifications and guidelines as regards the most relevant legal issues that a typical customer should take into consideration when dealing the terms of the provision of Grid/Cloud services with a technology provider. Two moments will be more specifically analysed: (i) the contract, or contracts, signed by the customer and the Grid/Cloud provider, i.e. formation, validity and enforceability of the agreement(s); (ii) the contractual relationship following the signing of the agreement, in connection with the liabilities of and the remedies at disposal of the parties. Special attention will be dedicated to security (and privacy) profiles, which are supposed to be the Achilles' heel in Grid and Cloud computing. A few notes will be dedicated also to one of the most relevant taxation issue. In other words, we ideally guide a typical customer in the process of entering into an agreement with a technology provider and therefore we will follow the negotia-

tions phase (if any) and the signing of the contract. Furthermore, we will show him the risks underlying the contract and will tell him how these risks can be reduced or avoided. When the agreement will be finally signed, our mission will end.

From a different perspective, then, the goal of the following pages is to show how legal barriers for customers can be reduced, taking into account, nevertheless, that these are heavily influenced by the business environment in which the Grid/Cloud provider and the client operate. In other words, in business to business (B2B) scenarios (this chapter does not address business to consumer – B2C – issues) the client does not receive special protection from the law, in light of the principle that businesses are basically in equal position at the moment of negotiations.[1] This statement is clearly unrealistic given the fact that, in most cases, the Grid/Cloud provider is a big international player and the customer is usually an SME or even a micro-enterprise. The latter, of course, will have basically no power to negotiate more favourable clauses and the only option is to sign or not to sign the contract drafted by the technology provider. Nevertheless, the customer should check whether this contract is too risky, in the sense, for instance, that the provider does not take any liability and the customer does not have the right to enforce the contract, or such enforcement is very limited.

This means that the non-legal categories of trust and reputation will play a pivotal role and will guide potential investors to opt for a Grid or Cloud provider instead of its competitors. Trust and reputation, although very important, are not enough: the customer, in other terms, does not have to be impressed by the brand of the Grid/Cloud provider but should verify whether he gets enough protection by the contract signed with him. Things are different, of course, if the parties are in the position to really negotiate the content of the agreement(s), and in this situation they should balance risks and liabilities between them. It is advisable, thus, that the contract(s) is as complete and balanced as possible, in the sense that it should encompass possible situations like non-compliance, litigation, etc and should motivate both parties to respect it.

In other terms, a contract which is too unbalanced in favour of the provider, for instance, is likely to offer him reasons not to supply the services at the promised quality and to favour bigger and more 'important' clients. Selection and differentiation between clients is an obvious practice from the business perspective, but it should not damage or discriminate a certain customer. The law and economics li-

[1] The literature pointed out, as regards civil procedure (but the statement is true also as regards other legal issues), that "because the consumer is the weaker party, who often pays in advance for the transaction to take place and cannot influence the unilateral terms of contract that are offered, the balance in relation to jurisdiction leans towards the consumer." (Storskrubb 2008)

terature showed, in fact, that one of the purposes of contract law is "to secure optimal commitment to performing" and, in particular, that "when liability is set at the efficient level, the promisor will perform if performance is more efficient than breaching, and the promisor will breach if breaching is more efficient than performing." (Cooter and Ulen 2004).

In light of these considerations, the first issue to address regards the contracts made by a Grid or Cloud provider and a customer aimed to regulate their business relationship. Special attention will be dedicated to the Service Level Agreement (SLA) and to its potentially related agreements.

2 The contractual relationship between Grid/Cloud provider and customer: the contract

The provision of Grid or Cloud services by a technology supplier shall obviously be regulated by a contract, or a group of contracts, that will govern the specific 'position' of each party in the relationship, i.e. the duties, liabilities, remedies etc of each contractor will be stated in the agreement and each party will be bound to respect the obligations contained there. The agreement that plays a pivotal role in a Grid and Cloud scenario is the SLA, which can be defined as "a part of the contract between the service provider and its customers. It describes the provider's commitments and specifies penalties if those commitments are not met." (Leff et al. 2003) As said above, and as it frequently happens in the practice, the Grid/Cloud provider and the customer can 'concentrate' all the provisions that will govern their relationship in the SLA or enter into more than one agreement. The SLA, then, will be focused on the most relevant technical specifications linked to the provision of the service, in other terms its main goal will be that of defining the quality of the service (QoS) promised by the supplier. QoS means, more specifically, the availability and performance levels, in other terms the level of performance guaranteed (it will be showed *infra* to what extent) by the provider.

All other clauses regarding liability, warranties, confidentiality, etc may be included in another contract (that can be called, for instance, Customer Agreement), and this is often the case in point with big international Grid/Cloud computing and storage capacity providers. Nevertheless, the reader should be aware that in practice many combinations are possible and frequent, e.g. the provision about fees can be included in the Customer Agreement while liabilities may be regulated by the SLA. The names of the agreements are not really relevant to the ends of our analysis: what is pivotal is the content of some sensitive clauses and the fact that the agreements made by the parties must be legally valid and enforceable. We illustrate this point with an example that involves two imaginary European companies: *SuperICTResources*, German technology provider, and *SaaSforyou*, Dutch

customer/SaaS provider. If we assume that they negotiate the content of their agreement, we see that it is probably easier for them to have a unique contract (SLA) instead of a plurality of agreements, unless this is necessary or useful in light of the specific situations and needs of the parties. Especially if more services are involved, it may be convenient to draft a frame agreement, aimed to regulate the overall relationships, and many SLAs tailored to the specific service provisions.

From a different perspective, then, it is important to point out the distinction – which is relevant from the legal point of view, in relation to the negotiation of contracts and therefore the content of the contractual provisions – between (i) agreements negotiated on a case-by-case basis by the parties (like in the case of *SuperICTResources* and *SaaSforyou*) and (ii) agreements drafted unilaterally by the Grid/Cloud provider and imposed to the client (e.g. if *SaaSforyou* buys Grid or Cloud capacity from Amazon, Sun, etc). In the latter case the customer, if he wants to buy the services of the provider, can only accept the SLA and the other agreements proposed by the supplier, with no possibility to change or amend the content of the provisions. With this regard it is in fact extremely unrealistic that a big provider, like for instance Amazon, Sun, etc, negotiates every agreement with its clients because of the high costs of negotiations and the risks of inefficiency linked to this.

Given the fact, therefore, that "a key goal of Grid computing is to deliver management on top of the allocated resources which include for example availability of resources (compute resources, storage, etc) and network performance (latency, throughput)" (Padgett et al. 2005), the typical minimum content of the SLA should be the following:

1. *Availability*: this clause indicates the percentage of time, usually on a monthly basis, in which the Grid/Cloud service supplied by the provider will be available. With this regard, it is very important to point out that Grid computing is expected to increase the quality of the services delivered and therefore the customer has many good reasons to require availability very close to 100 % (the same applies to Cloud computing). In our example, it is realistic to imagine that *SaaSforyou* chooses *SuperICTResources* as technology provider because the latter is able to offer an extremely high availability. In case of SLA specifically negotiated by the parties, the customer will be in the position to bargain and obtain a favourable and realistic level of availability, while in case of standard SLA drafted unilaterally by the provider the client can only accept or refuse the offer, i.e. he can enter or not enter into the agreement. The business practice shows nevertheless that big international Grid and Cloud computing providers guarantee an availability ranging usually from 99,9 % to 100 %, and this de-

monstrates clearly that Grid and Cloud computing has a notable impact on the QoS to which the provider commits himself.

