Consiglio Nazionale delle Ricerche

ITALIAN PAPERS ON FEDERALISM

Rivista giuridica on-line – ISSiRFA – CNR

MARIA NOVELLA CAMPAGNOLI

Buone e/o cattive ragioni del cloud. Considerazioni alla luce del General Data Protection Regulation (GDPR) *

SOMMARIO: 1. Brevi cenni introduttivi 2. Definizioni, caratteristiche, forme 3. Profili negoziali 4. Il Regolamento (UE) 2016/679. Quali le novità per la nuvola? 5. Un primo bilancio e qualche buona notizia.

1. Brevi cenni introduttivi.

Sempre più diffuso e utilizzato[1] il cloud computing (la c.d. nuvola informatica) è, già da alcuni anni, oggetto di dibattito e di attenzione da parte di giuristi e informatici. La ragione è presto detta: nell'ambito di quella che è stata definita come la quarta rivoluzione tecnologica[2], nella quale i dati[3] rappresentano la risorsa più importante (non solo a livello cognitivo ma anche e soprattutto economico[4]), il cloud – per sua natura direttamente chiamato in causa nei

* Articolo sottoposto a referaggio.

1 Non a caso, stando agli studi dell'"Osservatorio Cloud Transformation" della School of Management del Politecnico di Milano, il mercato del cloud in Italia, nel 2018, ha raggiunto i 2,34 miliardi di euro, con una crescita del 19% rispetto al 2017.

2 D'obbligo il rimando a L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano 2017.

3 "[...] Ogni giorno viene generato un numero sufficiente di dati da riempire tutte le biblioteche americane più di otto volte. [...] sono numeri che continueranno a crescere rapidamente e ininterrottamente nel prossimo futuro". Siamo, dunque, alle prese con un vero e proprio "[...] tsunami di dati che sta sommergendo il nostro ambiente" (*Ivi,* p. 13). In tal senso, anche Beyung-Chul Han: "ogni click che faccio viene registrato; ogni passo che compio diventa ricostruibile. Ovunque dietro di noi lasciamo tracce digitali" (*Nello sciame. Visioni del digitale*, trad, it., Roma 2015). In merito al controllo dei dati si veda anche G. Ziccardi, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era della tecnologia*, Milano 2015, in part. p. 143 e ss.

4 A proposito della crescente importanza economica dei dati, meritano d'esser qui ricordate le osservazioni di Mayer-SchÖnberger e Cukier: "dalle scienze all'assistenza sanitaria, dal settore bancario a Internet, i vari settori nel loro insieme raccontano una storia più o meno identica: la quantità di dati disponibili nel mondo sta crescendo rapidamente, e supera non solo la capacità delle nostre macchine ma anche la nostra immaginazione". "Ognuno di noi è investito da un 'diluvio digitale'", un flusso di dati che "possono diventare una fonte di potere economico". Si tratta di vere e proprie "nuove forme di valore" che modificano "i mercati, le organizzazioni, le relazioni fra cittadini e governi, e altro ancora" (*Big data. Una rivoluzione che sta trasformando il nostro modo di vivere e già minaccia la nostra libertà*, Milano 2013, pp. 18, 20, 22 e p. 16). Sul punto anche D. Talia *La società globale e i big data. Algoritmi e persone nel mondo digitale*, Soveria Mannelli 2018.

processi di archiviazione, gestione e trattamento delle informazioni – non può non acquisire un ruolo di primo piano.

Incarnazione e metafora di quella *de-territorializzazione* e di quella *de-centralizzazione* che, da sempre, individuano e connotano il Cyberspace[5], il cloud computing, come un novello Giano bifronte, mostra una certa ambiguità. Per un verso, rappresenta uno straordinario supporto ed un'irrinunciabile fonte di risorse, a cui – più o meno volontariamente e più o meno consapevolmente – ricorriamo di continuo, sia durante lo svolgimento delle attività lavorative che nel corso di quelle relazionali, ludiche o persino sportive (dall'invio delle mail ai servizi di messaggistica e alle chat; dalla condivisione di foto e filmati audio-video al salvataggio di file; dall'accesso alle piattaforme social all'uso di particolari e sempre nuove app[6]). Per un altro verso, però, il cloud è ammantato da un'alea di indeterminatezza e di incertezza. Non a caso, anche a causa di una scarsa o erronea conoscenza[7], la nuvola è tuttora oggetto di diffidenza e qualche volta anche di timori. Timori che, nella maggioranza dei casi, sono legati alle possibili ricadute sulla privacy e, in particolar modo, al rischio di perdere il controllo dei dati[8]. Dati, informazioni e profili, che – come si è già accennato all'inizio – rappresentano un valore e una ricchezza e che, proprio per questa ragione, vengono definiti come il petrolio del neocapitalismo digitale[9].

[5] Il Cyberspace, infatti, è contraddistinto dalla de-territorializzazione, in luogo della territorializzazione, e dalla de-centralizzazione, in luogo della centralizzazione. Ciò è da attribuirsi al fatto che "[...] la realtà virtuale che il cyberspace propone riduce drasticamente l'importanza dell'elemento geografico". Per questo motivo, ogni differenza si rarefà, diventa sfumata, fluida e, via via, i luoghi "reali" vengono soppiantati da i c.d. non-luoghi virtuali. Ovviamente, il Cyberspace è anche de-centralizzato. La Rete, difatti, non conosce centro, periferia e nemmeno gerarchie, in essa tutto è al contempo centro e periferia, tutto è qui e ora (A.C. Amato Mangiameli, *Informatica giuridica. Appunti e materiali ad uso di lezioni,* Torino 2015, pp. 72 e 74).

[6] L'elenco delle applicazioni di cui ci avvaliamo quotidianamente è in costante evoluzione e, per questa ragione, potenzialmente infinito. Tra le più note app, tuttavia, possono qui ricordarsi: *Google Eart* (che consente la visualizzazione della maggior parte dei luoghi a partire dalla digitazione di un indirizzo); *Waze* (app di condivisione delle informazioni sul traffico in tempo reale); *IOS Salute* (che consente il controllo degli indicatori del nostro stato di salute); *Runtastic* (che permette di scaricare piani e programmi di allenamento); *Period Calendar* (pensato per monitorare ciclo e periodi di fertilità); *Anti-Theft-Alarm* (che funziona da antifurto/allarme); *Emergency Light, Panic Button Red, BeSafe* e *Google Contatti fidati* (che hanno funzioni di allarme e difesa).

[7] È interessante ricordare che, già nel 2011, l'"Osservatorio Internet" condotto da Nextplora per conto di Microsoft aveva sottolineato che l'88% di chi navigava nel web utilizzava più o meno consapevolmente il cloud.

