Italy adopts its first “rules” on Cloud Service Providers: what are the possible next steps (including at EU level)?

Kluwer Copyright Blog
September 15, 2018

Gianluca Campus (University of Milan)

Please refer to this post as: Gianluca Campus, ‘Italy adopts its first “rules” on Cloud Service Providers: what are the possible next steps (including at EU level)?’, Kluwer Copyright Blog, September 15 2018, http://copyrightblog.kluweriplaw.com/2018/09/15/italy-adopts-first-rules-cloud-service-providers-possible-next-steps-including-eu-level/

---

1. Introduction and legal context

Italy has recently adopted its first “rules” dedicated to Cloud Service Providers (“CSP”) for Public Administrations. Last April the AgID (Agenzia per l’Italia Digitale) issued two Circulars (AgID Circulars n. 2 and n. 3 of 9th April 2018) published in the Italian Official Gazette dated 20th April 2018 and effective 30 days from publishing (the “AgID Rules”). As discussed in more detail below, it is clear that the key aspects are, on the one hand, data protection and recovery and, on the other hand, data interoperability and portability. Both aspects have implications for intellectual property rights, and, more specifically, copyright law. With regards to data protection and recovery of data, CSP should make available to the PA information on the location of their servers, so as to allow the PA to evaluate any possible impact of local rules on the data (including intellectual property rules). With regards to interoperability and portability, the CSP has to guarantee that the software provided is compatible with other software systems adopted by the PA and that the Application Programming Interface (API) for allowing interoperability is available to the PA (this means that, among other things, there should not be any limitations in the copyright regime applicable to the software provided by the CSP that could limit the interoperability and portability).

The AgID Rules have been introduced according to the Three-Year Plan (2017-2018-2019) for Informatics in the Public Administration approved by the Decree of the Presidency of the Council of Ministers of 31st May 2017.

The AgID Rules are part of the national plan for implementing the European Digital Agenda – and have the main purpose of setting the requisites for the qualification of: *(i)* the IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) CSPs (see Circular n. 2) and *(ii)* the SaaS (Software as a Service) CSPs (see Circular n. 3), all available via Cloud to the Public Administration, as well the procedure for qualification. Cloud Service Providers that intend to offer their services to the Italian Public Administration must meet the requirements of the AgID Rules.

The AgID Rules should contribute to the strategic goals of: (1) improvement of quality, security, resilience, energy efficiency and business continuity of public services; (2) establishing a Cloud environment for the Public Administration, by using both public and private dedicated resources; and (3) economic efficiency driven by consolidation of the resources for data centres by migrating them in Cloud.

It is worth noting that legal requirements are also part of the process for the qualification of the CSP as a supplier of the Italian Public Administration (see paragraph 2). Even with this commendable attempt to shed some light in the area of Cloud services, there are nevertheless many legal aspects that are not taken into account by the AgID Rules, mainly in the area of copyright and intellectual property rights more generally (see paragraph 3). Also, the status of the legislative process of the European Union confirms that there is a need to progress with the aim of establishing a European open public environment via Cloud.

2. The AgID Rules: definitions and requirements for legal compliance

AgID Rules introduce a legal definition of Cloud as “*a set of remote technical resources utilized as virtual resources for memorization and elaboration in the context of a service*”. According to this definition, the main features of the Cloud are that: *(a)* it entails a set of technical resources that are remotely available (this means essentially via online connection); *(b)* the resources are considered as virtual resources (this means only for their overall processing capacity and not as the sum of single hardware and software); *(c)* the resources are used for offering specific services (this means that there is a clear distinction between the services offered and the equipment used for providing such services). There are some differences between this definition and other definitions available at international level.

According to the NIST, the US National Institute of Standards and Technologies, “*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.*”

According to the EU Communication on the European Cloud Initiative dated 19th April 2016 – COM (2016) 178, “*the Cloud can be understood as the combination of three interdependent elements: the data infrastructures which store and manage data; the high-bandwidth networks which transport data; and the ever more powerful computers which can be used to process the data.*”

The NIST definition is more oriented to describe functional aspects of Cloud and the advantages in terms of accessibility and modularity of Cloud services, while the EU Commission definition focuses on structural and network aspects of Cloud. The AgID definition sounds pretty generic and does not mention some peculiar features of Cloud, such as the share of resources, the access on demand, the minimal management effort, the connection with high-bandwidth networks; the absence of such features entails that a wider variety of services can be considered Cloud services under the AgID Rules, even if they do not necessarily have some peculiar features of Cloud services.

The AgID Rules includes anyway – outside the definitions – a reference to NIST essential features of Cloud computing, but the correct relation of these definitions with NIST rules in the system of the sources of law is still to be clarified.

The requirements for being eligible to provide Cloud services to PA are categorized as “organizational” and “specific”. Only CSPs which meet these requirements can be included in the Marketplace Cloud, a digital platform with a catalogue of Cloud services available for the Public Administration (PA entities are also eligible and can offer Cloud services to another PA). Starting from 20th November 2018, Italian Public Administration can access Cloud services only through CSPs included in the Marketplace Cloud.

The specific requirements for legal compliance are RLC (Requisites of Legal Conformity) or RPP (Requisites for Privacy and Protection of data). Among these legal requirements there is the obligation for the CSP to make available to the PA the location of its servers, so as to inform the PA on whether there are special rules applicable at local level that could apply to data stored in the data centres used for the Cloud services. Special attention is dedicated where the data centres are located outside the EU, in which case special agreement or rules applicable to the data (e.g. US-EU Privacy Shield) should be declared by the CSP. In any case the compliance with the EU framework for the protection of personal data has to be guaranteed. All the aforementioned requirements must be satisfied via the CSP’s self-declaration.

