UNIVERSITÀ DEGLI STUDI DI SALERNO

DIPARTIMENTO DI SCIENZE ECONOMICHE E STATISTICHE

CORSO DI DOTTORATO DI RICERCA IN
ANALISI ECONOMICA, GIURIDICA E STATISTICA DELLE POLITICHE, DEI MERCATI E DELLE IMPRESE
XXIX CICLO
CURRICULUM: DIRITTO E MERCATO GLOBALE

TESI DI DOTTORATO
in
DIRITTO PRIVATO

Il Cloud Computing

Dottorando
dott. Francesco Aliperti

Coordinatore
Chiar.mo Prof. Sergio Destefanis

Tutor
Chiar.mo Prof. Marcello D'Ambrosio

Anno Accademico 2016/2017

Indice

CAPITOLO I

Cloud computing: definizione, elementi peculiari, descrizione e natura del fenomeno

CAPITOLO II

Evoluzione tecnologica e diritto alla riservatezza. Il trattamento dei dati personali in rete

CAPITOLO III

La tutela dei dati personali nell'era del *cloud computing*

CAPITOLO I

Cloud computing: definizione, elementi peculiari, descrizione e natura del fenomeno

Sommario: 1. Premessa. - 1.1. I problemi delle tecnologie *cloud*. - 2. Definizione e descrizione del fenomeno del *cloud computing*. - 2.1. Trattamento dei dati e utilizzo consapevole dei servizi *cloud*. - 3. La metafora della «nuvola». - 3.1. Da *internet* al *cloud*: le nuove metafore per descrivere il *cloud*. - 4. Elementi caratterizzanti. - 5. Modelli di «nuvole». - 6. Tipologie di servizi offerti dal *cloud*. - 7. Benefici del *cloud computing*. - 7.1. *Segue*. Rischi. - 8. Legge applicabile e giurisdizione competente.

1. Premessa.

Il *cloud computing* nasce negli USA, in cui ha un'operatività ormai consolidata, mentre in Europa e in Italia sta iniziando a muovere i primi passi. La corretta descrizione del fenomeno economico-sociale racchiuso nell'espressione inglese *cloud computing* si prospetta all'interprete come attività necessariamente prodromica rispetto alla trattazione e, successiva, risoluzione dei possibili problemi che tale fenomeno pone. Ciò nella ferma convinzione che «non basta la conoscenza della legge, l'interpretazione della disposizione legislativa, né ricostruire gli istituti, i concetti e quindi il sistema; necessario è confrontare il sistema con il fatto, la realtà sociale, i problemi concreti.».[1] È, in altri termini, essenziale il confronto tra interpretazione del dato normativo e peculiarità del fatto.[2]

Sulla base dell'insegnamento per il quale il giurista deve operare sulle cose e non sul modo con cui altri prima di lui hanno parlato di certe cose[3], nello studio del fenomeno *de quo*, sarà all'uopo indispensabile immergersi nel particolare della vita e dell'esperienza di codesto fenomeno, conducendo un'analisi che, dalla disamina della tecnologia *cloud*, dalla descrizione delle sue tipologie e dei servizi offerti, riesca in tal modo a individuarne i suoi

---

[1] P. PERLINGIERI, *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, 3ª ed., Napoli, 2006, p. 5 ss. L'a. prosegue affermando: «[…] per la conoscenza del fatto, della singola vicenda da regolare – fisiologicamente, in funzione preventiva –, o da giudicare – patologicamente, in caso di effettivo conflitto, nel momento della funzione, per cosí dire, mediatrice e contemperatrice o arbitrale –, occorre sempre, nell'una e nell'altra ipotesi, porre a confronto il sistema normativo con la realtà dei fatti, la scienza e la prassi.».

[2] Sul punto v. P. PERLINGIERI, *L'interpretazione della legge come sistematica ed assiologica. Il broccardo* in claris non fit interpretatio*, il ruolo dell'art. 12 disp. prel. c.c. e la nuova scuola dell'esegesi*, (1985), in ID., *Scuole tendenze e metodi. Problemi del diritto civile*, Napoli, 1989, p. 283 ss.

[3] N. BOBBIO, *Diritto e logica*, in *Riv. int. fil. dir.*, 1962, p. 25 s.

tratti fisionomici. Se non si comprendono le peculiarità di un fenomeno non lo si può capire fino in fondo e sarà oltremodo difficile coglierne le problematiche che attorno ad esso ruotano.

Esigenza questa che tanto piú s'impone oggi, in un panorama in cui la predetta tecnologia procede molto piú velocemente dell'attività del legislatore.[4] Lo richiede, d'altronde, la crescente complessità del mondo nel quale viviamo, caratterizzato oramai da una realtà complessa, nella quale «reale» e «virtuale» si intrecciano inestricabilmente.

In un mondo in cui il sistema delle telecomunicazioni ha reso possibile annullare la dimensione spaziale e temporale, un approccio statico ai nuovi fenomeni, che pretenda di utilizzare categorie giuridiche ormai obsolete, non piú attuali e non contestualizzate alla realtà dei fatti, rischia di non riuscire a coniugare lo sviluppo tecnologico con la tutela dei diritti inviolabili della persona. Nel panorama giuridico attuale, in cui il diritto ha rotto con schemi definiti, assoluti, immodificabili, è imprescindibile una dialettica costante tra testo e contesto, capace di fornire la disciplina piú adeguata alla contingenza concreta, senza chiedere al legislatore ciò che, a ben vedere, è di competenza dell'interprete.

Emerge, infatti, sempre di piú la difficoltà per il regolatore tradizionale, ancora prevalentemente legato al criterio della territorialità, di trasformare princípi, valori, diritti fondamentali propri del suo ordinamento nazionale o, al massimo, regionale[5], in norme giuridiche vincolanti per un'umanità globale. In misura crescente si evidenzia come il rapporto tra la tecnologia e i suoi molteplici utilizzi possa incidere e condizionare anche la tutela dei diritti fondamentali dei cittadini e in genere degli utenti, compresi quelli delle imprese che assicurano il funzionamento stesso di queste tecnologie[6].

---

[4] Manca ancora un quadro normativo aggiornato – in tema di *privacy*, ma anche in àmbito civile e penale – che tenga conto di tutte le novità introdotte dal *cloud computing* e sia in grado di offrire adeguate tutele nei riguardi delle fattispecie giuridiche connesse all'adozione di servizi distribuiti di elaborazione e di conservazione dati. Il nuovo Regolamento Europeo (679/2016) sulla protezione dei dati introduce un'unica legislazione in tutti gli Stati Membri dell'UE, ma sarà applicabile a decorrere dal 25 Maggio 2018 (art. 99). Esso regolamento rappresenta lo strumento atto a formalizzare il nuovo corso digitale della tutela dei dati personali, a livello comunitario ed extracomunitario. Questo mostra peculiarità rilevanti di tipo tecnico-giuridico: è obbligatorio e direttamente applicabile in tutti gli Stati membri senza necessità di recepimento; ha un'essenza informatico giuridica spiccata; implica tutele verso i cittadini dell'Unione europea anche da parte di nazioni extra UE; mira a responsabilizzare utenti e aziende sulle attività digitali che concedono e/o dispongono. Al riguardo v. *infra* cap. II e III.

[5] Ovviamente per «regionale» qui s'intende l'area territoriale interessata al rispetto di regole sovranazionali poste da una organizzazione che coinvolge gli Stati appartenenti a una regione del mondo. Un esempio classico di questa accezione del termine è la stessa Unione Europea.

[6] Sul punto si rinvia a F. PIZZETTI, *Dati e diritti nell'epoca della comunicazione elettronica*, in ID., *Il caso del diritto d'autore*, 2ª ed., Torino, 2013, p. 21 s.

Essendo il fatto, e non la parola, l'oggetto della scienza giuridica[7], occorrerà, allora, individuare il concreto atteggiarsi, nella prassi delle imprese (ma anche della pubblica amministrazione), dei servizi *cloud* per poi, in seguito, specificare le problematiche connesse all'adozione di tali servizi, anche in relazione agli aspetti di protezione dei dati personali.

Le nuove tecnologie necessitano di nuove regole, nuovi sistemi di relazioni tra persone (di diverse zone del mondo) che producano nuove regole, globali e universali. Ma nella consapevolezza che non tutto può essere regolato dal legislatore, sarà ancor piú necessario, allora, identificare le peculiarità funzionali e strutturali della fattispecie concreta[8] in modo tale da rinvenire, nel complesso sistema italo-comunitario delle fonti[9], regole e princípi, idonei a costruire, di volta in volta, la disciplina piú congrua[10].

Occorrerà rifuggire, anche in questo caso, da una ricostruzione concettualistica, formalistica, rigida degli istituti, procedendo, di converso, seguendo una prospettiva funzionale[11], ove i rimedi si giustificano in ragione degli interessi da tutelare[12], cosí superando il dato formale[13], attraverso un ragionamento per princípi, vòlto a valorizzare le peculiarità del caso concreto[14].

---

7 P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 93.

8 Sostenitore convinto del metodo del «caso concreto», tradizionalmente estraneo alla formazione del giurista italiano, P. PERLINGIERI, *o.c.*, p. 97 ss.; ID., *Fonti del diritto e "ordinamento del caso concreto"*, in *Riv. dir. priv.*, 2010, p. 7 ss. Sul metodo casistico-problematico v., tra gli altri, G. GORLA, *Il contratto. Problemi fondamentali trattati con il metodo comparativo e casistico*, I, *Lineamenti generali*, Milano, 1955 e ID., *Il contratto. Problemi fondamentali trattati con il metodo comparativo e casistico*, II, *Casistica e problemi*, Milano, 1955; ID., *Lo studio interno e comparativo della giurisprudenza e i suoi presupposti: le raccolte e le tecniche per la integrazione delle sentenze*, in *Foro it.*, 1964, V, c. 73 ss.; R.B. SCHLESINGER, *Il «nucleo comune» dei vari sistemi giuridici: un nuovo campo di studi comparativi all'orizzonte*, in *Riv. dir. civ.*, 1963, I, p. 73 ss.; G. ALPA, *Il metodo nel diritto civile*, in *Contr. impr.*, 2000, p. 450 ss., ed *ivi* ulteriore bibliografia.

9 Afferma la complessità e l'unitarietà dell'ordinamento giuridico, evidenziando la difficoltà nell'ammettere un ordinamento altro, inteso come comparto stagno rispetto al primo, P. PERLINGIERI, *Complessità e unitarietà dell'ordinamento giuridico vigente*, in *Rass. dir. civ.*, 2005, 1, p. 188 s.; ID., *Lo studio del diritto nella complessità e unitarietà del sistema ordinamentale,* in *Foro nap.*, 2014, 1, p. 100.

10 P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 352 ss.

11 Contro una ricostruzione concettualistica, formalistica, rigida degli istituti civilistici e a favore della prospettiva funzionale, P. PERLINGIERI, *La contrattazione tra imprese*, in *Riv. dir. impr.*, 2006, 3, p. 330 ss.

12 P. PERLINGIERI, *La contrattazione tra imprese*, cit., p. 342 ss.

13 P. PERLINGIERI, *L'interpretazione della legge come sistematica ed assiologica*, cit., *passim*. Che occorra superare il dato formale pare esserne convinta anche la Suprema Corte di Cassazione che, con sentenza n. 21994 del 6 dicembre 2012 (in *Foro it.*, 2013, I, c. 1205, con nota di A. PALMIERI), precisando che anche nella fase attuativa di un rapporto contrattuale trovano applicazione il dovere costituzionale di solidarietà, nonché i correlati doveri di correttezza e buona fede, ha statuito che nell'esercizio del potere del giudice di riduzione della penale, la valutazione de «*l'interesse che il creditore aveva al momento dell'adempimento*» va fatta non avendo riguardo al momento della stipulazione della clausola – come pure lascerebbe intendere il dato letterale della norma con l'uso del verbo «aveva» al tempo imperfetto – ma tenendo conto anche delle circostanze manifestatesi durante lo svolgimento del rapporto. È questa una tipica ipotesi di interpretazione costituzionalmente orientata (nel caso di specie in relazione all'art. 2 Cost.) di una norma del codice civile: tale

Anche il fenomeno del *cloud computing* e gli istituti che con esso entreranno in relazione richiedono una lettura (o rilettura) alla luce sia del personalismo[15] sia del solidarismo[16], non essendo questi valori estranei alle problematiche che siffatto fenomeno solleva. Il fenomeno in esame, poiché fenomeno giuridico, il quale si esprime mediante la complessità di princípi e valori giuridicamente rilevanti, comporta che il suo studio non potrà che fondarsi su un'interpretazione, dei concetti e dei temi a esso relativi, che non potrà che essere assiologica e sistematica[17].

Ebbene, trattamento dei dati e «rischio di perdersi nella nuvola», neutralità della rete[18], obbligo di denunciare le *serious breaches*[19], necessità di ridefinire le responsabilità nell'àmbito di catene complesse di trattamento dei dati, sono (alcuni) titoli di una tematica sempre piú vitale per la nostra società, per il nostro sviluppo economico, per la nostra libertà e convivenza democratica.

---

tipo di interpretazione permette anche, eventualmente, di superare un dato letterale apparentemente contrario.

[14] Sulla variabilità dei rimedi e sulla necessità che il rimedio sia adeguato rispetto agli interessi da tutelare v., per tutti, P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 352 ss.; ID., *Il "giusto rimedio" nel diritto civile,* in *Giusto proc. civ.*, 2011, 1, p. 3 ss.

[15] «Il principio personalistico ispira la Carta Costituzionale e pone come fine ultimo dell'organizzazione sociale lo sviluppo di ogni singola persona umana» (cosí Cass., 15 giugno 2012, n. 14103, in *Rep. Foro it.*, 2013, voce *Servitù*, n. 32).

[16] Sull'incidenza del principio personalista nell'interpretazione degli istituti patrimoniali e, quindi, depatrimonializzando, socializzando, umanizzando un diritto civile originariamente nato con una predominante concezione patrimoniale ed individualistica dei rapporti intersoggettivi, v. C. DONISI, *Verso la «depatrimonializzazione» del diritto privato,* in *Rass. dir. civ.*, 1980, p. 644 ss.

[17] Sull'interpretazione assiologica e sistematica v., ampliamente, P. PERLINGIERI *o.l.u.c.*, *passim*; ID., *La dottrina del diritto civile nella legalità costituzionale*, in *Rass. dir. civ.*, 2007, 2, p. 497 s.

[18] Il diritto ad un accesso neutrale ad *internet* è espressamente riconosciuto dalla «Dichiarazione dei diritti in internet» (art. 4), approvata e pubblicata il 28 luglio 2015 dalla «Commissione per i diritti e i doveri in internet» istituita presso la Camera dei deputati (XVII Legislatura). Tale diritto viene elevato a «condizione necessaria per l'effettività dei diritti fondamentali della persona» (art. 4, comma 2) e si sostanzia nel riconoscimento ad ogni persona del diritto a che «i dati trasmessi e ricevuti in Internet non subiscano discriminazioni, restrizioni o interferenze in relazione al mittente, ricevente, tipo o contenuto dei dati, dispositivo utilizzato, applicazioni o, in generale, legittime scelte delle persone» (art. 4, comma 1). Come si legge nel suo preambolo, la «Dichiarazione» in parola «è fondata sul pieno riconoscimento di libertà, eguaglianza, dignità e diversità di ogni persona. La garanzia di questi diritti è condizione necessaria perché sia assicurato il funzionamento democratico delle Istituzioni, e perché si eviti il prevalere di poteri pubblici e privati che possano portare ad una società della sorveglianza, del controllo e della selezione sociale» ed è «strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale».

[19] Si tratta di quelle «smagliature» o «rotture» (o, ancora, «falle») del sistema che sono ormai definite usualmente come «*data breaches*» e che possono compromettere l'una o l'altra fase del sempre piú articolato processo di trasmissione delle informazioni sul quale si basa la società delle telecomunicazioni. Ed è proprio l'espansione inarrestabile della circolazione dei dati, legata proprio al modo di essere e di vivere dell'umanità, che dipende sempre di piú dalla comunicazione globale assicurata dal sistema integrato delle comunicazioni elettroniche, a rendere ogni giorno piú rilevante il problema delle «falle» che possono verificarsi nel sistema.

Lo sviluppo, tuttavia, ha sempre un prezzo da pagare e ciò si rinviene nella semplice considerazione per la quale le imprese e gli operatori cui il mercato offre questi nuovi servizi pensano soprattutto alla diminuzione di costi o alle opportunità costante ammodernamento che queste tecnologie consentono, prestando scarsa attenzione al fatto che le stesse comportano, però, la perdita del possesso fisico dei dati e dei programmi operativi che utilizzano.

Ecco dunque la necessità e l'importanza di un avanzamento nella consapevolezza dei nuovi fenomeni tecnologici e, ciò premesso, l'esigenza e altresí l'urgenza di un bilanciamento degli interessi in gioco, guidata dall'interpretazione costituzionalmente e comunitariamente orientata.

Invero, l'avanzata delle nuove tecnologie non può e non deve essere fermata, né tantomeno ostacolata, ma deve essere indagata per poi essere regolata a garanzia di tutti. È chiaro come il progresso tecnologico non possa assolutamente sopprimere valori costituzionali supremi (*in primis* la dignità umana[20], ad esempio). L'eventuale mancanza di controllo (o una cattiva gestione) nel suo dipanarsi potrebbe comportare il serio rischio di un annullamento delle conquiste in tema di diritti fondamentali della persona. Questi devono sempre rappresentare la cornice nella quale disegnare, e ancor prima immaginare, lo sviluppo delle nuove tecnologie. Lo sviluppo senza la tutela dei diritti fondamentali della persona non è ammissibile.

Occorre, allora, che sempre piú spesso si illustrino gli aspetti essenziali delle piú avanzate innovazioni a disposizione del mercato, che si predispongano linee informative per rendere questi fenomeni piú comprensibili per gli utenti, nonché raccomandazioni dedicate agli operatori economici, insieme a indicazioni specifiche per le amministrazioni e i regolatori, a partire ovviamente dal Parlamento e dal Governo[21].

---

[20] Sulla rilevanza e preminenza della dignità umana v. la famosa sentenza Omega (Corte giust., 14 ottobre 2004, c. 36/02, Omega Spielhallen-und Automatenaufstellungs GmbH c. Oberbürgermeisterin der Bundesstadt Bonn, in *www.giurcost.org*), con la quale si è statuito che «[i]l diritto comunitario non osta a che un'attività economica consistente nello sfruttamento commerciale di giochi di simulazione di omicidi sia vietata da un provvedimento nazionale adottato per motivi di salvaguardia dell'ordine pubblico perché tale attività viola la dignità umana.».

[21] In tal senso, v. F. PIZZETTI, *Uomini e dati. Evoluzione tecnologica e diritto alla riservatezza*, in *Foro it.*, 2011, V, c. 230.

È sempre piú urgente, però, che gli utenti siano informati dagli stessi fornitori dei rischi connessi ai servizi offerti. Anche in quest'àmbito è necessaria un'informativa di rischio analoga, per esempio, a quelle sull'uso dei farmaci o sui pericoli dell'eccessiva velocità.[22]

1.1. I problemi delle tecnologie *cloud*.

Il diffondersi in misura sempre piú massiccia della tecnologia *cloud*, certamente destinata a crescere fino a diventare il modo normale di utilizzo dei dati in ambito ICT[23], comporta che tutto il sistema di protezione dei dati stia per entrare o, meglio, sia già entrato in una nuova dimensione.

Ciò in quanto l'aspetto piú significativo della tecnologia *cloud*, in realtà solo parzialmente nuova[24], è che essa renderà sempre piú netta la separazione fra la titolarità dei dati e dei trattamenti, e il possesso e il controllo fisico dei dati trattati o conservati. Ogni trattamento, anche il piú semplice, richiederà comunque la circolazione sulla rete. La relativa tutela e conservazione non solo dipenderà sempre piú anche da chi opera «in remoto», ma sarà anche affidata in misura crescente a soggetti che non sono né i «proprietari» dei dati (e cioè per usare il linguaggio europeo, «gli interessati»), né coloro che questi dati trattano (e cioè, sempre nel linguaggio europeo, i «titolari»).

A questo si deve aggiungere poi che il *cloud* richiede, per poter erogare un servizio su larga scala, una grande molteplicità di *server*, collocati nelle parti piú diverse del mondo

---

[22] F. PIZZETTI, *Uomini e dati*, cit.

[23] «Le tecnologie dell'informazione e della comunicazione, in acronimo TIC (in inglese *Information and Communications Technology*, in acronimo ICT), sono l'insieme dei metodi e delle tecnologie che realizzano i sistemi di trasmissione, ricezione ed elaborazione di informazioni (tecnologie digitali comprese). Dal secondo dopoguerra, l'uso della tecnologia nella gestione e nel trattamento delle informazioni assume crescente importanza strategica per le organizzazioni e per i cittadini in maniera crescente con il boom di *internet* a partire dagli anni novanta. Le istituzioni educative in particolare prevedono, attraverso il proprio progetto educativo, appositi percorsi di formazione ed utilizzo trasversale delle TIC per le diverse discipline. Oggi l'informatica (apparecchi digitali e programmi *software*) e le telecomunicazioni (le reti telematiche) sono i due pilastri su cui si regge la società dell'informazione.», cfr. voce *Tecnologie dell'informazione e della comunicazione*, in Wikipedia, all'indirizzo *web https://it.wikipedia.org/wiki/Tecnologie_dell%27informazione_e_della_comunicazione*.

[24] In realtà, gli utenti di *internet* già da molti anni fanno un uso (pressoché inconsapevole) dei servizi in modalità *cloud*. Si pensi ai servizi di *web-mail*, che consentono di accedere agevolmente a tutte le *e-mail* scambiate, in invio e in ricezione, da qualsiasi *computer* collegato a *internet*, e che sempre piú spesso vengono usati anche come archivio remoto dei nostri dati. Oppure, si pensi alle potenzialità degli *smartphone*, che amplificano il ricorso alle *e-mail* consentendoci l'accesso ai nostri dati in ogni momento delle nostre giornate, in treno o nella sala di attesa del medico, grazie a servizi sempre piú sofisticati e fornitori globali (come ad esempio *Blackberry*) che si occupano di archiviare la nostra posta in *server* localizzati al di fuori del Paese, e di recapitarcela istantaneamente, senza neppure la necessità di una nostra richiesta al *server*.

anche se sempre riconducibili alla medesima organizzazione che assume la responsabilità della conservazione, protezione e messa a disposizione tempestiva dei dati quando richiesti dai titolari. È facile, dunque, rendersi conto che tutto il quadro di fatto e di diritto del sistema ICT, almeno per la parte relativa al trattamento telematico dei dati, è in tumultuosa evoluzione. Va evidenziato che proprio la tecnologia *cloud*, che separa sempre di piú chi, avvalendosi del servizio, tratta i dati da chi li custodisce (il *provider*) e che implica inevitabilmente la loro custodia in enormi *server*, collocati in tutti i continenti, può determinare pericoli gravissimi non solo per il mondo delle imprese e per gli individui, ma anche per le grandi strutture pubbliche e private e, in particolare, quelle di giustizia e sicurezza. Sempre di piú enormi quantità di dati potranno essere allocati fuori dal controllo fisico e diretto delle autorità nazionali. Il rischio molto concreto è che fra questi vi siano anche dati di particolare valore per il funzionamento o la protezione delle nostre società, senza che siano adottate le necessarie misure di protezione e controllo. Si pensi, ad esempio, ai dati fondamentali per gli attori politici e istituzionali (dati relativi alle dichiarazioni dei redditi o a quelli contenuti nelle anagrafi e nei registri tenuti dalle pubbliche amministrazioni per le piú diverse finalità) e per il funzionamento delle moderne economie nazionali; o, ancora, a quelli necessari per la conoscenza della struttura e della composizione delle società (ad esempio i censimenti catastali), etc.

Il problema centrale delle tecnologie *cloud* è che esse possono rendere difficile per le Autorità nazionali sia l'accesso ai dati di loro interesse che la verifica in ordine alle misure di protezione adottate. Queste autorità, infatti, hanno un àmbito di competenza segnato dal limite territoriale, essendo il territorio, insieme alla popolazione e alla sovranità, l'elemento costitutivo di quella creazione giuridica sviluppatasi nella realtà del mondo non digitale chiamata Stato moderno. Dunque, ben difficilmente possono esercitare i loro poteri di *enforcement* al di fuori del proprio territorio, e questo obbliga tutti a interrogarsi se, e in che misura, sia possibile che, grazie al *cloud* e all'uso di *server* collocati in ogni parte del mondo, i dati siano trasferiti, senza vincoli e senza verifiche, al di fuori del territorio nazionale[25].

Non si tratta solo di interrogarsi su come far valere in questo nuovo contesto il limite da sempre posto dalla normativa europea circa il trasferimento di dati all'estero quando

[25] Evidenzia questi aspetti problematici, F. PIZZETTI, *Dati e diritti nell'epoca della comunicazione elettronica*, cit., p. 24 s.

manchino idonee garanzie da parte dei Paesi che li ricevono. La questione, cosí come ora si prospetta, è ancora piú importante. Si tratta, infatti, di trasferimenti di dati all'estero che possono rendere difficile non solo la difesa dei diritti dei cittadini interessati, ma anche la protezione delle nostre stesse società e delle loro informazioni strategiche.

Non vanno poi sottovalutati anche i problemi in materia di giurisdizione e di legge applicabile sia per quanto riguarda le regole che presiedono al trattamento dei dati, sia per quanto riguarda le decisioni relative alle eventuali controversie.

Altrettanto importante è la questione relativa alla portabilità o interoperabilità dei dati e, dunque, la migrazione degli stessi da un sistema *cloud* ad un altro o lo scambio di informazioni con soggetti che utilizzano servizi *cloud* di fornitori differenti.