[8] Consentendo l'accesso alle risorse distribuite e virtualizzate, il cloud "espone [l'utente-cliente] a particolari rischi e a diverse criticità. Tra questi, è da segnalare la pirateria informatica". Invero, "l'utilizzo simultaneo delle risorse [...] permette con più facilità ai criminali di monitorare attentamente l'entrata e l'uscita delle informazioni e di estrarre dati sensibili". Ragion per cui, sia nel caso di privati, che di imprese, che di pubbliche amministrazioni, "la sicurezza costituisce un ostacolo all'adozione della nuvola informatica" (A.C. Amato Mangiameli, *Reato e reati informatici. Tra teoria generale del diritto e informatica giuridica*, in A.C. Amato Mangiameli, G. Saraceni, *I reati informatici. Elementi di teoria generale e principali figure criminose*, Torino 2018, p. 27). In margine, per un'analisi dei rischi e delle perplessità legate all'adozione della nuvola, cfr. anche M.N. Campagnoli, *Il cloud computing: vantaggi e problematicità*, in *Rivista di Filosofia del Diritto*, V, 1/2016, pp. 109-126.

[9] Così D. Talia, *La società globale e i big data*, cit., pag. 48.

2. Definizioni, caratteristiche, forme.

Fornire una definizione univoca della nuvola non è cosa agevole. Svariate le caratteristiche, tante le implicazioni, moltissimi i risvolti che di volta in volta la contraddistinguono. In prima battuta, è importante sottolineare che il cloud non rappresenta, in senso proprio, una nuova tecnologia ma, più che altro, individua un nuovo paradigma tecnologico[10]. Invero, si tratta di una risorsa sussidiaria e propedeutica ad agevolare e a semplificare l'accesso e la fruizione di alcune ICT già esistenti. In modo particolare, anche grazie alla sua notevole versatilità di impiego – che lo rende utilizzabile da privati, imprese e pubbliche amministrazioni – il cloud contribuisce a rendere più agile, economico, scalabile e flessibile[11], l'utilizzo delle diverse risorse hardware e software disponibili online.

Di qui, come è ovvio, l'evidente ed indissolubile nesso che lega la nuvola alla Rete[12]. Basta infatti accedere ad Internet – da qualunque luogo e con un qualsiasi device – per poter godere della straordinaria capacità di storage, di analisi, di elaborazione e di condivisione che contraddistingue il cloud[13]. Ma non è tutto, perché la connessione alla Rete, oltre a rappresentare la chiave di accesso alle tante potenzialità offerte dalla nuvola, ne costituisce anche la *conditio sine qua non*. Altrimenti detto ed in breve, senza il Web il cloud non solo non sarebbe possibile, ma non sarebbe neppure pensabile.

Chiarito il *fil rouge* che lega il cloud ad Internet, è necessario passare a considerare quali sono le sue principali caratteristiche e le differenti tipologie di nuvola che, di volta in volta, possono aversi. Anzitutto, va detto che non esiste un solo cloud ma che se ne possono dare vari a seconda della struttura e/o dei servizi erogati[14].

Con riguardo alla collocazione spaziale e alla differente gestione, si possono distinguere:

- il *cloud privato*, che risponde alle esigenze di una specifica impresa ed è collocato all'interno della stessa, secondo la più tradizionale e consueta forma del *local hosting*. Va

[10] In modo particolare, il cloud rappresenta un "'nuovo' sviluppo di una tecnologia già disponibile [...]". Vale a dire, "un modo nuovo di organizzare e rendere fruibili le tecnologie esistenti, integrandone le componenti e presentando all'utente solo le loro funzioni di uso" (E. Acquati, S. Macellari, A. Osnaghi (a cura di), *Pubblica amministrazione che si trasforma: cloud computing, federalismo, interoperabilità*, Firenze 2012, pp. 32-33).

[11] La flessibilità – intesa quale possibilità di usufruire, di volta in volta, della tipologia e dell'esatto quantitativo di risorse tecnologiche di cui si ha necessità – costituisce senza dubbio uno dei maggiori "punti di forza" della nuvola (vd. ASTRID, *L'impatto del cloud computing sull'economia italiana*, con prefazione di F. Bassanini e E. Belloni, Roma 2011, p. 11).

[12] In merito al rapporto fra il cloud e la Rete, bisogna, però, sottolineare che – nonostante la relazione che i lega – il cloud è qualcosa di ulteriore e di diverso rispetto ad Internet. La nuvola non coincide col Web, non rappresenta né un "generico spazio di navigazione", né soltanto un luogo di condivisione di contenuti. Essa è, piuttosto, uno "spazio virtuale" che consente, a chi se ne serve, di utilizzare le risorse tecnologiche – solo ed esclusivamente – per il tempo necessario a soddisfare esigenze e bisogni, senza sostenere investimenti onerosi e senza sopportare costi fissi (G. Reese, *Cloud computing. Architettura, infrastrutture, applicazioni*, trad. it., Milano 2010, p. 2).

[13] Ad esempio, grazie al cloud, il titolare ha sempre accesso ai suoi dati e alle sue informazioni, a prescindere da dove si trovi in quel momento; inoltre, egli può visualizzare un documento o scaricare un file senza essere obbligato a ricorrere ad un pc o ad un altro dispositivo fisico.

[14] Riprendo, qui, la tradizionale e nota distinzione proposta anche dal Garante per la protezione dei dati personali, *Cloud computing. Proteggere i dati per non cadere dalle nuvole*, 2012, pp. 9-10.

da sé che, proprio perché si tratta di una nuvola "ad uso esclusivo"[15], essa non suscita problemi in ordine alla sicurezza o alla gestione delle informazioni;

- il *cloud pubblico*, per mezzo del quale un fornitore-provider mette a disposizione di una pluralità di utenti (privati, aziende o pubbliche amministrazioni) i propri sistemi di elaborazione e di archiviazione dei dati, condividendo con loro hardware e software. Rapportata alla nuvola privata, quella pubblica presenta una maggiore economicità e superiori livelli di performance, ma, al contempo, induce nell'utente anche una più elevata percezione dei rischi, aspetto che, molto spesso, ne frena la diffusione;
- i c.d. *cloud ibridi*, che presentano elementi tipici sia della nuvola privata che di quella pubblica e che si connotano per la loro infrastruttura mista, e le *community cloud*, nuvole comunitarie che vengono condivise da un gruppo di organizzazioni[16].