2. *Performance*: the objective of this provision is to assure the achievement of commonly accepted computing, storage, and network element performance capabilities according to the class of hardware and bandwidths installed. Legally speaking, the content of this clause will depend on the infrastructure adopted by the provider and therefore the margin for negotiations, especially if the customer is an SME or a private user (like, we assume, *SaaSforyou*), is usually quite limited.

3. *Downtime and service suspension*: this clause should not find room in an SLA (or other contract) in a Grid/Cloud environment, and in general in dispersed compute resources scenarios, provided that failures at the level of a single server or cluster (i.e. Grid/Cloud component) should be compensated by the other ones. Nevertheless, agreements unilaterally drafted by big international providers often state that access to and use of the service, or part of the service, may be suspended for the duration of (i) any unscheduled downtime or unavailability of a portion or all of the service and of (ii) scheduled downtime for maintenance or modifications to the service.

4. *Security*: this part of the SLA is of fundamental importance as it will commit the provider to a certain level of security in order to protect the information and data supplied by the customer and to avoid that harmful components are delivered to the customers' computers. The client should therefore pay great attention to this clause and, if the SLA is negotiated by the parties, should require that the security standards are set in the contract, so that the provider will be bound to respect them (see *infra* for further details). The business practice shows that usually the SLAs unilaterally drafted by the big Grid/Cloud players tend not to mention security requirements, so that the customer basically has to trust the supplier. Provided that trust, as pointed out above, is not a legal category, it is highly advisable that the provider accepts to follow and to implement a security strategy aimed to protect customer's data at multiple levels (i.e. mainly data security, data integrity, data privacy). Furthermore, the Grid/Cloud supplier shall apply security tools to his systems and should commit himself to maintain the customer's data on secured servers (e.g. located in a custom-built data centre with full physical access control). If the business carried on by the customer concerns extremely valuable (e.g. financial, medical, etc) data, the SLA may and should list the names of the employees authorised to have access to the servers. From a different perspective, the customer may have reasons to require that the provider uses only his servers and that he does not outsource Grid or Cloud capacity to other providers, thus limiting the security risks. This may appear to be against the rationale behind Grid (and Cloud) computing paradigm, but it can reasonable when losing or damaging customer's data would create a very big damage.

5. *Fees*: this clause will regulate the prices that the customer will pay to the provider for the supply of Grid/Cloud services.

6. *Support services*: these are particularly important for the client in order to minimise the damages in case of failures in the provision of the services, and it is advisable that the provider commits himself to respect a certain response time and to be available to solve problems as much and quickly as possible (e.g. on a 24/7 basis). This applies also to disaster recovery, which should be made as soon as possible by the supplier. The lack of contractual obligations for the provider to do so may result in tremendous damages for the customer without the concrete possibility to claim compensation.

Provided this minimum necessary content of the SLA (or other contract as applicable), the reader should be aware of some remarks as regards the validity of the agreement, more specifically the legal requirements to respect in order to have a contract which is valid and enforceable. This is a matter of national law, and therefore every jurisdiction sets specific rules in the field. Nevertheless, without entering into further details, it is possible to say that an offer made by the offeror followed by the acceptance of the offeree, together with the will to enter into an agreement, and provided that the parties have the necessary legal capacity required by the applicable law, is a valid contract (Beale et al. 2002). An additional requirement is the cause (in some civil law countries, like France, Italy, Belgium, etc) and the consideration (in common law jurisdictions, e.g. England and the United States): the former can be defined as the economic reasons behind the contract (e.g. payment of a fee in exchange for a service or good), while the latter can be described as "what the promise gives the promisor to induce the promise"[2] (Beale et al. 2002).

Special attention shall be devoted to the legal capacity of the person who signs the contract, more specifically the employee or director who enters into an agreement on behalf of his company should have the power to do this. A contract signed by a person with no legal capacity can be, depending on the applicable law and on the circumstances, void or voidable. Another aspect to take into account is whether the SLA and/or the other related contract should be made in written form (with signature of the parties). This also depends on the applicable legislation and, in general terms, the agreement for the provision of a service can be made in whatsoever form in Europe (Beale et al. 2002). With this regard, Article 9(2) of the Rome Convention[3] on contractual obligations states that "A contract con-

[2] "The delivery of a car, the painting of a house, or a promise to deliver crops may be consideration for a promise of future payment." (Cooter and Ulen 2004)

[3] 1980 Rome Convention on the law applicable to contractual obligations (consolidated version) [OJ C 27, 26/01/1998, p. 34-46]. For contracts concluded after 17 December 2009, Regulation (EC) 593/2008 of 17 June 2008 on the law applicable to contractual obligations (Rome I) [OJ L 177, 4/7/2008, p. 6-16] will apply. Art. 11(2) states that "A contract con-

cluded between persons who are in different countries is formally valid if it satisfies the formal requirements of the law which governs it under this Convention or of the law of one of those countries." This means that an agreement made, for instance, by a Dutch customer (*SaaSforyou*) and a German Grid or Cloud provider (*SuperICTResources*) is valid if it respects the formal requirements set forth by Dutch or German law.

If the parties are established in the same jurisdiction, Article 9(1), following the rationale behind the abovementioned second paragraph of Article 9 to recognise as much as possible the validity of an agreement (*favor negotii*), points out that "A contract concluded between persons who are in the same country is formally valid if it satisfies the formal requirements of the law which governs it under this Convention or of the law of the country where it is concluded."

The fact that the written form is not a validity requirement for the contract does not necessarily mean that it is not convenient for the parties to have a written and signed copy of the agreement in case it is needed or useful, especially in order to have an evidence of the existence of the contract and of its content. With this regard the Grid/Cloud provider and the customer can make an electronic contract to which the electronic signatures of the parties are attached, or, more traditionally, can make a paper-based copy of the contracts with 'real' signatures. In principle, provided the legal value conferred by the applicable legislation of the European Union (EU) to the electronic signature[4] , the two versions of the agreement shall have exactly the same validity and effects.

Finally, we focus on some other important clauses that the parties should include in the SLA (or in another contract, according to the case) or that are likely to be encountered in the agreements drafted by the big international providers:

1. *Description of the service*: a clear description of the service provided by the technology supplier, apart from the QoS, will avoid discussions and litigation. Listing if eventual extra services will be provided for free or under payment of a fee is equally important.