Partendo dell'assunto per il quale il *cloud* ha senza dubbio ad oggetto la fornitura di servizi, piuttosto che la vendita di prodotti, come naturale conseguenza della sua genesi nella storia dell'informatica, occorre poi fornire una qualificazione giuridica al contratto con il quale si regolamenta il rapporto tra utente e fornitore. Sarà quindi indispensabile individuare la tipologia, *rectius* le tipologie, di contratto riconducibili al *cloud*[26].

Inoltre, non da sottovalutare potrebbe essere l'interrogarsi sulla natura della condivisione dei dati nella «nuvola» e sui suoi possibili risvolti pratici. In buona sostanza, l'utilizzatore del servizio *cloud* che archivia, memorizza, conserva, quindi, potremmo dire, conferisce i dati, le informazioni, i *file* etc. nella nuvola, cosí da condividerli con gli altri membri, ai quali consente l'accesso alla nuvola stessa, con la possibilità di visionarli e

[26] Si possono individuare alcuni tratti contrattuali comuni in tutte le tipologie di *cloud*. Eloquente risulta l'impegno dell'utente a consegnare al fornitore i propri dati e l'assunzione dell'obbligo di quest'ultimo di custodirli e restituirli su richiesta del primo, caratteri tipici del contratto di deposito, in cui l'utente si identificherebbe come depositante ed il fornitore come depositario. Sussistono, inoltre, forti analogie con il contratto di somministrazione, mentre ci si può anche interrogare sulla possibile ricorrenza dei caratteri del contratto di appalto o di quelli tipici del contratto di licenza d'uso. Per una esaustiva disamina della qualificazione giuridica del contratto in discorso si rinvia a M. D'AMBROSIO, *Cloud computing*, in *Manuale di diritto dell'informatica*, 3ª ed., a cura di D. Valentino, Napoli, 2016, p. 413 ss., il quale evidenzia però (p. 415) i limiti di un approccio tradizionale alla tematica in parola, ritenendo «poco opportuno» il tentativo di inquadrare il *cloud computing* all'interno di rigide figure negoziali tipiche o atipiche, essendo «innanzitutto necessario accertare quale diritto – di quale ordinamento – sia applicabile alla fattispecie in base alla pattuizioni delle parti. Successivamente, l'interprete è chiamato a ricostruire la funzione concreta del negozio e ad assicurare l'applicazione della disciplina piú adeguata alla cura degli interessi coinvolti, rintracciandola all'interno dell'ordinamento nel suo complesso mediante un'attività ermeneutica sistematica. Non si coglie, pertanto, una significativa utilità nel tentativo di ricondurre, aprioristicamente, la fattispecie del *cloud computing* all'interno di uno specifico modello negoziale, sia questo disciplinato o no dal legislatore. A fronte della poliedrica regolamentazione degli interessi, si potrà ricorrere alla disciplina ora dell'appalto e ora della locazione, ma legittimo può ritenersi, pure, il rinvio alla figura del contrato di licenza d'uso o alle norme in tema di somministrazione. La qualificazione del negozio deve avvenire con riferimento al concreto profilo causale dell'atto, sí da assicurare la migliore regolamentazione degli interessi della parti.».

scaricarli sul proprio strumento *hardware*, salvo il limite della cancellazione, attribuisce, a tali soggetti autorizzati all'accesso nella nuvola, un diritto? Se si, quale? Questa «autorizzazione» all'accesso alla nuvola, come può qualificarsi giuridicamente? Una volta autorizzati, cosa possono fare e/o non fare i membri della *cloud*? E se è l'amministratore stesso a perdere, distruggere, cancellare definitivamente quei dati che aveva voluto condividere con altre persone, sarà civilmente responsabile?

2. Definizione e descrizione del fenomeno del *cloud computing*.

È fondamentale partire dal significato dell'espressione «*cloud computing*», per poi dare, al fenomeno che essa espressione identifica, una definizione in grado di descriverne, compiutamente ed esaustivamente, i suoi elementi peculiari. Di conseguenza, sarà piú agevole individuare il panorama giuridico in cui muoversi e applicare, cosí, correttamente le disposizioni normative.

L'espressione «*cloud computing*»[27], letteralmente, significa «nuvola informatica» e, in buona sostanza, consiste in risorse informatiche distribuite in remoto. Tal è la definizione contenuta nel Parere del Comitato economico e sociale europeo sul tema «Il *cloud computing* in Europa» (parere d'iniziativa, 2001/C 24/08), in G.U.C.E. del 28 gennaio 2012.

Con tale termine ci si riferisce ad un insieme di tecnologie e di modalità di fruizione di servizi informatici che favoriscono l'utilizzo e l'erogazione di *software*, la possibilità di conservare e di elaborare grandi quantità di informazioni via *internet*.[28]

Esso costituisce, quindi, una forma d'immagazzinamento e archiviazione di dati, informazioni e contenuti digitali (*file*, fotografie etc.) in una piattaforma intangibile[29] (*rectius*

---

[27] Come rileva G. TROIANO, *Profili civili e penali del cloud computing nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore*, in *Cib. dir.*, 2011, Vol. 12, n. 3, p. 233, «[n]on esiste una definizione univoca di *cloud computing*. Il termine *cloud*, con ogni probabilità, deriva dalla rappresentazione grafica che in informatica si utilizza per indicare la rete Internet, una nuvola appunto. Il termine *computing*, invece, attiene alla progettazione e realizzazione di *hardware* e *software* per la gestione dei dati. […]. In buona sostanza, il termine *cloud computing* è utilizzato oggi per indicare le risorse informatiche (di un computer) collocate in più luoghi della rete Internet e tramite la stessa utilizzabili […]».

[28] Il *cloud* offre, a seconda dei casi, il trasferimento della conservazione o dell'elaborazione dei dati dai *computer* degli utenti ai sistemi del fornitore. Il *cloud* consente, inoltre, di usufruire di servizi complessi senza doversi necessariamente dotare né di *computer* e altri *hardware* avanzati, né di persone in grado di programmare o gestire il sistema. Sugli aspetti concernenti i vantaggi e i rischi del *Cloud computing*, v. *infra*, § 7 e 7.1.

[29] In questi termini, E. RENGIFO GARCÍA, *Computaciòn en la nube*, in *Revista la propiedad inmaterial*, 2013, n. 17, p. 223.

virtuale[30]); un nuovo modo di salvare e conservare dati sorto con lo sviluppo delle nuove tecnologie.

È, pertanto, quell'insieme di tecnologie che permette l'erogazione di un servizio offerto da un *provider* a un utente, consistente nel memorizzare/archiviare e/o elaborare dati, grazie all'utilizzo di risorse *hardware/software* che sono allocate in *internet*.[31]

La definizione maggiormente accettata dalla dottrina, per quanto concerne il *cloud computing*, è quella proposta dal *National Institute of Standards and Technology* (NIST) dell'*U.S. Departement of Commerce*, ossia: «*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 rapidely provisioned and released with minimal management effort or service provider interaction*».[32]

Secondo la codetta definizione, il *cloud computing* è caratterizzato da cinque elementi essenziali (*on-demand self-service, broad network access, resource pooling, rapid elasticity, measured service*), articolato in tre *service models* (*Software, Platform, Infrastructure*) e quattro *deployment models* (*private cloud, community cloud, public cloud, hybrid cloud*)[33].

Per intendere correttamente il suo concetto e la sua portata, la dottrina ha fatto ricorso alla seguente analogia: «si pensi al *cloud computing* come un servizio pubblico, come un servizio di energia elettrica. In un servizio di fornitura di energia elettrica, le parti contrattuali sono le grandi imprese fornitrici - che prestano il servizio - e i clienti – consumatori e imprese - che utilizzano e pagano per il servizio. Lo stesso modello di base

---

[30] Scrive G. COLANGELO, *L'enforcement del diritto d'autore nei servizi cloud computing*, in *Dir. aut.*, 2012, p. 175: «il *cloud computing* incarna pienamente l'immagine di un universo della conoscenza virtuale, rappresentando un paradigma in cui si genera un'astrazione delle risorse computazionali, le quali vengono offerte tramite Internet come servizio al di fuori del proprio ambiente e rese fruibili agli utenti a consumo (*pay-per-use*)». Siamo in presenza di un insieme di tecnologie e risorse informatiche non localizzate in un personal computer o in un altro dispositivo digitale ma accessibili direttamente online grazie allo sviluppo delle reti di comunicazione […]»; G. TROIANO, *Profili civili e penali del cloud computing*, cit., p. 237 s., individua nella virtualizzazione e nella ridondanza gli elementi peculiari del modello *cloud computing*.

[31] Cosí M.C. DE VIVO, *Il contratto e il cloud computing*, in *Rass. dir. civ.*, 2013, fasc. 4, p. 1001.

[32] P. MELL-T. GRANCE, *The NIST Definition of Cloud Computing*, 2011, disponibile al sito *Internet* «http://esre.nist.gov/publications/nistpubs/800-145/SP800-145.pdf». Si rifanno a codesta definizione, tra gli altri: G. COLANGELO, *L'enforcement del diritto d'autore*, cit., p. 175; E. RENGIFO GARCÍA, *Computaciòn en la nube*, cit., p. 223; M.C. DE VIVO, *Il contratto e il cloud computing*, cit., p. 1003; D. LÓPEZ JIMÉNEZ, *La "computación en la nube" o "cloud computing" examinada desde el ordenamiento jurídico español*, in *Rev. de Derecho de la Pontificia Universidad Católica de Valparaíso XL*, 2013, p. 694; G. TROIANO, *o.c.*, p. 233; C. FLICK-V. AMBRIOLA, *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, in *federalismi.it*, 2013, n. 6, p. 2, per i quali, sinteticamente: «il NIST […] definisce il *cloud computing* come un modello che abilita l'accesso tramite internet a risorse condivise di calcolo, utilizzabili dinamicamente ed efficacemente a fronte di limitate attività di gestione».

[33] G. COLANGELO, *o.c.*, p. 175.

esiste nel *cloud computing*. Le compagnie di servizi informatici come Google, Microsoft e Amazon sono i fornitori della nuvola. Gli utenti, consumatori e imprese, che utilizzano i servizi offerti dai fornitori sono i clienti della nuvola».[34]

In questo peculiare caso, i servizi somministrati sono risorse informatiche.[35]

In pratica accade che l'utente, attraverso un qualsiasi strumento tecnologico in grado di collegarsi a *internet*, può accedere a una determinata nuvola in grado di fornirgli i servizi o i dati richiesti; inoltre può «trasportare» i propri dati dal proprio dispositivo in una «nuvola» da lui stesso contattata, cosí da poterli avere sempre consultabili, ovunque si trovi.[36]

L'innovazione e il successo delle *cloud* (le nuvole informatiche) risiede nel fatto che, grazie alla raggiunta maturità delle tecnologie che ne costituiscono la base, tali risorse sono facilmente configurabili e accessibili via rete, e sono caratterizzate da particolare agilità di fruizione che, da una parte semplifica significativamente il dimensionamento iniziale dei sistemi e delle applicazioni mentre, dall'altra, permette di sostenere gradualmente lo sforzo di investimento richiesto per gli opportuni adeguamenti tecnologici e l'erogazione di nuovi servizi.

Il *cloud computing* è il risultato di un «percorso circolare nella storia dell'informazione».[37] Negli anni '80, quando i *computer* domestici non avevano risorse sufficienti per custodire ed elaborare tante informazioni, i dati erano memorizzati e processati attraverso i piú potenti sistemi informativi dei governi, dei centri di ricerca e delle istituzioni. Di questi sistemi si utilizzavano anche il linguaggio di programmazione e in molti casi venivano utilizzati come *repository* per dati o programmi, attraverso una «*sorta di cloud abusivo*». A partire dalla metà degli anni '90, con il drastico calo dei costi delle memorie e dei processori, l'utilizzatore informatico iniziò a custodire i dati sui sopporti presso il proprio domicilio privato o luogo di lavoro poiché, in sostanza aveva «*una percezione di maggior sicurezza nel tenere tutti i dati presso*

---

[34] Ricorre a tale analogia, per spiegare il fenomeno del *cloud computing*: E. RENGIFO GARCÍA, *Computaciòn*, cit., p. 224, il quale, a sua volta, richiama (in nota 2) T. J. CALLOWAY, *Cloud Computing, Clickwrap Agreements, and Limitation on Liability Clauses: A Perfect Storm?*, en: [http://scholarship.law.duke.edu/cgi/viewcontent cgi?article=1232&context=dltr].

[35] E. RENGIFO GARCÍA, *o.c.*, p. 224.

[36] M.C. DE VIVO, *Il contratto e il cloud computing*, cit., p. 1003.

[37] G. TROIANO, *o.c.*, p. 234, il quale richiama (in nota 3) G. ZICCARDI, *Cloud computing tra criminalità, investigazioni e (r)esistenza elettronica*, Roma, 2011 e G. ZICCARDI, *Hacker – Il richiamo della libertà*, Venezia, 2011.

do sé». Nel nuovo millennio il dato *«abbandona l'utente e ritorna sui grandi sistemi»*, nella nuvola, il piú delle volte anche inconsapevolmente[38].

Spesso utilizziamo tecnologie *cloud* senza neppure saperlo. Oggi, ad esempio, reti sociali come *Facebook* e *MySpace*, sistemi di posta elettronica, come il popolare «*gmail*» del motore di ricerca *Google*, ricorrono a questo servizio (si pensi a *Google Drive*[39] o a *Dropbox*[40], *ICloud*[41], *SkyDrive*[42], per esempio). Questi servizi sono, infatti, «sulle nuvole».

Infatti, acquisire servizi *cloud* significa acquistare presso un fornitore di servizio risorse (ad esempio *server* virtuali o spazio disco) oppure applicazioni (ad esempio posta elettronica e strumenti per l'ufficio). In tal modo:

• I dati non risiedono piú su *server* «fisici» dell'utente, ma sono allocati sui sistemi del fornitore (cosí si può fare a meno di copie in locale).

• L'infrastruttura del fornitore del servizio è condivisa tra molti utenti per cui sono fondamentali adeguati livelli di sicurezza.

• L'utilizzo del servizio avviene via *web* tramite la rete *internet*, che assume dunque un ruolo centrale in merito alla qualità dei servizi fruiti ed erogati.

• I servizi acquisibili presso il fornitore del servizio sono a consumo e, in genere, è facile far fronte a eventuali esigenze aggiuntive (ad esempio piú spazio disco o piú potenza elaborativa).

---

[38] La ricostruzione storica è di G. TROIANO, *o.c.*, p. 234, il quale, a sua volta, richiama (in nota 5,6,7) nel virgolettato in corsivo: G. ZICCARDI, *Cloud computing*, cit. e G. ZICCARDI, *Hacker – Il richiamo,* cit., ed evidenzia (in nota 8) come «il sistema operativo Android per dispositivi mobili, per esempio, prevede una sincronizzazione pressoché totale dei dati attraverso un account Google. *"[alla fine il telefono diventa meno importante: lo perdete, ne comprate un altro e quello nuovo diventa identico a quello vecchio […]"*».

[39] *Google drive* è il servizio di *cloud computing* offerto da *Google* ed è stato definito come «a place where you can safely store your files online and access them from anywhere» (M. PROCOPIO, *Instant Google Drive Starter*, Birmingham, 2013, p. 2).

[40] *Dropbox* è un programma multipiattaforma *cloud based* sviluppato da *Even- flow Inc.*, che offre un servizio di *hosting* e sincronizzazione automatica di documenti tramite *web*; come nota L. LORENZETTI, *Scrivere 2.0: Gli strumenti del Web 2.0 al servizio di chi scrive*, Milano, 2010, p. 58 s. «La particolarità di Dropbox è la possibilità per l'utente di utilizzare anche un client (*software*) apposito per la gestione dei file, gratuito e disponibile per Windows, Mac OS X e Linux. Questa applicazione crea automaticamente una cartella sul nostro computer chiamata «My dropbox», il cui contenuto è costantemente sincronizzato con il nostro spazio remoto sul server Dropbox».

[41] *ICloud* è il programma che ha sostituito il 6-6-2011 il noto *MobileMe*, fra gli antesignani del *cloud computing*. Su di esso v. le riflessioni di S. POIER, *As blurred as a cloud. Preliminary notes questioning some social-legal aspects of cloud computing*, in *Cib. dir.*, 2010, p. 319 s.

[42] *SkyDrive* è il servizio *cloud* offerto da *Microsoft*. Una tabella sinottica delle caratteristiche dei programmi evocati — di proprietà, rispettivamente, delle società *Dropbox* (già *Evenflow*), *Google*, *Apple* e *Microsoft* — è consultabile all'indirizzo http://www.androidworld.it/2012/04/24/google-drive-a-confronto-con-i cloud-dropbox-e -skydrive-con-sondaggio 85011/.

• Esternalizzare i dati in remoto non equivale ad averli sui propri sistemi: oltre ai vantaggi, ci sono anche delle controindicazioni che bisogna conoscere e approfondire.

Lo studio[43] *"Cloud Computing Report 2011"*, *Nextvalue report*, ipotizzava che nel 2015 il *cloud* sarebbe stato utilizzato da oltre 2,5 miliardi di persone con oltre dieci miliardi di apparati diversi collegati a *internet*.

Della sua importanza si è accorta anche la *DG Information Society and Media Directorate* (DG INFSO)[44] della Commissione europea che, nell'àmbito della *Digital Agenda for Europe*[45], ha inserito il *cloud* tra i temi prioritari da sviluppare entro il 2020 ed ha organizzato una consultazione pubblica per tutte le parti interessate.

2.1. Trattamento dei dati e utilizzo consapevole dei servizi *cloud.*

Non v'è dubbio che il tema *cloud computing* sia quanto mai popolare e ampiamente dibattuto per i suoi tanti vantaggi operativi e di riduzione dei costi, ma anche per i dubbi che si sollevano, soprattutto riguardo agli aspetti di sicurezza e di controllabilità dei dati, problematiche contrattuali, conformità alle leggi applicabili.[46]

Pertanto, in àmbito nazionale, il *cloud computing* è stato recentemente analizzato dall'Autorità garante per la protezione dei dati personali (Garante *Privacy*) che ha focalizzato l'attenzione degli utenti sui pericoli che può comportare un uso inconsapevole.

Quanto attiene agli aspetti di protezione dei dati personali e *privacy* assume, infatti, una particolare importanza, giacché i dati e il loro trattamento sono l'oggetto della maggioranza dei servizi offerti dal sistema *cloud*, che riguardano, già adesso e ancor di piú nel futuro,

---

[43] Aspetto evidenziato da G. TROIANO, *o.c.*, p. 235.

[44] Dal primo luglio 2015, la *DG Information Society and Media Directorate* (DG INFSO) ha cambiato il suo nome in *Directorate General for Communications Networks, Content and Technology* (DG CONNECT).

[45] L'Agenda digitale dell'UE è gestita dalla Direzione Generale della Commissione Europea per Le Reti di Comunicazione, contenuti e tecnologia (anche denominata DG Connect). Il nome individua la gamma degli argomenti in cui tale organismo è attivo e la sua struttura favorisce il lavoro della DG con le politiche chiave dell'UE per il prossimo decennio: garantire che le tecnologie digitali possono contribuire a realizzare la crescita che ha bisogno l'Unione europea . La DG *Connect* lavora per il Progetto «mercato unico digitale». *Team* guidato dal vicepresidente della Commissione europea, *Andrus Ansip*, e dal membro della Commissione europea responsabile per il mercato unico digitale, *Günther Oettinger*. Maggiori informazioni sulla DG *Connet*, quali priorità, obbiettivi principali, *mission* e struttura organizzativa sono disponibili al sito *web* http://ec.europa.eu/dgs/connect/.

[46] Aspetti, questi, che saranno affrontati singolarmente nel corso della trattazione.

pressoché tutti i contesti lavorativi nel settore privato, nella pubblica amministrazione e nel sociale.

Il Garante per la protezione dei dati personali è, quindi, intervenuto piú volte al fine di favorire un utilizzo consapevole e corretto del sistema *cloud*, in particolare, dettando accurate informazioni per l'utilizzo dello stesso in modo da tutelare al meglio i dati personali degli utenti che si affidano a un contratto di *cloud computing*. In tal senso, di notevole rilevanza è la Scheda di documentazione del 23 giugno 2011 "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi"*, nelle cui premesse si legge:

«L'Autorità nell'ottica di promuovere un utilizzo corretto delle nuove modalità di erogazione dei servizi informatici, specie per quelli erogati tramite cloud pubbliche (public cloud), che comportano l'esternazione di dati e documenti, ritiene opportuna e doverosa un'opera di informazione orientata a tutelare l'importante patrimonio informativo costituito dai dati personali. Tali indicazioni si propongono, quindi, di offrire un primo insieme di indicazioni utili a tutti gli utenti di dimensioni contenute e di limitate risorse economiche (singoli, piccole e medie imprese, amministrazioni locali quali i piccoli comuni, ecc.) destinatari della crescente offerta di servizi di cloud computing (pubbliche o ibride), con l'obiettivo di favorire l'adozione consapevole e responsabile di tale tipologia di servizi. Le avvertenze di seguito enucleate costituiscono un primo quadro di cautele che favoriscono il corretto trattamento dei dati personali attraverso l'utilizzo dei predetti servizi virtuali e, pertanto, si indirizzano anche ai fornitori, i quali possono fare riferimento a tali indicazioni nella predisposizione dei loro servizi, con l'accortezza di informare opportunamente gli utenti in ordine alla loro adozione. L'Autorità – nella consapevolezza che l'utilizzo dei servizi di cloud computing prefigura problematiche ben difficilmente risolvibili a livello nazionale che richiedono, invece, una riflessione condivisa a livello sia europeo sia internazionale, e in considerazione di tutte le sue implicazioni in relazione al trattamento dei dati personali – intende in ogni caso continuare a seguire l'evoluzione del fenomeno, anche partecipando con altri decisori internazionali a specifici tavoli di lavoro aperti in materia […]. L'autorità, inoltre, si riserva, laddove ne rilevasse la necessità, di

adottare in futuro specifiche e dettagliate prescrizioni indirizzate a utenti e fornitori, specie sotto il profilo delle misure si sicurezza»[47].

---

[47] Cfr. *"Cloud computing: indicazioni per l'utilizzo consapevole dei servizi"*. Scheda di documentazione dell'Autorità garante per la protezione dei dati personali pubblicata congiuntamente alla Relazione Annuale del 2010 - http://www.garanteprivacy.it/garante/document?ID=1819933. In questa sede, si ritiene opportuno riportare integralmente quella parte del documento che spiega come utilizzare consapevolmente i servizi offerti in *cloud computing*: *«6. Indicazioni per l'utilizzo consapevole dei servizi cloud. · Ponderare prioritariamente rischi e benefici dei servizi offerti. Prima di optare per l'adozione di servizi di cloud computing, è opportuno che l'utente verifichi la quantità e la tipologia di dati che intende esternalizzare (es. dati personali identificativi o meno, dati sensibili oppure particolarmente delicati come quelli genetici o biometrici, dati critici per la propria attività come ad esempio progetti riservati). È necessario innanzitutto valutare gli eventuali rischi e le possibili conseguenze derivanti da tale scelta sotto il profilo della riservatezza e della loro rilevanza nel normale svolgimento della propria attività. Tale analisi valutativa dovrà evidenziare l'opportunità o meno di ricorrere a servizi cloud (limitandone l'uso ad esempio a determinati tipi di dati), nonché l'impatto sull'utente in termini economici e organizzativi, l'indisponibilità, pur se parziale o per periodi limitati, dei dati esternalizzati o, peggio, la loro perdita o cancellazione.*

·Effettuare una verifica in ordine all'affidabilità del fornitore. Gli utenti dovrebbero ragionevolmente accertare l'affidabilità del fornitore prima di migrare sui sistemi virtuali i propri dati più importanti, tenendo in considerazione le proprie esigenze istituzionali o imprenditoriali, la quantità e la tipologia delle informazioni che intendono allocare nella cloud, i rischi e le misure di sicurezza. In funzione della tipologia di servizio che necessitano, oltre che della criticità dei dati, è opportuno che valutino la stabilità societaria del fornitore, le referenze, le garanzie offerte in ordine alla confidenzialità dei dati e alle misure adottate per garantire la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti. Gli utenti dovrebbero valutare, inoltre, le caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità. Ulteriori criteri in base ai quali è possibile valutare l'affidabilità di un fornitore emergono dall'impiego di personale qualificato, dall'adeguatezza delle infrastrutture informatiche e di comunicazione, dalla disponibilità ad assumersi responsabilità, esplicitamente previste dal contratto di servizio, derivanti da eventuali falle nel sistema di sicurezza o a seguito di interruzioni di servizio.

·Privilegiare i servizi che favoriscono la portabilità dei dati. È consigliabile ricorrere a servizi di cloud computing nelle modalità SaaS, PaaS o IaaS in un'ottica lungimirante, vale a dire privilegiando servizi basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi. Ciò al fine di scongiurare il rischio che eventuali modifiche unilaterali dei contratti di servizio da parte di uno qualunque degli operatori che intervengono nella catena di fornitura si traducano in condizioni peggiorative vincolanti o, comunque, per facilitare eventuali successivi passaggi da un fornitore all'altro.

·Assicurarsi la disponibilità dei dati in caso di necessità. Nell'utilizzo dei servizi di cloud computing, in assenza di stringenti vincoli sulla qualità formalizzati attraverso il contratto con il fornitore, si raccomanda di mantenere una copia di quei dati (anche se non personali) dalla cui perdita o indisponibilità potrebbero conseguire danni economici, per l'immagine o in generale relativi alla missione e alle finalità perseguite dall'utente. Ciò specie quando ci si affidi a servizi gratuiti o a basso costo quali, ad esempio, a servizi di hard-disk remoto, mail, soluzione per la conservazione documentale e così via, che potrebbero non presentare adeguate garanzie di disponibilità e prestazioni tipiche, invece, dei servizi professionali. Certamente, nel caso in cui i dati trattati non siano i propri, come avviene per aziende e pubbliche amministrazioni che raccolgono e detengono informazioni di terzi, l'adozione di servizi che non offrono adeguate garanzie di riservatezza e di continuità operativa può avere rilevanti ripercussioni nel patrimonio informativo dei soggetti cui i dati si riferiscono. In tal senso, il titolare del trattamento dei dati a fronte del contenimento di costi dovrà comunque provvedere al salvataggio (backup) dei dati allocati nella cloud, ad esempio creandone una copia locale (eventualmente sotto forma di archivio compresso), allo scopo di gestire gli eventuali rischi insiti nell'acquisizione di servizi che, pur con i vantaggi dell'economicità, potrebbero tuttavia non offrire sufficienti garanzie di affidabilità e di disponibilità.

