

## ABSTRACT

### *Il cloud computing*

Nella contemporanea realtà sociale, ove attraverso le tecnologie informatiche si svolge l'attività sociale ed è diffusa l'essenza delle persone, merita particolare attenzione il fenomeno del *cloud computing*, che consiste, secondo la definizione del *National Institute for Standards and Thecnology* (NIST), in un insieme di servizi, accessibili *on demand* e in *modalità self-service* tramite *internet*, basati su risorse condivise e utilizzabili dinamicamente e efficacemente a fronte di limitate attività di gestione; una nuova forma di archiviazione, memorizzazione, elaborazione di dati in una piattaforma virtuale. Nel primo capitolo, si definisce il fenomeno *de quo*, se ne descrivono i modelli e le tipologie, evidenziandone i benefici e i rischi, oltre che i problemi giuridici ad esso legati. In particolare, riscontrato come i dati e il loro trattamento rappresentino l'oggetto dei servizi offerti dal sistema *cloud*, si rileva come di particolare importanza siano proprio quegli aspetti legati alla protezione dei dati personali degli utenti dei servizi *cloud*, chiarendo come sia necessaria, quanto preliminare, una politica di prevenzione, volta ad informare sui rischi. Aspetti questi messi in risalto dal Garante per la protezione dei dati personali che, a più riprese, è intervenuto al fine di favorire un utilizzo consapevole e corretto del sistema *cloud*. Nel secondo capitolo, s'indaga il diritto alla riservatezza nell'attuale contesto dell'evoluzione tecnologica. Ripercorrendone la sua evoluzione, si chiarisce come il diritto in parola (che ha visto ampliarsi il proprio contenuto venendo a compendiarsi anche del diritto alla protezione dei dati personali) sulla scorta di quanto affermato dalla Corte di Giustizia dell'Unione europea, non è prerogativa assoluta, ma va considerato alla luce della sua funzione sociale. Si passano in rassegna alcune fondamentali pronunce della giurisprudenza europea (sentenze: *Lindqvist*, *Costeja*, *Scherms*) in tema di tutela della riservatezza in *internet*, evidenziandone i punti di contatto e di distanza con quella italiana, con un riferimento anche ad una recente sentenza del *Tribunal Supremo* spagnolo. Si constata, seppur nella diversità delle soluzioni offerte, come il conflitto tra i diversi interessi in gioco possa risolversi solo in ragione di un attento bilanciamento dei medesimi. Nel prosieguo, si analizza il Regolamento europeo 2016/679 (che sarà direttamente applicabile, in tutti gli Stati dell'Unione europea, a partire dal 25 maggio 2018), rilevandosi come esso rappresenti lo strumento atto a formalizzare il nuovo corso digitale della tutela dei dati personali, a livello comunitario e extracomunitario.

In particolare, si analizzano le novità da esso introdotte e gli architravi su cui esso poggia tutto il sistema *privacy*. Si tenta, inoltre, di specificarne l'ambito di applicazione territoriale, alla luce dei criteri enunciati nel suo articolo 3. Nel terzo capitolo, focalizzando l'attenzione sull'aspetto piú significativo della tecnologia in disamina (ossia la netta separazione tra titolarità dei dati e dei trattamenti e possesso e controllo degli stessi), la ricerca analizza il tema del «trattamento» dei dati personali alla luce dei Pareri dell'Autorità garante italiana ed europea (Gruppo Art. 29) e, in particolare, del recente Regolamento europeo 2016/679 e del *Code of Conduct*, 26 September 2016 del CISPE. Tematica che inevitabilmente interferisce con la tecnologia *cloud*, soprattutto oggi in un contesto in cui la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo consentendo, tanto alle imprese private quanto alle autorità pubbliche, di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Ciò anche in considerazione del fatto che i servizi *cloud* consentono di «trattare» e «conservare» i dati su sistemi di *server* dislocati nelle diverse parti del pianeta, ove occorrerà verificare la sussistenza di un «livello di protezione adeguato», al fine di assicurare all'interessato una protezione «sostanzialmente equivalente» a quella garantita all'interno dell'Unione. All'uopo, sulla imprescindibile premessa per la quale è gioco forza necessario informare sui rischi, la ricerca si propone di chiarire, alla luce delle previsioni del Regolamento *privacy* 2016 e del *Code of Conduct*, 26 September 2016 del CISPE, questioni quali: la ripartizione di ruoli e obblighi tra cliente-titolare (*rectius*, secondo la terminologia inglese, *controller*) e *provider* fornitore-responsabile (*rectius*, secondo la terminologia inglese, *processor*); le omissioni informative del gestore del servizio e inconsapevolezza dell'utente; la conservazione dei dati in *cloud computing* e il trasferimento degli stessi verso un «Paese terzo» dopo le sentenze della Corte di Giustizia; la questione della portabilità dei propri dati su altro Csp (problema del c.d. «*vendor lock-in*»); la *data breach notification* e gli obblighi di protezione dei dati nella relazione cliente-fornitore.