---

cluded between persons who, or whose agents, are in different countries at the time of its conclusion is formally valid if it satisfies the formal requirements of the law which governs it in substance under this Regulation, or of the law of either of the countries where either of the parties or their agent is present at the time of conclusion, or of the law of the country where either of the parties had his habitual residence at that time." With this regard, Art. 19(1) specifies that "For the purposes of this Regulation, the habitual residence of companies and other bodies, corporate or unincorporated, shall be the place of central administration."

[4] See, in particular, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures [OJ L 13, 19/1/2000, p. 12-20].

2. *Modification of the agreement*: this clause basically should state whether the provider can unilaterally modify the service and the agreement (and if so, how and to what extent) or whether only modifications negotiated and agreed by the parties are acceptable.

3. *Termination of the agreement*: it is practically important to state when the contract will end and how it can be renewed (automatically, or after new negotiations and signing of a new contract). Furthermore, the parties should state whether or not they can unilaterally terminate the agreement and, if so, which notice period applies. It is common practice that severe violations of the contractual obligations by one party give the other the right to terminate the agreement. Examples of such violations by the customer include being in default with payments, misuse of the service, attempt to break security mechanisms, bankruptcy proceedings, etc. The agreement should also regulate the effects of termination, like data preservation (the technology supplier could not erase the data provided by the client) and post-termination assistance.

4. *Prohibited services*: it is advisable that the Grid or Cloud provider, in order to avoid any potential liability, requires to insert in the SLA or other agreement a clause prohibiting the customer to use the Grid/Cloud infrastructure to operate a site or a service that, for instance, permits gambling, facilitates child pornography or other illegal activities, engages in practices like phishing or pharming, distributes viruses, spyware or other malicious applications, violates third parties' copyright, etc.

5. *Licenses*: this provision will state that whatever software, if any, distributed by the Grid/Cloud provider to the customer will only be licensed, under specific terms, to the client (with no transfer of 'ownership'). Usually the license will be limited, non-exclusive and non-transferable.

6. *Confidentiality*: all confidential information regarding either the provider or the customer may not be disclosed without prior authorization during the contractual relationship and for a certain period of time after the termination of the agreement. Confidential information are deemed to be information designated by the disclosing party as confidential or that, given the nature of the information and the circumstances of its disclosing, reasonably should be understood to be confidential. Possible exceptions to confidentiality obligations are, *inter alia*: (i) if the information is or becomes public knowledge (without fault of the party concerned); or (ii) if and to the extent that information is required to be disclosed by a party to a regulatory or governmental authority or otherwise by law.

7. *Intellectual property rights*: the clause will state that every party keeps his intellectual property rights over the service provided, any technology or software supplied and any content or data sent or shared. In particular, the *de facto* situation of enjoyment and use of these rights does not modify the legal situation of

'ownership'.

3 The contractual relationship between Grid/Cloud provider and customer: the relationship

In the previous paragraph we addressed how the relationship between a Grid/Cloud provider and a customer can be established and we analysed the minimum necessary content of the SLA that regulates such a relation. A contractual connection can be compared to the life of a person: the signing of the agreement corresponds to his birth, the breaches of the contract and liabilities to sicknesses, the contractual and extra-contractual remedies to the medicines taken to cure the illness, the termination of the agreement to his death. The focus of this paragraph will be on the life and on the sicknesses of this imaginary person whose name is contract.

It is pivotal to point out that also the contractual relationship between a Grid/Cloud provider and an end user undoubtedly depends on the negotiating power of the parties, and this is in particular true as regards liabilities of the technology supplier. As it will be showed *infra*, big international providers, when dealing with 'normal' customers (basically individuals and small businesses) tend to exclude as much as possible their liabilities, so that the risk is entirely shifted to the customer. This means that, in practice, a person or small undertaking willing to enter into Grid/Cloud-enabled business should be aware of the fact that, unless he is able to negotiate specific and more favourable clauses with a technology provider, he will basically have no remedies in case the technology provider does not supply the services according to the promised QoS or if he does not provide them at all because, for instance, his business winds up. This topic is extremely important and has a great impact on the operations of the customer, but firstly the reader should be acquainted with the law governing the contract, i.e. how the contractual relationship is managed from the legal point of view.

3.1 The law applicable to the contract

As we said above, *SuperICTResources*, German technology supplier, provides Grid or Cloud capacity to *SaaSforyou*, small enterprise established in the Netherlands. The parties enter into an SLA which entirely regulates their contractual relationship, from QoS and security to liabilities and termination. The content of the agreement is quite wide and the negotiators, who do not have a legal background,

do not take into account a very important question: which law will govern this SLA?

We will provide the reader with an answer (focused on the applicable European legal framework) to this question, pointing out firstly that it is extremely advisable that the contract states expressly which law is applicable to it, in order to avoid potential problems linked to the interpretation of the applicable legal sources (that may be, in many circumstances, rather obscure). The contracts unilaterally drafted by big international providers always have such a clause and, if the supplier is an American company, it is highly likely that the applicable law will be one of the States of the federation. This poses practical problems for European customers that are not familiar with American law and is expected to increase the costs in case of litigation or disputes due to the need to consult a local expert.

At European level, the legal source that indicates which law will be applicable to the contract made by *SuperICTResources* and *SaaSforyou* is the abovementioned Rome Convention, which states – Art. 3(1) – the basic principle that "A contract shall be governed by the law chosen by the parties."[5] In our example the negotiators forgot to choose which law will govern the contract, and therefore Art. 4(1) is applicable, and thus "To the extent that the law applicable to the contract has not been chosen in accordance with Article 3, the contract shall be governed by the law of the country with which it is most closely connected."[6]

Two issues have to be addressed: firstly, what does it mean 'governing the contract'? Then, how is it possible to assess to which country the agreement is most closely connected? The answer to the first question can be found in Art. 10(1) of the Convention, pursuant to which "The law applicable to a contract…shall govern in particular: (a) interpretation; (b) performance; (c) within the limits of the powers conferred on the court by its procedural law, the consequence of breach, including the assessment of damages in so far as it is governed by rules of law; (d) the various ways of extinguishing obligations, and prescription and limitation of actions; (e) the consequences of nullity of the contract." This mean that, in our ex-

[5] This provision then points out that "The choice must be expressed or demonstrated with reasonable certainty by the terms of the contract or the circumstances of the case. By their choice the parties can select the law applicable to the whole or a part only of the contract." Paragraph 2 then specifies that "The parties may at any time agree to subject the contract to a law other than that which previously governed it, whether as a result of an earlier choice under this Article or of other provisions of this Convention. Any variation by the parties of the law to be applied made after the conclusion of the contract shall not prejudice its formal validity…or adversely affect the rights of third parties."