·Selezionare i dati da inserire nella cloud. Alcune informazioni che si intende inserire sui sistemi del fornitore di servizio, per loro intrinseca natura, quali ad esempio i dati sanitari, genetici, reddituali, biometrici o quelli coperti da segreto industriale, possono esigere particolari misure di sicurezza. In tali casi, poiché dal relativo inserimento nella cloud consegue comunque una attenuazione, seppur parziale, della capacità di controllo esercitabile dall'utente, ed una esposizione di tali informazioni a rischi non sempre prevedibili di potenziale perdita o di accesso non consentito, l'utente medesimo dovrebbe valutare con responsabile attenzione se ricorrere al servizio di cloud computing oppure mantenere in house il trattamento di tali tipi di dati.

·Non perdere di vista i dati. È sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto anche verificando se i dati rimarranno nella disponibilità fisica dell'operatore proponente, oppure se questi svolga un ruolo di intermediario, ovvero offra un servizio progettato sulla base delle tecnologie messe a disposizione da un operatore terzo. Si pensi ad esempio a un applicativo in modalità cloud nel quale il fornitore del servizio finale (Software as a Service) offerto all'utente si avvalga di un servizio di

Anche in àmbito europeo, il *cloud computing* è stato oggetto di studi, tanto che il primo luglio 2012, il Consesso dei Garanti Europei per la protezione dei dati personali ha adottato un importante parere al riguardo[48].

---

stoccaggio dati acquisito da un terzo. In tal caso, saranno i sistemi fisici di quest'ultimo operatore che concretamente ospiteranno i dati immessi nella cloud dall'utente.

·Informarsi su dove risiederanno, concretamente, i dati. Sapere in quale Stato risiedono fisicamente i server sui quali vengono allocati i dati, è determinate per stabilire la giurisdizione e la legge applicabile nel caso di controversie tra l'utente e il fornitore del servizio. La presenza fisica dei server in uno Stato comporterà per l'autorità giudiziaria nazionale, infatti, la possibilità di dare esecuzione ad ordini di esibizione, di accesso o di sequestro, ove sussistano i presupposti giuridici in base al singolo ordinamento nazionale. Non è, quindi, indifferente per l'utente sapere se i propri dati si trovino in un server in Italia, in Europa o in un imprecisato Paese extraeuropeo. In ogni caso, l'utente, prima di inserire i dati nella nuvola informatica, dovrebbe assicurarsi che il trasferimento tra i diversi paesi in cui risiedono le cloud avvenga nel rispetto delle cautele previste a livello di Unione europea in materia di protezione dei dati personali, che esigono particolari garanzie in ordine all'adeguatezza del livello di tutela previsto dagli ordinamenti nazionali per tale tipo di informazioni.

·Attenzione alle clausole contrattuali. Una corretta e oculata gestione contrattuale può supportare sia l'utente, sia il fornitore nella definizione delle modalità operative e dei parametri di valutazione del servizio, oltre a individuare i parametri di sicurezza necessari per la tipologia di attività gestita. In ogni caso, è importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di cloud con riferimento ad obblighi e responsabilità in caso di perdita, smarrimento dei dati custoditi nella nuvola e di conseguenze in caso di decisione di passaggio ad altro fornitore. Costituiscono elementi da privilegiare la previsione di garanzie di qualità chiare, corredate da penali che pongano a carico del fornitore eventuali inadempienze o le conseguenze di determinati eventi (es. accesso non consentito, perdita dei dati, indisponibilità per malfunzionamenti, ecc.). Si suggerisce, inoltre, di verificare eventuali soggetti terzi delegati alla fornitura di servizi intermedi e che concorrono all'erogazione del servizio finale rivolto all'utente, ovvero la preventiva identificazione dei diversi fornitori successivamente coinvolti nel trattamento. Si raccomanda, infine, di accertare quale sia la quantità di traffico dati prevista dal contratto oltre la quale vengono addebitati oneri economici supplementari.

·Verificare le politiche di persistenza dei dati legate alla loro conservazione.

In fase di acquisizione del servizio cloud è opportuno approfondire le politiche adottate dal fornitore, che si dovrebbero poter evincere dal contratto, relative ai tempi di persistenza dei dati nella nuvola. Da una parte l'utente dovrebbe accertare il termine ultimo, successivo alla scadenza del contratto, oltre il quale il fornitore cancella definitivamente i dati che gli sono stati affidati. Dall'altra, il fornitore dovrà presentare adeguate garanzie, assicurando che i dati non saranno conservati oltre i suddetti termini o comunque al di fuori di quanto esplicitamente stabilito con l'utente stesso. In ogni caso, i dati dovranno essere sempre conservati nel rispetto delle finalità e delle modalità concordate, escludendo duplicazioni e comunicazioni a terzi.

·Esigere e adottare opportune cautele per tutelare la confidenzialità dei dati. Nell'ottica di proteggere la confidenzialità dei propri dati, l'utente dovrebbe valutare anche le misure di sicurezza utilizzate dal fornitore per consentire l'allocazione dei dati nella cloud. In generale si raccomanda di privilegiare i fornitori che utilizzano a tal fine tecniche di trasmissione sicure, tramite connessioni cifrate (specie quando i dati trattati sono informazioni personali o comunque dati che devono restare riservati), coadiuvate da meccanismi di identificazione dei soggetti autorizzati all'accesso, la cui complessità sia commisurata alla criticità dei dati stessi. Nella maggior parte dei casi risulta adeguato l'utilizzo di semplici meccanismi di identificazione, basati su username e password, purché le password non siano banali e vengano scelte di lunghezza adeguata. Nell'ipotesi in cui il trattamento riguardi particolari tipologie di dati - quali quelli sanitari, genetici, reddituali e biometrici o, più in generale, dati la cui riservatezza possa considerarsi "critica" - si raccomanda oltre all'utilizzo di protocolli sicuri nella fase di trasmissione, anche la conservazione in forma cifrata sui sistemi del fornitore di servizio.

·Formare adeguatamente il personale. Il personale preposto al trattamento di dati attraverso i servizi di cloud computing dovrebbe essere sottoposto a specifici interventi formativi, che evidenzino adeguatamente le modalità più idonee per l'acquisizione e l'inserimento dei dati nella cloud, la consultazione e in generale l'utilizzo dei nuovi servizi esternalizzati e delle indicazioni sin qui illustrate, allo scopo di mitigare rischi per la protezione dei dati derivanti non solo da eventuali comportamenti sleali o fraudolenti, ma anche causati da errori materiali, leggerezza o negligenza: circostanze queste che potrebbero dare luogo ad accessi illeciti, perdita di dati o, più in generale, trattamenti non consentiti».

[48] Parere 05/2012 sul Cloud Computing - WP 196, adottato il 1° luglio 2012, disponibile al sito *Internet*: http://ec.europa.eu/justice/policies/privacy/index_en.htm. Il Gruppo di lavoro per la tutela dei dati *ex* art. 29 è stato, appunto, istituito in virtú dell'articolo 29, della Direttiva 95/46/CE. È l'organo consultivo

Il parere in disamina evidenzia come la diffusione su vasta scala dei servizi *cloud computing* comporti una serie di rischi per la protezione dei dati personali e, in particolare, si segnala una mancanza di controllo sugli stessi, cosí come l'insufficienza d'informazioni in merito alle regole, al luogo e all'esecutore del trattamento/subtrattamento dei dati.

Si avverte come gli enti pubblici e le imprese private, che intendano avvalersi di servizi di *cloud computing*, debbano attentamente valutare questi rischi. Il parere esamina, poi, i problemi connessi alla condivisione di risorse con altre parti, la scarsa trasparenza di una catena di esternalizzazione, costituita da molteplici incaricati del trattamento e subcontraenti, la mancanza di un quadro di riferimento comune globale sulla portabilità dei dati e, inoltre, l'incertezza in merito all'ammissibilità del trasferimento di dati personali a fornitori di servizi *cloud* al di fuori del SEE.

Allo stesso modo, il parere pone l'accento sulla mancanza di trasparenza (aspetto fonte di grave preoccupazione), in termini d'informazioni che un titolare del trattamento è in grado di fornire a un interessato sulle modalità di trattamento dei suoi dati personali. Gli interessati devono innanzitutto essere informati su chi procede al trattamento dei loro dati e per quali finalità e per essere in grado di esercitare i diritti loro spettanti a tale proposito.

Il parere lancia un monito alle imprese e alle amministrazioni, che intendono utilizzare servizi di *cloud computing*, le quali dovrebbero innanzitutto eseguire un'analisi del rischio, completa e approfondita. Tutti i fornitori di servizi *cloud* nel SEE dovrebbero fornire al cliente tutte le informazioni necessarie per valutare correttamente i pro e i contro dell'adozione di un simile servizio. Sicurezza, trasparenza e certezza giuridica per i clienti dovrebbero essere princípi fondamentali alla base dell'offerta di servizi di *cloud computing*.

---

indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30, della Direttiva 95/46/CE e all'articolo 15 della Direttiva 2002/58/CE. Le funzioni di segreteria sono espletate dalla direzione C (Diritti fondamentali e cittadinanza dell'Unione) della Commissione europea, direzione generale Giustizia, B -1049 Bruxelles, Belgio, ufficio LX-46 01/190. Nel suddetto parere, il Gruppo di lavoro articolo 29 prende in esame tutte le questioni rilevanti per i fornitori di servizi di *cloud computing* operanti nello Spazio economico europeo (SEE) e per i loro clienti, specificando tutti i principi applicabili della direttiva UE sulla protezione dei dati (95/46/CE) e della direttiva *e-privacy* 2002/58/CE (modificata dalla direttiva 2009/136/CE), dove pertinenti. Senza dubbio, la diffusione del *cloud computing*, come paradigma tecnologico globale, rappresenta una sfida, come, del resto, è in qualsiasi processo evolutivo. Il parere in questione, pertanto, si può considerare un passo importante nel definire i compiti che la comunità della protezione dei dati dovrà assumere a questo proposito nei prossimi anni. Sul punto, v. anche l'analisi di G. MARCOCCIO, *Cloud Computing: l'Opinione dei Garanti Privacy Europei*, 2012, in *www.diritto.it*, disponibile all'indirizzo: http://www.diritto.it/docs/33706-cloud-computing-l-opinione-dei-garanti-privacy-europei.

Nelle raccomandazioni si mettono in evidenza le responsabilità del cliente di servizi *cloud* perché titolare del trattamento e si raccomanda, pertanto, che il cliente selezioni un fornitore che garantisca la conformità alla normativa UE in materia di protezione dei dati. Riguardo alla necessità di adeguate garanzie contrattuali, il parere prevede che un contratto tra cliente e fornitore di servizi *cloud* debba fornire garanzie sufficienti in termini di misure tecniche e organizzative. Risulta, quindi, sempre piú evidente come la formazione del rapporto contrattuale tra cliente e fornitore rappresenti uno snodo essenziale per una predisposizione coerente con le effettive necessità del cliente e gli adempimenti e le responsabilità richieste dalla legge.

Importante è anche la raccomandazione secondo cui il cliente dovrebbe verificare se il fornitore può garantire la legalità di eventuali trasferimenti transfrontalieri di dati.

3. La metafora della «nuvola».

Internet nasce come una rete di *computer* elaborata da accademici e ricercatori e finanziata dalle forze armate statunitensi, per poi essere aperta al mondo agli inizi degli anni novanta, così cambiando letteralmente il mondo che conoscevamo in precedenza[49].

L'*internet* originale era caratterizzato da una struttura orizzontale, dall'assenza di controlli, da un codice aperto e il suo *ethos* risiedeva nella condivisione (*sharing*)[50].

---

[49] Se prima del 1995 *Internet* era una rete dedicata alle comunicazioni all'interno della comunità scientifica e tra le associazioni governative e amministrative, dopo tale anno si assiste alla diffusione costante di accessi alla rete da parte di computer di utenti privati fino al *boom* degli anni 2000 con centinaia di milioni di *computer* connessi in rete, in parallelo alla diffusione sempre più spinta di PC al mondo, all'aumento dei contenuti e servizi offerti dal *Web* e a modalità di navigazione sempre più usabili, accessibili e *user-friendly*, nonché a velocità di trasferimento dati a più alta velocità di trasmissione passando dalle connessioni ISDN e V.90 alle attuali e ben note connessioni a banda larga tramite sistemi DSL.

[50] D. LAMETTI, *Cloud computing: verso il terzo Enclosures Movement?*, 2012, in *Riv. crit. dir. priv.*, p. 367 s., cosí descrive, usando delle metafore, la struttura (dell') *internet* originale: « – Una Rete orizzontale. […] serie di computer connessi a server che, a loro volta, sono tutti collegati tra loro. Tutti questi server permettono lo spacchettamento delle informazioni, che così circolano nella rete per poi essere riassemblate. […] Nessuna strada era obbligata per le informazioni nell'autostrada della rete. Non era necessario nessun percorso di controllo (o di restringimento), dal momento che erano presenti miriadi di percorsi informatici sui quali veicolare le informazioni spezzettate, fino alla loro destinazione finale per il riassemblamento. […] – Codice aperto. […] Internet è stato coscientemente concepito come una struttura aperta. Il termine rilevante in questo frangente è interoperabilità: tutte le parti sono state ideate per operare insieme. […] i primi programmatori dei protocolli internet – […] – scelsero appositamente di realizzare i propri codice sorgente operativi interoperabili, una pratica che continua tuttora, consentendo ai programmatori continue modifiche. […]. – Pochi punti di controllo e una fitta interazione tra gli utenti. Tale struttura orizzontale implica una decentralizzazione del potere. […] la presenza di utenti sparsi in tutto il mondo, dotati di elaboratori

In principio, quindi, il ricorso alla metafora della «nuvola» era usato, tradizionalmente nel mondo delle telecomunicazioni, come sinonimo di mezzo per la «trasmissione» delle informazioni che si consideravano disponibili, in modo permanente e trasparente, per un determinato utente. Quest'ultimo, nella maggior parte delle ipotesi, aveva interesse a che le sue informazioni fossero trasmesse secondo la sua necessità, senza doversi preoccupare della struttura sottostante.

La «nuvola» indicava, quindi, quella «rete» (mondiale) di *computer*, quale mezzo di comunicazione di massa, che offriva (e offre tutt'ora) all'utente una vasta serie di contenuti e servizi, divenendo cosí quel canale generalizzato della comunicazione, che oggi ben conosciamo. La nuvola, in atri termini, simbolizzava *internet*.

Adesso, quando ci si riferisce alla «nuvola», in considerazione del passaggio da *internet* al *cloud*[51], si allude a una metafora (potremmo dire, «nuova») che, senza dubbio, cambia sostanzialmente il suo significato, posto che alla «trasmissione», di dati (informazioni e altro), succede il «trattamento», degli stessi, in tutta la sua estensione del termine.

In altre parole, il «trattamento» (ossia la gestione, custodia, sicurezza, conservazione, portabilità, cancellazione etc.) dei dati diventa quell'aspetto peculiare (giacché connaturato in ogni suo servizio) del *cloud*, perno sul quale ruota tutto il fenomeno da esso rappresentato e, di conseguenza, centro gravitazionale di tutte le questioni e le problematiche ad esso relative. Tutto ruota intorno a tale aspetto, base sulla quale modellare i contratti e le tutele per i servizi *cloud*. Contratti che dovranno necessariamente ispirarsi al principio basilare della trasparenza (tra cliente ed interessati e tra cliente e fornitore), attraverso una loro predisposizione che ne garantisca chiarezza e completezza. Il trattamento dovrà, allora, essere limitato alle specifiche finalità consentite, assicurando la necessaria certezza nelle operazioni di conservazione e cancellazione dei dati, attraverso la predisposizione di (chiare) misure tecnico-organizzative all'uopo necessarie.

---

relativamente potenti, comporta pochi controlli e un'elevata autonomia. Proprio la pochezza dei controlli aumenta le possibilità degli utenti di poter stabilire essi stessi come useranno la rete […]. – Condivisione. L'ethos dominante di internet, a dispetto dei tentativi delle grandi aziende titolari di copyright, rimane la condivisione. Fin dall'inizio, i codici furono aperti e presto i contenuti vennero condivisi, in movimenti quali *wikis*. Ad ogni tentativo di soffocare tale condivisone, la tecnologia reagiva attraverso nuovi e più efficaci mezzi di sharing e diversi modelli d'impresa vennero costruiti su tale concetto […]».

[51] D. LAMETTI, *Cloud computing*, cit., p. 363 s., nel descrivere il passaggio dalla rete alla nuvola, parla di «cambio di metafore» e, piú specificamente (a p. 367), di «modifica del paradigma metaforico da internet alla *Cloud*».

Infatti, se da un lato il *cloud* consente la persistenza di un modello di *internet business* apparentemente libero, dall'altro garantisce, a coloro i quali stanno insidiando tale modello, sempre maggiore accesso a sempre maggiori quantità di dati. Tali preoccupazioni sono reali e devono imporre una riflessione: con un cosí grande numero d'informazioni personali depositate all'interno del *cloud*, non basta la semplice fiducia sociale ad assicurare che tali dati rimangano privati e siano utilizzati per i soli scopi ai quali il titolare degli stessi ha acconsentito.

Il nuovo, variegato (e, ancora, non compitamente esplorato) scenario che ora si manifesta, la nuvola appunto, nella sua nuova accezione, anche essendo molto conveniente, da una prospettiva prettamente commerciale, può, tuttavia, dar luogo a un meccanismo che trascuri, indipendentemente dai benefici che innegabilmente porta con sé, gli evidenti rischi riguardanti la riservatezza, sicurezza e legalità dei procedimenti di archiviazione e gestione da remoto di documenti informatici[52].

3.1. Da *internet* al *cloud*: le nuove metafore per descrivere il *cloud*.

Come esposto in precedenza, l'immagine tradizionale di *internet* era quella di una rete orizzontale di scambi e interazioni, con scarsi controlli, molti partecipanti (di cui molti muniti di elaboratori relativamente potenti), una sostanziale eguaglianza tra gli utenti in termini di potenza degli elaboratori e, di conseguenza, una grande quantità di capacità di elaborazione e di contenuti in condivisone.

Il *cloud computing* consente ai meccanismi di archiviazione ed elaborazione dati e ai servizi di rete di muoversi dal singolo *computer* (portatile, fisso o altro tipo di strumento) e da un *server* locale per unirsi al resto delle risorse raggruppate all'interno di un elaboratore o di una serie di elaboratori centralizzati. Tale operazione in linea di principio sposta i procedimenti informatici di archiviazione e elaborazione dalla periferia della rete al centro operativo del *cloud*. Cosí, ad esempio, se un utente di un programma tradizionale come *Word* o di un'applicazione *email* come *Outlook* compie tale operazione sul *computer* personale, al contrario, un'applicazione *cloud* come *Google Docs* o *Microsoft Office Live* per i *software word* o

[52] Evidenzia questi aspetti problematici del *cloud*, D. LÓPEZ JIMÉNEZ, *La "computación en la nube" o "cloud computing"*, cit., p. 691.

Gmail per le *email*, utilizza meccanismi informatici di elaborazione non locali ma centralizzati.

Attraverso un procedimento denominato *«virtualization»* un'interfaccia *software* si sostituisce ai precedenti collegamenti *hardware* e interagisce con gli apparecchi del cliente (come *Google* e i *Microsoft's servers*). Gli apparecchi del cliente sono convinti di relazionarsi esclusivamente con i programmi di elaborazione di un singolo *computer*, quando in realtà stanno condividendo taluni processi di elaborazione con un altro cliente o usando piú di un singolo *computer*. Il modello è dinamico e costruito in base ai bisogni dell'utente. Il risultato è un utilizzo dell'*hardware* piú efficiente e a costi piú contenuti: l'offerta di servizi *cloud*, come il deposito di dati *on line*, genera, in tal modo, maggiori profitti.

Possiamo, allora, ricorrendo a delle metafore, descrivere il *cloud* come segue.

- Una struttura centralizzata e gerarchica.

Attraverso la centralizzazione delle elaborazioni informatiche, in alcuni snodi chiave che fungono da punti d'accesso, il *cloud* impone una gerarchia all'interno della rete. In buona sostanza, si passa dalla struttura orizzontale caratteristica di *internet* a quella verticale tipica del *cloud*. Questo cambiamento rappresenta un elemento centrale del modello di *business* proprio del *cloud*[53].

- Punti di controllo reali.

Ecco cosí che, in un sistema centralizzato e gerarchico, come quello in discorso, diventano possibili tutte quelle attività impossibili in una rete decentralizzata e orizzontale. Infatti, la gerarchia del modello *cloud* inserisce maggiori controlli all'interno della rete, in coincidenza con i punti di immagazzinamento dei dati e dove si situano i meccanismi di elaborazione. Tali snodi offrono punti di controllo del traffico *online*, raccolgono dati, regolano gli accessi, fungono da censori, etc.[54]

---

[53] D. LAMETTI, *o.c.*, p. 378 s., mette in risalto la struttura verticale del sistema *cloud*, quale elemento centrale del modello di *business* proprio di esso, evidenziando che proprio «per questo motivo le aziende che forniscono i servizi *Cloud* stanno adottando una strategia di marketing aggressiva per poter vendere la «propria» *Cloud* agli utenti. I modelli individuati da questi *provider* garantiscono una serie di servizi utili che vengono erogati gratuitamente o a basso costo, così da invogliare gli utenti ad utilizzare una particolare *Cloud*, nella speranza che si fidelizzino. Un chiaro vantaggio è rappresentato dal costo davvero irrisorio dei servizi erogati, dato lo sviluppo di questa tecnologia, tutto ciò permette ai provider di mantenere i prezzi minimi durante il periodo di fidelizzazione. I *provider* di servizi *Cloud* conservano la struttura verticale aumentando i costi per l'utente che desidera spostarsi da un *provider* all'altro. Nel lungo termine, tali pratiche rafforzeranno il potere il potere dei *provider* nella loro relazione con gli utenti».

[54] D. LAMETTI, *o.c.*, p. 378 s., evidenzia come i grandi attori della rete – *Facebook*, *Amazon*, *Apple* e altri – si stiano attivando per attirare gli utenti nelle loro *Cloud* attraverso i loro punti di accesso o, come lo stesso li

- Sistemi chiusi (fuori dal mio *cloud*!).

La struttura verticale promossa dal *cloud* si basa, in buona sostanza, sulla fornitura di una serie di servizi integrati che, all'inizio, sono convenienti per gli utenti, per poi rivelarsi un mezzo per trattenerli all'interno del sistema del *cloud* stesso.[55]

Con sistema chiuso, si vuol significare che il *cloud computing* non si sottrae a quel concetto, formatosi nel mondo dell'economia, sin da tempi non sospetti, denominato *«vendor lock-in»*. È possibile, quindi, che l'utente resti vincolato all'utilizzo di «*standard* proprietari» scelti dal fornitore. Tale pratica presenta, essenzialmente, due rilevanti rischi:[56]

a) non sarà possibile l'esportazione dei dati se non nel formato di *standard* scelto dal fornitore, per cui, nel caso di risoluzione o cessazione del contratto non sarà agevole, almeno non a costi contenuti, il trasferimento degli stessi a un altro fornitore:

b) non sarà possibile, se non con sistemi e programmi che riconoscano lo «*standard* proprietario» utilizzato dal fornitore, l'interoperabilità con altri sistemi o programmi e, precipuamente, l'interconnessione e interazione dei sistemi informativi.

Questi rischi si chiamano anche, in termini economici, rischi di «monopolio»[57], che, date le caratteristiche ontologiche di tale forma di mercato, determina una situazione di vantaggio per il venditore, ben potendo lo stesso esercitare una forzatura sul compratore per indurlo a continuare ad acquistare a condizioni monopolistiche, costringendolo a portare aventi la scelta iniziale[58].

---

chiama, i propri «punti nodali». L'autore avverte circa la potenziale pericolosità di tali posti di controllo, i quali, per l'appunto, garantiscono che l'interezza del traffico, che scorre all'interno della nuvola, possa essere analizzato e sorvegliato. Infatti, lo stesso afferma: «sinora i punti di accesso sono stati liberi […], ma con l'evolversi della *Cloud*, si può andare incontro ad una situazione per la quale vi saranno meno punti di accesso e soprattutto controllori più potenti a sorvegliarli».

55 Riflessione di D. LAMETTI, *o.c.*, p. 379, il quale segnala altresí come la possibilità di creare incompatibilità tecnologiche per realizzare un modello d'impresa si sia accresciuta nel tempo e come le stesse incompatibilità tecnologiche siano il miglior mezzo di gestione e controllo dei diritti digitali che oggi esista. Testualmente: «[s]e l'obiettivo è l'esclusione, una riduzione dell'interoperatività è la migliore strategia», facendo il seguente esempio calzante: «è come se si costruisse un magnifico giardino circondato da mura, la visione di tale giardino viene garantita solo a coloro che sono all'interno e che normalmente sono anche gli stessi che hanno pagato per poterlo ammirare».

56 Evidenzia i rischi sottesi all'annosa questione del c.d. «*vendor lock-in*», G. TROIANO, *o.c.*, p. 241.

57 Evidenzia quest'aspetto, G. TROIANO, *o.c.*, p. 242. Nello stesso senso, prevede la formazione di monopoli come esito probabile, D. LAMETTI, *o.c.*, p. 380.