## ABSTRACT

### *Cloud computing*

According to the definition of National Institute of Standards and Technology (NIST) dell'U.S. Department of Commerce, *cloud computing* consists of 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 service) that can be rapidly provisioned and released with minimal management effort or service provider interaction; a new form of storage and data processing on a virtual platform. The first chapter defines the phenomenon, describing the models and typologies, highlighting the benefits and the risks, as well as the legal problems associated with it. In particular, as the data and their processing are the object of the services offered by the cloud system, it is of particular importance that those aspects of the protection of the personal data of cloud service users are clarified as necessary, preliminary, a policy of prevention, aimed at informing about the risks. These issues are highlighted by the Guarantor for the Protection of Personal Data, which, more than once, has intervened in order to encourage a conscious and correct use of the cloud system. In the second chapter, the right to privacy is investigated in the current context of technological evolution. Some fundamental judgments of European jurisprudence are reviewed (judgments: *Lindqvist*, *Costeja*, *Scherms*) on the protection of privacy in the internet, highlighting the points of contact and distance to the Italian one, with reference also to a recent judgment of the Spanish High Tribunal. It is noted, however, that in the diversity of solutions offered, conflict between the various interests at stake can only be solved by reason of their careful balancing. Looking back on its evolution, it is clear that the right in question (which has expanded its content by including the right to the protection of personal data), in the light of what the European Court of Justice has stated, is not absolute prerogative, but must be considered in the light of its social function. The following is a review of European Regulation 2016/679 (which will be directly applicable in all EU countries from 25 May 2018), as it represents the instrument for formalizing the new digital course for the protection of Personal data, at Community and non-EU level. In particular, they analyze the novelties it introduces and the archives on which it relies on the entire privacy system. It is also intended to specify the spatial scope of application, in the light of the criteria set out in Article 3 thereof. In the third chapter, focusing on the most significant aspect of the technology under discussion (the clear separation between data ownership and processing and possession and control of data), the research analyzes the topic of 'processing' personal data in the light of the opinions of the Italian and European Regulatory Authority (Art. 29 Group) and, in particular, of the recent European Regulation 2016/679 and of the Code of Conduct, 26 September 2016 of the CISPE. The topic that inevitably interferes with cloud technology, especially today, in a

context where the scope for sharing and personal data collection has increased significantly, allowing both private companies and public authorities to use personal data, such as in the pursuit of their activities. This also in view of the fact that cloud services allow to ‘process’ and ‘store’ data on server systems deployed in different parts of the planet, where it is necessary to verify the existence of an ‘adequate level of protection’ in order to ensure to the party concerned a ‘substantially equivalent’ protection to that guaranteed within the Union. To this end, the essential premise for which it is necessary to inform about the risks is to clarify, in the light of the provisions of the Privacy Policy 2016 and of the Code of Conduct, 26 September 2016 of CISPE, issues such as: roles and obligations between controller and processor; the informational omissions of the service provider and the user’s unknowingness; keeping data in cloud computing and transferring them to a ‘third country’ after the judgments of the Court of Justice; the question of the portability of their data on other Csp (problem of the c.d. ‘*vendor lock-in*’); the data breach notification and the data protection in the relationship between consumer and provider.