[6] Furthermore, "Nevertheless, a separable part of the contract which has a closer connection with another country may be by way of exception be governed by the law of that other country."

ample, the governing law will assess how *SuperICTResources* must deliver the services, how the agreement must be interpreted, how much damages (if any) the company has to pay to the customer for breach of contract, etc.[7]

The latter issue can be solved in light of Art. 4(2), pursuant to which "It shall be presumed that the contract is most closely connected with the country where the party who is to effect the performance which is characteristic of the contract has, at the time of conclusion of the contract, his habitual residence, or, in the case of a body corporate or unincorporated, its central administration. However, if the contract is entered into in the course of that party's trade or profession, that country shall be the country in which the principal place of business is situated or, where under the terms of the contract the performance is to be effected through a place of business other than the principal place of business, the country in which that other place of business is situated." In the above example, provided that the performance characteristic of the contract is the provision of the service, the criterion to take into account is that of the principal place of business. We imagine that *SuperICTResources* is established in Germany and the service is provided from there, therefore German law will be applicable.

The solution would not be different in case the Grid/Cloud provider has its principal place of business outside the EU. Although the Rome Convention is a source of European law (Quigley 1997), its applicability is universal, and as a consequence, pursuant to Art. 2, "Any law specified by this Convention shall be applied whether or not it is the law of a Contracting State." If *SuperICTResources* would be established, for instance, in Israel, the laws of this country would be applicable to the agreement with the Dutch company *SaaSforyou*. The same conclusion can be reached for contracts concluded after 17 December 2009, day of entry into force of the abovementioned Regulation 593/2008, provided that Art. 4(1)(b) sets forth that "a contract for the provision of services shall be governed by the law of the country where the service provider has his habitual residence."[8]

Having said that, it is advisable that the parties state in the agreement which law governs the contract and the contractual relationship between them. Which law will be applicable, i.e. the law of the country of the provider or of the customer (or hypothetically the law of a third country), is a matter of negotiation between the parties. For the technology provider it is undoubtedly more logical to insist for

---

[7] Art. 10(2) then points out that "In relation to the manner of performance and the steps to be taken in the event of defective performance regard shall be had to the law of the country in which performance takes place."

[8] For the notion of 'habitual residence' pursuant to Art. 19(1) of the Regulation, please see *supra*. It is interesting to highlight here that paragraph 3 of Art. 19 states that "For the purposes of determining the habitual residence, the relevant point in time shall be the time of the conclusion of the contract."

the adoption of 'his' law with the aim to simplify the management of his customers and of possible disputes and litigation.

The same applies as regards the individuation of the competent court or, in more general terms, of the system adopted to solve the disputes arising between the parties. These have the possibility, in fact, to decide that all future disputes between them will be solved out of court, i.e. with an alternative dispute resolution (ADR) proceeding. This means that a private referee, or a group of referees, will judge the dispute and will find a solution to it. It would go beyond the scope of this chapter to provide the reader with an in-depth analysis of ADR systems, therefore we will focus only on the jurisdictional (i.e. before a State judge) dispute resolution mechanisms. At European level the most relevant legal source is Regulation 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matter.[9] This Regulation allows assessing which court is competent to judge the disputes between the Grid/Cloud provider and the customer.

Going back to the above example, let us imagine that the negotiators of *SuperICTResources* and *SaaSforyou* forgot to include in the SLA a provision about jurisdiction, so that in case of litigation they do not know which court will be competent. The basic principle, set forth by Art. 2(1) of the Regulation, is that "Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State." The first problem to solve regards the determination of the domicile of the parties, in light of the consideration that "with contracts made over the Internet, it is difficult to determine where the party is domiciled, even though the plaintiff can identify the party and locate the transaction" (Wang 2008). Art. 60(1) gives the solution and says that "a company or other legal person or association of natural or legal persons is domiciled at the place where it has its: (a) statutory seat, or (b) central administration, or (c) principal place of business."[10] We can assume therefore that *SuperICTResources* is domiciled in Germany and *SaaSforyou* in the Netherlands.

In order to assess whether German or Dutch courts will be competent, it is necessary to refer to Art. 5(1), which sets a so-called 'special jurisdiction'. To be more precise, a person or company, domiciled in an EU Member State, may be sued in another Member State (contrary to the principle of Art. 2) "in matters re-

[9] Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [OJ L 12, 16/1/2001, p. 1-23].

[10] Art. 60(2) sets a special rule for British and Irish companies: "For the purposes of the United Kingdom and Ireland 'statutory seat' means the registered office or, where there is no such office anywhere, the place of incorporation or, where there is no such place anywhere, the place under the law of which the formation took place."

lating to a contract, in the courts for the place of performance of the obligation in question.[11]" The expression "place of performance of the obligation in question" seems rather obscure and of difficult practical implementation: point (b) of Art. 5(1) specifies with this regard that this place shall be "in the case of the provision of services, the place in a Member State where, under the contract, the services were provided or should have been provided."

The literature reasonably pointed out that this criterion is likely to encounter major difficulties when applied to e-commerce scenarios (Gillies 2001[12]; Wang 2008[13]). In our view, in case of Grid services (and the same applies to Cloud services), it is extremely difficult, if not impossible, to assess the place of provision of the services, so that the application of the relevant provision of the Regulation encounters major obstacles. The statement, proposed by the literature as regards Internet, that "businesses fear that the determination of Internet jurisdiction could be uncertain because unlike paper based contracts, online contracting is not executed in one particular place" (Wang 2008), is even truer in a Grid/Cloud scenario. The solution to this issue is left to the courts that have to implement the Regulation, if a solution that makes sense from the technological and legal point of view can be found[14].

What we said so far shows the necessity for the parties to state in their SLA or in another contract which court will be competent to judge their disputes[15] (Leible 2006). This possibility is recognised by the Regulation, and art. 23(1) in fact states that "If the parties, one or more of whom is domiciled in a Member State, have agreed that a court or the courts of a Member State are to have jurisdiction to settle any disputes which have arisen or which may arise in connection with a particular

---

[11] Art. 5(1)(a).

[12] "Whilst it is to be applauded that the European Union sought to distinguish between the place of performance of goods and services, what definition will be given for the place of performance of digital goods or services purchased on-line has yet to be tested."

[13] According to Article 5(1)(b) of the Brussels I Regulation, the place of performance should be deemed to be the place of delivery. Since it is very difficult to ascertain the place of performance with digitalized goods involving online delivery, in my opinion, the recipient's place of business should be considered as a connecting factor."

[14] It has been pointed out in the literature that "there is still a latent complexity and a necessity for citizens or small enterprises, as either claimants or defendants, to have access to intricate legal analysis if they are to be fully aware if their rights and the potential business risks and transactions costs." (Storskrubb 2008)

[15] It has been pointed out in the literature that "a well-drafted contract, which has factual links with more than one country, will contain a choice of jurisdiction or court clause. This is often referred to as an "exclusive" clause, providing that all disputes between the parties arising out of the contract must be referred to a named court or the courts of a named country." (Wang 2008).

legal relationship, that court or those courts shall have jurisdiction. Such jurisdiction shall be exclusive unless the parties have agreed otherwise." In the above example, *SuperICTResources* and *SaaSforyou* can decide that, for instance, the court of Amsterdam or that, more generally, Dutch courts[16] will be competent, and no other courts in principle could judge the disputes arising from the contract(s) between the parties.