58 Se, ad esempio, si acquista una stampante a getto d'inchiostro, per la stessa saranno utilizzabili esclusivamente quelle cartucce della stessa marca. Quelle di marca diversa sono incompatibili con la stampante acquistata, per tanto si sarà costretti ad acquistare quelle determinate cartucce e non altre. L'inconveniente di tale pratica consiste nel fatto che le cartucce potrebbero avere un costo comparabile a quello della stampante. Lo stesso può valere per l'acquisto di certe macchine per il caffè che accettano solo alcune cialde.

In altri termini, l'adozione da parte del fornitore del servizio di tecnologie proprie può, in taluni casi, rendere complessa per l'utente la migrazione dei dati e documenti da un sistema *cloud* ad un altro o lo scambio di informazioni con soggetti che utilizzano servizi *cloud* di fornitori differenti, ponendo quindi a rischio la portabilità o l'interoperabilità dei dati. Questa evenienza potrebbe dare luogo a politiche commerciali poco trasparenti. In un primo momento, il fornitore potrebbe ad esempio presentare al cliente un'offerta di servizi *cloud* economicamente vantaggiosa e con adeguate garanzie a protezione dei dati. In un secondo momento, una volta acquisito il cliente, potrebbe invece cambiare le condizioni del contratto a proprio vantaggio con la certezza che il cliente – considerata l'impossibilità pratica di trasferire agevolmente i dati presso un altro fornitore e di recedere dal servizio – non potrà far altro che accettarle.

Storicamente ciò che evita o, quantomeno, attenua l'effetto *lock-in* è, sicuramente, l'esistenza di *standard* aperti, ossia utilizzabili da chiunque e sotto il controllo di nessuno.[59]

Standardizzazione è, quindi, l'antidoto contro il fenomeno del *«vendor lock-in»*, che è sempre piú elevato nel *cloud*.

Allora, per superare gli ostacoli derivanti dall'adozione di *standard* diversi l'Unione Europea ha adottato, con proprie definizioni istituzionali, il principio dell'interoperabilità[60].

Vista la rilevanza del *cloud* per il futuro dello sviluppo dell'informazione, l'interoperabilità dovrebbe essere considerata caratteristica imprescindibile dello stesso, dovendo quindi garantirsi la possibilità di scambio e trasmissione dei dati, cosí come la lettura e la scrittura sullo stesso *file*, utilizzando lo stesso protocollo per farlo.

Interoperabilità è standardizzazione sono aspetti complementari, due facce della stessa medaglia, dei *software* utilizzati nel *cloud*, infatti «l'assenza di interoperabilità non può che essere quindi mancanza di standardizzazione (di uso di standard comuni) nella fase di progettazione del programma».[61]

---

[59] In questo modo in uno stesso ufficio possiamo avere stampanti di diverse marche, l'importante è che accettino uno standard ISO per il formato della carta (ad esempio l'A4 nello standard ISO 216). Se ogni fornitore accettasse solo il proprio standard per la carta, e nessuno potesse offrire lo stesso, si sarebbe in una situazione insostenibile, con il rischio di pagare la carta molto di più di quanto la si paghi attualmente.

[60] Cfr. Considerando 10, 11 e 12 della Direttiva 91/250/CEE.

[61] G. TROIANO, *o.c.*, p. 242, il quale avverte sulle rilevanti conseguenze economiche dell'uso o meno di interoperabilità nello sviluppo di prodotti tecnologici. E testualmente riferisce che: «[s]e prodotti tra loro concorrenti non sono interoperabili (a causa della presenza di brevetti, segreti industriali o semplicemente mancanza di coordinazione nell'uso di standard comuni), il risultato non può che essere la nascita di un monopolio o il fallimento del mercato.».

Con il c.d. «*eEurope Action Plan*», la Commissione Europea si è impegnata a supportare l'interoperabilità dei servizi, ovviamente in forma digitale, offerti ai cittadini ed alle imprese che vivono e svolgono attività commerciali nell'àmbito del territorio dell'UE. Su tali basi è nato un progetto di studio da cui è scaturito il documento *European Interoperability Framework* (EIF)[62]. Inoltre, nell'àmbito dello "Europe 2020"[63], si inserisce la *Digital Agenda for Europe*[64] che ha tra le sue finalità essenziali l'interoperabilità e il *cloud*, appunto. Secondo questi princípi, la società dell'informazione può progredire e svilupparsi solo se si basa su piattaforme e *standard* aperti e interoperabili.

- *Streaming* e non *sharing* (una struttura fondata sui servizi).

Il *cloud* postula una struttura basata sui servizi. Gli utenti, invece di acquistare le copie di ciò che necessitano (e conservarle per sempre) o di scaricarle nel momento in cui non sono disponibili per la vendita (e conservarle per sempre), acquistano servizi di cui hanno bisogno[65]. *Ergo*, gli utenti sono meri ricevitori di informazioni, secondo il modello in esame, anziché essere condivisori di informazioni. Infatti, dal momento che interagiscono con la rete attraverso apparecchi dotati di minore capacità di elaborazione dati, gli utenti accettano passivamente i contenuti invece di generarli.[66] L'accesso ai servizi, pertanto, diviene cosí la regola e lo *streaming* precede lo *sharing* come paradigma descrittivo dominante.

- *Thin Clients*.

---

62 Lo scopo del quadro europeo di interoperabilità (EIF) è di: a) promuovere e sostenere l'erogazione di servizi pubblici europei, favorendo l'interoperabilità *cross-sectoral* e *cross-border*; b) guidare le amministrazioni pubbliche nel loro lavoro per fornire servizi pubblici europei a imprese e cittadini; c) integrare e legare insieme i vari quadri nazionali di interoperabilità (NIF) a livello europeo. Per *interoperability framework* si intende un approccio concordato di interoperabilità per le organizzazioni che desiderano a lavorare insieme per la fornitura congiunta di servizi pubblici . Nel suo àmbito di applicazione , essa specifica una serie di elementi comuni quali lessico, concetti, principi, politiche, linee guida, raccomandazioni, norme. L'interoperabilità è sia un prerequisito che un facilitatore per un efficiente sviluppo dei di pubblici servizi europei. L'interoperabilità risponde alla necessità di facilitare: la cooperazione tra le amministrazioni pubbliche con l'obiettivo di istituire servizi pubblici; lo scambio di informazioni tra le pubbliche amministrazioni per soddisfare i requisiti legali o impegni politici; la condivisione e il riutilizzo di informazioni tra le amministrazioni pubbliche al fine di aumentare l'efficienza amministrativa e ridurre la burocrazia per i cittadini e le imprese. Il risultato al quale esso mira è: il miglioramento dei servizi pubblici ai cittadini e alle imprese , facilitando il *one-stop –shop* nell'erogazione di servizi pubblici; ridurre i costi per le pubbliche amministrazioni , imprese e cittadini a causa della consegna efficiente di servizi pubblici. Per ulteriori informazioni v. il sito: http://ec.europa.eu/idabc/en/document/2319/5938.html.

63 Strategia a lungo termine adottata dalla Commissione Europea, per gli ultimi aggiornamenti si consulti il sito http://ec.europa.eu/europe2020/europe-2020-in-a-nutshell/index_it.htm.

64 Accennata al § 2 (nota 44).

65 D. LAMETTI, *o.c.*, p. 380, parla, richiamando e ringraziando per l'espressione coniata Dan Grecu, di modello «pay now for what you receive now», il quale espone gli utenti ad un rischio maggiore nel momento in cui non possono più permettersi il determinato servizio.

66 D. LAMETTI, *o.c.*, p. 380, avverte: «gli stessi modelli open software saranno più difficili da mantenere si i Cloud provider continueranno ad optare per dei sistemi chiusi».

I *client* sono dispositivi con scarsa capacità di elaborazione dati o che hanno bisogno di compiere elaborazioni informatiche per loro conto. I *thin client*, ossia *smartphone*, lettori musicali e *tablet*, compiono sono alcune funzioni specifiche e sono vòlti a facilitare l'utilizzo da parte di un utente medio. Infatti, per funzionare uno *smartphone* (o un dispositivo simile) non necessita di una capacità di elaborazione paragonabile a quella esercitabile da un computer «*general-purpose*»[67], sia fisso o portatile. Inoltre, tali dispositivi sono legati al loro particolare sistema operativo: le funzioni che possono eseguire e le applicazioni che sono eseguite sono settate o controllate (a distanza) dal sistema «madre». In tal modo non è possibile aggiungere una nuova funzione o è possibile farlo solo con estrema difficoltà[68]. La tipologia dei servizi offerti dal *cloud*, la sua struttura centralizzata e gerarchia, fa sí che i *thin client* abbiano una certa efficacia nel limitare gli utenti all'utilizzo delle sole funzioni considerate appropriate e necessarie dall'operatore del *cloud*.

In breve, è davvero difficile per un utente comprendere come utilizzare questi dispositivi per compiere un'operazione che esula dalle funzioni per le quali sono stati pensati e che non si serve di servizi e delle applicazioni create per tali scopi. Per queste ragioni, tali dispositivi differiscono notevolmente dai *computer* fissi e portatili. In conclusione, il modello che si fonda sul *thin client* comporta una maggiore dipendenza dalla *cloud*, in ogni aspetto: contenuti, applicazioni, cosí come per i servizi piú popolari (memoria digitale, *computing power*, etc.).[69]

---

[67] «In elettronica e informatica per dispositivi *general purpose* si intendono dispositivi elettronici che non siano dedicati ad un solo possibile utilizzo, ma dispositivi versatili che di solito caricano componenti *software* che sono invece soluzioni specifiche a una particolare esigenza. L'esempio che tutti abbiamo sotto gli occhi è sicuramente quello dei personal computer (PC). Questi *software* vanno personalizzati per poterli utilizzare in un contesto specifico. Al contrario vengono definiti *special purpose* quei dispositivi che vengono realizzati per compiti specifici. Possiamo intuire il significato di *special purpose* pensando ai dispositivi di controllo, installati sulle moderne autovetture, che segnalano eventuali guasti o anomalie». Cfr. voce *General purpose* all'indirizzo *web* https://it.wikipedia.org/wiki/General_purpose.

[68] D. LAMETTI, *o.c.*, p. 381, rende l'idea usando icasticamente il seguente esempio: «il giardino murato è accessibile solo a patto di utilizzare le applicazioni e i *software* predisposti dal sistema del giardiniere».

[69] D. LAMETTI, *o.c.*, p. 382 s., avverte «anche per coloro tecnologicamente più esperti, è arduo immaginare che questi apparecchi thin client possano garantire un facile accesso ai servizi IaaS e PaaS o a molti dei tanti servizi SaaS e di certo non attraverso un modello informatico libero e autonomo. Questi potenti servizi rimarranno riservati a coloro che continueranno a utilizzare gli apparecchi *general-purpose*.». L'autore concepisce il sistema *cloud* come spazio chiuso e organizzato gerarchicamente, soprannominandolo «*third enclosure movement*» (pag. 384).

4. Elementi caratterizzanti.

I servizi prestati attraverso il *cloud computing* presentano tre caratteristiche essenziali[70] che devono sussistere per potersi configurare il relativo contratto di servizi di *cloud*.

a) Lo schema di funzionamento del *cloud computing* consiste essenzialmente nell'archiviazione in maniera permanente dei dati in *server* e banche dati, accessibili attraverso *internet*. Quest'accesso ai *server,* tuttavia*,* non si realizza da parte di un solo cliente, ma i dati in esso contenuti sono condivisi da una pluralità di utenti, di modo che piú persone possono utilizzarli in maniera concorrente[71].

b) Il cliente, per accedere ai servizi prestati attraverso il *cloud computing*, basta che abbia un'adeguata struttura di telecomunicazioni che gli consenta l'accesso a *internet* (un *personal computer*, un *tablet* o, anche, uno *smartphone*), non essendo necessario l'installazione di nessun *software* aggiuntivo, dato che, abitualmente, si usano *browsers* o motori di ricerca par accedere a tutti i servizi offerti in *cloud*. Questa circostanza fa sí che il modello *cloud* abbia una maggiore compatibilità e capacità d'integrazione con il resto delle applicazioni informatiche di cui altresí dispongono le imprese clienti.

Il cliente si può avvalere unilateralmente del tempo di utilizzazione del servizio, della capacità di archiviazione nella rete, etc. secondo le necessità imprenditoriali di quel determinato momento, in modo rapido ed elastico e senza che si richieda l'interazione umana con il *provider* del servizio.

c) I sistemi informatici disponibili mediante *cloud computing* controllano e ottimizzano l'uso delle risorse in maniera automatica. L'uso di queste risorse da parte dei clienti può seguirsi, controllarsi e segnalarsi, il che conferisce un'enorme trasparenza nella gestione del contratto per entrambe le parti.

Queste caratteristiche implicano la necessità che i contratti di *cloud computing* contemplino questi aspetti mediante accordi personalizzati che contemplino i livelli delle prestazioni dei servizi con modelli precisi per la gestione delle informazioni, per la predisposizione di modelli d'isolamento e segmentazione dei suoi dati in relazione con i terzi, tenendo in

---

[70] Tali caratteristiche sono ben evidenziate da R. GARCÍA DEL POYO, *Cloud computing: aspectos jurídicos clave para la contratación de estos srvicios*, in *Revista Española de Relaciones Internacionales*, 2012, nº 4, p. 48 s.

[71] La dottrina iberoamericana, al riguardo, parla di modello di «*multiposesión*» (*multi tenancy*), individuando in esso un elemento caratterizzante i servizi di *cloud computing* (la c.d. *computación en la nube*). Sul punto, vedi R. GARCÍA DEL POYO, *Cloud computing: aspectos jurídicos clave*, cit., p. 49.

conto che i servizi si prestano sotto uno schema di condivisione (*esquema de multiposesion*[72]), senza dimenticare che il contratto deve altresí riflettere tutte le funzionalità che la nuvola permette di ottenere[73].

5. Modelli di «nuvole».

Esistono quattro forme fondamentali di prestazioni di servizi in *cloud*[74], distinguendosi, pertanto, tra *pubblic*, *private*, *community* e *ibrid cloud*, cosí da tener conto dell'utenza a cui è rivolta la fornitura dei servizi e l'uso delle risorse. Questi modelli differiscono essenzialmente per le caratteristiche dell'infrastruttura informatica utilizzata.

a) Il «*pubblic cloud*» è gestito da imprese prestatrici di codesto servizio e si rivolge a una pluralità di clienti (tanto il pubblico in generale, quanto un gruppo industriale, etc.) attraverso l'utilizzazione di *server*, di sistemi di archiviazione dei dati e altre infrastrutture che si utilizzano in forma condivisa.

Piú specificamente, l'infrastruttura è di proprietà di un fornitore specializzato in quest'àmbito tecnologico, il quale mette a disposizione degli utenti, e quindi condivide tra di loro, la propria infrastruttura garantendo l'erogazione via *web* di servizi, di capacità di calcolo e di memorizzazione permanente. La fruizione di tali servizi avviene tramite la rete *internet* e implica il trasferimento dei soli dati o anche dell'attività di elaborazione presso i sistemi del fornitore del servizio, il quale assume un ruolo importante in ordine all'efficacia delle misure adottate per garantire la protezione delle informazioni che gli sono state affidate. Con il *cloud* pubblico l'utente insieme ai dati, infatti, cede una parte importante del controllo esercitabile su di essi. Il «*pubblic cloud*» è rivolto a una platea di utenti, che, in molti casi, non hanno alcun rapporto tra di loro.

b) Il «*private cloud*» è quell'infrastruttura progettata in favore di un solo cliente, il quale decide gli utenti che sono autorizzati all'utilizzo della stessa e che controlla le applicazioni, i

---

[72] R. GARCÍA DEL POYO, *o.c.*, p. 50.

[73] R. GARCÍA DEL POYO, *o.c.*, p. 50.

[74] In merito si veda il *vademecum* del Garante per la protezione dei dati personali, CLOUD COMPUTING, PROTEGGERE I DATI PER NON CADERE DALLE NUVOLE, in *www.granteprivacy.it*, con il quale sono state offerte alcune indicazioni valide per tutti gli utenti, in particolare imprese e pubbliche amministrazioni, con l'obiettivo precipuo di far riflettere su alcuni importanti aspetti giuridici, economici e tecnologici nel settore in disamina e promuovere un utilizzo concreto delle nuove modalità di erogazione dei servizi informatici. Sul punto vedi anche: C. FLICK-V. AMBRIOLA, *Dati nelle nuvole*, cit., p. 2 s.; R. GARCÍA DEL POYO, *o.c.*, p. 51 s.

server, etc. In questo caso, l'infrastruttura, che è dedicata alle esigenze di un'unica organizzazione, può essere gestita in proprio (*in house*) oppure da un soggetto terzo (un semplice *hosting server* oppure un vero e proprio *outsourcer*). Il «*private cloud*» permette di consolidare l'infrastruttura e le applicazioni informatiche necessarie per la gestione delle risorse e l'erogazione dei servizi, a vantaggio di un significativo aumento di efficienza ed efficacia. La scelta delle tecnologie da adottare è affidata al responsabile informatico delle singole organizzazioni, si tratti di soggetti privati o pubblici.

c) Nel «*community cloud*» l'infrastruttura è utilizzata da utenti che hanno obiettivi comuni: una specifica comunità nel cui àmbito si condividono particolari obiettivi o esigenze (ad esempio finalità, requisiti di sicurezza, politiche di gestione). L'infrastruttura può essere gestita dalla stessa comunità o da un soggetto esterno e può essere organizzata come una rete. Questo modello è sovente ritenuto quello che piú corrisponde alle esigenze della pubblica amministrazione, intesa come insieme di organizzazioni distinte che operano in uno stesso contesto giuridico/amministrativo, che hanno analoghi requisiti di sicurezza, di conformità e di politiche di gestione e che possono così inter operare in maniera più efficace, imponendo – se del caso – al fornitore di adottare *standard* di sicurezza adeguati alle esigenze.

d) L'«*ibrid cloud*», il c.d. modello ibrido, detto anche *intermediate cloud*, si caratterizza, invece, per il fatto che l'infrastruttura è composta da due o piú tipi di *cloud*, separati tra loro, ma che condividono *standard* o tecnologie per la portabilità dei dati e l'interoperabilità delle applicazioni. Trattandosi di modelli derivanti dalla combinazione di piú tipologie di *cloud*, si può assumere che un ibrido rappresenti il secondo passo nell'approccio al *cloud computing*; una possibile configurazione ibrida può, ad esempio, prevedere l'utilizzo di servizi erogati da strutture private accanto a servizi acquistati da *cloud* pubblici.[75]

Le caratteristiche principali del *cloud computing*, comuni ai diversi modelli, possono essere cosí schematizzate:

- I dati elaborati e memorizzati nell'infrastruttura non risiedono fisicamente su risorse di calcolo dell'utente, ma del fornitore;

[75] C. FLICK-V. AMBRIOLA, *o.c.*, p. 3 s.

- L'infrastruttura è (o può essere) condivisa tra molti utenti, per cui è fondamentale da parte del fornitore l'adozione di sistemi di sicurezza che garantiscano la riservatezza dei dati e controllino i diritti di accesso all'infrastruttura;
- L'accesso all'infrastruttura avviene via *web* tramite *internet*, che assume dunque un ruolo centrale in merito al livello di qualità dei servizi fruiti e offerti;
- I servizi sono acquisibili a consumo dal fornitore, che può affrontare efficacemente le situazioni eccezionali in cui sono necessarie risorse aggiuntive rispetto a quelle utilizzate di norma[76].

6. Tipologie di servizi offerti dal *cloud*.

I servizi offerti dall'infrastruttura, in particolare da quella tipica del *public cloud*, possono essere a loro volta suddivisi in tre tipologie: a) *Infrastructure as a Service* (IaaS), *Software as a Service* (SaaS), *Platform as a Service* (PaaS)[77]. La parola chiave per tutti i modelli è virtualizzazione[78], ovvero, la creazione di una versione virtuale di una risorsa normalmente fornita fisicamente. Le memorie magnetiche di tipo stabile, ovvero le memorie che custodiscono dati attraverso la memorizzazione di tratti di un determinato supporto (per es. *hard disk*), con il *cloud* sono virtualizzate. Qualunque risorsa *hardware* o *software* può essere virtualizzata: sistemi operativi, server, memoria, spazio disco, sottosistemi[79].

a) *Infrastructure as a Service* (IaaS).

In questa tipologia di servizi, il fornitore mette a disposizione un'infrastruttura (ossia gli strumenti *hardware* e *software* di base quali: spazi di memoria, sistemi operativi, programmi di virtualizzazione, etc.) in sostituzione o in aggiunta a sistemi che l'utente ha già a disposizione. In questo caso, le risorse messe a disposizione dell'utente, non sono predefinite a priori, ma individuate di volta in volta, in base alle effettive esigenze che si

[76] C. FLICK-V. AMBRIOLA, *o.c.*, p. 3 s.
[77] In merito si veda il *vademecum* del Garante per la protezione dei dati personali, CLOUD COMPUTING, PROTEGGERE I DATI, cit.; vedi anche C. FLICK-V. AMBRIOLA, *o.c.*, p. 3 s.; R. GARCÍA DEL POYO, *o.c.*, p. 52 s.; G. TROIANO, *o.c.*, p. 237; E. RENGIFO GARCÍA, *o.c.*, p. 224.
[78] G. TROIANO, *o.c.*, p. 237 s., individua nella virtualizzazione e ridondanza le componenti essenziali del *cloud*. Come già visto, G. COLANGELO, *o.c.*, 2012, p. 175, parla di «universo della conoscenza virtuale» per spiegare il fenomeno *cloud*; mentre E. RENGIFO GARCÍA, *o.c.*, p. 224, sostanzialmente nello stesso senso, descrive la *"computación en la nube"* come piattaforma «intangibile».
[79] G. TROIANO, *o.c.*, p. 237 s.

presentano al momento. I fornitori del servizio in questione sono in genere operatori di mercato specializzati, che dispongono di un'infrastruttura tecnologica, complessa e spesso distribuita in aree geografiche diverse.

b) *Software as a Service* (SaaS).

Il fornitore, nel caso di SaaS, eroga direttamente i servizi via *internet*, spesso in sostituzione di quelli già installati dagli utenti sui loro sistemi. Tra i piú diffusi vi sono fogli di calcolo e strumenti di elaborazione dei testi, applicazioni per il protocollo informatico, rubrica dei contatti, calendari condivisi, sistemi di posta elettronica.

c) *Platform as a Service* (PaaS).

In questo terzo caso, il fornitore offre gli strumenti per sviluppare e ospitare le applicazioni. Generalmente questa modalità è rivolta a operatori di mercato che sviluppano in proprio applicazioni mirate sia all'assolvimento di esigenze interne che alla fornitura di servizi a terzi (ad esempio applicativi per la gestione finanziaria, della contabilità o della logistica). Il vantaggio consiste anche nel fatto che l'utente non si deve dotare di proprie risorse di calcolo o di applicazioni specifiche o aggiuntive. L'utente che usufruisce di questi strumenti non ha il controllo diretto dell'infrastruttura, salvo che non abbia a disposizione una piattaforma informatica che può gestire direttamente: in questo modo si configura una sorta di *private cloud* gestito direttamente dall'utente.

L'architettura informatica sottesa in ogni caso a tutte le specie le *species* del *cloud* è quella che consente l'interazione tra il *computer* dell'utente e quello del fornitore ovvero il sistema *client-server*. Tutte le applicazioni che comunicano tramite reti seguono quest'unico paradigma, senz'altro ciò avviene nel *cloud*.

I programmi che attendono passivamente di essere contattati sono detti *server*, mentre quelli che effettivamente contattano un destinatario sono detti *client*. In particolare nel *cloud*, il *client* si collega al *server* per accedere anche a risorse di *computing*, che gli consentono di elaborare dati e che, diversamente, dovrebbe richiedere localmente[80].

Oltre alla virtualizzazione, anche la ridondanza[81] è una componente essenziale del *cloud*, finalizzata alla ottimizzazione delle risorse informatiche. Infatti, quando, e se, gli algoritmi

---

[80] G. TROIANO, *o.c.*, p. 237 s., il quale (in nota 17) riprende il significativo esempio del *Chromebook* di *Google*, con il sistema operativo *Chrome OS*, sempre di *Google*.

[81] G. TROIANO, *o.c.*, p. 238, individua nella ridondanza un elemento peculiare del *cloud*. Ridondanza è l'installazione di un componente duplicato all'interno di un sistema così che, al guastarsi del componente primario, la riserva possa entrare in azione garantendo la continuità di funzionamento dell'apparato nel suo

di gestione delle stesse dovessero verificare la presenza di criticità o eccessivi «carichi di lavoro», tutte le risorse potrebbero essere spostate automaticamente su un altro *server* (operazione di c.d. *load balancing*). Di fatto, quindi, il *client* non accede sempre allo stesso *server*, ma a quello sul quale risultano essere collocate le risorse richieste. In tal guisa, la stabile e certa collocazione fisica dei dati viene meno. Questi possono essere memorizzati contemporaneamente sui diversi *server*, collocati anche in stati al di fuori dell'UE in Paesi che non offrono un'adeguata tutela.[82]

7. Benefici del *cloud computing*.

Dal punto di vista degli utenti, diversi sono i vantaggi dell'utilizzo del *cloud computing*.

Poiché le risorse e le applicazioni sono direttamente accessibili via *internet*, l'utente che se ne avvale non deve acquisire beni caratterizzati da una rapida obsolescenza, ma può ottenerli sotto forma di servizio; gli utenti non devono occuparsi direttamente della gestione dell'infrastruttura, lasciando tale compito a terzi; i dati possono essere trattati in remoto tramite *internet* e generalmente senza dover installare in locale applicazioni specifiche; è possibile disporre di spazi di memoria, anche di grandi dimensioni, dove archiviare i propri documenti senza utilizzare supporti esterni.