Abbandonando gli aspetti prettamente strutturali-organizzativi e considerando la tipologia dei servizi offerti, emergono ulteriori distinzioni[17]:

- il *cloud infrastructure as a service* (*IaaS*), che, dietro pagamento di un canone commisurato all'utilizzo, fornisce hardware virtuali che possono essere impiegati a supporto o in sostituzione delle infrastrutture di proprietà dell'utente-cliente[18]. Emblematici i CPU, le RAM, gli spazi di storage, le schede di rete e i *server* virtuali;
- il *cloud software as a service* (*SaaS*), per mezzo del quale vengono erogate applicazioni di uso comune e servizi che non richiedono particolari prerequisiti tecnici. È il caso, ad esempio, delle webmail oppure dei social network;
- il *cloud platform as a service* (*PaaS*), che fornisce piattaforme software e soluzioni di sviluppo pensate appositamente per rispondere alle necessità di un determinato utente-cliente[19]. Basti pensare agli applicativi utilizzati in ambito finanziario, a quelli adoperati

[15] Il principale vantaggio del cloud privato è costituito proprio dal fatto che i servizi sono erogati forniti da elaboratori collocati in un ambiente di proprietà dell'utente, che, per questo motivo, conserva il pieno controllo delle macchine deputate alla conservazione e all'elaborazione dei dati (cfr. Agenzia per l'Italia digitale, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica amministrazione*, 2012, pp. 8 e 9).

[16] Sulle community cloud cfr., fra gli altri, F. Bassanini, E. Belloni, *L'impatto del cloud computing sull'economia italiana*, Roma 2011, p. 12.

[17] Ripropongo qui la classificazione del "National Institute for Standards and Technology" (NIST).

[18] "Il modello di servizio *Infrastructure as a Service* prevede che il servizio offerto consista in una infrastruttura con capacità computazionale, di memorizzazione, e di rete, sulla quale l'utente possa installare ed eseguire il software a lui necessario, dal sistema operativo alle applicazioni. Nel caso di servizio computazionale, l'utente può richiedere al fornitore di servizi un insieme di macchine virtuali, sulle quali può installare (o richiedere che venga installato direttamente dal fornitore stesso) i sistemi operativi ed i software necessari a risolvere il suo problema. L'utente può richiedere che le macchine virtuali siano connesse tra di loro da una rete virtuale. Le macchine virtuali sono raggiungibili per la loro gestione ed utilizzo tramite l'interfaccia offerta dal fornitore del servizio. Una volta che le macchine virtuali sono state assegnate all'utente, egli può richiederne delle nuove o rilasciarne alcune, in base alle sue esigenze. Nel caso di servizio di memorizzazione, invece, l'utente può richiedere uno spazio di memorizzazione per caricarvi i suoi dati e, successivamente, può aumentarlo o ridurlo a seconda delle sue esigenze" (Agenzia per l'Italia digitale, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica amministrazione*, 2012, p. 7).

[19] "Il modello di servizio *Platform as a Service* prevede che il fornitore del servizio metta a disposizione dell'utente una interfaccia di programmazione (API) con la quale l'utente può scrivere applicazioni che interagiscono con il servizio. Le specifiche funzionalità offerte dalla API dipendono dal servizio offerto, e la loro esecuzione viene assicurata dal fornitore del servizio. Il fornitore può mettere a disposizione dell'utente anche un ambiente di

per la gestione della contabilità, oppure a quelli che trovano impiego nel settore della logistica.

- il *cloud desktop as a service* (*DaaS*), grazie al quale è possibile accedere a dati e/o applicazioni con la modalità *pay-per-use* e *on-demand*;
- il *cloud disaster recovery as a service* (*DraaS*), una particolare tipologia di nuvola in grado di fornire soluzioni di disaster recovery efficaci e all'avanguardia che, proprio in virtù del costo particolarmente contenuto, possono essere adottate anche da imprese di piccole e medie dimensioni;
- il *cloud backup as a service* (*BaaS*), con il quale vengono messi a disposizione dell'utente sistemi di salvataggio dei dati notevolmente più aggiornati e sicuri di quelli normalmente disponibili in *local hosting*;
- il *cloud storage as a service* (*StaaS*), grazie al quale è possibile il salvataggio, la condivisione e la sincronizzazione dei dati su più device. Si pensi a *ICloud*, a *Dropbox*, a *Google Drive* e a *One Drive*;
- il *cloud security as a service* (*SECaaS*), che mette a disposizione degli utenti firewall virtuali contro i possibili attacchi informatici;
- il *cloud network as a service* (*NaaS*), in grado di migliorare e ottimizzare la connettività.

Al di là delle evidenti differenze e delle moltissime specificità, ciò che accomuna tutti i cloud è l'economicità, ovvero la capacità di ridurre sensibilmente le spese di utilizzo e di gestione delle infrastrutture tecnologiche, grazie all'approvvigionamento in outsoursing. E proprio l'economicità – unita alla scalabilità e alla flessibilità – concorre a far sì che la nuvola rappresenti una soluzione tecnologica, non solo estremamente efficiente[20], ma anche particolarmente duttile ed appetibile[21]. Una soluzione che, favorendo la diffusione di nuovi servizi e di nuove applicazioni, ha già modificato buona parte del nostro stesso modo di vivere[22].

---

sviluppo (e di *testing*) per le applicazioni che sfruttano le sue API. Un esempio di servizio cloud di tipo PaaS è costituito da Windows Azure Compute, che permette di utilizzare il framework .NET per sviluppare applicazioni. Poiché utilizza IIS7, è anche possibile gestire applicazioni sviluppate utilizzando ASP.NET, Windows Communication Foundation (WCF) o altre tecnologie Web. Inoltre, supporta anche linguaggi quali PHP e Java" (*ivi*, pp. 7 e 8).

[20] È sufficiente pensare al passaggio dalla *capacity on demand* alla *capability on demand*, alla scalabilità delle soluzioni, come pure alla possibilità di favorire l'attività delle amministrazioni pubbliche. (A proposito del passaggio dal diritto di proprietà al c.d. diritto d'accesso cfr. J. Rifkin, *L'era dell'accesso. L'evoluzione della new economy*, trad. it., Milano 2000, p. 5 ss. Invece, circa i possibili vantaggi del cloud per la pubblica amministrazione, soprattutto con riferimento all'interoperabilità e alla cooperazione applicativa, si vedano E. Acquati, S. Macellari, A. Osnaghi (a cura di), *Pubblica amministrazione che si trasforma: cloud computing, federalismo, interoperabilità*, cit., p. 135 ss.).

[21] Non a caso, già nel 2012, la Commissione Europea aveva indirizzato al Parlamento Europeo, al Consiglio, al Comitato Economico e Sociale Europeo, e al Comitato delle Regioni, la Comunicazione *Sfruttare il potenziale del cloud computing in Europa* (COM(2012)529), con la quale esortava gli Stati Membri ad aderire alla tecnologia *cloud*, così da superare i divari e favorire lo sviluppo di un mercato unico digitale (cfr. Agenzia per l'Italia Digitale, *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione*, cit., p.7).