Particularly relevant for legal compliance are the specific requirements named RIP (Requirements on Interoperability and Portability). The CSP must issue the API so as to also allow the Cloud services to be interconnected with other informatic systems used by the PA or by other PAs. The CSP must also offer the possibility for the PA to extract in any moment all relevant data and metadata of the PA uploaded to the Cloud, thus including the Derived Data, which originates from the interaction of the PA systems with the Cloud (number and type of interactions, requested configurations and customizations). In addition, if the PA intends to terminate the supply of the Cloud service, the CSP must allow the PA to recover all the data memorized in the Cloud, with all the Derived Data and the back-up copies, but only after a migration period is guaranteed.

3. The other legal issues related to Cloud Service Providers

From the analysis of the legal requirements explicitly mentioned in the AgID Rules, it is clear that the main points of attention are, on the one hand, the data protection and recovery and, on the other hand, the data interoperability and portability. Both aspects underline some implications on intellectual property rights, and in more detail, on copyright laws.

It is still to be clarified to what extent digital copies of copyrighted works which are resident in the Cloud can circulate without impacting the right of reproduction and the right of distribution. This means that PAs as users of Cloud services should be allowed to transfer digital copies sold by the CSP even if they are resident in the Cloud (but the same principle should apply to digital copies sold by the PA to users via Cloud). The CJEU has argued that the interpretation of art. 4.2 Software Directive in the light of the principle of equal treatment confirms that the exhaustion of the right of distribution is effective following the first sale of a copy of a program in the Union by the copyright holder or with his consent, regardless of whether the sale is a tangible or intangible copy of the program (CJEU, 3rd July 2012, C-128/11, UsedSoft GmbH vs. Oracle International). Such approach could have limited application in the context of SaaS (Software as a Service), where the software is not sold but used for supply of services, but could have wider application where other digital contents are impacted.

Users of PA services should also be able to make copies for private purposes of documentation and contents available via Cloud (e.g. access to digital contents of public archives or libraries) and API of services provided by the PA should be available for developing services destined to interoperate with PA systems.

With regards to the private copies, we can imagine a service dedicated to retrieval and storage of digital copies of documents and contents of the PA on a user’s request. The CJEU has recently interpreted Directive 2001/29/EC (Infosoc Directive), with particular reference to article 5, paragraph 2, letter b), stating that the Infosoc Directive precludes national legislation that allows a company to provide a remote recording service to users via Cloud without consent of the rightsholder and based on the private copying exception (CJEU, 29th November 2017, C-265/16, VCast Ltd / RTI); but it seems that the main reason for excluding such a service was the active role of the CSP in making unauthorized copies of copyrighted materials.

With regards to the API, we can imagine the case of private users that intend to develop *apps* based on processing of information produced by the PA and needing automated access to such information (e.g. alert systems or data analytics); in all such cases the PA should make available API in a coherent copyright fashion (open source software seems the most appropriate).

Finally, it is still to be investigated whether the processing of data uploaded in the Cloud for purposes of data analytics can amount to results that should be protected themselves as trade secrets or through new rights to be specifically attributed to the CSP (for a critical review see Hugenholtz P.B.). It also remains to be clarified whether the algorithms used for processing data can be protected under copyright laws in a way that should prevent access to the source code (see Campus G. on recent Italian case law).

4. Cloud Services and EU Agenda

In its Communication dated 19th April 2016 on the European Cloud Initiative, the EU Commission has pointed out two pillars. The first pillar is the development of an adequate European infrastructure (European Data Infrastructure), consisting of networks for ultra-fast connectivity and adequate HPC (High Performance Computing) resources. The second pillar is the provision of European research for a high-quality Cloud system that focuses on the principle of data sharing (European Open Science Cloud – EOSC). If, for the European Data Infrastructure, the issues to be addressed are typical of the infrastructure policy, including the use of European funds and the modalities of private public cooperation, the second pillar deserves a brief analysis – as the process to realize the EOSC it is central to the problem of the relationship between new services and protection of rights. The main objective of the EU Commission through the EOSC is to overcome the current fragmentation of databases and the inadequate integer capacity, and facilitate the sharing and reuse of information.

The perspective is a platform for Public Administrations to provide services and data in an open format (*Government-as-a-service*). Subsequently, access could also be granted to companies, including SMEs, through structured cooperation with the private sector. It should be noted that the Public Administration, investing in the quality of the EOSC, can indirectly contribute to increasing the trust of the users in the use of the Cloud services. The EOSC provides the opportunity to promote best practices in terms of security and access to information (through anonymization, the isolation of personal data in non-shared spaces and so on).

In the context of the Digital Single Market Strategy there are also some other provisions that are relevant for Cloud service providers. Reference is made in particular to: *(a)* the General Data Protection Regulation, already adopted and in force from 25th May 2018; *(b)* the proposed regulation on a framework applicable to the free movement of non-personal data in the European Union (Free Flow of Data Policy); *(c)* the EU Cybersecurity Strategy; and *(d)* the proposed Directive on copyright in the Digital Single Market. As part of this last text, some rules on the liability of providers of Internet services will be included.

It is clear from this brief review that even if there is some consideration at EU level of the legal issues related to Cloud and CSP, there are still some delays in the implementation of the European Cloud Initiatives and there is an urgent need for a comprehensive approach to a wide range of issues in the field of intellectual property rights and in the interconnection of IPR with antitrust and privacy issues.