Infine, il fatto che le risorse, comprese le infrastrutture necessarie per rendere disponibili i servizi, siano generalmente condivise tra molti utenti, permette di ottenere economie di scala e di garantire elevati livelli di sicurezza a costi ragionevoli.

Di certo il modello *cloud* presenta grandi opportunità. Il raggruppamento di risorse reso possibile da un tale strumento comporta un fondamentale abbassamento dei costi (attraverso un abbattimento dei costi per i *provider* con conseguente diminuzione del costo dei servizi offerti agli utenti), maggiore capienza dei depositi *on line*, un impiego piú

---

insieme. Essa consiste nella duplicazione dei componenti critici di un sistema con l'intenzione di aumentarne l'affidabilità e la disponibilità, in particolare per le funzioni di vitale importanza per garantire la sicurezza delle persone e degli impianti o la continuità della produzione. Cfr. Wikipedia, consulta indirizzo *web* https://it.wikipedia.org/wiki/Ridondanza_(ingegneria).

[82] Aspetto questo messo in evidenza da G. TROIANO, *o.c.*, p. 238, il quale riporta come esempio l'informativa sulla *privacy* (*Privacy Policy*, alla pagina http://www.google.co.uk/intl/en/privacy/privacy.html) dei prodotti e servizi di *Google* (tra i quali *Gmail*, *Calendar*, *Docs*, *Groups*, *Web Search*, *Picasa* ecc.), cui milioni di utenti affidano i propri dati personali e sensibili, ove si legge testualmente: *"Google processes personal information on our servers in the United States of America and in other contries. In some cases, we process personal information outside your own country"*.

efficiente della capacità di elaborazione informatica in eccesso (e nuovi modelli di *business* basati su tale sfruttamento) che implicano un uso più produttivo della latenza e un miglior utilizzo dell'*hardware*. E può anche significare una maggiore affidabilità nel lungo termine.[83]

7.1. *Segue*. Rischi.

Il prezzo da pagare per ottenere i vantaggi sopra elencati sta nella necessità di trasformare in servizi erogati da altri delle attività in precedenza gestite in proprio. Ciò comporta, per l'utente, una potenziale perdita di controllo sui dati propri o trattati per conto terzi (clienti, cittadini e quant'altro), nonché la cessione di un potere notevole nelle mani del fornitore.

Piú in generale, se vi sono pochi soggetti (società multinazionali) idonei a erogare i servizi, si corre il rischio di concentrare nelle loro mani un'ingente e preziosa quantità di dati (i c.d. *Big Data*).

Come anticipato, poiché l'utente può accedere via *internet* ai suoi dati, le risorse fisiche in cui questi dati sono effettivamente conservati risiedono in un luogo diverso da quello da cui avviene l'accesso. La complessità dell'infrastruttura, nonché la sua dislocazione in luoghi sconosciuti all'utente, anche al di fuori dei confini nazionali, oltre a determinare difficoltà oggettive nell'individuazione dell'esatto luogo di conservazione dei dati, rende difficile anche l'esatta conoscenza del loro spostamento da una sede all'altra, per esigenze di carattere organizzativo, tecnico o economico del fornitore. L'utente non può, quindi, sapere dove si trovino in un certo momento i dati trattati dall'infrastruttura e se la normativa del paese in cui l'infrastruttura è fisicamente ospitata garantisce il rispetto dei diritti tutelati nel paese, ove egli risiede.

In secondo luogo, le caratteristiche di qualità dell'infrastruttura devono essere tali da assicurare sia la disponibilità continua dei servizi che la sicurezza dei dati. Ne consegue la necessità di garantire, e rispettivamente di assicurarsi, che a fronte di una specifica richiesta da parte dell'utente vi siano da un lato la disponibilità del servizio, dall'altro l'accessibilità ai dati.

[83] D. LAMETTI, *Cloud computing: verso il terzo Enclosures Movement?*, 2012, in *Riv. crit. dir. priv.*, p. 377.

È inoltre indispensabile assicurare la riservatezza dei dati rispetto ad accessi non autorizzati, ciò in considerazione del fatto che generalmente i fornitori custodiscono dati di singoli o di organizzazioni diverse, che potrebbero avere esigenze o interessi differenti, se non addirittura contrastanti.

Infine, l'adozione da parte del fornitore di proprie tecnologie (*close source*) può non garantire l'interoperabilità con altre infrastrutture, rendendo complessa per l'utente la portabilità dei dati e lo scambio di informazioni con soggetti che utilizzano servizi di fornitori differenti. A questo proposito non si può trascurare che l'eventuale fornitura dei servizi di *cloud computing* da parte di pochi soggetti può determinare anche un aumento dei costi connessi al passaggio da un fornitore all'altro e da un modello a uno differente.

8. Legge applicabile e giurisdizione competente.

Per l'individuazione della legge che regolerà il contratto e radicherà la giurisdizione competente per le controversie tra utente e fornitore in un contratto di servizi *cloud*, occorre prendere in esame il Regolamento CE n. 593/2008 (denominato Roma I) ed il Regolamento CE n. 44/2001.

L'art. 3[84] del Regolamento CE n. 593/2008 sancisce il principio della libertà di scegliere la legge regolatrice del contratto[85]. La libertà di scelta è ampia: difatti la scelta di legge può essere anche tacita (art. 3.1) ed i contraenti possono rinviare alla legge di un Paese con cui il

[84] Articolo 3 (Libertà di scelta), del Regolamento CE n. 593/2008, recita:
1. Il contratto è disciplinato dalla legge scelta dalle parti. La scelta è espressa o risulta chiaramente dalle disposizioni del contratto o dalle circostanze del caso. Le parti possono designare la legge applicabile a tutto il contratto ovvero a una parte soltanto di esso.
2. Le parti possono convenire, in qualsiasi momento, di sottoporre il contratto ad una legge diversa da quella che lo disciplinava in precedenza per effetto di una scelta anteriore effettuata ai sensi del presente articolo o per effetto di altre disposizioni del presente regolamento. Qualsiasi modifica relativa alla determinazione della legge applicabile, intervenuta posteriormente alla conclusione del contratto, non ne inficia la validità formale ai sensi dell'articolo 11 e non pregiudica i diritti dei terzi.
3. Qualora tutti gli altri elementi pertinenti alla situazione siano ubicati, nel momento in cui si opera la scelta, in un paese diverso da quello la cui legge è stata scelta, la scelta effettuata dalle parti fa salva l'applicazione delle disposizioni alle quali la legge di tale diverso paese non permette di derogare convenzionalmente.
4. Qualora tutti gli altri elementi pertinenti alla situazione siano ubicati, nel momento in cui si opera la scelta, in uno o più Stati membri, la scelta di una legge applicabile diversa da quella di uno Stato membro ad opera delle parti fa salva l'applicazione delle disposizioni di diritto comunitario, se del caso, come applicate nello Stato membro del foro, alle quali non è permesso derogare convenzionalmente.
5. L'esistenza e la validità del consenso delle parti sulla legge applicabile sono disciplinate dagli articoli 10, 11 e 13.

[85] Quello della scelta delle parti è, quindi, il «primo criterio di collegamento».

contratto non ha alcun altro legame obiettivo (art. 3.3), sottoporre parti distinte dell'accordo a leggi diverse (art. 3.1) e determinare la *lex contractus* prima o dopo la sua stipulazione, eventualmente modificando una loro scelta anteriore (art. 3.2). Vi sono tuttavia alcuni limiti alla libera scelta di legge: anzitutto la convenzione non consente la scelta della *lex mercatoria*[86] o comunque di una normativa di origine non statale come *lex contractus* e conseguentemente il richiamo che i contraenti vi effettuano ha efficacia soltanto nei limiti in cui esso è riconosciuto dalla legge statale applicabile al contratto; ed inoltre l'art. 3.3 sottopone i contratti interni alle norme inderogabili dello Stato in cui essi sono localizzati quando la legge scelta dalle parti come *lex contractus* li pregiudica[87].

A parte questi limiti, è chiaro che il fornitore di servizi *cloud* predeterminerà quasi sempre una clausola contrattuale nella quale indicherà la legge di uno Stato che regolamenterà il contratto e nella scelta, ovviamente, terrà conto solo delle sue esigenze.

Per ostacolare l'operatività di questo meccanismo, palesemente in danno dell'utente finale dei servizi *cloud*, si potrebbe ritenere, come sostenuto in dottrina[88], che il criterio in parola, ossia quello della scelta di legge, non costituisca un criterio di collegamento di natura internazionalprivatistica. Secondo questa impostazione, l'art. 3 non può pertanto essere assimilato alle norme di conflitto che devono rinviare ad un diritto di origine statale,

---

[86] La dottrina individua nell'azione della c.d. *lex mercatoria* un ulteriore fenomeno di limitazione al normale funzionamento della norma di diritto internazionale privato. Essa può essere definita come un insieme di norme, condizioni generali di contratto, clausole *standard*, prassi uniformi, vigenti in alcuni settori del commercio internazionale. Tale sistema si caratterizza per l'origine non statale: si tratta di norme derivanti o dalla volontaria e ripetuta osservanza di determinate regole da parte di operatori economici (*lex mercatoria* consuetudinaria)o dalla codificazione espressa formulata, sulla base dell'esperienza degli operatori e della maggiore idoneità a soddisfarne le esigenze di tutela e certezza, delle associazioni di categoria di organizzazioni internazionali non statali. Si possono ricordare i c.d. *Incoterms*, un prontuario delle pratiche standard dei contratti di vendita e le raccolte di regole ed usi uniformi effettuate e periodicamente aggiornate dalla Camera di Commercio internazionale. Tra le clausole di *lex mercatoria* piú diffuse si possono ricordare quelle relative al trasporto di merci c.d. FOB sul rischio di perimento durante il trasporto e CIF sull'assicurazione del trasporto o carico del venditore. La *lex mercatoria*, quindi, costituisce una garanzia di terzietà delle fonti del diritto e, pertanto, assicura una potenziale situazione di parità alle parti.

[87] La convenzione definisce opportunamente all'art. 3.3 queste norme inderogabili come «disposizioni imperative». Esse sono quelle norme che non possono essere derogate dai privati secondo il diritto interno di uno Stato. Le norme imperative si distinguono dalle disposizioni di applicazione necessaria. Queste ultime sono tutte quelle norme che vogliono applicarsi anche alle fattispecie con caratteri di estraneità. A ben veder alcune norme imperative possono costituire anche norme di applicazione necessaria: ciò si verifica quando esse sono non soltanto inderogabili ma anche desiderose di applicarsi a situazioni internazionali. Per una piú ampia disamina sul punto si rinvia a B. UBERTAZZI, *Il regolamento Roma I sulla legge applicabile alle obbligazioni contrattuali,* Milano, 2008, p. 121 ss.

[88] G. CARELLA, *La scelta della legge applicabile da parte dei contraenti*, in AAVV., *Il nuovo diritto europeo dei contratti: dalla Convenzione di Roma al Regolamento Roma I,* Milano*,* 2007, p. 82, critica l'art. 3 della convenzione, ritenendo che la scelta di legge «svolge la funzione di esercizio dell'autonomia sostanziale internazionale» e non costituisce quindi un criterio di collegamento di natura internazionalprivatistica.

ma dev'essere ricompreso in quelle relative all'autonomia sostanziale; quest'ultima può essere esercitata senza limiti (salvo ovviamente il rispetto delle norme inderogabili); le parti devono pertanto poter richiamare liberamente norme non statali di qualunque natura. Se si segue tale ragionamento, ne consegue che l'art. 3.2 è ingiustamente limitativo di tale scelta. Opererebbe cosí un limite all'applicazione della norma straniera all'uopo indicata dal fornitore di servizi *cloud*, e a questi piú favorevole, con riemersione della *lex mercatoria* che, costituendo una garanzia di terzietà delle fonti del diritto, assicurerebbe una potenziale situazione di parità alle parti.

In assenza di scelta della legge regolatrice il contratto è regolato dalla legge individuata dall'art. 4[89] della convenzione. Questa disposizione è estremamente complessa. Il suo comma 1 sancisce infatti il c.d. principio di prossimità, secondo cui il contratto deve essere regolato dalla legge dello Stato con cui è piú strettamente collegato. L'art. 4.2 concretizza il comma 1 e pone una presunzione per cui l'accordo è maggiormente collegato allo Stato in

---

89 Articolo 4 (Legge applicabile in mancanza di scelta), del Regolamento CE n. 593/2008, recita:
1. In mancanza di scelta esercitata ai sensi dell'articolo 3 e fatti salvi gli articoli da 5 a 8, la legge che disciplina il contratto è determinata come segue:
a) il contratto di vendita di beni è disciplinato dalla legge del paese nel quale il venditore ha la residenza abituale;
b) il contratto di prestazione di servizi è disciplinato dalla legge del paese nel quale il prestatore di servizi ha la residenza abituale;
c) il contratto avente per oggetto un diritto reale immobiliare o la locazione di un immobile è disciplinato dalla legge del paese in cui l'immobile è situato;
d) in deroga alla lettera c), la locazione di un immobile concluso per uso privato temporaneo per un periodo di non oltre sei mesi consecutivi è disciplinata dalla legge del paese nel quale il proprietario ha la residenza abituale, purché il locatario sia una persona fisica e abbia la sua residenza abituale nello stesso paese;
e) il contratto di affiliazione (franchising) è disciplinato dalla legge del paese nel quale l'affiliato ha la residenza abituale;
f) il contratto di distribuzione è disciplinato dalla legge del paese nel quale il distributore ha la residenza abituale;
g) il contratto di vendita di beni all'asta è disciplinato dalla legge del paese nel quale ha luogo la vendita all'asta, se si può determinare tale luogo;
h) il contratto concluso in un sistema multilaterale che consente o facilita l'incontro di interessi multipli di acquisto e di vendita di terzi relativi a strumenti finanziari, quali definiti all'articolo 4, paragrafo 1, punto 17, della direttiva 2004/39/CE, conformemente a regole non discrezionali e disciplinato da un'unica legge, è disciplinato da tale legge.
2. Se il contratto non è coperto dal paragrafo 1 o se gli elementi del contratto sono contemplati da più di una delle lettere da a) ad h), del paragrafo 1, il contratto è disciplinato dalla legge del paese nel quale la parte che deve effettuare la prestazione caratteristica del contratto ha la residenza abituale.
3. Se dal complesso delle circostanze del caso risulta chiaramente che il contratto presenta collegamenti manifestamente più stretti con un paese diverso da quello indicato ai paragrafi 1 o 2, si applica la legge di tale diverso paese.
4. Se la legge applicabile non può essere determinata a norma dei paragrafi 1 o 2, il contratto è disciplinato dalla legge del paese con il quale presenta il collegamento più stretto.

cui ha la propria residenza abituale il debitore della c.d. "prestazione caratteristica"[90]. La presunzione dell'art. 4.2 è tuttavia derogata per i contratti relativi a beni immobili e per quelli di trasporto di merci, che vengono sottoposti dall'art. 4 co. 3 e rispettivamente co. 4 alla *lex rei sitae* ed alla legge dello Stato in cui il vettore ha la sua sede principale al momento della conclusione del contratto. L'art. 4.5 sancisce infine la c.d. clausola d'eccezione: in deroga all'art. 4.2 quando la prestazione caratteristica non può essere determinata e all'art. 4 co. 2, 3 e 4 quando il contratto ha un legame più significativo con uno Stato diverso da quello di residenza del prestatore caratteristico: perché in questi ultimi casi la legge regolatrice è individuata in base all'art. 4.1.

È, allora, da chiarire il rapporto tra i co. 1, 2 e 4, che non sembrerebbe essere molto chiaro. Il punto è chiarire se il comma 2 dell'art. 4 (criterio della prestazione caratteristica) costituisca una regola vincolante o un mero criterio giuda, tale da poter essere liberamente derogabile e, quindi, specificare i suoi rapporti con il co. 4 (che prevede il principio del collegamento più stretto): norma eccezionale e, quindi, da interpretare in modo restrittivo, o invece generale (ossia disposizione centrale dell'art. 4) e quindi tale da giustificarne un'interpretazione estensiva?

La questione, non meramente teorica, presenta notevoli risvolti pratici, poiché se il principio del collegamento piú stretto è la disposizione centrale dell'art. 4 e può essere interpretato in modo estensivo, non occorrerà piú ricercare la prestazione caratteristica del contratto, ma sarà possibile individuare direttamente lo Stato a cui esso è maggiormente collegato *ex* art. 4 co. 4, ed applicarne la relativa legislazione contrattuale. In tal caso, però, l'organo giudicante disporrà conseguentemente di una grande discrezionalità, così generandosi una situazione di incertezza giuridica.

Venendo al tema dei servizi *cloud*, individuata la «prestazione caratteristica», in base al comma 2, nella fornitura di servizi, si applicherà la legge del paese in cui il fornitore dei servizi, ossia colui che tale prestazione deve effettuare, ha la residenza abituale. Pertanto, se, ad esempio, il nostro fornitore risiede negli Stati Uniti, si applicherà tale legge, alla quale sarà soggetto l'utente italiano, che con tale fornitore ha stipulato il contratto. Se, invece, si interpreta estensivamente il co. 4, si applicherà al contratto la legge dello Stato con il quale

[90] Sul criterio della prestazione caratteristica v.: M. MAGAGNI, *La prestazione caratteristica nella convenzione di Roma del 19 giugno 1980*, Milano, 1989; M. E. ANCEL, *La prestation caractéristique du contrat*, Paris, 2002.

esso è maggiormente collegato. Nel nostro esempio, occorrerà a questo punto chiarire a quale Stato, gli Stati Uniti o l'Italia, il contratto ha il collegamento piú stretto.

Allora, da un lato la certezza della residenza abituale del fornitore, dall'altro l'incertezza del principio del collegamento piú stretto (quasi che sarebbe preferibile l'incerto per il certo), fanno si che, in ogni caso, è altamente probabile (o quasi certo) che non si applicherà la legge del paese nel quale l'utente risiede. Ben si comprende come l'utente rischia di essere privato della tutela che la propria legge nazionale gli garantisce.

Di tale tutela non può però essere privato l'utente consumatore. Infatti, anche se la *lex contractus* ed il giudice competente sono stati predeterminati, la scelta effettuata incontra dei limiti in materia di contratti con i consumatori.[91]

I contratti con i consumatori sono attualmente regolati dall'art. 6[92] della convenzione, che permette la scelta di legge, ma la sottopone al limite del necessario rispetto delle norme imperative dell'ordinamento che avrebbe altrimenti regolato il contratto in mancanza di *electio iuris*, quando esse siano piú favorevoli al consumatore; ed utilizza come criterio di

---

[91] Ai sensi dell'art. 6 del Regolamento CE n. 593/2008 e dell'art. 15 del Regolamento CE n. 44/2001 il consumatore è la persona fisica che conclude un contratto per scopi estranei all'attività imprenditoriale o professionale. Per un'ampia analisi delle tematiche concernenti il consumatore telematico si veda S. GIOVA, *La tutela del consumatore telematico nel D. lgs. n. 21 del 2014*, in *Rivista giuridica del Molise e del Sannio*, Napoli, 2014, p. 109 ss.

[92] Articolo 6 (Contratti conclusi da consumatori), del Regolamento CE n. 593/2008, recita:

1. Fatti salvi gli articoli 5 e 7, un contratto concluso da una persona fisica per un uso che possa essere considerato estraneo alla sua attività commerciale o professionale («il consumatore») con un'altra persona che agisce nell'esercizio della sua attività commerciale o professionale («il professionista») è disciplinato dalla legge del paese nel quale il consumatore ha la residenza abituale, a condizione che il professionista:

a) svolga le sue attività commerciali o professionali nel paese in cui il consumatore ha la residenza abituale; o b) diriga tali attività, con qualsiasi mezzo, verso tale paese o vari paesi tra cui quest'ultimo; e il contratto rientri nell'ambito di dette attività.

2. In deroga al paragrafo 1, le parti possono scegliere la legge applicabile a un contratto che soddisfa i requisiti del paragrafo 1 in conformità dell'articolo 3. Tuttavia, tale scelta non vale a privare il consumatore della protezione assicuratagli dalle disposizioni alle quali non è permesso derogare convenzionalmente ai sensi della legge che, in mancanza di scelta, sarebbe stata applicabile a norma del paragrafo 1. 3. Se i requisiti di cui al paragrafo 1, lettere a) o b) non sono soddisfatti, la legge applicabile a un contratto tra un consumatore e un professionista è determinata a norma degli articoli 3 e 4.

4. I paragrafi 1 e 2 non si applicano ai contratti seguenti: a) ai contratti di fornitura di servizi quando i servizi dovuti al consumatore devono essere forniti esclusivamente in un paese diverso da quello in cui egli risiede abitualmente; b) ai contratti di trasporto diversi dai contratti riguardanti un viaggio «tutto compreso» ai sensi della direttiva 90/314/CEE del Consiglio, del 13 giugno 1990, concernente i viaggi, le vacanze ed i circuiti «tutto compreso» (1); c) ai contratti aventi per oggetto un diritto reale immobiliare o la locazione di un immobile diversi dai contratti riguardanti un diritto di godimento a tempo parziale ai sensi della direttiva 94/47/CE; d) ai diritti e obblighi che costituiscono uno strumento finanziario e ai diritti e obblighi costitutivi delle clausole e condizioni che disciplinano l'emissione o l'offerta al pubblico e le offerte pubbliche di acquisizione di valori mobiliari, e alla sottoscrizione e al riacquisto di quote di organismi di investimento collettivo, nella misura in cui tali attività non costituiscono prestazione di un servizio finanziario;

e) ai contratti conclusi nell'ambito del tipo di sistema che rientra nel campo di applicazione dell'articolo 4, paragrafo 1, lettera h).

collegamento sussidiario, destinato appunto ad operare quando le parti non scelgono la legge regolatrice, quello del luogo in cui risiede il consumatore, ma a condizione che anche il professionista svolga le sue attività commerciali o professionali nel medesimo paese o diriga tali attività, con qualsiasi mezzo, verso questo paese[93]. In assenza di queste condizioni, la legge applicabile sarà quella del paese in cui il fornitore ha la residenza abituale o la sede se persona giuridica.

[93] *Ex* art. 6, co. 1, Regolamento CE n. 593/2008.

CAPITOLO II

Evoluzione tecnologica e diritto alla riservatezza. Il trattamento dei dati personali in rete.

Sommario: 1. Il diritto alla riservatezza e la sua evoluzione. - 1.1. Bilanciamento dei diritti. La libertà di espressione. - 1.2. Il diritto alla riservatezza nell'epoca della conoscenza e della esposizione globale. - 2. La storia del pacchetto protezione dati. - 2.1. La Direttiva 95/46/CE e il trasferimento dei dati personali verso un paese «terzo». - 3. Tutela dei dati personali e loro libera circolazione su *internet*. Il caso *Lindqvist*. - 3.1. *Segue*. La sentenza «*Costeja*». - 3.2. Casistica giurisprudenziale italiana dopo la sentenza «*Costeja*»: il Tribunale di Roma. - 3.3. La decisione «*Safe Harbour*» e il suo annullamento. Il caso *Maximillian Schrems*. - 3.4. Il nuovo «Scudo *Privacy*» per il trasferimento dei dati personali tra UE e USA. - 4. Il trattamento dei dati personali alla luce del Regolamento europeo sulla *privacy*. Disposizioni generali. - 4.1. I Princípi del Regolamento europeo sulla *privacy*. - 4.1.1. *Segue*. I princípi specifici di trasparenza, di *accountability*, di *privacy by design* e *privacy by default*. - 4.1.2. *Segue*. Le principali novità. - 4.1.3. *Segue*. Le garanzie sul trasferimento di dati personali al di fuori dell'UE. - 4.1.4. *Segue*. Il comitato europeo per la protezione dei dati. - 4.1.5. *Segue*. Reclamo e ricorso giurisdizionale. - 4.1.6. *Segue*. Diritto al risarcimento e responsabilità.

1. Il diritto alla riservatezza e la sua evoluzione.

Il diritto alla riservatezza[94], quale diritto di ogni individuo alla intimità della vita privata e familiare, contro ingerenze altrui, a prescindere dalla tutela dell'onore, del decoro, della reputazione ed anche del diritto all'immagine, gode oggi di una tutela sempre piú ampia[95],

[94] La letteratura in argomento è assai ampia. Si vedano, *ex multis*, A. DE CUPIS, *Il diritto all'identità personale*, Milano, 1949; ID., *I diritti della personalità*, 2ª ed., Milano, 1982; P. PERLINGIERI, *La personalità umana nell'ordinamento giuridico,* Camerino-Napoli, 1972, p. 174 ss.; S. RODOTÀ, *La* privacy *tra individuo e collettività*, in *Pol. dir.*, 1974, p. 550; ID., *Repertorio di fine secolo*, Bari, 1992; ID., *Tecnologie e diritti*, Bologna, 1995; ID., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 586; ID., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997; D. MESSINETTI*, voce* Personalità *(diritti della)*, in *Enc. dir.*, XXXIII, Milano, 1983, p. 355; ID., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1999, p. 339; G. ALPA, M. BESSONE, L. BONESCHI e G. CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983; V. ZENO-ZENCOVICH, *Onore e reputazione nel sistema del diritto civile*, Napoli, 1985; ID., voce *Personalità (diritti della)*, in *Dig. disc. priv., sez. civ.*, XII, Torino, 1995, p. 456; ID., voce *Onore e reputazione*, in *Dig. disc. priv., sez. civ.*, XIII, Torino, 1995, p. 91; ID., *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Juris*, 1997, p. 466; G.B. FERRI, *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, I, p. 801; P. RESCIGNO, voce *Personalità (diritti della)*, in *Enc. giur.*, XXIV, Roma, 1991, p. 2; N. CIPRIANI, *Dall'identità personale all'identità commerciale*, in *Riv. dir. comm.*, 1997, II, p. 267 ss.; G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997; V. CUFFARO e V. RICCIUTO (a cura di), *La disciplina di dati personali*, Torino, 1997; S. GIOVA, *Introduzione*, in *Tutela della persona, beni comuni e valorizzazione dei nuovi diritti* (a cura di), Napoli, 2008, p. 9 ss.; ID., *Tutela della persona beni comuni e valorizzazione dei nuovi diritti. Atti del convegno di Campobasso e Isernia, 14-15 novembre 2007*, Napoli, 2008, p. 1 ss.