[22] Sulle ricadute delle ICT sulla nostra esistenza e, in modo particolare, sulla dimensione giuridica, cfr. A.C. Amato Mangiameli, *Tecno-regolazione e diritto. Brevi note su limiti e differenza*, in *Diritto dell'informazione e*

3. Profili negoziali.

Passando all'analisi degli aspetti negoziali, ci si rende immediatamente conto che con il cloud computing siamo di fronte ad un contratto del tutto particolare[23]. In primo luogo, perché esso presenta elementi propri dell'appalto, della licenza e dell'outsourcing[24]; in secondo luogo, perché – a causa dell'intrinseca *a-geograficità*[25] e *geo-ambiguità*[26] che connota la nuvola – il contratto di cloud solleva tutta una serie di perplessità e di criticità. Si pensi alla difficoltà nell'individuare la normativa applicabile e il foro competente, come pure, al bisogno di garantire adeguati livelli di sicurezza a quello sciame di dati[27] che, per mezzo della nuvola, viene immesso in data center delocalizzati. Criticità che, soprattutto a seguito della nota pronuncia della Corte Europea del 6 ottobre del 2015[28], hanno iniziato ad essere oggetto di attenzione e di revisione[29] da parte del legislatore europeo.

---

dell'informatica, XXXII, 2/2017, pp. 147-167; e Id., *Tecno-diritto e tecno-regolazione. Appunti su uso e abuso*, in *Rivista di Filosofia del Diritto*, VI, Numero speciale, 2017, pp. 87-111.

[23] In verità, circa la qualificazione del contratto di cloud computing, la dottrina appare divisa: per alcuni, si tratterebbe di un contratto *atipico* o *innominato*, per altri, invece, sarebbe un contratto di tipo *misto*. (Con specifico riferimento ai contratti atipici o innominati, fra i tanti, cfr.: G. De Nova, *Il tipo contrattuale*, Padova 1974; M. Costanza, *Il contratto atipico*, Milano 1981; F. Messineo, *Contratto innominato*, in *Enc. dir.*, X, pag. 95; C. Bianca, *Il contratto*, Milano 1997, pp. 449-450 e 450-452. Sui contratti misti, invece: G. De Gennaro, *I contratti misti*, Padova 1934; A. Cataudella, *La donazione mista*, Milano 1970; G. Sicchiero, *Il contratto a causa mista*, Padova 1995).

[24] Sul confronto fra il contratto di cloud e l'outsourcing, si vedano: A.R. Popoli, *Il contratto di cloud computing: natura giuridica e clausole limitative di responsabilità*, in *Giustizia Civile*, 11/2015, p. 4 ss.; G. Fioriglio, *Contratto di cloud computing*, in *#Diritto dell'informatica.it*, settembre 2014; A. Mantelero, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali e aziendali*, in *Il diritto dell'informazione e dell'informatica*, 26, 4-5/2010, pag. 673; Id., *Il contratto per l'erogazione alle imprese di servizi di cloud computing*, in *Contratto e impresa*, 4-5/2012, p. 1216 ss.; F. Tosi, *Il contratto di outsourcing di sistema informatico*, Milano 2001; M. Pittalis, *Outsourcing*, in *Contratto e impresa*, 16, 2/2000, p. 1010 ss.

[25] Cfr. M.M. Winkler, J. Mosca, *Cloud computing e protezione dei dati personali*, in M. Fumagalli Meraviglia (a cura di), *Diritto alla riservatezza e progresso tecnologico. Coesistenza pacifica e scontro di civiltà?*, Napoli 2015, pp. 130 ss.

[26] Vd. F.F. Wang, *Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction*, in *Eur. Bus. Law Rev.*, 2013, in part. p. 595. Sulle difficoltà legate alla de-localizzazione tipica della nuvola anche W.K. Hon, *Data Localization Laws and Policy*, Northampton 2017.

[27] Faccio mia la suggestiva ed efficace espressione B.-C. Han, *Nello sciame*, cit.

[28] Ossia della pronuncia relativa alla causa *C-362/14 Schrems/Data Protection Commissioner*, che ha visto contrapposti il cittadino austriaco Maximillian Schrems e l'Autorità irlandese per la protezione dei dati immessi su Facebook. Si tratta di una pronuncia che potremmo definire "storica" anche perché ad essa è seguito l'annullamento dell'accordo *Safe Harbor*.

[29] Fra i più importanti interventi dell'Unione Europea in tema di tutela dei dati, meritano d'esser qui ricordati: la *Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato i dati a carattere personale* del 28.01.1981 e il relativo *Protocollo addizionale*; la *Raccomandazione del Comitato dei Ministri del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale nel contesto della attività di profilazione*, del 23.11.2010; il Parere del Garante europeo della protezione dei dati dal titolo *Meeting the challenges of big data; a call for transparency, user control, data protection by design and accountability*, del 19.11.2015; il Parere del Garante europeo dal titolo *Opinion on coherent enforcement of fundamental rights in the age of big data*, del 23.09.2016; la *Dichiarazione del Gruppo di Lavoro "Articolo 29" sull'impatto dello sviluppo dei big data sulla protezione delle persone rispetto al trattamento automatizzato dei loro dati personali nell'Unione Europea*, del 16.09.2014; la *Relazione del Parlamento Europeo, Commissione per le libertaÌÂÂÂ civili, la giustizia e gli affari interni sulle implicazioni dei big data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto* (2016/2225(INI)); le

Quanto ai soggetti coinvolti, va detto subito che, di solito, il contratto di cloud computing prevede almeno due figure: quella del *cloud provider*[30] – cioè del fornitore che gestisce le infrastrutture e che assicura l'esecuzione dei programmi e delle applicazioni – e quella del *cloud consumer* – ovvero del cliente-utente finale (che, come s'è accennato, può essere un privato, un'impresa, un ente o una pubblica amministrazione).

A questi possono affiancarsi altri soggetti, come, ad esempio:

- il *cloud carrier*, il c.d. cliente amministratore, ovvero colui che funge da intermediario fra il fornitore del servizio e l'utente finale;
- il *cloud auditor*, a cui è affidato il controllo del rispetto degli standard di servizio e di sicurezza;
- il *cloud broker*[31], una figura di congiunzione fra quella del provider e dei consumer, che si occupa dell'integrazione dei servizi.

Una peculiarità non trascurabile è data dal fatto che, di norma, il documento contenente il testo dell'accordo (*Term of Service*)[32] è accompagnato da allegati tecnici che stabiliscono i livelli di qualità dei servizi (i c.d. *Service Level Agreement*)[33] e la privacy policy (l'*Acceptable Use Policy*)[34].