The reader should be aware that this clause[17] shall be in writing or evidenced in writing, pursuant to Art. 23(1)(a)[18] and, with this regard, paragraph 2 of Art. 23 points out that "Any communication by electronic means which provides a durable record of the agreement shall be equivalent to 'writing'". This means that "a contract stored in a computer as a secured word document (i.e. a read-only document or document with entry password), or concluded by email and click-wrap agreement falls within the scope of Article 23(2)[19]" (Wang 2008). As regards click-wrap agreements, "it seems to be preferable that the party receives the text of the choice-of-court clause (including the other provisions of the contract) separately, for instance in a pop-up window that can be printed and saved as an html, doc or pdf file" (Leible 2006). In practice it is advisable that the Grid/Cloud provider adopts this technique in order to avoid any doubt as regards the validity of the contract.

We want to finally highlight that very often the SLA or other contract drafted unilaterally by big international technology providers state that the competent court will be an American court, for the very fact that these companies are established in the United States. These clauses are not negotiable and this means, in practice, that the customer will not enforce his rights due to the high costs of liti-

[16] In this case the national rules of civil procedure will apply to determine which judge will be *in concreto* competent.

[17] The choice-of-court can be a clause in the SLA (or other contract) or a standalone agreement. The requisite of the written form apply to both cases.

[18] Unless the following point (c) is applicable: "in international trade and commerce, in a form which accords with a usage of which the parties are or ought to have been aware and which in such trade or commerce is widely known to, and regularly observed by, parties to contracts of the type involved in the particular trade or commerce concerned." The agreement made by clicking on an 'I agree' button in a webpage seems to be the case in point, provided that it is common practice to conclude contracts in this way on the Internet.

[19] "This provision covers the agreement on a choice-of-court clause by exchanging e-mails. E-mails provide a durable record because they are saved either in the mailbox or on the hard disk and because they can be printed out on paper. An electronic signature according to the rules of the Signature Directive is not required." (Leible 2006)

gation[20], given the fact that "to decide whether to initiate a suit, a rational plaintiff compares the cost of the complaint and the expected value of the legal claim" (Cooter and Ulen 2004).

3.2 Liabilities of the Grid/Cloud provider

One of the most important issues for the customer is the liability of the Grid/Cloud provider, i.e. when he will liable and for what. The basic legal principle, if not stated otherwise in the agreement, is that the supplier will be liable if he does not deliver the promised services at all of if he does not match the expected QoS. In these cases, therefore, he shall pay damages (direct, indirect, consequential, etc according to the applicable legal framework), if any, to the customer, and the parties can state that the provider will pay a certain amount of money in case of non-compliance even if the client did not suffer any real and measurable damage.

The application of the legal principle of liability (expressed, for instance, by Art. 1218 of the Italian Civil Code, Art. 1142 of the French and Belgian Civil Code, § 280(1) of the German Civil Code), however, can be limited by the parties in their agreement, and this is (very usually, if not always) the case in point in the contracts (SLAs, Customer Agreements, etc) unilaterally drafted by big international technology providers. The customer should read very carefully the clauses on liability and above all those regarding limitation of liability, for the very fact that in practice the supplier can be in the position to decide if and to what extent it is convenient for him not to respect his contractual obligations without the risk to be sentenced to pay damages. The importance of these clauses as regards security issues will be more specifically assessed *infra*.

Before analysing the limitation of liability frequently imposed by the big technology providers, it is important to point out that, even if no contractual limitations are set forth in the agreement, the supplier will not be liable basically if (i) he did not have the possibility to respect his contractual obligations or if (ii) the customer, with his positive or negative behaviour, made the delivery of the service impossible or extremely difficult. In other words, if the Grid or Cloud provider cannot supply the service due to, for instance, a power outage, Internet failures, a natural disaster like an hurricane or a violent storm, etc – in the English-speaking countries, these facts are called 'acts of God', and often the French expression *force majeure* is widely used – (Beale et al. 2002), he will not be liable for that. From a different perspective, if, for instance, the Grid/Cloud provider expressly

20 "In America, each side usually pays his own legal costs. In Europe (and much of the rest of the world), the loser usually pays most of the winner's legal costs." (Cooter and Ulen 2004)

states that certain system or software requirements are necessary in order to receive the service, and the customer does not update his systems or does not comply with such requirements, the provider will not be liable if the service cannot be delivered.

Having said that, the legal limitations of liability are not enough to 'protect' the Grid/Cloud providers and let them maximise the profits with basically no risks of being sued and sentenced to pay damages, especially in innovative business sectors in which it is not always clear to assess whether the contractual obligations have been respected and, if not, who is liable for that. For these reasons, non-negotiated (i.e. imposed) agreements that state that the provider does not warrant (i.e. guarantees) that the service will function as described in the SLA and that it will be uninterrupted or error free are common. In other words, the technology supplier will not be responsible for any service interruptions, including, but not limited to, the so-called acts of God.

In practice this means that the customer will take all the risks and that he is required to simply trust the Grid or Cloud provider, without receiving any legal guarantee that the service will be supplied as expected and promised in the SLA. Legally speaking this is a case of obligation with no sanction, and the supplier is in the position to decide if and how to deliver the service. According to the law and economics literature, this kind of agreement is not efficient, provided that "cooperation is efficient when the promisor invests in performing at the efficient level and the promisee relies at the efficient level" (Cooter and Ulen 2004), but it is undoubtedly very convenient for the provider.

From this consideration we can infer that an SLA (or other contract) negotiated by a Grid/Cloud provider and a customer should balance the risks between the parties and should 'motivate' both of them to respect their obligations (provided that the main and basically only obligation of the customer is to pay the fees). This implies that, for instance, the agreement should prevent the Grid/Cloud provider from reducing the quality of the services delivered to the customer in order to satisfy the requests of other, more 'important', clients and, if he decides to do so, he should at least pay the damages suffered by the former customer or to compensate him in a different way.

Such a different way is usually the service credit system. It is common practice in fact that the SLA states that, in case the availability level or, in general, the QoS has not been reached during a certain period of time, e.g. on a monthly or yearly basis, the customer will be entitled to receive a 'credit' equal, for instance, to 10 % of the bill for that period. To make an example, the SLA between *SuperICTResources* and *SaaSforyou* states that the availability of the service will be 99,95 % on a monthly basis and that, if such level has not been reached, the customer will be entitled to receive a service credit of 10 %. In a certain month *SuperICTRe-*

sources is able to provide the service only for 85 % of the time, and this means that in the next month *SaaSforyou* will pay his bill with a 'discount' of 10 %.