[95] Si pensi, ad esempio, alla tutela contro il c.d. *spamming*, di cui all'art. 9, d.lg. n. 70/2003, consistente nel diritto a non dover subire per posta elettronica informazioni commerciali non sollecitate.

ma non viene espressamente menzionato dalla nostra Costituzione. La ragione, probabilmente, è da rinvenire nella circostanza che, «dopo un periodo storico di oppressione dei diritti individuali, il nostro Costituente ha voluto in ogni modo assecondare la funzione dinamica dell'individuo in seno alla società, garantendogli la possibilità di parlare»[96] (e non, invece, accordandogli una tutela di senso opposto, negativa, volta all'isolamento morale, come presupposta dal diritto alla riservatezza «domestica»).

La tutela costituzionale dell'interesse al riserbo può essere però cercata, secondo un orientamento dottrinale, nell'art. 21 cost., alla stregua di una sua lettura in chiave negativa. S'è detto, infatti, che libertà di manifestazione del pensiero significa, positivamente, libertà di comunicare il proprio pensiero, ma anche, negativamente, libertà di tacere[97] o di limitarne la diffusione, manifestandolo a taluni e non ad altri[98]. A ben vedere, il richiamo all'art. 2 cost. è destinato ad apparire piú solidamente fondato in quanto «l'esigenza di riserbo, [...] "necessità addirittura biologica" dell'uomo, è aspetto inalienabile della persona umana, il cui svolgimento e sviluppo trovano garanzia negli artt. 2 e 3, 2° co., Cost.»[99].

Tale ricostruzione sembra essere la piú corretta e convincente, soprattutto alla luce della considerazione per la quale «[l]'art. 2 cost. è norma direttamente applicabile ed esprime un principio fondamentale di tutela della persona umana: il suo contenuto non si limita a riassumere i diritti tipicamente previsti da altre disposizioni della Costituzione, ma consente di estendere la tutela a situazioni atipiche.»[100].

---

96 Cosí G. ARIETA, *Il problema della tutela della vita privata e le nuove leggi sulle intercettazioni telefoniche*, in *Temi Romana*, 1974, p. 532.

97 C. ESPOSITO, *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958, p. 35, nota 80; C. MORTATI, *Istituzioni di diritto pubblico*, II, 2 ed., Padova, 1967, p. 390.

98 F. MANTOVANI, *Mezzi di diffusione e tutela dei diritti umani*, in *Arch. giur.*, 1968, p. 390. Da tale ricostruzione A. CATAUDELLA, *La tutela civile della vita privata*, Milano, 1972 e, successivamente, nello stesso senso, A. CERRI, *Libertà negativa di manifestazione del pensiero e di comunicazione. Diritto alla riservatezza: fondamento e limiti*, in *Giur. cost.*, 1974, p. 610 ss., s'è dedotto un potere di controllo della persona sulla conoscenza altrui delle vicende proprie, intaccato da ogni comportamento volto a carpire notizie o a diffonderle oltre la cerchia di persone cui sono destinate.

99 Cosí A. CATAUDELLA, *Riservatezza (diritto alla)*, in *Enc. giur.* Treccani, XXVII, Roma, 1990, il quale richiamando A.F. WESTIN, Privacy and Freedom, New York, 1967, p. 8, evidenzia come la fruizione di periodi di isolamento, materiale e psicologico, è un'esigenza addirittura biologica dell'uomo. L'autore, ritiene meno appropriato il richiamo all'art. 3, comma 1, poiché qui l'accento è posto sulla dignità (e sulla parità nella stessa) della persona, che è cosa che attiene alla reputazione ed al decoro piú che alla riservatezza.

100 Cosí P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 719 s. L'a. respinge la natura programmatica (ossia la non diretta applicabilità) e riassuntiva (mancanza di contenuto proprio) dell'art. 2 cost., che tutela i «diritti inviolabili dell'uomo», cosí criticando fermamente le teorie che sostengono la tipicità dei diritti della personalità i quali, di converso, con l'avvento della Costituzione, sono divenuti atipici. L'esistenza di una serie aperta di diritti della personalità trova il suo fondamento normativo proprio nella nuova concezione dell'art. 2 cost., ossia norma direttamente applicabile ed espressiva di un principio

Ciò premesso, la non espressa menzione del diritto in parola nella nostra Costituzione non priva lo stesso di una sua propria rilevanza nell'ordinamento, poiché aspetto della nostra esistenza, meritevole di tutela anche in via giudiziale (art. 24 cost.) e, essendo la personalità un valore unitario[101], «ogni previsione particolare non potrebbe mai essere esaustiva e lascerebbe fuori alcune manifestazioni ed esigenze della persona che, anche per il progredire della società, esigono una considerazione positiva.».[102]

Infatti, «[n]el principio generale di tutela della persona (art. 2 cost.) rientrano tutti gli interessi e gli atteggiamenti soggettivi mediante i quali si realizza la personalità»[103].

Il diritto alla riservatezza è, in ogni caso, contemplato positivamente all'art. 8 della Convenzione europea sui diritti dell'uomo[104], che garantisce il diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza, e stabilisce le condizioni alle quali il diritto alla protezione dei dati personali può essere soggetto a restrizioni[105].

---

fondamentale di tutela della persona umana. L'a. spiega che «[d]ove oggetto di tutela è la persona, la prospettiva deve mutare: diviene necessità logica riconoscere, per la speciale natura dell'interesse protetto, che è proprio la persona a costituire ad un tempo il soggetto titolare del diritto e il punto di riferimento oggettivo del rapporto. La tutela della persona non può essere frazionata in isolate fattispecie concrete, in autonome ipotesi tra loro non collegate, ma deve essere prospettata come problema unitario, data l'unitarietà del valore della persona che ne è a fondamento. Questo non può essere scisso in tanti interessi, in tanti beni, in isolate situazioni, al modo delle teorie atomistiche. La personalità è dunque un *valore* (il valore fondante dell'ordinamento) ed è alla base di una serie aperta di situazioni esistenziali, nelle quali si traduce la sua incessantemente mutevole esigenza di tutela». […] Non esiste un numero chiuso di ipotesi tutelate: tutelato è il valore della persona senza limiti, salvo quelli posti nell'interesse della persona stessa o di altre persone.». Sul punto v. anche ID., *La personalità umana*, cit., pp. 175 e 183 ss. e P. D'ADDINO SERRAVALLE, *Le trasformazioni chirurgiche del sesso nella sentenza n. 98 della Corte Costituzionale*, nota a Corte cost., 1 agosto 1979, n. 98, in *Rass. dir. civ.*, 1980, p. 507 ss.

101 P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 720 e 721.

102 P. PERLINGIERI, *o.u.c.*, cit., p. 720.

103 P. PERLINGIERI, *o.u.c.*, cit., p. 722, e in particolare nota 25, alla quale rinvia la nota 28, ove lo stesso a., richiamando un suo scritto, osserva «che esigenze esistenziali della persona umana – destinate poi a ricevere formale riconoscimento e tutela in specifici provvedimenti normativi – quali l'informazione e l'accesso alle sue fonti, la riservatezza dei fatti privati, il mutamento di sesso, l'integrità psichica oltre che fisica, trovano nella previsione generale di tutela della persona un fondamento normativo preciso, idoneo a qualificare tali esigenze come giuridicamente meritevoli con immediate conseguenze nelle stesse relazioni intersoggettive.». Sull'art. 2 cost. quale punto di riferimento unitario degli interessi della personalità, v. anche M. NUZZO, *Nome (diritto vigente)*, in *Enc. dir.*, XXVIII, Milano, 1978, p. 309 ss.; N. LIPARI, *Diritti fondamentali e categorie civilistiche*, in *Riv. dir. civ.*, 1996, I, p. 419. In giurisprudenza, per tutte, Cass., 9 giugno 1998, n. 5658, in *Corr. giur.*, 1998, p. 1170.

104 A. CATAUDELLA, *Riservatezza (diritto alla)*, cit.

105 L'art. 8 della Convenzione europea sui diritti dell'uomo, rubricato «Diritto al rispetto della vita privata e familiare», stabilisce che: «1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.».

Con propria giurisprudenza, la Corte EDU ha affrontato il tema della protezione dei dati in piú casi, non ultimi quelli riguardanti l'intercettazione delle comunicazioni[106], le varie forme di sorveglianza[107], nonché le garanzie rispetto alla conservazione dei dati personali da parte delle autorità pubbliche[108]. La Corte ha chiarito che l'articolo 8 della CEDU non solo obbliga gli Stati ad astenersi da qualsiasi azione che possa violare questo diritto previsto dalla Convenzione, ma impone anche loro, in talune circostanze, l'obbligo di garantire attivamente l'effettivo rispetto della vita privata e familiare[109].

L'emergere delle tecnologie dell'informazione negli anni '60 ha determinato un crescente bisogno di norme piú dettagliate per tutelare i dati personali. A metà degli anni '70, il Comitato dei ministri del Consiglio d'Europa ha adottato varie risoluzioni in materia di protezione dei dati personali, facendo riferimento all'articolo 8 della CEDU[110]. Nel 1981 è stata aperta alla firma una Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (Convenzione n. 108)[111]. La Convenzione protegge l'individuo dagli abusi che possono accompagnare la raccolta e il trattamento dei dati personali e, nel contempo, cerca di regolamentare il flusso transfrontaliero di dati personali. Per quanto concerne la raccolta e il trattamento dei dati personali, i princípi stabiliti nella Convenzione riguardano, in particolare, la correttezza e liceità della raccolta e del trattamento automatizzato dei dati, archiviati per specifici scopi legittimi, non destinati a un uso incompatibile con tali scopi, né conservati oltre il tempo necessario. Tali princípi riguardano anche la qualità dei dati, in particolare in riferimento alla loro adeguatezza, pertinenza e non eccedenza (proporzionalità), nonché esattezza.

La Convenzione, in assenza di adeguate garanzie giuridiche, vieta il trattamento dei dati «sensibili», come la razza, le opinioni politiche, la salute, la religione, l'orientamento sessuale

---

106 Cfr., per esempio, Corte EDU, 2 agosto 1984, n. 8691/79, Malone c. Regno Unito; Corte EDU, 3 aprile 2007, C-62617/00, Copland c. Regno Unito.

107 Cfr., per esempio, Corte EDU, 6 settembre 1978, n. 5029/71, Klass e a. c. Germania; Corte EDU, 2 settembre 2010, n. 35623/05, Uzun c. Germania.

108 Cfr., per esempio, Corte EDU, 11 luglio 1985, n. 9248/81, Leander c. Svezia; Corte EDU, 4 dicembre 2008, n. 30562/04, S. e Marper c. Regno Unito.

109 Cfr., per esempio, Corte EDU, 17 luglio 2008, n. 20511/03, I. c. Finlandia; Corte EDU, 2 dicembre 2008, n. 2872/02, K.U. c. Finlandia.

110 CDE, Comitato dei ministri (1973), Risoluzione (73) 22 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore privato, 26 settembre 1973; CDE, Comitato dei ministri (1974), risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico, 20 settembre 1974.

111 CDE, Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, Consiglio d'Europa, STCE n. 108, 1981.

o i precedenti giudiziari di un individuo. Essa sancisce inoltre il diritto dell'individuo di essere informato della conservazione di informazioni che lo riguardano e di chiederne la rettifica, se del caso. Le restrizioni dei diritti stabiliti nella Convenzione sono possibili solo quando sono in gioco interessi prevalenti, quali la sicurezza o la difesa dello Stato. Sebbene preveda la libera circolazione dei dati personali tra le parti contraenti, la Convenzione impone anche alcune restrizioni su tali flussi verso paesi in cui la regolamentazione giuridica non conferisce una protezione equivalente.

Tutti gli Stati membri dell'UE hanno ratificato la Convenzione n. 108, che nel 1999 è stata emendata per consentire all'UE di diventarne parte contraente[112]. Nel 2001 è stato adottato un Protocollo addizionale alla Convenzione n. 108, che introduce disposizioni in materia di flussi transfrontalieri dei dati verso le parti non contraenti, i cosiddetti paesi terzi, e l'istituzione obbligatoria delle autorità di controllo nazionali per la protezione dei dati[113]. La Convenzione n. 108 è aperta all'adesione degli Stati non membri del CDE, compresi i paesi extraeuropei. Finora, 45 delle 46 parti contraenti della Convenzione n. 108 sono Stati membri del CDE. L'Uruguay, il primo paese extraeuropeo, vi ha aderito nell'agosto 2013.

Oggi il diritto alla protezione dei dati personali è riconosciuto e definito come diritto fondamentale delle persone anche dalla Carta di Nizza[114], alla quale ora è stato attribuito il

---

[112] CDE, emendamenti alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (STE n°108) che consente alle Comunità europee di accedervi, adottati dal Comitato dei ministri, a Strasburgo, il 15 giugno 1999; articolo 23, paragrafo 2, della Convenzione n. 108 nella sua versione modificata.

[113] CDE, Protocollo addizionale alla Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, concernente le autorità di controllo e i flussi transfrontalieri di dati, STCE n.°181, 2001.

[114] La Carta dei diritti fondamentali dell'Unione Europea 7 dicembre 2000 (c.d. *Carta di Nizza*), riconosce ad ogni persona il diritto al rispetto della vita privata e della vita familiare (art. 7) e il diritto alla protezione dei dati di carattere personale (art. 8), specificando altresí che il trattamento degli stessi debba avvenire secondo il principio di lealtà, per finalità determinate e sulla base del consenso della persona interessata o un altro fondamento purché legittimo e previsto dalla legge (comma 2, art. 8); affida inoltre il rispetto di tali regole al controllo di un'autorità indipendente. L'art. 8, testé citato, come si legge nel preambolo della «Dichiarazione dei diritti in Internet» - elaborata dalla «Commissione per i diritti e i doveri relativi ad *internet*» a seguito della consultazione pubblica, delle audizioni svolte e della riunione della stessa Commissione del 14 luglio 2015, approvata e pubblicata il 28 luglio 2015 - costituisce «il riferimento necessario per una specificazione dei principi riguardanti il funzionamento di Internet, anche in una prospettiva globale.». Tale «Dichiarazione dei diritti in Internet», evidenzia L. RUGGERI, *I Domain names*, in *Manuale di diritto dell'informatica*, 3ª ed., a cura di D. Valentino, Napoli, 2016, p. 82, «vuole essere un punto di rifermento non solo nazionale per la promozione della tutela delle persone e dei loro diritti nell'accesso e nell'uso della Rete». La novità della «Dichiarazione» in parola, afferma S. RODOTÀ, *Verso una Dichiarazione dei diritti di Internet*, in www.camera.it, «è rappresentata dal fatto che per la prima volta la proposta di un Internet Bill of Rights non proviene da singoli studiosi, da associazioni, da dynamic coalitions, da imprese, da gruppi di stakeholders, ma da un soggetto istituzionale.» e la sua funzione è quella di «costruire, con modalità diverse da quelle del passato, le regole costituzionali

medesimo valore giuridico dei Trattati europei[115]. Non solo: il diritto alla protezione dei dati personali è riconosciuto anche dal Trattato sul funzionamento dell'Unione, che ne estende l'applicazione anche nei settori della sicurezza esterna e lo qualifica, a pieno titolo, come un diritto della persona anche nel settore della giustizia e della sicurezza[116].

Nel quadro europeo si tratta ormai di un diritto fondamentale della persona (di ogni persona, senza distinzione alcuna), riconosciuto è garantito a livello dei Trattati dell'Unione: «un diritto dunque che caratterizza intrinsecamente il nostro modo di considerare la persona umana e i diritti dei quali essa è titolare»[117].

Nella giurisprudenza italiana, un primo espresso riconoscimento del diritto alla riservatezza si è avuto con la storica sentenza del 1975 relativa al caso *Soraja*[118], ove se n'è affermato il suo rango costituzionale[119]. Successivamente, sulla base della normativa comunitaria (in particolare con l'emanazione della direttiva 95/46/CE[120], alla quale

---

indispensabili perché la Rete possa mantenere il suo carattere di luogo di libertà e democrazia, il più grande spazio pubblico che l'umanità abbia conosciuto.».

115 Art. 6 del Trattato sull'Unione Europea per il quale «L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati».

116 Art. 16 del TFUE prevede che « 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 è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea».

117 F. PIZZETTI, *o.u.c.*, p. 37.

118 Cass., 27 maggio 1975 n. 2129, in *Foro it.*, 1976, I, 2895. Con questa sentenza, la Cassazione prende decisa e diretta posizione sul diritto alla riservatezza. Dopo aver negato per molto tempo l'ammissibilità di una protezione autonoma del rispetto della vita privata, il Supremo Collegio, conformandosi ad una copiosa giurisprudenza di merito, perviene all'affermazione che l'ordinamento giuridico riconosce e tutela l'interesse di ciascuno a che non siano resi noti fatti o avvenimenti di carattere riservato senza il proprio consenso. La sentenza afferma che costituisce lesione della *privacy* la divulgazione di immagini o avvenimenti non direttamente rilevanti per l'opinione pubblica, anche quando tale divulgazione venga effettuata con mezzi leciti e per fini non esclusivamente speculativi. Cosí si legge nella pronuncia, relativa ad una delle controversie instaurate da *Soraya Esfandiari* contro alcuni giornali che avevano pubblicato delle fotografie ritraenti l'*ex*-imperatrice in atteggiamenti intimi con un uomo, nelle mura della sua abitazione.

119 Cass., 27 maggio 1975 n. 2129, cit., individua il fondamento normativo del diritto alla riservatezza negli artt. 3,13,14,15,27,29 e 41 della Costituzione.

120 Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo la trattamento dei dati personali, nonché alla libera circolazione di tali dati. La Direttiva viene anche definita «Direttiva madre», proprio in quanto costituisce il testo di riferimento, a livello europeo, in materia di protezione dei dati personali. L'emanazione della dir. 1995/46/CE rappresenta una vera svolta, poiché siffatto provvedimento normativo introduce in sede europea una disciplina quadro del trattamento dei dati personali, che riceve attuazione nel nostro Paese con la l. 31 dicembre 1996, n. 675, collegata alla legge delega, di pari data, n. 676. Sulla direttiva in parola v., *infra*, § 2.1.

seguirono poi altre direttive piú specifiche di settore[121]), il diritto alla protezione dei dati personali è stato riconosciuto, nel nostro Paese, con la l. 31 dicembre 1996, n. 675[122] e con il codice in materia di protezione dei dati personali (codice *privacy*, d.lg. 196 del 2003[123]).

L'articolato impianto normativo disegna un sistema complesso nel quale la possibilità di trattare i dati personali altrui è, in linea di principio, subordinata al consenso [che, *ex* art. 23 d.lg. 196/2003, dev'essere: informato[124], riferito «ad un trattamento chiaramente individuato», espresso liberamente, anche se non necessariamente in forma scritta, ma solo «documentato per iscritto» (forma *ad probationem*), mentre è solo il consenso al trattamento di dati sensibili che deve essere «manifestato in forma scritta» (forma *ad substantiam*)] del soggetto cui i dati si riferiscono, sempreché non si versi in uno dei casi nei quali è normativamente prevista l'inessenzialità di questo assenso abilitante (art. 24 d.lg. 196/2003). Là dove rilevante, ai fini della liceità del trattamento, il consenso in parola, benché idoneo a legittimare l'utilizzazione dei dati, non implica, però, la dismissione definitiva di ogni potere di controllo sugli stessi da parte del soggetto cui i medesimi si riferiscono. Non soltanto, infatti, quand'anche permanga l'assenso al trattamento il titolare, al fine di tutelare un diritto all'identità personale, sarà tenuto, a richiesta, a utilizzare dati in parte diversi (in quanto eventualmente «rettificati», «aggiornati» o «cancellati» *ex* art. 7, comma 3) da quelli in origine consensualmente raccolti, ma soprattutto, il sistema si spinge ad ammettere persino la reversibilità integrale di detto assenso che, per la dottrina piú autorevole[125] può estrinsecarsi in una vera e propria revoca[126], avente effetto radicalmente

---

121 In particolare la direttiva sulla *privacy* nel settore delle telecomunicazioni (97/66/CE), poi abrogata e sostituita dalla direttiva detta «*e-privacy*», in matria di *privacy* nelle comunicazioni elettroniche (2002/58/CE), facente parte di un «pacchetto Telecom», successivamente emendato dalle direttive 2009/136/CE e 2009/140/CE. Per completezza si ricorda anche la direttiva 2006/24/CE in materia di conservazione dei dati di traffico telefonico e telematico per finalità di polizia e di giustizia.

122 La l. 31 dicembre 1996, n. 675 dà attuazione, nel nostro Paese, alla dir. 95/46/CE. Per un'analisi della citata legge sulla *privacy* v., ad esempio: G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997; V. CUFFARO, V. RICCIUTO, V. ZENO-ZENCHOVICH, *Trattamento dei dati e tutela della riservatezza*, Milano, 1998; V. FRANCESCHELLI, (a cura di) *La tutela della privacy informatica*, Milano, 1998; E. GIANNANTONIO, M.G. LOSANO, V. ZENO-ZENCHOVICH, *La tutela dei dati personali commentario alla L. 675/1996*, Padova, 1999; E. TOSI, *Prime osservazioni sull'applicabilità della disciplina generale della tutela sui dati personali a internet e al commercio elettronico*, in *Dir. inf.*, 1999, p. 591.

123 D.lg. 30 giugno 2003, n. 196, «Codice in materia di protezione dei dati personali».

124 L'art. 13, d.lg. 196/2003, prevede l'obbligo di informare preventivamente, oralmente o per iscritto, l'interessato o la persona presso la quale sono raccolti i dati personali.

125 S. RODOTÀ, *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997, p. 591.

126 Ai fini della revoca del consenso, l'art. 8, del d.lg. in commento, stabilisce che i diritti di accesso ai dati, anche al fine di ottenere l'aggiornamento, la rettificazione, l'integrazione, la cancellazione, la trasformazione in

preclusivo di qualsivoglia trattamento successivo. Il consenso dell'interessato risulta, però, insufficiente ai fini del trattamento dei dati personali normativamente definiti «sensibili», in quanto «idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale» (art. 4, comma 1, lett. d).

Ai sensi dell'art. 26, infatti, tali dati possono essere oggetto di trattamento «solo con il consenso scritto dell'interessato e previa autorizzazione» del Garante per la protezione dei dati personali (organo di garanzia deputato a vigilare sull'osservanza della normativa in disamina e in quanto tale investito, secondo il legislatore, di «responsabilità costituzionale») il che se ha evidentemente l'effetto di non rimettere per intero al potere dispositivo dell'interessato la definizione della regola di circolazione di simili, delicate informazioni[127], sottintende di riflesso la non attitudine di detto soggetto a gestire autonomamente in modo adeguato il conseguenziale rischio di pregiudizio quando l'interesse di cui è portatore deve, secondo la gerarchia dei valori stabilita dal legislatore, essere considerato di rango superiore a quello (che si pone all'origine della richiesta di consenso) volta per volta antagonista[128].

La predetta regola non è però senza eccezioni, poiché è espressamente previsto (*ex* art. 137) l'esonero, per il trattamento dei dati sensibili nell'esercizio della professione di giornalista, dall'autorizzazione del Garante e dal consenso dell'interessato. La giurisprudenza ha precisato che, in tal caso, non può comunque prescindersi dal rispetto, oltre che del diritto di cronaca e dell'essenzialità dell'informazione, anche dei princípi stabiliti dal codice deontologico delle attività giornalistiche, cui deve riconoscersi natura di fonte normativa[129]. Inoltre, si condiziona l'esonero in parola - fermo restando il rispetto dei limiti del diritto di cronaca, e in particolare dell'essenzialità dell'informazione riguardo a

---

forma anonima e il blocco dei dati, sono esercitati con richiesta «senza formalità» al titolare o al responsabile «anche per il tramite di un incaricato». Sul punto, cfr. Cass., 01 settembre 2015, n. 17399, in CED Cassazione, 2015, per la quale «[…], la revoca del consenso al trattamento dei dati personali può essere espressa dall'interessato con richiesta rivolta senza formalità al titolare o al responsabile del trattamento, anche per il tramite di un difensore di fiducia».

127 G. BUTTARELLI, *Banche dati e tutela della riservatezza*, Milano, 1997, p. 377.

128 F.D. BUSNELLI, *Spunti per un inquadramento sistematico, in Tutela della* privacy. *Commentario*, a cura di M.C. Bianca e F.D. Busnelli, in *Nuove leggi civ.*, 1999, p. 230.

129 Cass. pen., 05 marzo 2008, n. 16145, in *Corr. giur.*, 2008, 9, p. 1228, con nota di S. SICA. La Sprema Corte ha disatteso l'assunto dei giudici di merito secondo cui la mancanza, da parte del citato art. 137, di un esplicito richiamo al codice deontologico, conduceva a non ritenere piú necessario, a differenza del previgente regime, il rispetto dello stesso ai fini di un lecito trattamento dei dati, in particolare relativi a salute e sfera sessuale.

fatti di interesse pubblico - alla intervenuta divulgazione dei fatti ad opera degli stessi interessati, direttamente od attraverso un loro comportamento pubblico[130].

Il *corpus* legislativo si è di recente arricchito del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016[131], che - in quanto avente una validità «automatica», conferendo diritti e impongono obblighi agli Stati membri, ai loro organi ed ai privati, con la stessa forza coercitiva di una legge nazionale - a seguito della sua entrata in vigore, è destinato ad incidere sul nostro codice *privacy* (d.lg. 196/2003).