Un altro aspetto di grande rilievo è rappresentato dal fatto che si tratta di un contratto standard. Vale a dire, di un negozio nel quale l'utente si limita ad aderire, senza che vi siano margini di trattazione, modifica o deroga rispetto alle condizioni e alle clausole generali previste. Come è intuitivo, tale aspetto – associato al diverso grado di conoscenza e di competenza tecnologica che differenzia il fornitore rispetto all'utente – concorre a determinare un'asimmetria contrattuale ed una sorta di sbilanciamento a favore del provider[35], che di solito stabilisce *ex ante*, ed in maniera del tutto unilaterale, termini e

---

linee guida internazionali sui big data e sulla tutela dei dati personali *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, *Consultative committee of the convention for the protection of individuals with regard to automatic processing of personal data*, del 23.01.2017; il *General Data Protection Regulation* (GDPR) 2016/679; la *Risoluzione del Parlamento europeo sull'adeguatezza della protezione offerta dallo scudo UE-USA per la privacy*, del 05.07.2018.

[30] È importante sottolineare che si danno diversi "livelli" di cloud provider. Al c.d. primary cloud provider che eroga i servizi direttamente all'utente finale, si aggiunge anche il c.d. intermediary cloud provider che eroga servizi provenienti da altri provider.

[31] Si noti che, diversamente dal cloud intermediary, il cloud broker offre un'unica interfaccia che raccoglie i servizi offerti da più cloud providers. Inoltre, mentre il cloud intermediary ingloba nel suo servizio finale tutti i servizi provenienti dal primary cloud provider, il cloud broker rende nota la provenienza di tali servizi da altri cloud providers.

[32] Vd. S. Branshaw, C. Millard, I. Walden, *Standard contracts for cloud services*, in C. Millard (a cura di), *Cloud Computing Law*, Oxford 2014, pp. 44-46.

[33] Cfr. G. Rizzo, *La responsabilità contrattuale nella gestione dei dati nel cloud computing*, in *Diritto Mercato Tecnologia* (DMT), 08.04.3013.

[34] S. Branshaw, C. Millard, I. Walden, *Standard contracts for cloud services*, cit., p. 44.

[35] Cfr., fra gli altri, E. Bellisario, *Cloud computing*, Assago 2011, p. 13 ss. Sul ruolo dei contratti nella regolazione dei rapporti fra i vari livelli della *governance* della Rete, si vedano L. Bygrave, *Contract versus statute in Internet governance*, in I. Brown (a cura di), *Research Handbook on Governance of the Internet*, Oxford 2012, pp. 168-197 e U.

modalità del servizio[36]. Si aggiunga, poi, che alle questioni di carattere generale, riguardanti la durata del contratto, il corrispettivo previsto, la legge applicabile e la giurisdizione competente, si accompagnano pure quelle di natura informativa. Vale a dire, quelle che attengono espressamente alla gestione e alla sicurezza dei dati e che, solitamente, ricadono nei c.d. *Non Disclosure Agreement* (NDA)[37].

Di qui – e non potrebbe essere altrimenti – la necessità di interrogarsi sulla reale possibilità da parte dei buyer (siano essi privati, imprese e/o pubbliche amministrazioni) di imporre al fornitore regole di ingaggio che garantiscano un'adeguata tutela dei dati personali e che prevedano delle responsabilità del provider in caso di violazioni.

Va da sé che i nodi più problematici della nuvola siano quelli connessi alle nozioni di *privacy*[38], di *sicurezza* e di *responsabilità* e sono legati alla paura che il trasferimento e la concentrazione dei dati possa determinare una perdita di controllo sugli stessi[39]. Timori che – come si vedrà – possono però essere facilmente superati se si considera che, pur ricadendo nella disponibilità del fornitore-provider, i dati e le informazioni inserite nella nuvola restano pur sempre di proprietà esclusiva dell'utente che, infatti, in qualsiasi momento, può disporne il trasferimento e la migrazione[40].

Da un lato, la *privacy*, la *sicurezza* e la *responsabilità* sono le tre parole chiave attorno alle quali orbitano tutti i dibattiti sul cloud e sulle quali si incentrano, sia coloro che guardano alla nuvola con preoccupazione[41], sia coloro che la considerano un imprescindibile ed

---

Pagallo, *The Realignment of the Sources of the Law and their Meaning in an Information Society*, in *Philosophy & Technology*, I, 28, 2015, pp. 57-73.

[36] Vd. A.R. Popoli, *Il contratto di cloud computing: natura giuridica e clausole limitative di responsabilità*, in *Giustizia civile*, 11/2015, p. 10.

[37] Autentici accordi di riservatezza con i quali le parti individuano le informazioni che intendono mantenere confidenziali e che – come tali – si impegnano a non svelare (né rendere accessibili) a terzi.

[38] Per un interessante approfondimento sul diritto alla *privacy* e nell'era digitale vd.: A.C. Amato Mangiameli, *Sul diritto alla privacy. Variazioni sul tema e spunti normativi*, in Id., *Informatica giuridica,* cit., p. 319 ss.; G. Ziccardi, *La fine della privacy e la svendita dei dati,* in Id., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era della tecnologia*, cit., p. 143 ss.; T. Frosini, *Liberté Egalité Internet*, Napoli 2015, p. 90 ss., D. Bianchi, *Difendersi da Internet. Dalla privacy al diritto all'oblio: i nuovi scenari della responsabilità in rete*, Milano 2014, come pure, E. Bertolini, V. Lubello, O. Pollicino, *Internet: regole e tutela dei diritti fondamentali*, Roma 2013, pp. 27 ss.

[39] Nel panorama italiano, particolarmente significative, le osservazioni G. Sartor, *L'informatica giuridica e le tecnologie dell'informazione. Corso di informatica giuridica*, Torino 2012, pag. 64; A. Mantelero, *Processi di outsourcing informatico e cloud computing: la gestione dei dati personali e aziendali*, in *Il Diritto dell'Informazione e dell'Informatica*, 26, 4-5/2010, pp. 691-692. A livello europeo e internazionale, invece, si vedano Sun MIcrosystems, *Introduction to Cloud Computing Architecture. White Paper*, 2009, p. 29 s. e l'Agenzia Europea per la Sicurezza delle reti e dell'informazione (ENISA), *Cloud computing. Benefits, risks and recommendations for information security*, 2012.

[40] Rischi che sono oggetto di dibattito e, sui quali, l'Agenzia per l'Italia Digitale (AgID) – già alcuni anni fa – è intervenuta (cfr. *Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione* e alle *Linee guida dell'Agenzia per l'Italia Digitale. Caratterizzazione dei sistemi cloud per la Pubblica Amministrazione*, entrambe del 2012; *Strategia per la crescita digitale 2014-2020* e *Strategia italiana per la banda ultralarga*).

