EJLT European Journal of Law and Technology

Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution

Alessandro Mantelero [1]

Cite as: Mantelero, A, 'Cloud computing, trans-border data flows and the European Directive 95/46/EC: applicable law and task distribution', European Journal for Law and Technology, Vol. 3, No. 2, 2012

1. Italian case law

In order to define the fundamental issues concerning trans-border data flows and their consequences on applicable law, we consider three different cases decided by the Italian Data Protection Authority (*Garante per laprotezione dei dati personali*). In the first case a website located in the U.S. disseminated personal information and offensive opinions regarding some researchers criticized for their experiments conducted on animals. Leaving aside the aspects relating to freedom of expression, the Italian authority considered the case from the perspective of data protection and deemed that the violations were committed through websites not subject to Italian data protection law as they were located in countries outside the European Union. [2]

The second lawsuit concerned a company (Google Inc.) based, like in the first case, outside E.U., but in this case the equipment used was situated in Italy. Under Article 4 of the Directive 95/45/EC the national provisions concerning data protection are applied by each Member State when the controller:

> '…is not established on Community territory and, for the purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community'. *[3]*

In line with this, the Italian DPA considered that the processing of personal data made by Google Inc. was subject to the Italian data protection law, adopted pursuant to the above mentioned Directive, because 'done using tools located in the State'. [4] The DPA drew this conclusion analysing the way in which the images were acquired in Italy by Google's cars and sent automatically to the company's server in the U.S. [5]

Finally we consider a typical case of outsourcing services involving trans-border data flows: Heinz Italia S.p.a. asked the Italian DPA for a preliminary evaluation concerning its new tool called 'Heinz 360 Feedback' which aims to introduce 'a new model of business skills' based on feedback provided 'by all stakeholders' who come into contact with the employees. This feedback was to be sent to an outsourcee, located in the United States of America, compliant with Safe Harbor and qualified as a processor. [6] The Italian DPA decided that this transfer of personal data was compliant with Italian law, adopted following the EU Directive, since the data processing was related to an employment contract and the consent of data subject had been required. [7] [8]

These three cases describe the different situations in which personal data can be processed outside EU borders, with different consequences in term of applications of the European Directive. In the following paragraphs, after some general considerations about the European framework on data protection, this paper will examine the effect of the Directive on task distribution and regulation of data flows between a service provider and business or consumer clients, focusing the attention on the interaction based on the emerging technology of cloud computing. [9] Cloud architectures pose several challenges with regard to data management. Firstly, it is difficult to determine who has the effective control over the data and assumes the

related liability, in a model where ITC companies provide cloud services to their clients, but at the same time define the levels and the features of the services and have a relevant control over the software and hardware resources. Secondly, the trans-national nature of cloud computing structures amplifies the issue concerning the applicable law, due to the continuous fast flow of data between the different data centers located in various parts of the globe.

2. The European framework on data protection

The *Directive 95/46/EC* defines the European common framework on data protection through a general and comprehensive regulation regarding every sector (private or public) and purpose (commercial or non-commercial). The Directive was inspired not only by the intention of removing the obstacles to flows of personal data in order to facilitate economic activities, but also by the aim of offering a high level of protection of individual rights. This particular approach differs from those adopted in other countries where, as in the case of the U.S., there are different regulations which consider only some specific aspects of data protection and there is no general and comprehensive regulation. Furthermore, in some legislation, data protection rules are more oriented towards an economic and business perspective rather than inspired by the purpose of protecting personal rights.

In this context the European model, defined by the *Directive 95/46/EC*, (hereafter 'the Directive) is particularly attractive, as is demonstrated by the laws adopted in other countries following the European pattern. This result is due to the influence of European legal culture, but perhaps it is more closely related to the specific content of art. 25 of the Directive, which allows trans-border data flows from the EU to other countries only when the 'third country in question ensures an adequate level of protection'. [10] The indirect effect of this rule is to induce the countries interested in having commercial relations with the EU to adopt similar data protection laws. In the absence of these laws, local companies are not be able to work with European partners, because they cannot receive personal data concerning consumers, suppliers and partners. Faced by the choice between adopting European standards on data protection or losing commercial relations requiring trans-border data flow, the United States has also come to terms with the European Commission. [11]