Non solo si è dato fondamento normativo al diritto alla riservatezza, ma il suo contenuto è stato progressivamente ampliato da dottrina e giurisprudenza. Negli anni '50 la riservatezza veniva infatti definita in termini di «*right to be let alone*» e dunque come un interesse a contenuto negativo, «volto all'isolamento morale»[132]. A partire dagli anni '70, con l'avvento dei *computer,* la riservatezza veniva invece definita in termini di «controllo sui dati personali»[133] e, dunque, come un diritto non solo a contenuto negativo ma anche positivo[134]. Con l'ingresso nella società di *internet,* la riservatezza viene invece definita come un diritto multidimensionale, in grado di tenere conto adeguatamente di molteplici e differenti interessi[135].

L'avvento di *internet* rende inoltre sempre piú difficile il controllo del flusso continuo di dati che corre, senza limiti e confini controllabili, lungo una rete a dimensione mondiale ma

---

130 Cass. pen., 24 aprile 2008, n. 23086, in CED *on line*.

131 «Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)». Il citato Regolamento, pubblicato sulla Gazzetta Ufficiale dell'Unione europea (GUUE) in data 4 maggio 2016, è entrato in vigore venti giorni dopo la sua pubblicazione in GUUE, per diventare definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale e le disposizioni del Regolamento.

132 V. al riguardo T.A. AULETTA, *Riservatezza e tutela della personalità*, Milano, 1978, p. 27. Il primo in Italia a usare il termine diritto alla riservatezza è stato A. RAVÀ, *Istituzioni di diritto privato,* Padova, 1938, 157. Il diritto alla *privacy,* inteso come «*right to be let alone»,* è stato per la prima volta teorizzato da S.D. WARREN e L.D. BRANDEIS, *The right of privacy,* in *Harv. L. Rev.*, 1890, p. 193.

133 S. RODOTÀ, *La* «privacy» *tra individuo e collettività*, in *Politica del diritto,* 1974, p. 545.

134 Ad esempio G.B. FERRI, *Privacy e libertà informatica,* in *Banche dati telematica e diritti della persona*, a cura di Alpa Bessone, Padova, 1984, p. 47, ha infatti osservato che il diritto alla riservatezza si caratterizzava per: a) l'aspetto negativo che consente alla persona di impedire la raccolta di dati; b) l'aspetto positivo che consente «il potere, cioè, del titolare del dato raccolto di conoscere, controllare l'uso, modificare, aggiornare». In dottrina la tesi del controllo sui dati personali è stata largamente accolta: v. ad esempio G. ALPA, *Gli interessi tutelati e le tecniche di tutela risarcitoria*, in *L'informazione e i diritti della persona*, a cura di Alpa, Bessone, Boneschi, Caiazza, Napoli, 1983, p. 24; ID., «*Privacy*» *e statuto dell'informazione*, in *Riv. dir. civ.*, 1979, I, p. 72.

135 Sul punto vedi R. PARDOLESI, *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità,* in *Diritto alla riservatezza e circolazione dei dati personali,* Milano, 2003, p. 1.

anche, attraverso le tecnologie *cloud*, con una vera e propria «dislocazione» dei dati oggetto di trattamento nelle parti piú diverse del mondo[136].

In questo nuovo scenario, allora, il problema si sposta sul come accrescere la protezione dei dati personali in tutte quelle tecnologie in àmbito ICT. Pertanto, già a metà degli anni '90, il contesto internazionale ha evidenziato il cambiamento apportato alla *privacy* proponendo le c.d. PET (acronimo di *Privacy Enhancing Technologies*)[137].

Successivamente s'è sviluppato il concetto di *privacy by design* che, inizialmente sostenuta soprattutto dall'Autorità di protezione dati dell'Ontario[138], è stata sempre una prospettiva generalmente condivisa da tutte le Autorità di protezione dei dati personali e in particolare da quelle europee del WP29[139] ed è stata oggi introdotta dal Regolamento (UE) 2016/679, all'art. 25.

La *privacy by design* riguarda il principio di incorporazione della *privacy* a partire dalla progettazione di un processo aziendale con le relative applicazioni informatiche di supporto. È quindi un ulteriore tassello nella evoluzione dei princípi relativi alla protezione dei dati personali e rappresenta il futuro della *privacy*. Secondo questa impostazione, l'utente è considerato il centro del sistema *privacy* (per definizione, quindi, è «*user centric*»). Qualsiasi progetto (sia strutturale sia concettuale) va realizzato considerando dalla progettazione (*by design*, appunto) la riservatezza e la protezione dei dati personali. In altri termini, ogni volta che un progetto inizia deve prendere in considerazione, prima di tutto, il ruolo dell'utente, progettando tutto attorno alla persona fisica. Secondo tale approccio metodologico, la *privacy* va considerata già nella fase di progettazione, pertanto, esso esclude che si possa

---

136 F. PIZZETTI, *o.u.c.*, p. 39.

137 PET, ovverosia *Privacy Enhancing Technologies* (tecnologie per il miglioramento della *privacy*). Le PET sono state introdotte dalla Commissione europea la quale promuove lo sviluppo di tutte quelle tecnologie di rafforzamento della tutela della vita privata (PET) per la prevenzione dei rischi derivanti da un uso fraudolento dei dati personali. La Commissione ritiene che: «L'uso delle PET può contribuire all'ideazione di sistemi e servizi di informazione e comunicazione che permettono di ridurre al minimo la raccolta e l'uso di dati personali e di favorire il rispetto delle norme sulla protezione dei dati. L'uso delle tecnologie PET dovrebbe consentire di contrastare i furti di identità, le frodi e la profilazione discriminatoria». Per una disamina approfondita dell'argomento vedi A. GUZZO, *Il concetto di* Privacy Enhancing Technologies (PET), in *Sicurezza informatica e tutela della* privacy del 26/02/2009 e consultabile sulla pagina *web http://www.diritto.it/docs/27375-il-concetto-di-privacy-enhancing-technologies-pet*.

138 Il concetto di *privacy by design* è da attribuire ad Ann Cavoukian, studiosa ed esperta di *privacy* e da molti anni *Privacy Commissioner* per la Provincia dell'Ontario in Canada.

139 Il Gruppo Articolo 29, sottolineandone piú volte l'esigenza, ne ha fatto oggetto anche di specifica raccomandazione alla Commissione affinché fosse introdotta nella revisione della direttiva 95/46/CE. Un apposito capitolo al tema è stato dedicato nell'ampio contributo denominato "*The Future of Privacy*" con cui il Gruppo ha fornito spunti alla Commissione europea in vista della revisione della direttiva 95/46/CE (WP168, http://ec.europa.eu/justice/policies/privacy/docs/wpdcs/2009/wp168_en.pdf).

effettuare una valutazione di conformità alla normativa successivamente alla redazione del progetto o comunque posteriormente in occasione di un evento[140].

Nel 2010 la 32ma Conferenza mondiale dei Garanti *privacy* ha adottato la risoluzione sulla *Privacy by Design* (PbD)[141] rendendo in tal modo ufficiale questo nuovo concetto. Con la PbD si è inteso istituzionalizzare il cambiamento e l'evoluzione della *privacy* che, pertanto, richiede un nuovo approccio per garantire una migliore protezione dei dati personali.

Un altro concetto introdotto con il Regolamento (UE) 2016/679, sempre all'art. 25, è quello della *privacy by default*, ossia il principio di «tutela della vita privata per impostazione predefinita».

La discussione, approvato il summenzionato Regolamento, si incentra dunque su come si possa garantire che il titolare del trattamento (*Data controller*) applichi i princípi di cui sopra e, sul come, il responsabile della protezione dei dati[142](*Data Protection Officer*), possa compiutamente adempiere ai suoi compiti[143] individuati dall'art. 39 del citato Regolamento.

1.1. Bilanciamento dei diritti. La libertà di espressione.

Il diritto fondamentale alla protezione dei dati a carattere personale, ai sensi dell'articolo 8 della Carta, «non appare tuttavia come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale»[144]. L'articolo 52, paragrafo 1, della Carta riconosce che possano essere apportate limitazioni all'esercizio di diritti come quelli sanciti dagli articoli 7 e 8 della medesima, purché tali limitazioni siano previste dalla legge, rispettino il contenuto

---

[140] Per un approfondimento sul tema, v. N. FABIANO, Privacy by Design: *l'approccio corretto alla protezione dei dati personali*, Diritto24ilsole24ore, http://www.diritto24.ilsole24ore.com/art/dirittoCivile/2015-04-20/privacy-by-design-approccio-corretto-protezione-dati-personali-123915.php, il quale sostiene «la opportunità e la necessità di sviluppare e strutturare norme uniformi per uno standard privacy internazionale che garantisca, nel rispetto delle normative degli Stati, un framework comune di riferimento con cui agevolare i trattamenti di dati personali e garantirne la protezione nel rispetto della privacy».

[141] Vedi N. FABIANO, *Approvata dalla Conferenza mondiale dei Garanti la risoluzione sulla* Privacy by Design, in http://www.istitutoitalianoprivacy.it/it/2010/11/02/approvata-dalla-conferenza-mondiale-dei-garanti-la-risoluzione-sulla-privacy-by-design/.

[142] Ulteriore novità introdotta dal Regolamento UE, ossia l'obbligo, per le imprese con oltre 250 dipendenti e per tutti gli enti pubblici, di nominare un *Privacy Officer*, interno o esterno, con un'ampia conoscenza della normativa, che sarà in relazione diretta con i vertici aziendali. Allo stesso verrà affidato il compito di analizzare, valutare e disciplinare la gestione del trattamento e della salvaguardia dei dati personali all'interno di un'azienda, secondo le direttive imposte dalle normative vigenti. Sul punto si tornerà in seguito.

[143] Sul punto v., *infra*, § 4.1.2.

[144] Cfr. Corte giust., 9 novembre 2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen, punto 48, in *www.curia.eu*.

essenziale di detti diritti e libertà e, nel rispetto del principio di proporzionalità, siano necessarie e rispondano effettivamente a finalità d'interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui[145].

«Così, neppure i diritti alla libertà d'espressione e alla libertà di riunione pacifica garantiti dalla CEDU - contrariamente ad altri diritti fondamentali sanciti dalla medesima convenzione, quali il diritto di ciascuno alla vita ovvero il divieto della tortura, nonché delle pene o di trattamenti inumani o degradanti, che non tollerano alcuna restrizione - appaiono come prerogative assolute, ma vanno considerati alla luce della loro funzione sociale.»[146].

Nel sistema giuridico della CEDU la protezione dei dati è garantita dall'articolo 8 (il diritto al rispetto della vita privata e familiare) e, come nel sistema giuridico della Carta, questo diritto deve essere esercitato rispettando l'ambito di applicazione di altri diritti concorrenti. Ai sensi dell'articolo 8, paragrafo 2, della CEDU, «non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria […] alla protezione dei diritti e delle libertà altrui».

Di conseguenza, sia la Corte EDU sia la Corte di Giustizia dell'Unione europea hanno ripetutamente affermato che un esercizio di contemperamento con altri diritti è necessario in caso di applicazione e interpretazione dell'articolo 8 della CEDU e dell'articolo 8 della Carta[147]. Diversi esempi significativi illustrano come si perviene a tale contemperamento.

---

145 *Ibidem*, punto 50.

146 Corte giust., 12 giugno 2003, C-112/00, Eugen Schmidberger, Internationale Transporte und Planzüge e Repubblica d'Austria, punto 80, in *www.curia.eu*. Logica conseguenza di ciò, prosegue la Corte di Giustizia, è che «possono essere apportate restrizioni all'esercizio di tali diritti, a condizione che tali restrizioni rispondano effettivamente ad obiettivi di interesse generale e non costituiscano, rispetto allo scopo perseguito da tali restrizioni, un intervento sproporzionato e inaccettabile tale da ledere la sostanza stessa dei diritti tutelati» […] In tali circostanze, occorre effettuare un bilanciamento tra gli interessi di cui si tratta ed accertare, con riferimento a tutte le circostanze di ciascuna fattispecie, se sia stato osservato un giusto equilibrio tra tali interessi. A tal proposito le autorità competenti dispongono di un ampio potere discrezionale. Si deve tuttavia verificare se le restrizioni imposte agli scambi intracomunitari siano proporzionate con riferimento al legittimo obiettivo perseguito, ossia nella fattispecie la tutela dei diritti fondamentali» (punti 81 e 82).

147 Corte EDU, *Von Hannover c. Germania (n. 2)* [GC], nn. 40660/08 e 60641/08, 7 febbraio 2012; Corte giust., 24 novembre 2011, cause riunite C-468/10 e C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado, in *www.curia.eu*, punto 48; Corte giust., 29 gennaio 2008, C-275/06, Productores de Música de España (Promusicae) c. Telefónica de España SAU, in *www.curia.eu*, punto 68. Cfr. anche Consiglio d'Europa (2013), giurisprudenza della Corte europea dei diritti dell'uomo riguardante la protezione dei dati personali, giurisprudenza (2013) PD, consultabile all'indirizzo: http://www.coe.int/t/dghl/standardsetting/dataprotection/judgments_en.asp.

Uno dei diritti che ci si attende possa entrare in conflitto con il diritto alla protezione dei dati è il diritto alla libertà di espressione. Essa è sancita dall'articolo 11 della Carta («Libertà di espressione e d'informazione»). Tale diritto include la «libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera». L'articolo 11 corrisponde all'articolo 10 della CEDU. Ai sensi dell'articolo 52, paragrafo 3, della Carta, nella misura in cui prevede diritti corrispondenti a quelli garantiti dalla CEDU, «il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione». Le limitazioni che possono legittimamente essere imposte al diritto garantito dall'articolo 11 della Carta non possono pertanto andare oltre quelle previste all'articolo 10, paragrafo 2, della CEDU, vale a dire, devono essere previste dalla legge e devono essere necessarie in una società democratica «[…] alla protezione della reputazione o dei diritti altrui». Questo concetto si estende al diritto alla protezione dei dati.

Il rapporto tra la protezione dei dati personali e la libertà di espressione è disciplinato dall'articolo 9 della direttiva sulla tutela dei dati, intitolato «Trattamento di dati personali e libertà d'espressione», secondo il quale gli Stati membri sono chiamati a prevedere determinate deroghe o limitazioni alle disposizioni in materia di tutela dei dati, e quindi del diritto alla vita privata, previste nei capi II, IV e VI di detta direttiva. E consentito applicare tali deroghe esclusivamente per scopi giornalistici o di espressione artistica o letteraria, rientranti nel diritto fondamentale della libertà d'espressione, soltanto nei limiti in cui esse risultino necessarie per conciliare il diritto alla vita privata con le norme che disciplinano la libertà d'espressione.

Nella causa *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia* Oy[148], la Corte di Giustizia è stata chiamata a interpretare l'articolo 9 della direttiva sulla tutela dei dati e a definire la relazione tra protezione dei dati e libertà di stampa. La Corte ha dovuto esaminare la divulgazione, da parte di *Markkinapörssi* e *Satamedia*, dei dati fiscali di circa 1,2 milioni di persone fisiche legittimamente ottenuti dalle autorità fiscali finlandesi. In particolare, la Corte doveva verificare se il trattamento di dati personali, messi a disposizione dalle autorità fiscali, volto a consentire agli utenti di telefonia mobile di ricevere i dati fiscali relativi ad altre persone fisiche, dovesse essere considerato come

[148] Corte giust., 16 dicembre 2008, c. 73/07, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy, in *www.curia.eu*, punti 56, 61 e 62.

un'attività esercitata esclusivamente a scopi giornalistici. Dopo aver concluso che le attività di *Satakunnan* consistevano in un «trattamento di dati personali» ai sensi dell'articolo 3, paragrafo 1, della direttiva sulla protezione dei dati, la Corte è poi passata all'interpretazione dell'articolo 9 della stessa direttiva, rilevando anzitutto l'importanza riconosciuta alla libertà di espressione in ogni società democratica e ribadendo la necessità di interpretare in senso ampio le nozioni a essa correlate, tra cui quella di giornalismo. La Corte ha poi osservato che, al fine di raggiungere un contemperamento tra i due diritti fondamentali, le deroghe e le limitazioni del diritto alla protezione dei dati devono applicarsi solo nella misura in cui esse siano strettamente necessarie. In tali circostanze, la Corte ha ritenuto che attività come quelle svolte da *Markkinapörssi* e *Satamedia*, relative ai dati provenienti da documenti che sono di dominio pubblico ai sensi della legislazione nazionale, possono essere qualificate come «attività giornalistiche» qualora siano dirette a divulgare al pubblico informazioni, opinioni o idee, indipendentemente dal mezzo di trasmissione utilizzato. La Corte ha anche stabilito che queste attività non sono riservate alle imprese operanti nel settore dei media e possono essere connesse a uno scopo di lucro. Tuttavia, relativamente al caso di specie, la CGUE ha rimesso la valutazione in questione al giudice nazionale.

Per quanto riguarda la conciliazione del diritto alla protezione dei dati con il diritto alla libertà di espressione, la Corte EDU ha emesso diverse sentenze importanti.

Nella causa *Axel Springer AG c. Germania*[149], la Corte EDU ha considerato che il divieto imposto da un tribunale nazionale al responsabile di un giornale, che intendeva pubblicare un articolo sull'arresto e sulla condanna di un noto attore, costituisse una violazione dell'articolo 10 della CEDU. La Corte EDU ha ribadito i criteri stabiliti nella propria giurisprudenza in materia di contemperamento del diritto alla libertà di espressione con il diritto al rispetto della vita privata: a) in primo luogo, se il fatto pubblicato dall'articolo in questione rivesta un interesse generale: l'arresto e la condanna di una persona erano un fatto giudiziario pubblico e quindi d'interesse pubblico; b) in secondo luogo, se l'interessato sia un personaggio pubblico: la persona in questione era un attore sufficientemente noto per figurare quale personaggio pubblico; c) in terzo luogo, in che modo l'informazione sia stata ottenuta e se sia affidabile: l'informazione era stata fornita dall'ufficio della procura e

[149] Corte EDU, *Axel Springer AG c. Germania* [GC], n. 39954/08, 7 febbraio 2012, punti 90 e 91.

l'esattezza delle informazioni contenute in entrambe le pubblicazioni non era oggetto di contenzioso tra le parti.

Pertanto, la Corte EDU ha stabilito che le restrizioni alla pubblicazione imposte al giornale non erano state ragionevolmente proporzionate rispetto allo scopo legittimo di proteggere la vita privata del ricorrente. La Corte ha concluso riscontrando una violazione dell'articolo 10 della CEDU.

Nella causa *Von Hannover c. Germania (n. 2)*[150], la Corte EDU non ha riscontrato alcuna violazione del diritto al rispetto della vita privata ai sensi dell'articolo 8 della CEDU quando alla principessa Carolina di Monaco è stato negato un provvedimento inibitorio contro la pubblicazione di una fotografia che ritraeva lei e il marito durante una vacanza sulla neve. La fotografia era corredata di un articolo che riportava, tra l'altro, le cattive condizioni di salute del principe Ranieri. La Corte EDU ha concluso che i tribunali nazionali avevano accuratamente conciliato il diritto delle case editrici alla libertà di espressione con il diritto al rispetto della vita privata dei ricorrenti. La qualificazione, da parte dei tribunali nazionali, della malattia del Principe Ranieri come un evento della società contemporanea non poteva essere ritenuta irragionevole e la Corte EDU ha potuto convenire che la fotografia, considerata alla luce di questo articolo, ha contribuito almeno in qualche misura a un dibattito d'interesse generale. La Corte ha concluso che non vi era stata alcuna violazione dell'articolo 8 della CEDU.

Nella giurisprudenza della Corte EDU, uno dei criteri fondamentali per quanto riguarda il contemperamento di questi diritti è quello di stabilire se la forma di espressione oggetto di valutazione contribuisca o meno a un dibattito d'interesse pubblico generale.

Nella causa *Mosley c. Regno* Unito[151], un settimanale nazionale ha pubblicato fotografie private del ricorrente. Questi ha addotto una violazione dell'articolo 8 della CEDU poiché non gli era stato possibile chiedere un provvedimento inibitorio prima della pubblicazione delle foto in questione, a causa della mancanza di un obbligo di notifica preliminare per il quotidiano in caso di pubblicazione di materiale che potesse violare il diritto alla vita privata. Sebbene la divulgazione di materiale di tale genere avesse generalmente finalità d'intrattenimento e non d'informazione, la stessa godeva indubbiamente della protezione

[150] Corte EDU, 7 febbraio 2012, nn. 40660/08 e 60641/08, *Von Hannover c. Germania (n. 2)* [GC], punti 118 e 124.
[151] Corte EDU, 10 maggio 2011, n. 48009/08, *Mosley c. Regno Unito*, punti 129 e 130.

prevista dall'articolo 10 della CEDU, sul quale possono prevalere gli interessi giuridici tutelati dall'articolo 8 della CEDU nel caso in cui l'informazione sia di natura intima e privata e la divulgazione sia priva di interesse pubblico. Tuttavia, particolare attenzione deve essere rivolta in sede di esame delle restrizioni che possono costituire una forma di censura prima della pubblicazione. Alla luce dell'eventuale effetto dissuasivo che insorgerebbe in caso di obbligo di notifica preliminare, dei dubbi sulla sua efficacia e dell'ampio margine di apprezzamento in questo ambito, la Corte EDU ha concluso che l'esistenza di un obbligo di notifica preliminare vincolante non era richiesta ai sensi dell'articolo 8. Di conseguenza, la Corte ha concluso che non vi era stata alcuna violazione dell'articolo 8.

Nella causa *Biriuk c.* Lituania[152], la ricorrente ha chiesto il risarcimento del danno nei confronti di un quotidiano per la pubblicazione di un articolo che ne riportava la sieropositività. Tale informazione era stata presumibilmente confermata dai medici dell'ospedale locale. La Corte EDU ha ritenuto che l'articolo in questione non contribuisse ad alcun dibattito d'interesse generale e ha ribadito che la protezione dei dati personali, e non ultimo dei dati sanitari, è fondamentale affinché una persona possa godere del proprio diritto al rispetto della vita privata e familiare sancito dall'articolo 8 della CEDU. La Corte ha attribuito particolare rilievo al fatto che, secondo l'articolo del giornale, il personale medico di un ospedale avesse fornito informazioni sull'infezione da HIV della ricorrente in manifesta violazione dell'obbligo al segreto medico. Di conseguenza, lo Stato non era riuscito a garantire il diritto della ricorrente al rispetto della vita privata. La Corte ha concluso asserendo una violazione dell'articolo 8 della CEDU.

1.2. Il diritto alla riservatezza nell'epoca della conoscenza e della esposizione globale.

Nell'era attuale della globalizzazione e della galoppante evoluzione tecnologica, la portata della condivisione e della raccolta di dati personali è aumentata in modo assai significativo. Ciò comporta nuove sfide per la protezione dei dati personali. La tecnologia attuale consente, tanto alle imprese private quanto alle autorità pubbliche, di utilizzare dati

[152] Corte EDU, *Biriuk c. Lituania*, n. 23373/03, 25 novembre 2008.

personali, come mai verificatosi in precedenza, nello svolgimento delle loro attività. Sempre piú spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. Ecco che, attraverso l'utilizzo dei moderni dispositivi (facilmente collegabili ad *internet*), ognuno di noi si autoespone in un mondo parallelo virtuale, spesso anche inconsapevolmente. Proprio questa inconsapevolezza di rendere pubblico ciò che ci riguarda, non dev'essere tenuta sottovalutata, visti i suoi possibili effetti collaterali. È necessaria, allora, una preventiva campagna di informazione e prevenzione sui possibili rischi di una siffatta esposizione in rete. Tuttavia, la libera circolazione dei dati non dev'essere arrestata, anzi, in un'epoca in cui l'avvento della tecnologia ha trasformato l'economia e le relazioni sociali, dovrebbe dalla stessa essere facilitato ancora di piú il loro trasferimento all'interno dell'Unione, nonché verso paesi terzi e organizzazioni internazionali, garantendo però al tempo stesso un elevato livello di protezione dei dati personali.

In questi anni molte cose sono cambiate nella protezione dei dati personali, soprattutto per due ordini di fattori. Da un lato, è cambiato il rapporto tra il diritto alla riservatezza e la tutela di altri valori, primi fra tutti il diritto alla sicurezza e il diritto alla conoscenza: aspetti centrali nel mondo contemporaneo, che trovano nelle tecnologie del controllo e delle comunicazioni strumenti sempre piú avanzati. Da un altro lato, lo sviluppo dei sistemi di telecomunicazione offre continuamente nuove possibilità di acquisizione, conservazione, utilizzazione dei dati e delle informazioni, a costi sempre piú contenuti. L'incrocio di questi fenomeni è il terreno sul quale la protezione dei dati personali è costantemente sfidata.

Emerge, pertanto, l'esigenza di proteggere piú che di prescrivere, di avvisare e informare piú che di vietare, a mettere tutti, cittadini, istituzioni, imprese, organizzazioni sociali e culturali, di fronte ai mutamenti del nostro tempo, aiutandoli a comprendere i fenomeni in atto e a essere piú consapevoli dei rischi delle nuove tecnologie[153]. Occorre, allora, trovare il giusto equilibrio tra tutela dei diritti e innovazione, in modo da non ostacolare né il ricorso alle tecnologie, né l'utilizzo di modalità di azione piú efficienti per la pubblica

[153] Sul punto si rinvia al § 2.1., Cap. I, ove è stato richiamato l'intervento del Garante per la protezione dei dati personali vòlto a favorire un utilizzo consapevole e corretto del sistema *cloud*, dettando, in particolare, accurate informazioni per l'utilizzo dello stesso in modo da tutelare al meglio i dati personali degli utenti. In particolare, v. nota 53, per la disamina del contenuto della Scheda di documentazione del 23 giugno 2011, "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi*".

amministrazione, legate all'agenda digitale e alla moltiplicazione dei punti di accesso ai servizi per i cittadini.