[41] Tanti gli autori che, occupandosi del *cloud*, ne mettono in evidenza i possibili rischi. Fra questi: M. Limone, *Cloud computing. Aspetti contrattuali, risvolti normativi e tutela della privacy*, Lecce 2018; A. Caldarelli, L. Ferri, M. Maffei, *I rischi derivanti dall'implementazione del cloud computing: un'indagine empirica nelle PMI Italiane*, Milano 2016; M.C. De Vivo, *Cloud computing. Il contesto giuridico e le aziende di fronte ad un fenomeno controverso,* in *JLIS.it*, vol. 6, n.

irrinunciabile volano di cambiamento[42]. Da un altro lato, e quasi specularmente, proprio la *privacy*, la *sicurezza* e la *responsabilità* costituiscono le questioni alle quali il General Data Protection Regulation (GDPR) ha dedicato maggiore attenzione. Ciò anche, e soprattutto, nel rispetto di quanto sancito dall'articolo 8 della Carta dei Diritti Fondamentali[43] e dall'articolo 16 del Trattato sul Funzionamento dell'Unione Europea (TFUE)[44], che annoverano il diritto alla protezione dei dati di carattere personale fra i diritti fondamentali dei cittadini europei.

4. Il Regolamento (UE) 2016/679. Quali le novità per la nuvola?

Adottato il 27 aprile del 2016 ed entrato in vigore il 25 maggio del medesimo anno, il *General Data Protection Regulation* (GDPR) è pienamente operativo in Italia e in tutti gli altri Stati dell'Unione Europea a decorrere dal 25 maggio del 2018; con significative ricadute in tema di privacy e tutela dei dati personali. Basti notare che nel nostro Paese, a seguito della L. 25 ottobre 2017 n. 163 con la quale il Governo è stato delegato a riordinare e ad adeguare il quadro normativo nazionale a quello europeo, sono state emanate le *Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679* (D. Lgs.10 agosto 2018 n. 101). Disposizioni che hanno apportato variazioni di rilievo sia al *Codice in materia di protezione dei dati personali* (D. Lgs. 30 giugno 2006, n. 196), sia alle *Disposizioni complementari al codice di procedura civile in materia di riduzione e semplificazione dei procedimenti civili di cognizione* (D. Lgs. 1 settembre 2011, n. 150)[45].

Va detto subito che, con il GDPR, l'Unione Europea ha voluto porre fine alla previgente situazione di incertezza e di frammentarietà normativa in tema di trattamento, circolazione e

2, 2015; G. Noto La Diega, *Cloud Computing e protezione dei dati nel web 3.0*, in *http://www.giustiziacivile.it*, 2014; M. Limone, *Il contratto di cloud*, in *www.comparazionedirittocivile.it*, 2013.

[42] Molti anche coloro che mettono in luce le potenzialità della nuvola. Si ricordino, ad esempio: F. Pirozzi, *Il cloud computing*, Milano 2016; E. Prandelli, *Il vantaggio competitivo in rete. Dal web 2.0 al cloud computing,* Milano 2011; A. Ferrari, E. Zanleone, *Cloud computing. Aspettative, problemi, progetti e risultati di aziende passate al modello "as a service"*, Milano 2011.

[43] Così, l'articolo 8: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole eÌÂÂÂ soggetto al controllo di un'autorità indipendente".

[44] Nel quale può leggersi: "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme eÌÂÂÂ soggetto al controllo di autorità indipendenti".

[45] A commento della normativa, si veda L. Bolognini, E. Pelino, *Codice privacy: tutte le novità del D. Lgs. 101/2018*, Milano 2018.

condivisione dei dati personali[46], e ha tentato di ovviare alle svariate criticità emerse nel corso di questi anni. Criticità che, come è noto, sono poi culminate nell'annullamento dell'accordo *Safe Harbor*[47] e nell'adozione del *Privacy Shield*[48].

Autentico esempio di convergenza normativa transnazionale, il regolamento europeo per la protezione dei dati concorre in modo davvero significativo alla realizzazione di uno spazio comune di libertà, sicurezza e giustizia[49] all'interno dell'Unione Europea. In particolare, la tutela dei dati personali dei cittadini europei viene rafforzata e parificata, indipendentemente dalla nazionalità e dalla residenza dei soggetti interessati.

Com'è naturale, tale regolamento ha già avuto – e sta via via avendo – delle ricadute determinanti anche sulla nuvola, ridefinendone i parametri di sicurezza e riducendo sensibilmente i rischi connessi alla perdita di controllo delle informazioni e alla c.d. data gravity, ossia alla coagulazione incontrollata dei dati presso i data lake[50].

Il nesso fra il cloud e il GDPR è dunque stretto oltre che decisamente intenso. Si tratta di un legame che nasce dall'attenzione per la tutela dei dati personali – quali diritti fondamentali – e che si estende ai big data. Vale a dire, a quell'incessante proliferare di enormi masse di

[46] Basti pensare alla vertenza fra Cambridge Analytica e Facebook (in tema, cfr. D. Messina, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Analytica"*, in *Federalismi.it*, 20/2018.

[47] Come è noto, l'accordo *Safe Harbor* (letteralmente "approdo sicuro"), in virtù del quale le aziende americane potevano "spostare" i dati personali dei cittadini europei nei server di provider collocati negli Stati Uniti, è stato annullato a seguito dalla menzionata sentenza della Corte di Giustizia Europea del 6 ottobre del 2015. In quella sede, infatti, la Corte ha rilevato l'inadeguatezza di tale accordo a garantire il diritto alla tutela dei dati dei cittadini europei. In commento, si veda: A. Mantelero, *Il trattamento dati nelle imprese nel post Safe Harbour. Strategie di breve, medio e lungo periodo*, in *Diritto dell'Informazione e dell'Informatica*, 4-5/2015, p. 887 ss.; D. Borrelli, *Safe Harbour: gli USA non sono poi così sicuri*, in Inside Marketing, ottobre 2015; O. Pollicino, M. Bassini, *Schrems. La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *Roma Tre-Express* (disponibile e on-line al sito *http://romatrepress.uniroma3.it/ojs/index.php/PTD/article/view/5/*).

[48] A proposito dell'adozione del Privacy Shield, cfr.: G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbor principles" al "Privacy Shield"*, Roma 2016.

[49] Imprescindibile il richiamo agli articoli 3 e 67 del TFUE. Disposizioni in cui, nell'ordine, può leggersi: "L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, che garantisce la libera circolazione delle persone, insieme a misure appropriate in materia di controllo delle frontiere esterne, d'asilo, d'immigrazione, oltre alla prevenzione della criminalità e la lotta contro questo fenomeno" (articolo 3, paragrafo 2). "1. L'Unione realizza uno spazio di libertà, sicurezza e giustizia nel rispetto dei diritti fondamentali nonché dei diversi ordinamenti giuridici e delle diverse tradizioni giuridiche degli Stati membri. 2. Essa garantisce che non vi siano controlli sulle persone alle frontiere interne e sviluppa una politica comune in materia di asilo, immigrazione e controllo delle frontiere esterne, fondata sulla solidarietà tra Stati membri ed equa nei confronti dei cittadini dei paesi terzi. [...] 3. L'Unione si adopera per garantire un livello elevato di sicurezza attraverso misure di prevenzione e di lotta contro la criminalità, il razzismo e la xenofobia, attraverso misure di coordinamento e cooperazione tra forze di polizia e autorità giudiziarie e altre autorità competenti, nonché tramite il riconoscimento reciproco delle decisioni giudiziarie penali e, se necessario, il ravvicinamento delle legislazioni penali. 4. L'Unione facilita l'accesso alla giustizia, in particolare attraverso il principio di riconoscimento reciproco delle decisioni giudiziarie ed extragiudiziali in materia civile" (articolo 67).