The fundamental principles of European regulations are: data quality and lawfulness of data processing (Articles 6 and 7 of the Directive), right of access to data (Article 12 of the Directive), consent given by the data subject (Article 7 of the Directive) based on information about data processing (Article 10 of the Directive), confidentiality and security of processing (Articles 16 and 17 of the Directive). Regarding the different aspects of the internal organization of data processing activities, the European Union has adopted a specific model in order to also guarantee the correct identification of the person responsible for data protection and the proper identification of the subjects whose role is to enforce the rights ascribed to the data subject. This model must be preserved even when a company uses third party services and especially when these are provided using infrastructures outside the European Union, in countries with a low level of data protection, or none at all, assured by legislation.

In order to determine whether European regulation is applicable or not to cloud providers offering their services in EU, we should consider four different elements: the nature of the activity of the user, the kind of data processed the task distribution in processing the information and the place where data is processed. Among these factors the first and the last are the most significant in determining whether the Directive is applicable. The Article 3 (2) states that the Directive 'shall not apply to the processing of personal data […] by a natural person in the course of a purely personal or household activity'; therefore in such cases data protection under EU law is not relevant. [12] The only aspects not included in this exception concern the traffic data generated using the service and the information the cloud provider asks the user for different purposes (e.g. to define a personal profile for marketing); in these cases the data is under the control of the provider and used in accordance with purposes related to its business.

In these last two situations the place where data is processed will be decisive, as national laws implementing the Directive are applied where the processing is carried out in the context of an establishment of the subject who manages the process within the territory of the Member State or when equipment situated there is used (Article 4 of the Directive).[13] [14] This element is also decisive when the user utilizes the services in the cloud for business or professional purposes, not only with reference to traffic data or to the information requested by the cloud provider, but also in relation to the aspects concerning data flows generated by the outsourcing processes realized through cloud computing. [15] Because in this case a company manages its

data using cloud computing for business proposes Article 3 (2) exception does not apply and the European data protection law is applied in accordance with the criteria defined by Article 4, discussed above.

In the following paragraphs we will see that in these cases task distribution frequently gives control of data processing to the data exporter. An exception could occur in the case of the creation of a joint-venture between cloud client and cloud provider, with joint control on data processing.

3.1 Task distribution and regulation of trans-border data flows: the business-to-business model

The legal qualification of the subjects involved in trans-border data flow is fundamental in order to apply the principles from the Directive and to define the responsibilities and the obligations of the parties. In general terms, legislation on data protection has a data-centric structure, whereby the role assumed by the authors of the processing activity is determined on the basis of the relationship with the information, rather than by virtue of the nature of the inter-subjective relationship. The organization of data processing focuses on three major figures: 'controller', 'processor' and 'persons who, under the direct authority of the controller or the processor, are authorized to process the data'. This model is not necessarily consistent with the organization chart of the companies, nor does it reflect the degree of autonomy of the parties involved in the process. The power of decision making about data processing is the measure used to distinguish the roles (see Article 29 Data Protection Working Party, Opinion 1/2010), not the nature of the contractual and economic relationship which links the different actors, nor again the status of outsourcee or the outsourcer. This distinction between the roles taken by each party is relevant not only with regard to the organization of data processing, but also from the perspective of related liability.

In the specific context of cloud computing, considering the relationship that usually exists between the cloud provider and the user, the first usually has the role of the processor and the second is the controller. Various elements confirm this. First of all, even if the cloud provider maintains a degree of autonomy and decision-making, tasks and specifications are clearly and strictly defined by the user through the contract (though often only formally, by virtue of the use of standard clauses). Secondly, only the user is directly empowered by the data subject to process the data and the cloud provider receives the information to be processed in the interest of the user. Finally, the typical arrangements of cloud computing services, as happens in the outsourcing agreements, give broad significance to service performances and service level agreement (SLA), binding the parties in a such way that it is not possible to consider them as two autonomous controllers. [16] For these reasons we must conclude that the cloud client takes on the role of controller and the cloud provider takes the role of processor. [17]Confirmation also comes from the fact that the services offered by cloud providers are only part of the processing which users carry out. In addition, cloud providers do not have the specific or exclusive competences necessary to play a dominant role in managing the data, which entails a high degree of autonomy. Usually cloud providers simply offer a higher standard in the provision of services previously carried out by the company. [18]