First of all, service credits will usually not be applicable in case of act of God (e.g. the availability level could not be reached due to failures at the level of the Internet network) or in other circumstances stated in the SLA (usually, unavailability of the service that results from any actions or inactions of the customer or any third party, that derives from the client's and/or third party's equipment, software or other technology, etc). Secondly, and from a different perspective, it is important to highlight the distinction between service credits and liability for damages. The above example is useful to explain this distinction. The SLA between *SuperICTResources* and *SaaSforyou* sets forth, apart from the applicability of the service credits, that the Grid/Cloud provider will not be liable for any direct or indirect damage suffered by the customer and arising from the non compliance with the promised QoS. *SaaSforyou* needs the provision of Grid/Cloud capacity to supply services based on the SaaS paradigm to other companies that require a fast and efficient service with no failures. In some cases, like for instance the provision of Grid/Cloud-based services to hospitals, the client of the service provider absolutely needs an uninterrupted provision of the service in order to save lives and avoid to be sentenced to potentially huge compensations to the patients or their families.

We can imagine, as said above, that *SuperICTResources* delivers in a certain month the service only with an availability of 85 %, and if the fee for the service is set at € 1,000 per month, *SaaSforyou* will pay the next month only € 900. The service credit does not take into account the damages possibly suffered by the customer, like for instance the loss of clients or the damages (if any) he has to pay to his clients[21]. In the most dramatic scenario, contractual failures of the technology provider, especially if they are frequent, may have serious consequences on the customer's business and this explains the absolute necessity for the client to negotiate and balance the risks with the Grid/Cloud provider in the SLA (or other contract).

3.3 Security issues: further (potential) liability of the Grid/Cloud provider

All the abovementioned elements of a typical SLA (or other contract) in a Grid or Cloud scenario, like QoS, availability, performance, etc are undoubtedly of pi-

[21] The SLA between *SaaSforyou* and the clients, in fact, can state that the former will not be liable for any damages suffered by the customer, at least in case the failure to provide the service is due to Grid/Cloud outages.

votal importance. An unstable or unreliable Grid/Cloud provision can create severe problems to the customer and ultimately can damage his business. Nevertheless, if a customer is unsatisfied with a technology provider, he can terminate the contract and start a new relationship with another supplier. At least in principle, a client who is not happy with the supply of the Grid/Cloud service can move to another provider before it is too late, i.e. before his reputation is badly affected and his clients migrate to another service supplier. *SaaSforyou*, for example, can terminate the contract with *SuperICTResources*, which is often in breach of its obligations as regards availability and QoS, and enter into a new agreement with another provider before *SaaSforyou*'s customers decide to opt for a different SaaS supplier.

When we talk about security risks this possibility, in practice, very often does not exist. In other words, the customer who provided data or content to the Grid/Cloud supplier may suffer fatal consequences if such data are lost or damaged. An example will clarify the point. *SaaSforyou* provides simulation services for aerospace companies using the paradigm of SaaS and, specifically, it collects data from the clients in order to create tailored simulations. In order to make such simulations, which require huge compute capacity, *SaaSforyou* opted for the Grid or the Cloud, and therefore the clients' data are processed in the *SuperICTResources*'s infrastructure before being delivered back to the final customers.

One day, for technical reasons, the data processed in the Grid/Cloud network get corrupted or lost, so that *SaaSforyou* is not able to deliver the promised simulations to the clients. The damage for the company is huge, in terms of image, reputation and, ultimately, it affects the existence of the enterprise. *SaaSforyou* could not foresee this problem and therefore it just has to face and solve the consequences. The company will expect some sort of compensation from the technology provider and for these reasons the contractual clauses on security and limitations of liability are absolutely fundamental. From the technology provider's side, he is supposed to limit (or to try to limit, during the negotiations) as much as possible his liability for security failures, while the customer should try to allocate the risks to the supplier. If the SLA (or other agreement) is negotiated between the parties, the customer should avoid that clauses similar to those frequently imposed by big international providers are adopted.

These provisions state that the technology supplier will have no liability for any unauthorised access or use, corruption, deletion, destruction, loss etc of any customer's data or content, in other terms he does not guarantee that he will be successful at keeping such data and content secure. In case of Grid/Cloud-based storing capacity, the provider will impose that he does not warrant that the data stored by the customer will be secure or not otherwise lost or damaged. These clauses shift all security risks onto the customer, who should be aware of that. The practice of Grid/Cloud-capacity provision by big international market players induces

many practitioners and commentators to point out the security risks of Grid and Cloud computing (Brodkin 2008) and ultimately we could wonder whether the use of dispersed resources will prove to be a successfully business model.

What should the customer ultimately do to protect his business? It is advisable to follow a twofold strategy: firstly, the client shall require the provider to list his security measures and systems in the SLA. A well drafted and complete clause commits the technology supplier to adopt some specific standards, and whit this regard a provision like 'the provider will do his best to keep customer's data and content secure' is too vague. In case of litigation, in fact, it will be necessary to assess whether the provider really did his best to adopt security measures, therefore safe and concrete criteria shall be preferred. At the same time the list of security measures shall be flexible enough to contemplate future updates, so that the provider must be obliged to respect in any case the most recent and efficient security measures even if they are not listed in the SLA. If the parties do not draft this clause, the abovementioned general legal principle of liability applies and, *in concreto*, the provider will not be liable if he can prove that he was diligent in protecting the customer's data. Giving an evidence of this, nevertheless, may be cumbersome. The same applies to the client if he wants to prove that the supplier did not implement in his systems the best (or at least adequate) security measures. The standard of care required to the debtor, i.e. the Grid/Cloud provider, depends on the applicable national legislation, and of course it can be difficult to assess what 'care of a reasonable person' or 'reasonable care and skills' in practice mean. The relevant legal sources are, for instance, Art. 1147 of the French civil code, Art. 1176 of the Italian civil code, § 276(1) of the German civil code.

Secondly, the security obligations of the provider shall not be without sanction. It is pointless for the customer, in fact, that the supplier commits himself to keep the data and content secure if he will not be liable for not doing so. The relevant clause in the SLA (or other contract) therefore should balance the risks between the parties and specifically should state that the provider is liable for not guaranteeing the protection of the customer's data and content and he is not liable whenever security measures shall efficiently be adopted by the client himself. This means, in practice, that the customer shall be obliged to use encryption technology to protect his data and content, to routinely archive it, etc. At the same time, the provider shall not be liable for the security risks at the level of the transmission of the data, e.g. on the Internet, if such transmission (or a portion of it) is not under his control.

Similar considerations apply to the relationship between the customer (in our example, *SaaSforyou*) and his clients. The SLA (or other contract) should balance risks and liabilities between the parties and shall clearly state that the processing of the client's data is made using a Grid or Cloud infrastructure owned and ma-

naged by a third party. Keeping informed the end user is surely the best strategy, also as regards privacy issues.

3.4 Privacy

Together with security issues, privacy has to be assessed as part of the contractual relationship between the Grid/Cloud provider and the customer. First of all, according to the applicable European sources[22], privacy should be a concern of the parties only if some personal data are processed. Pursuant to Art. 2(a) of the Data Protection Directive, personal data "shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". In other words, phone numbers, addresses, e-mail addresses of clients, customers (as far as they are physical persons and not companies[23]), employees etc are deemed to be personal data and should be adequately protected. Conversely, all other sorts of data, like company's information, industrial data to be processed in a simulation, etc are not personal data.