[50] Particolari ambienti di archiviazione dei dati nel loro formato nativo o in copia, quasi perfetta, del loro formato nativo. Tali ambienti semplificano e, al contempo, amplificano le capacità e le possibilità di stoccaggio, gestione e analisi delle informazioni e in particolare dei big data. Non a caso, lo scopo dei data lake è quello di condividere e correlare fra loro ingenti masse di dati.

dati, originate dall'accumulo e dalla ricombinazione, continua e casuale, di tutte quelle tracce digitali e di quelle informazioni granulari che, ogni giorno, inconsapevolmente generiamo[51].

A riprova dell'importanza che il Regolamento 2016/679 riconosce ai dati personali e al loro trattamento, è sufficiente richiamare i considerando iniziali[52]. In essi, infatti, si sottolinea anche che l'evoluzione tecnologica, unita alla sempre condivisione e alla circolazione dei dati, richiede un quadro normativo *adeguato*, *solido*, *coerente* ed *uniforme*, capace di garantire un *effettivo*, ed *eguale*, godimento dei diritti fondamentali in tutti gli Stati membri, in modo che non si possano più dare differenze in ordine alle modalità di trattamento e agli standard di sicurezza[53].

Oggetto, finalità e ambito di applicazione del nuovo regolamento sono individuati dall'articolo 1[54] e dall'articolo 2[55], mentre i principi che ne compongono l'architrave e che

[51] Per un'interessante approfondimento rinvio ad A.C. Amato Mangiameli, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di Filosofia del diritto*, VII, 1/2019, pp. 107-124.

[52] In modo particolare dei punti 2 e 4: "I principi e le norme a tutela delle persone fisiche con riguardo al trattamento dei dati personali dovrebbero rispettarne i diritti e le libertà fondamentali, in particolare il diritto alla protezione dei dati personali, a prescindere dalla loro nazionalità o dalla loro residenza. Il presente regolamento è inteso a contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica, al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche". "Il trattamento dei dati dovrebbe essere al servizio dell'uomo [...]".

[53] Così, nell'ordine, i punti 6, 7, 10 e 14: "La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. [...] Sempre più spesso le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. [...]". "Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche". "Al fine di assicurare un livello coerente ed elevato di protezione delle persone fisiche e rimuovere gli ostacoli alla circolazione dei dati personali all'interno dell'Unione, il livello di protezione dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di tali dati dovrebbe essere equivalente in tutti gli Stati membri. È opportuno assicurare un'applicazione coerente e omogenea delle norme a protezione dei diritti e delle libertà fondamentali delle persone fisiche con riguardo al trattamento dei dati personali in tutta l'Unione. [...]". "È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. [...]".

[54] "1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. 3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali".

[55] "1. Il presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. 2. Il presente regolamento non si applica ai trattamenti di dati personali: a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse". [56] Sulla libertà del consenso, cfr. S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e Diritto Privato*, 2/2016, pp. 513-557; Id., *I requisiti al consenso del trattamento dei dati personali*, Santarcangelo di Romagna 2016.

vanno ad incidere in senso proprio sul trattamento e sulla tutela dei dati si ritrovano soprattutto negli articoli 5 e 7.

Nel dettaglio, l'articolo 5 stabilisce che il trattamento dei dati deve sempre essere *lecito*, *corretto* e *trasparente*:

"1. I dati personali sono:

a. trattati in modo lecito, corretto e trasparente nei confronti dell'interessato [...];
b. raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità [...];
c. adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati [...];
d. esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati [...];
e. conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato [...];
f. trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali [...]".

L'articolo 7, invece, richiede che il consenso dell'interessato sia sempre *libero*, *specifico*, *informato*, *inequivocabile*, *revocabile* e *non-condizionat*[56]:

"1. Qualora il trattamento sia basato sul consenso, il titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali.

2. Se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. [...].

3. L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca. Prima di esprimere il proprio consenso, l'interessato è informato di ciò. Il consenso è revocato con la stessa facilità con cui è accordato.

[56] Sulla libertà del consenso, cfr. S. Thobani, *La libertà del consenso al trattamento dei dati personali e lo sfruttamento economico dei diritti della personalità*, in *Europa e Diritto Privato*, 2/2016, pp. 513-557; Id., *I requisiti al consenso del trattamento dei dati personali*, Santarcangelo di Romagna 2016.

4. Nel valutare se il consenso sia stato liberamente prestato, si tiene nella massima considerazione l'eventualità, tra le altre, che l'esecuzione di un contratto, compresa la prestazione di un servizio, sia condizionata alla prestazione del consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto".

Ulteriori, e non trascurabili, conquiste in termini di tutela sono introdotte dagli articoli 17 e 21. L'articolo 17[57], infatti, prevede il c.d. diritto all'oblio, ovvero, il diritto dell'interessato ad ottenere dal titolare del trattamento la cancellazione dei propri dati. Mentre, l'articolo 21 sancisce il diritto di opposizione al trattamento dei propri dati, compresa la profilazione.

A queste importanti novità[58], se ne aggiungono delle altre, che comportano ricadute significative soprattutto sulla gestione e sull'erogazione dei servizi cloud, dal momento che impongono specifici oneri in capo ai titolari del trattamento.

In tal senso, senza dubbio significativa è l'introduzione – di cui all'articolo 37[59] – dell'obbligo dei titolari e dei responsabili del trattamento di designare un responsabile della protezione dei dati: il *Data Protection Officer* (DPO) a cui è affidato il compito di assicurarne la corretta gestione[60].

Ma non è tutto. Il GDPR ha, infatti, anche stabilito in capo al titolare del trattamento l'onere di adottare tutta una serie di misure tecniche (articolo 24) e di accortezze atte a garantire un'efficace e concreta tutela dei dati personali. Fra queste, spiccano la *pseudonimizzazione* (consistente nel ricorso a tecniche di pseudonimia e di cifratura che, in

[57] Nel quale, si legge: "L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: *a)* i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; *b)* l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; *c)* l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; *d)* i dati personali sono stati trattati illecitamente; *e)* i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; *f)* i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. 2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato [...] a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali".

[58] In merito al consenso e ai diritti riconosciuti all'interessato dal Regolamento (UE) 2016/679, cfr. A.C. Amato Mangiameli, *Algoritmi e big data*, cit., in part. p. 115.