With specific regard to trans-border data flows, the EU has a great interest in the regulation of cross-border data flows in order to maintain the entire system of guarantees defined by the data protection Directive, as we have seen above. In the absence of adequate data protection legislation (Articles 25 and 26 of the Directive), the parties can provide the safeguards requested by European law by means of appropriate contractual clauses (Articles 26, §§ 2 and 4, of the Directive), also adopting the standard clauses approved by the European Commission.[19] [20] However some difficulties arise when the cloud provider (processor), established in the EU, employs third parties established in third countries as sub-processors. There are no specific standard clauses for this purpose, and the parties can only adopt one of the following solutions: a direct contract between the EEA-based controller (cloud service user) and the non-EEA-based sub-processors; a mandate from the EEA-based controller (cloud service user) to the EEA-based processor in order to use *Model Clauses 2010/87/EU* in the name of the controller and on its behalf; an ad-hoc contract. [21]

3.2 Task distribution and regulation of trans-border data flows: the business-to-consumer model

In § 3.1 we considered trans-border data flows assuming that they concern information collected and processed by a controller established in the EU, but it is also possible that personal information is collected

in the EU by controllers based outside European Union borders. This happens especially with regard to cloud services for consumers (i.e. web based e-mail services, social networks, etc.) because of they are in many cases provided by U.S. companies. In these situations the provision of Article 4 of the Directive, considered above, is fundamental in order to distinguish the case in which the controller, although not established on Community territory, uses equipment situated on the territory of a Member State 'for purposes of processing personal data' and the different situation in which it does not use any of the equipment or use it only for purposes of transit.

From this perspective the notion of 'equipment' assumes a remarkable importance and it seems to have been the means used by European authorities in order to extend their power to regulate and control outside the EU. The European Article 29 Data Protection Working Party has clearly affirmed, in different documents, that 'equipment' could simply be cookies sent to the users by the service provider. Even if this interpretation can be criticized, because of its pan-European vision, it seems to be endorsed by the EU Justice Commissioner who identified in the 'protection regardless of data location' one of the four pillars of the future framework of European privacy rights. [22] From this perspective she declared that 'there should be no exceptions for third countries' service providers controlling our citizens' data. [23] Any company operating in the EU market or any online product that is targeted at EU consumers must comply with EU rules' and she also affirmed that homogeneous privacy standards for European citizens should apply independently of the area of the world in which their data is being processed, they should apply 'whatever the geographical location of the service provider and whatever technical means used to provide the service'. [24]

Considering that a cloud computing service uses technical devices which are more complex than a cookie, both the present (extensive) interpretation of article 4 of the Directive 95/46 /EC and the guidelines for its future review draw the conclusion that cloud providers can be considered subject to EU law on data protection. However from one side this conclusion seems to be inconsistent considering the present wording of the directive and from another point of view the future changes of the directive in order to ensure a wider protection of information regarding European citizens will probably not be very easy to enforce. To avoid twisting the wording of the directive, it would be more accurate to give a narrower interpretation of the term 'equipment', implying a case-by-case analysis in order to verify the effective existence of 'equipment' used by the cloud provider. [25] In this context the position adopted by the Italian data protection authority assumes importance because it is more restricted.

---

[1] Alessandro Mantelero is Assistant Professor of Private Law at the Fourth School of Engineering - Economics and Management of the Politecnico di Torino. He is member of the Department of Management and Production Engineering and Faculty Fellow at the Nexa Center for Internet and Society.

[2] See decision issued by the Italian DPA on 24 May 2006, doc. web n. 1299063; see also the following decisions: 18 gennaio 2006, doc. web n. 1242501; 3 novembre 2009, doc. web n. 1687662; 13 maggio 2010, doc. web n. 1735420. These decisions are available on Internet at http://www.garanteprivacy.it.