To illustrate which privacy measures should be adopted by the parties we can imagine that *SaaSforyou* offers to his clients solutions in the field of employees' management based on the SaaS paradigm. The customers/end users send data regarding their employees to *SaaSforyou* that will process them and will deliver back the payrolls and/or calculation of contributions to pay. All these data are processed in the Grid or Cloud of *SuperICTResources*, with which *SaaSforyou* has an agreement as specified in the previous paragraphs. What do the parties have to take into account in order to avoid any breach of legal provisions?

In our case, and the same may apply in similar situations, the companies, customers of the SaaS provider are the data controllers as they determine the purposes and means of the processing of personal data; *SaaSforyou* is the data processor,

[22] Namely Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive) [OJ L 281, 23/11/1995, p. 31-50] and Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [OJ L 201, 31/7/2002, p. 37-47].

[23] The reader shall be aware that as soon as a company/person has or manages data of contact persons within a company, then data protection legislation becomes applicable.

which processes data on behalf of the controller, following the instructions contractually given by the above customers; *SuperICTResources*, subcontractor of *SaaSforyou*, is also a data processor[24]. The reader should be aware that the distinction between data processor and controller should be assessed on a case-by-case basis and it depends on the level of decision power of the parties involved. According to the concrete modalities of providing the services and to the opinions expressed by the national data protection authorities concerned, *SaaSforyou* and/or *SuperICTResources* may be deemed to be data controllers, and therefore more stringent requisites will apply (it is therefore highly advisable that the parties verify first the provisions stated in the applicable national legislation and the positions of the competent national data protection authority)[25].

From a practical perspective, then, it is pivotal to state that *SaaSforyou* and its clients shall enter into a contract regulating privacy aspects (to be notified by the client[26] to his national data protection authority), preferably annexed to the SLA, aimed to regulate some specific privacy issues related to the processing of the data provided by each client. In particular, this contract shall describe the modalities of the processing of the data provided by the customer (and with this regard the fact that a Grid/Cloud-based delivery model is adopted should be explicitly mentioned), list the security measures applied by *SaaSforyou* and the employees that have access to the data. A fundamental point is also the proxy to subcontract the processing of the data to other companies, like *SuperICTResources*. Without this proxy, which can refer to a specific technology provider or to a list of Grid/Cloud suppliers, *SaaSforyou* cannot outsource the processing of data to another party, i.e. cannot send the customers' data to *SuperICTResources* in order to deliver back the service. This is a very important aspect to highlight, especially in the field of

[24] See Art. 2(d) and (e) of the Data Protection Directive.

[25] Therefore, the controller is the person who bears the responsibility to implement the data protection principles and to comply with the obligations they set forth. It is thus important to define clearly who is considered as controller of the data processing. The concept is not always clear and should be distinguished from the processor. Both concepts have been introduced by the 95/46/EC Directive. The controller is the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data. The processor is the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller. Processors are usually sub-contractors who perform specific tasks on basis of the instructions given by the controller. They are compelled to follow the instruction provided and to ensure the security of the personal data they processed. The actual ability to decide upon the purpose and means of the processing will be the core criteria to distinguish controllers from processors. This analysis should be carried out on a case-by-case basis.

[26] Art. 4 of the Data Protection Directive states basically that the place of establishment of the data controller determines the national law applicable to the processing of the data.

SaaS, provided that the SaaS paradigm relies on the involvement of a technology provider in order to deliver services[27].

Furthermore, if the Grid/Cloud supplier is established in an EU-Member State or in another non-European country that has been acknowledged by the European Commission or the competent national data protection authority as providing an adequate level of protection, there are no particular problems, given the fact that such level of protection to the processed data is supposed to be similar. Things are different if the technology provider is located in a third country (like the United States): in this case the specific regime regulating international transfers of personal data applies and, provided that this involves additional obligations for both controllers and processors, specific contracts may need to be signed based on the model contracts published by the European Commission to that effect[28]. Those contracts are expected to be 'automatically' accepted, when notified, by the national data protection authorities of the Member States. From a different perspective, it is also advisable that *SaaSforyou* communicates to its clients if the Grid/Cloud provider changes, preferably in written form submitting to the customers a proposal of addendum to/modification of the abovementioned privacy contract (please be aware that this applies also when the Grid or Cloud provider/sub-contractor is based in the EU).

Apart from that, another privacy contract shall be signed by the customer/service provider (i.e. *SaaSforyou*) and the Grid/Cloud provider. A trilateral agreement between service provider/technology supplier/end user is also theoretically possible, although quite unrealistic. This contract, to be notified, if such notification is required by the applicable national legislation, to the data protection authority of the country of establishment of the end user (the same as for the privacy contract between end user and service provider), shall basically state the modalities applied to the data processing.

Another important aspect to analyse regards finally the location of the Grid/Cloud components, i.e. of the servers, nodes, clusters, etc that form part of the Grid or Cloud infrastructure. If such components are located in the EU, no problems are likely to arise. If this is not the case, the privacy contract between the end user and the service provider shall indicate in which countries the Grid/Cloud

---

[27] In other words: any transfer of personal data between parties involves the signing of a contract regulating privacy obligations of the parties. This includes onward transfers to third parties that should always be notified to counterparts. This point is pivotal in so far as the controller may be subject to an obligation of notification of such transfer to the national data protection authority.

[28] See http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm (retrieved 27/2/2009).

components are located and shall specify that the data will be transferred outside the EU.

4 Taxation: Grid/Cloud computing and the concept of Permanent Establishment

Taxation is one of the most relevant issues to take into account when a technology provider wants to commercialise Grid/Cloud-based solutions, as it may be a major barrier to financial success of Grid or Cloud businesses. Taxation has to be analysed from many perspectives, and in this paper we will focus on direct (i.e. income) taxation. With this regard, the main issue to assess is the relation between Grid and Cloud computing and permanent establishment.

According to the principles commonly accepted at international level, and set forth primarily by the Organisation for Economic Cooperation and Development (OECD) a business presence (e.g. a branch or a factory: technically speaking, a permanent establishment) of a company in another State justifies the taxation, by the authorities of the State, of the profits generated by that permanent establishment itself.[29] This principle is likely to affect Grid and Cloud providers if they have servers, nodes, clusters etc (i.e. Grid/Cloud components) in several countries. In other words, in case of a transnational Grid and Cloud, the portions of profit generated by its components can be taxed respectively in all the countries where these components are located. This in principle means high compliance costs for technology providers, risks of litigation with the tax authorities concerned and, ultimately, a great uncertainty when calculating the portions of profit generated by each Grid/Cloud component (Parrilli 2008).