[59] Dove, nel paragrafo 1, si legge: "Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un responsabile della protezione dei dati ogniqualvolta: *a)* il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali; *b)* le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure *c)* le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10. [...]".

[60] Sulla figura del DPO, cfr., fra i tanti, G. Satta, *La nuova figura del Data Protection Officer*, in *Amministrazione e finanza*, 3/2018, pp. 49-54; Aiea, *La figura del Data Protection Officer nel nuovo Regolamento Europeo*, maggio 2017.

assenza di informazioni aggiuntive, rendono i dati personali non direttamente attribuibili all'interessato) e la *minimizzazione* (volta a limitare le operazioni di trattamento dei dati personali dell'interessato a quelle che sono strettamente necessarie al perseguimento delle finalità del titolare) (articolo 25).

Sempre al fine di scongiurare eventuali trasgressioni e di rafforzare la tutela effettiva dei dati personali, il GDPR prescrive la tenuta di appositi registri delle attività di trattamento (articolo 30); richiede il rispetto di determinati livelli di sicurezza (articolo 32); prevede, da parte del titolare del trattamento, l'obbligo di notifica delle eventuali violazioni all'autorità di controllo (articolo 33); stabilisce che il titolare – senza ingiustificato ritardo – debba avvisare l'interessato dell'avvenuta violazione dei dati nel caso in cui si diano dei rischi per i diritti e per le libertà delle persone fisiche (articolo 34); incoraggia l'istituzione di meccanismi di certificazione e promuove l'adozione di sigilli e di marchi che garantiscano la conformità dei trattamenti effettuati (articolo 42); individua le condizioni e i limiti al trasferimento dei dati personali dei cittadini europei verso i paesi terzi e/o le organizzazioni internazionali[61]. Condizioni e limiti, in cui rientra anche la valutazione di adeguatezza (e in certi casi persino l'autorizzazione) della Commissione al trasferimento dei dati[62].

Parecchie, dunque, le novità introdotte dal Regolamento 2016/679. Novità che, come è *ictu oculi* evidente, sono destinate ad avere un riverbero immediato e, almeno ad avviso di chi scrive, alquanto positivo sulla nuvola. Non foss'altro perché, più o meno direttamente, ne elevano i livelli di sicurezza.

5. Un primo bilancio e qualche buona notizia.

Tra buone e/o cattive ragioni, censure e difese, rischi e vantaggi, tirare le fila del percorso svolto e abbozzare un primo bilancio degli effetti che il General Data Protection Regulation sta avendo sul cloud non è per nulla semplice. Non soltanto perché il quadro normativo (così come quello dottrinale e giurisprudenziale) è in continuo divenire, ma anche perché – al di là di quelle che sono le attese – il recente regolamento europeo deve ancora sostenere la prova dei fatti. Invero, per quanto i principi sanciti siano senza dubbio promettenti, non è detto che l'adozione del GDPR si dimostri sufficiente ad ovviare a tutte le criticità che, soprattutto negli ultimi anni, si sono registrate in tema di tutela dei dati e di utilizzo della nuvola.

[61] In tal senso, l'articolo 44 afferma: "Qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale, ha luogo soltanto se il titolare del trattamento e il responsabile del trattamento rispettano le condizioni di cui al presente capo, fatte salve le altre disposizioni del presente regolamento. Tutte le disposizioni del presente capo sono applicate al fine di assicurare che il livello di protezione delle persone fisiche garantito dal presente regolamento non sia pregiudicato".

[62] All'articolo 45 paragrafo 1, infatti, si legge "Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche".

Detto ciò, non si può fare a meno di notare che ci sono dei segnali che lasciano ben sperare in quanto, muovendosi nella direzione tracciata dal regolamento, denotano la concreta volontà di tradurne in pratica i principi. Uno di questi è senza dubbio rappresentato dalla nascita del *Cloud Infrastructure Services Providers in Europe* (CISPE): una coalizione alla quale – conformemente all'articolo 40 del GDPR[63] – hanno aderito i provider di sedici Stati membri[64]. Coalizione alla quale, si deve l'adozione del primo codice di condotta dei fornitori dei servizi cloud.

Vari i meriti del codice CISPE: non solo offre risposte concrete alle esigenze e alle istanze degli utenti, ma chiarisce anche le ripartizioni di responsabilità tra cliente e provider, assicura un determinato livello di trasparenza, soddisfa i requisiti di adeguatezza richiesti, individua un marchio di conformità agli standard di sicurezza, consente il controllo della collocazione dei dati – scongiurando, fra le altre cose, il pericolo che il gestore li riutilizzi o li rivenda a terzi – e, ancora, utilizza una connessione sicura *end-to-end* e si avvale della crittografia Advanced Encryption Standard (AES).

Al CISPE, di recente, si è aggiunto anche un altro importante segnale positivo, che testimonia la volontà di dare seguito al GDPR e di permettere un uso più consapevole e soprattutto più sicuro del cloud. Si tratta della costituzione del nuovo Comitato per la Protezione dei Dati (EDPB)[65], che ha sostituito il Working Party art. 29. L'EDPB ha fondamentale, e delicatissimo, compito di vigilare sulla corretta applicazione del Regolamento europeo da parte delle Autorità nazionali.

Ed è proprio all'EDPB che si debbono, ad esempio, le recentissime *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, del 9 aprile 2019. Linee Guida destinate ad avere implicazioni sui servizi online, come pure sulla tutela della concorrenza e dei consumatori, e che per il momento – e sino al prossimo 24 maggio – sono oggetto di consultazione pubblica[66].

[63] Che, così, recita: "Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del presente regolamento, in funzione delle specificità dei vari settori di trattamento e delle esigenze specifiche delle micro, piccole e medie imprese".

[64] Fra i provider CISPE: *Arsys, Art of Automation, Aruba, BIT, Daticum, Dominion, Fasthosts, FjordIT, Gigas, Hetzner Online, Home, Host Europe Group, IDS, Ikoula, LeaseWeb, Lomaco, Outscale, OVH, Seeweb, Solidhost, UpCloud, VTX, XXL Webhosting, 1&1 Internet.*

[65] Organo europeo indipendente, l'EDPB contribuisce all'applicazione coerente delle norme sulla protezione dei dati all'interno dell'Unione e promuove la cooperazione tra le autorità competenti in materia di protezione dei dati. L'EDPB è composto dai rappresentanti delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati (cfr. https://edpb.europa.eu/about-edpb/about-edpb_it).

[66] Cfr. F. Pizzetti, *GDPR, tutela della concorrenza e dei consumatori: le linee guida EDPB sui servizi online*, in *Agenda Digitale*, 03.05.2019 (articolo disponibile online: https://www.agendadigitale.eu/sicurezza/privacy/gdpr-tutela-della-concorrenza-e-dei-consumatori-le-linee-guida-edpb-sui-servizi-online/) .