[3] The controller is the person or body which determines the purposes and means of the processing of personal data, see Directive 95/46/EC, Article 2 (d).

[4] See Italian Personal Data Protection Code 2003, Article 5.

[5] See decision issued by the Italian DPA on 15 October 2010, doc. web n. 1759972, available at http://www.garanteprivacy.it.

[6] See *Directive 95/46/CE*, Article 2 (e).

[7] See decision issued by the Italian DPA on 4 November 2010, doc. web n. 1771838, available at http://www.garanteprivacy.it.

[8] See *Directive 95/46/CE*, Article 26 (1) (a) and (b), which provides that Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition tat "the data subject has given his consent unambiguously to the proposed transfer" or "the transfer is necessary for the performance of a contract between the data subject and the controller". See also *Italian Personal Data Protection Code 2003*, Article 43 (1) (a) and (b).

[9] See NIST, The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology, September 2011, available at http://csrc.nist.gov.

[10] Article 25 *Directive 95/46/EC*, The Article 25 (2) states that the adequacy of the level of protection afforded by a third country "shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country. See also *Directive 95/46/CE*, Article 26 (2).

[11] See Safe Harbor Privacy Principles and annexed Frequently Asked Questions approved by European Commission with decision 2000/520/CE, 26 july 2000, available at http://eur-lex.europa.eu.

[12] Article 3 (2), Directive 95/46/EC

[13] See ECJ judgment of 4 July 1985, Bergholz, (Case 168/84, ECR [1985] p. 2251, paragraph 14) and judgment of 7 May 1998, Lease Plan Luxembourg / Belgische Staat (C-390/96, ECR [1998] p. I-2553). See also Article 29 Data Protection Working Party, Opinion 8/2010, p. 12 et sqq., available at http://ec.europa.eu.

[14] If there are several establishments the application of national legislation will be distributed depending on the activities of each establishment; see Article 4 (1) (a) dir. 95/46/CE.

[15] Although cloud computing and outsourcing agreements have the same purpose of transferring processes which an organization previously performed internally to an independent organization, there are significant differences between them. In both cases the provision of specific services represents the core of the business model and of the related agreement, but cloud computer services are standardized, offered by a few big players and involve mainly software and hardware resources rather than human resources. All these aspects have a significant influence on the nature of the agreements. Cloud agreements are defined by providers by using standard models, with an extremely limited possibility of negotiating the terms. At the same time the standardization permits to cloud client to switch from a cloud provider to another and the digital nature of the information reduces the inconvenience of changing the provider. Finally the existence of few big cloud providers gives them a considerable power in unilaterally determining terms, conditions and policies.

[16] See Hustinx, P (2010), European Data Protection Supervisor, Data protection and Cloud Computing under EU law, Third European Cyber Security Awareness Day, European Parliament, 13 April 2010, available athttp://www.edps.europa.eu.

[17] See Article 29 Data Protection Working Party, Opinion 05/2012 on Cloud Computing, available at http://ec.europa.eu.

[18] See Article 29 Data Protection Working Party, Opinion 1/2010, available at http://ec.europa.eu.

[19] See above § 2.

[20] See the contractual clauses for the transfer of personal data to processors established in third countries defined in European Commission decision C(2010)593 of 5 February 2010, available at http://eur-lex.europa.eu.

[21] See Article 29 Data Protection Working Party, FAQs in order to address entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive, available at http://ec.europa.eu.

[22] See Reding, V (2011), Your data, your rights: Safeguarding your privacy in a connected world, SPEECH/11/183, Brussels, 16 March 2011

[23] See Reding, V (2011), Your data, your rights: Safeguarding your privacy in a connected world, SPEECH/11/183, Brussels, 16 March 2011

[24] See Reding, V (2011), Your data, your rights: Safeguarding your privacy in a connected world, SPEECH/11/183, Brussels, 16 March 2011.

[25] A more easy and uniform evaluation will characterize the services based on geolocation through mobile device; see Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, p. 12, available at http://ec.europa.eu: "It is important to underline that the specific device is

instrumental in calculating its location [...] Such a device also fulfills the criterion of article 4.1(c) of the data protection directive, equipment situated on the territory of a Member State".