These considerations are valid, of course, if those tax authorities believe that Grid/Cloud components are permanent establishments of the technology provider. The general principle, stated by the OECD and followed by many national fiscal administrations, is that servers (and therefore Grid/Cloud components) are permanent establishments of the technology provider if they are fixed, they carry out totally or partially the business of the company and such activities are not of preparatory or auxiliary nature.[30] It must be assessed on a case-by-case basis if these conditions are met, but in principle we can say that Grid/Cloud components are deemed to be permanent establishments of the technology provider and, as a consequence, the profits generated by them will be taxed in the country where the components are located. From a comparative perspective, many countries (i.e. the

[29] See OECD, Model Convention with Respect to Taxes on Income and on Capital [as they read on 28 January 2003].

[30] See OECD, Commentary to the Model Tax Convention on Income and on Capital.

United States, France, Italy, Spain, etc) follow this principle, with the notable exception of the United Kingdom (where servers are not considered to be permanent establishments) (Parrilli 2008).

From the practical perspective, this risk can be mitigated through a careful tax planning policy regarding the location of Grid/Cloud components. Technology providers basically have two alternatives: (i) centralise the Grid or the Cloud in one country, so that no issues related to multiple taxation of the same profits and/or right assessment of profits among the components arise; or (ii) locate the Grid/Cloud components in countries where servers are not deemed to be permanent establishments of the technology provider.

The above described tax planning may also be linked to the tax-effective location of the headquarter of the Grid/Cloud provider. If and when the Grid/Cloud components can be remotely managed, in fact, the technology supplier can decide to be established (i.e. to locate the central place of management of the company) in a low-tax country while the Grid or the Grid components operate in countries that are attractive from the tax point of view and that have good network connections (the same applies to Cloud computing).

5 Conclusions

The main message coming out from the previous pages is that legal issues should not be perceived as barriers to invest in Grid and Cloud computing and to start up a successful business. The law, in a very broad sense, does not prevent Grid/Cloud computing from showing all its potential and proving to be innovative technologies able to create new business opportunities, reduce the costs and maximise the profits of the users. It is nevertheless true that in some circumstances the legal sources are not fully able to encompass all existing scenarios, including Grid/Cloud-based business. In the previous lines, for instance, we saw that the criterion of the provision of the service, set forth by Art. 5(1)(b) of Regulation 44/2001, cannot operate in a Grid or Cloud environment. The use of dispersed resources and the possibility to enjoy and use the services supplied by the technology provider everywhere in the world, e.g. through a web portal, makes many legal principles and criteria simply not applicable. In a typical Grid and Cloud scenario, in particular, the volatility of the traditional concept of space is evident. The laws are by definition slow, definitely slower than technology, but this is a natural consequence of the (more or less) democratic process that should guide their creation: discussions take time.

Maybe the future will be a world without laws, or, on the contrary, a world with a huge quantity of laws regulating every aspect of citizens' and businesses'

life (and probably this will be the case: if the industrial production is declining at global level, the lawmakers produce more and more laws). In any case, technology providers and their customers should use as much as possible their contractual freedom to set their own contractual 'laws'. This advice applies also to the existing reality, characterised by many laws that are not able to encompass all business scenarios, and ultimately the reader should not rely too much and exclusively on the law. It would go beyond the scope of this chapter to assess whether the positive legal system is complete or not. Personally, we believe that the system is incomplete and open, and the parties may fill its gaps according to their needs. The abovementioned lacuna contained in the Regulation 44/2001 could be easily filled with a contractual clause stating which court will be competent. A few minutes' discussions during the negotiation phase can prevent much longer arguments and uncertainties in case of litigation.

Therefore, whenever it is possible, Grid/Cloud providers and their customers should engage in negotiations aimed to produce a contract which is as much as possible complete. They have to think about all major aspects of their future relationship and see how this can be made easy to manage. This means avoiding gaps and doubts in every possible case. If the law that ultimately governs and gives effects to the agreement is incomplete, the contract should be complete. Complete and fair, in the sense that liabilities and risks should be balanced between the parties and not completely shifted upon the customer or the end user.

Nevertheless, potential customers planning to enter into the market of Grid/Cloud-based services should be aware of the fact that SLAs and other contracts imposed by big international technology providers are not fair, at least according to the common sense of justice. Buying Grid or Cloud capacity from one of the big players may be cheaper and efficient, but it is risky. The customer is required to trust the supplier, but his contractual protection is basically very limited and it often consists in service credits. We do not want to say that the services they provide are not good or that they are likely not to respect what they promise in the SLA. We just want to highlight that possibilities of failures always exist and that the price of such failures will be (basically entirely) paid by the customer.

Negotiations carried out between the parties and tailored SLAs (or other contracts) should balance these failure risks and make at the end more attractive Grid and Cloud computing for the customers and, at the same time, should urge providers to invest in technology in order to be able to supply excellent services and respect all security standards and requirements. The success of Grid (and in general of technologies based on dispersed resources, like Cloud computing) depends also on the contractual practices that the actors in the market will create and impose. Fair agreements will undoubtedly render Grid and Cloud computing very interesting for both providers and customers.

References

Beale S et al (2002) Contract Law: IUS Commune Casebooks for the Common Law of Europe. Hart Publishing, Oxford

Brodkin J (2008) Gartner: Seven cloud-computing security risks. http://www.infoworld.com/article/08/07/02/Gartner_Seven_cloudcomputing_security_risks_1.html. Accessed: 25 February 2009

Cooter R, Ulen T (2004) Law and Economics. Pearson Addison Wesley, Boston

Gillies L (2001) A Review of the New Jurisdiction Rules for Electronic Consumer Contracts Within the European Union. J. Inf. Law. Tech. (1). http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/gillies. Accessed 25 February 2009

Leff A, Rayfield J, Dias DM (2003) Service-Level Agreements and Commercial Grids. IEEE Internet Computing: 44-50

Leible (2006) Negotiation and Conclusion of the Contract: Formal and Substantive Validity, Choice-of-Court and Choice-of-Law Clauses – An Introduction. In: Schulz A (ed) Legal Aspects of an E-commerce Transaction: International Conference in The Hague, 26 and 27 October 2004, Sellier, Munich

Padgett J, Djemame K, Dew, P (2005) Grid Service Level Agreements Combining Resource Reservation and Predictive Run-time Adaptation. http://www.allhands.org.uk/2005/ proceedings/papers/526.pdf. Accessed 25 February 2009

Parrilli DM (2008) The Server as Permanent Establishment in International Grids. In: Altmann J (ed) Grid Economics and Business Models. Springer, Heidelberg

Parrilli DM, Stanoevska K, Thanos G (2008) Software as a Service (SaaS) Through a Grid Network: Business and Legal Implications and Challenges. In: Cunningham P (ed) Collaboration and the Knowledge Economy: Issues, Applications, Case Studies. IOS Press, Amsterdam

Quigley C (1997) European Community Contract Law: The Effect of EC Legislation on Contractual Rights, Obligations and Remedies. Kluwer Law International, Alphen a/d Rijn

Storskrubb E (2008) Civil Procedure and EU Law: A Policy Area Uncovered. Oxford University Press, Oxford

Wang FF (2008) Obstacles and Solutions to Internet Jurisdiction. A Comparative Analysis of the EU and US Laws. J. Int'l Comm. Law Tech 3(4):233-241