Sembra farsi strada, oggigiorno, l'idea che non vi debbano essere limiti né al desiderio o all'aspettativa di conoscere, né al diritto di diffondere dati ed informazioni. Si va affermando una concezione della trasparenza che ormai va ben oltre il rapporto tra cittadino e pubblica amministrazione o il controllo sul comportamento di chi ha responsabilità pubbliche. La pretesa, e in alcuni casi la convinzione, dell'esistenza di un generale diritto a conoscere si estende verso forme di potenziale controllo di tutti su tutti.

Una crescente sfiducia verso le istituzioni e le strutture di potere, siano esse pubbliche o private, unita all'utilizzazione delle nuove forme di comunicazione legate all'uso degli *smartphone* e dei *social network*, ci spinge a rivendicare il diritto a tutto sapere e tutto denunciare.

Fino a un paio di decenni fa il timore era di vedere ingiustamente invasa la propria vita e controllati i propri comportamenti e quelli dei propri cari: la tutela della riservatezza era non a caso posta al centro dei diritti di quarta generazione. Oggi la prospettiva probabilmente si è capovolta: l'esposizione di sé e dei propri amici e conoscenti impera sui *blog*, sui *social network*[154], in ogni programma televisivo e in ogni intervista a persone coinvolte, a qualunque titolo, in fatti di cronaca, talvolta particolarmente terribili. Viviamo nel mondo dell'autoesposizione e della trasparenza globale che sta diventando, senza che ce ne accorgiamo, quello del controllo globale. Parlare di diritto alla riservatezza e, ancora di piú, di diritto all'oblio, rischia di essere sentito, ogni giorno di piú, come un'inaccettabile pretesa di limitare il diritto a conoscere e a sapere. È sempre piú difficile distinguere fra cosa sia la libertà di stampa e di manifestazione del pensiero, e cosa invece il diritto di conoscere e quello di comunicare.

Tanto ciò è vero che, di recente, la *Wikimedia Foundation*, organizzazione *no-profit* che gestisce *Wikipedia*, ha presentato una petizione al Consiglio di Stato francese per «sostenere l'accesso alla conoscenza». L'enciclopedia *online* si è schierata a sostegno di *Google* nel caso

[154] Sul punto M. D'AMBROSIO, Social network *e diritti della personalità. Considerazioni in tema di* privacy *e responsabilità civile*, in *Riv. giur. Mol. Sannio*, 2012, p. 331, evidenzia come il (nuovo) concetto di «piazza», quale fulcro dell'attività relazionale umana, nella sua nuova forma digitalizzata non determina soltanto il mutamento dello spazio virtuale di incontro, ma con esso si trasforma anche lo strumento comunicativo, che si avvale di nuova modalità di trasmissione delle informazioni mediante un'innovativa sollecitazione percettiva supportata da immagini o musica, il tutto assicurando un grado di complessità all'interazione superiore rispetto al semplice scambio di parole.

che vede la compagnia contrapposta alla Commissione nazionale per l'informatica e la libertà (Cnil), il garante francese per la *privacy*, sul diritto all'oblio davanti ai giudici d'oltralpe. In buona sostanza il Garante *Privacy* francese sostiene che il diritto all'oblio per essere efficace deve essere globale, mentre *Google* e *Wikipedia* si oppongono proclamando il primato del diritto di libero accesso alla conoscenza, del diritto all'informazione e alla libertà di espressione; la questione dovrà essere risolta dal Consiglio di Stato.

È essenziale interrogarsi se esista, e in che limite, il diritto a diffondere liberamente in rete non solo i comportamenti e sentimenti propri ma anche quelli degli altri[155]. È altresí essenziale indagare i possibili risvolti sul diritto alla riservatezza, in particolare sui suoi presupposti. Valga a tal fine la seguente vicenda giunta all'attenzione del Tribunale di Napoli[156], al quale si viene prospettata, da una delle parti in causa, un'interpretazione evolutiva, legata al contesto dell'evoluzione tecnologica e alla mutata realtà sociale, delle norme a tutela della riservatezza (e segnatamente: art. 10 c.c. e artt. 96 e 97 della l. 22 aprile 1941, n. 633), sí da superare l'essenzialità del consenso per la liceità della pubblicazione dell'immagine di una persona[157].

Prima di vedere la decisione del Tribunale, sembra chiaro a chi scrive che per superare il valore del consenso è giocoforza indispensabile individuare il fondamento valoriale sul quale basarsi, nel senso che l'interpretazione evolutiva dev'essere un'interpretazione

---

155 Se l'accesso ad *internet* è «diritto fondamentale della persona e condizione per il suo pieno sviluppo individuale e sociale» (art. 2, comma 1, «Dichiarazione dei diritti in Internet», della Commissione per i diritti e i doveri in *internet*, Camera dei deputati, del 28 luglio 2015) e l'uso e la diffusione della conoscenza in rete è bene accessibile e fruibile da parte di ogni soggetto (art. 3, comma 1, «Dichiarazione dei diritti in Internet», cit.), l'uso di *internet* deve però essere consapevole, poiché «fondamentale garanzia per lo sviluppo di uguali possibilità di crescita individuale e collettiva, il riequilibrio democratico delle differenze di potere sulla Rete tra attori economici, Istituzioni e cittadini, la prevenzione delle discriminazioni e dei comportamenti a rischio e di quelli lesivi delle libertà altrui.» (art. 3, comma 5, «Dichiarazione dei diritti in Internet», cit.).

156 Trib. Napoli, 15 luglio 2014, n. 12749, in *Foro nap.*, 2016, 1, p. 153 ss., con commento di M. D'AMBROSIO, D*iritto all'immagine e utilizzo (in)consapevole della rete internet*, nota a Trib. Napoli 15 luglio 2014, per il quale «[l]'ordinanza in commento adotta una soluzione pienamente condivisibile dalla quale si deduce mediante la normativa vigente uno schema di protezione dei diritti in parola pienamente effettivo.».

157 La vicenda portata a conoscenza del Tribunale partenopeo è la seguente. Una signora pubblica nella propria pagina *Facebook* alcune fotografie che la ritraggono in atteggiamenti affettuosi con il marito, con il quale pende un giudizio di separazione personale; tali fotografie non riprendono casualmente (anche) costui, ma sono chiaramente ritratti della coppia, la cui visibilità viene però ristretta ai soli amici della moglie. V'è da chiedersi se, in tal caso, la signora abbia violato o meno il diritto alla riservatezza - nascente dalla lettura coordinata dell'art. 10 c.c. e artt. 96 e 97 della l. 22 aprile 1941, n. 633 - del marito ove quest'ultimo, se ragionevolmente può aver prestato il consenso ad essere ritratto (le fotografie, ad esempio, mostrano la coppia in luoghi di vacanza o durante ricorrenze familiari, quali il compleanno del figlio), non ha però prestato il proprio consenso alla pubblicazione. Ciò premesso, la soluzione giuridica sta tutta nel valore da attribuire al consenso alla pubblicazione dell'immagine altrui nel nuovo contesto dei *social network*.

costituzionalmente orientata, cioè conforme alla legalità costituzionale[158]. Occorre quindi chiedersi quali princípi/valori del nostro ordinamento possano legittimare una siffatta interpretazione, rintracciando la stessa all'interno dell'ordinamento nel suo complesso, mediante un'attività ermeneutica sistematica. Ciò unitamente alla considerazione, non secondaria tra l'altro, per la quale il mondo di *internet*, non è un mondo a parte, isolato dalla realtà, una «zona franca» nella quale tutto è consentito e nulla vietato. È sí realtà virtuale, ma comunque realtà che non si sottrae a quell'insieme di regole e princípi connaturati alla tutela dell'interesse al riserbo (cosí come alla tutela di altri interessi costituzionalmente garantiti) e che, se può di certo indurre ad un approccio storicizzato e relativizzato, non può però spingersi sino al punto di cancellarne il suo espresso riconoscimento nel nostro ordinamento. Se cosí non fosse, la riservatezza, che la Corte Costituzionale ha fatto espressamente rientrare nel novero dei diritti inviolabili dell'uomo[159], sarebbe sempre sacrificata nel mondo del *web*, che cosí consentirebbe, soprattutto a chi volesse dare sfogo alla sua rabbia[160], l'aggiramento delle regole poste a sua tutela senza nessuna responsabilità. Una «valvola di sfogo» senza conseguenze, cosa che non è consentita e soprattutto non costituzionalmente approvata.

Su queste basi, l'interprete di oggi sarà chiamato a valutare se sia lecita, e a quali condizioni, la pubblicazione di immagini e pensieri altrui, cosí come la stessa pubblicazione di propri. Orbene, inserire una fotografia nella propria pagina di un *social network* equivale a pubblicazione in quanto fatto potenzialmente idoneo a mostrare la foto ad un pubblico

---

158 P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., *passim*.

159 Corte Cost., 12 aprile 1973, n. 38, in *Foro it*., 1973, I, 1708.

160 Si pensi allo studente bocciato che offende liberamente i proff. su *Facebook*, dando libero sfogo alla sua rabbia per l'ingiusta, a suo dire, bocciatura. Si pensi ancora alla vicenda approdata in Cassazione della studentessa di Ferrara che - accusando una ricercatrice universitaria (che anni prima l'aveva assistita nell'elaborazione della tesi di laurea) di aver copiato il suo elaborato e di aver pubblicato un libro a proprio nome, a suo dire, identico alla propria tesi di laurea - pubblica in diversi *social network* messaggi del seguente tenore: «*Volete comprare il libro di MT? Allora vi vendo la mia tesi di laurea ... identica al libro di T ... o meglio è il libro che è identico alla mia tesi!!! Proprio così, la pregevole dottoressa ha copiato tutto il mio lavoro ... e se l'è pubblicato col suo nome sopra … tanto si sa che l'università italiana è un'elitaria fogna dove lavorano solamente raccomandati, lecchini e puttane*». La Suprema Corte, nel caso sopra rappresentato, ha ritenuto integrato il reato di diffamazione, sussistendone l'elemento costitutivo della «comunicazione con più persone», peraltro aggravata dall'aver commesso il fatto con «altro mezzo di pubblicità» ai sensi dell'art. 595, comma 3, c.p. Su quest'ultimo aspetto, la Corte rileva che «proprio l'utilizzazione della disgiuntiva - 'se l'offesa è recata col mezzo della stampa' 'o' con qualsiasi 'altro mezzo di pubblicità' - contemplata all'art. 595, comma 3 c.p., consente di ritenere che la circostanza aggravante si riferisca anche ad internet, che pacificamente rientra nella nozione di 'altro mezzo di pubblicità'». Quest'ultima categoria, infatti, prosegue la Corte, include «tutti quei sistemi di comunicazione e, quindi, di diffusione, – dal fax ai social media – che, grazie all'evoluzione tecnologica, rendono possibile la trasmissione di dati e notizie ad un numero ampio o addirittura indeterminato di soggetti». Il riferimento è a Cass. pen. 22 febbraio 2017, n. 8482, in CED *on line*.

indifferenziato di utenti, a differenza dell'inserimento della fotografia in un album o in una cornice conservati a casa.[161] Né rileva la circostanza che la visibilità delle fotografie sia ristretta solo agli amici della moglie, perché siffatta regola di riservatezza può essere agevolmente superata. Pertanto, una interpretazione evolutiva delle norme, che tenga conto dell'evoluzione tecnologica e del mutato costume sociale, non può giungere sino a ritenere lecita la pubblicazione dell'immagine di una persona senza il suo consenso. Infatti, l'estrema diffusività della pubblicazione su *internet* di una fotografia aggrava notevolmente, rispetto a qualsiasi altro mezzo, la violazione del diritto all'immagine, anche perché le eventuali regole di *privacy* possono essere aggirate da navigatori esperti[162].

Il consenso[163] sembra conservare quindi il suo carattere di elemento essenziale e insuperabile, pena l'illegittimità della pubblicazione dell'immagine di una persona[164]. Non sembrerebbe esserci ancora un diritto/principio alla libera diffusione di immagini altrui, non avendo lo stesso, ad oggi, superato il vaglio della compatibilità con la legalità costituzionale. Infatti, non è dato comprendere quale possano essere i valori del nostro ordinamento, nel suo complesso considerato, atti a giustificarne la tutela.

Al contrario, proprio la pubblicazione dell'immagine di taluno, dei suoi dati e/o pensieri personali, su un *social network* consentirebbe un accesso massiccio e indifferenziato degli utenti del *web* nella sua sfera privata e ciò sarebbe contrario ai valori fondamentali protetti dal nostro ordinamento. Tale ingerenza nella vita privata di ciascuno senza che vi sia una

---

161 Trib. Napoli, 15 luglio 2014, n. 12749, cit.

162 Trib. Napoli, *ibidem*.

163 La rilevanza del consenso per la liceità della raccolta e del trattamento dei dati personali è consacrata anche nella «Dichiarazione dei diritti in Internet», della Commissione per i diritti e i doveri in *internet*, Camera dei deputati, del 28 luglio 2015 e precisamente nell'art. 5, comma 5 e 6.

164 Sulla rilevanza del consenso ai fini della legittimità della pubblicazione dell'immagine di una persona, anche nell'ordinamento spagnolo la giurisprudenza (Tribunal Supremo, Sala de lo Civil, Pleno, 15 febbraio 2017, n. 91/2017, in Instituto de Derecho Iberoamericano, *www.idibe.org*) ha statuito che non è lecito illustrare la notizia con un'immagine utilizzata dal titolare della stessa come profilo *Facebook*, senza il suo consenso. Nella specie, un giornale spagnolo, nel riportare quanto accaduto del ricorrente - ossia l'essere stato ferito con un'arma da fuoco dal fratello poi suicidatosi - pubblicava anche una fotografia dello stesso, che era stata presa dal suo profilo *Facebook*. Il Tribunal Supremo, sulla premessa per la quale nel giornale non era stata pubblicata una fotografia del ricorrente - vittima del fatto delittuoso oggetto del *reportage* - ottenuta sul luogo dei fatti, ma presa dal suo profilo *Facebook*, evidenzia come «*la publicación en el periódico de una fotografía del demandante, acompañando a la información sobre el hecho noticioso y a otras fotografías que ilustraban tal información, por más que el demandante tuviera una momentánea relevancia pública involuntaria en tanto que víctima del suceso violento sobre el que versaba el reportaje periodístico, obtenida de su cuenta de Facebook , sin recabar el consentimiento expreso del afectado para realizar tal publicación, no puede considerarse autorizada y constituye por tanto una intromisión en tal derecho fundamental que no está justificada del modo previsto en el art. 8.1 de la Ley Orgánica 1/1982. Tampoco puede considerarse justificada la publicación de la fotografía del demandante por aplicación del art. 8.2.c de dicha ley orgánica. La fotografía, pese a no ser de gran tamaño (solo incluía la imagen del demandante de cintura para arriba), tenía por único protagonista al demandante, de modo que identificaba directamente a la víctima del suceso violento sobre el que versaba el reportaje periodístico*.».

ragione giustificativa in nome di un interesse superiore, meritevole di tutela, non è accettabile. L'idea che, sulla rete, il principio di responsabilità sia travolto dal prevalere sempre e comunque della libertà di comunicazione e diffusione del pensiero è un'idea appunto, non un valore e, pertanto, nella sua radicalità, non può essere accolta. D'altronde, neanche l'interesse all'acquisizione di informazioni trova tutela costituzionale, poiché esistono norme che, garantendo l'inviolabilità personale, del domicilio e della corrispondenza (artt. 13, 14 e 15 Cost.), precludono ingerenze volte all'acquisizione di informazioni e perciò privilegiano rispetto ad esse la tutela del riserbo. Né, d'altro lato, è dato individuare la norma costituzionale che possa costituire la base di un diritto ad acquisire informazioni[165].

Una siffatta ingerenza potrebbe, tuttavia, essere ammessa solo ove risultasse oggettivamente giustificata e necessaria per la tutela di un interesse tutelato ad eguale livello, come quello, ad esempio, della sicurezza nazionale o della repressione della criminalità e sulla base del fatto che esistono garanzie adeguate e verificabili di tutela della persona. Solo un interesse meritevole di tutela potrebbe, nella contingenza concreta, autorizzare un'ingerenza altrimenti vietata. Occorrerà, allora, individuare le peculiarità del caso concreto[166] e, nel complesso sistema italo-comunitario delle fonti[167], i valori/princípi idonei a costruire, di volta in volta, la disciplina piú congrua[168]. Si tratta, quindi, di effettuare un non sempre agevole bilanciamento di interessi in conflitto e, in tale ottica, verificare la sussistenza di ragioni di interesse pubblico all'acquisizione e diffusione di informazioni idonee a giustificare la prevalenza di detto interesse su quello antagonista alla riservatezza.

Pertanto, tornando al caso di cui prima, potrebbe considerarsi lecita la pubblicazione delle fotografie in questione, senza il preventivo consenso del marito, allorquando ciò sia giustificato dai concreti comportamenti tenuti dallo stesso prima e dopo la pendente separazione. Se costui, ad esempio, non accettando la separazione, ha posto in essere

---

165 A. CATAUDELLA, cit. Di diverso avviso: N. LIPARI, *Intervento*, in *Il riserbo e la notizia*, Atti del Convegno di Macerata del 1982, Napoli, 1983, p. 247 s.; V. CUFFARO, *Profili civilistici del diritto all'informazione*, Napoli, 1986, p. 105 ss.

166 Sul punto v., *retro*, cap. I, § 1, nota 8.

167 Afferma la complessità e l'unitarietà dell'ordinamento giuridico, evidenziando la difficoltà nell'ammettere un ordinamento altro, inteso come comparto stagno rispetto al primo, P. PERLINGIERI, *Complessità e unitarietà dell'ordinamento giuridico vigente*, in *Rass. dir. civ.*, 2005, 1, p. 188 s.; ID., *Lo studio del diritto nella complessità e unitarietà del sistema ordinamentale,* in *Foro nap.*, 2014, 1, p. 100.

168 P. PERLINGIERI, *Il diritto civile nella legalità costituzionale*, cit., p. 352 ss.

condotte persecutorie[169] nei confronti della moglie, rendere pubblica la sua immagine può facilitarne la sua individuazione da parte di chiunque possa reprimere le stesse, cosí evitando ulteriori e peggiori conseguenze in danno della moglie. In tal caso, non si può invocare il diritto alla riservatezza da chi sta violando la legge (nella specie commettendo un reato) e, quindi, ecco che l'interesse della moglie alla libertà morale, nonché alla sua incolumità prevale, nella peculiarità del caso concreto, sulla riservatezza del marito (al quale sono riconosciute garanzie adeguate e verificabili di tutela, *ex* artt. 13, 24, comma 2, 111 cost.) e dev'essere giocoforza tutelato.

Il problema, a ben vedere, riguarda ogni forma di comunicazione[170] che coinvolga un numero tendenzialmente illimitato di utenti in comunità virtuali sempre piú globali. E il rischio è che ciascuno diventi allo stesso tempo il potenziale controllore e il possibile controllato, il cacciatore e la preda.

---

[169] Il delitto di atti persecutori è previsto art. 612-*bis* c.p., introdotto con il d.l. 23.02.2009, n. 11.

[170] Involge il concetto di comunicazione nel *web*, differenziandosi tuttavia dalla tematica in esame per l'oggetto della tutela, il tema il silenzio elettorale da rispettare nel giorno precedente e in quelli stabiliti per le votazioni. Anche qui, l'interprete dovrà interrogarsi sul se il divieto di propaganda elettorale valga anche sul *web*. Sul punto, il riferimento normativo è il comma 1, dell'articolo 9, l. 4 aprile 1956 n. 212, per il quale: «[n]el giorno precedente ed in quelli stabiliti per le elezioni sono vietati i comizi, le riunioni di propaganda elettorale diretta o indiretta, in luoghi pubblici o aperti al pubblico, la nuova affissione di stampati, giornali murali o altri e manifesti di propaganda». Chiaramente, nel 1956, il legislatore non aveva pensato a *Facebook*, *Twitter*, *Google+* e in generale alla diffusione di notizie tramite il *web*. In un contesto in cui la propaganda politica si svolgeva con comizi, riunioni, giornali, stampati e altri manifesti in generale, è chiaro che il divieto della stessa riguardasse i soli veicoli attraverso i quali il pensiero politico si diffondeva, che non potevano che essere quelli testé richiamati. Oggi che buona parte dell'informazione avviene tramite il *web* la disposizione di legge è ormai obsoleta e necessiterebbe di una rivisitazione da parte del legislatore - sí da includere lo strumento di comunicazione piú utilizzato in questi anni - che, guarda caso, è silente. Della questione, allora, dovrà farsi carico l'interprete che potrà tuttavia ricercare il principio che il legislatore dell'epoca voleva perseguire con la disposizione in commento. Ebbene, dal testo della norma, è possibile comunque individuare, quale principio di fondo, l'intenzione del legislatore di tenere a distanza la capacità persuasiva della politica, dagli elettori, almeno nelle ultime ventiquattro ore che precedono il voto, invitandoli a frenare la propaganda e le comunicazioni rivolte ai cittadini. Inoltre, stando sempre al testo, il legislatore parla oltre che di «affissioni di stampati», «giornali murali» o «manifesti di propaganda», anche di «luoghi pubblici o aperti al pubblico». Allora, la domanda è: il *web* è un luogo aperto al pubblico? La risposta a questa domanda sembra essere affermativa, se consideriamo che anche il *web* è una piazza pubblica, accessibile da chiunque, pertanto anche in esso dovrebbe valere la regola del silenzio elettorale. Non sembra, però, peregrina un'altra e difforme interpretazione. Si potrebbe, infatti, ritenere che, cosí come non è assolutamente vietato, nel giorno precedente e in quelli in cui si vota, comunicare ai propri amici incontrati nella piazza o al bar del paese la propria preferenza elettorale, allo stesso non sembrerebbe vietato «postare» la stessa cosa su *Facebook*, poiché, si potrebbe dire, altro non sarebbe che comunicazione del proprio pensiero ai propri amici, in questo caso «virtuali». A ben vedere questa interpretazione non appare convincente, se si considera la potenziale capacità persuasiva sugli elettori di una siffatta comunicazione nel *web* che la normativa di riferimento vuole scongiurare a poche ore e durante il voto.

Come opportunamente sottolineato dall'Autorità garante[171], i flussi di informazione costituiscono ormai una modalità imprescindibile per il funzionamento del sistema economico globale. Per la loro attività, infatti, le imprese hanno necessità di «esportare» dati da un Paese all'altro.

Proprio il trasferimento dei dati, in particolare il trasferimento verso un Paese «terzo»[172], è ciò che piú deve interessare e, inoltre, preoccupare lo studioso della tematica in questione, se è vero com'è vero, come già anticipato, che il *cloud* richiede, per poter erogare un servizio su larga scala, una grande molteplicità di *server*, collocati nelle parti piú diverse del mondo, nelle quali, appunto, i dati vengono traferiti.

Pertanto, occorre, con ordine, ripercorrere la normativa europea e nazionale, relativa a siffatto trasferimento, anticipando, sin da subito, che la tematica è stata «scossa» da una recente, quanto dirompente, sentenza della Corte di Giustizia dell'Unione Europea[173], nonché interessata dal nuovo Regolamento europeo[174] in materia di protezione dei dati personali - che abroga e sostituisce la direttiva 95/46/CE - e dalla Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini[175], costituente il c.d. «pacchetto protezione dati».

---

171 *Newsletter* 8-14 ottobre 2001, n. 98.

172 Il Paese «terzo» è il Paese non appartenente all'Unione europea o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein. Siffatto trasferimento non può avvenire *sic et sempliciter*, in considerazione del fatto che non è scontata l'esistenza nel Paese «terzo», appunto, di un corpo normativo organico sulla tutela della *privacy* paragonabile a quello vigente in Europa, infatti lo stesso necessità di un'apposita autorizzazione del Garante emessa «sulla base di adeguate garanzie per i diritti dell'interessato» (art. 44, d.lg. n. 196/2003), individuate dal Garante stesso (lett. a, art. 44 cit.) o con le decisioni previste dalla direttiva 95/46/CE (lett. b, art. 44 cit.). Sul punto si rinvia al par. 2.

173 Corte giust., 6 ottobre 2015, C-362/14, Maximillian Schrems c. Data Protection Commissioner, in *www.curia.eu*, che ha dichiarato invalido il regime introdotto in virtú dell'accordo «Approdo sicuro» (*Safe Harbor*), facendo venire meno il presupposto di legittimità per il trasferimento negli Usa di dati personali dei cittadini europei per chi utilizzava questo strumento. Sul tema si tornerà in seguito, al § 3.3. cap. II.

174 «Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).». Il citato Regolamento, pubblicato sulla Gazzetta Ufficiale dell'Unione europea (GUUE) in data 4 maggio 2016, è entrato in vigore venti giorni dopo la sua pubblicazione in GUUE, per diventare definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018 (art. 99), quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale e le disposizioni del Regolamento.

175 «Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.». La citata Direttiva, pubblicata sulla Gazzetta Ufficiale dell'Unione europea (GUUE) in data 4 maggio 2016, è entrata in vigore il 5 maggio 2016 e da quel momento impegna gli Stati membri a recepire le sue disposizioni nel diritto nazionale entro 2 anni.

2. La storia del pacchetto protezione dati.

Nel gennaio 2012, la Commissione europea presentava ufficialmente il cosiddetto «pacchetto protezione dati», con lo scopo di garantire un quadro coerente ed un sistema complessivamente armonizzato in materia nell'Unione europea.

Esso si costituiva di due diversi strumenti:

a) una proposta di Regolamento concernente «la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati», volta a disciplinare i trattamenti di dati personali sia nel settore privato sia nel settore pubblico, e destinata a sostituire la Direttiva 95/46;
b) una proposta di Direttiva indirizzata alla regolamentazione dei settori di prevenzione, contrasto e repressione dei crimini, nonché all'esecuzione delle sanzioni penali, che sostituirà (ed integrerà) la decisione quadro 977/2008/CE sulla protezione dei dati personali scambiati dalle autorità di polizia e giustizia (che l'Italia non ha, peraltro, ancora attuato).

L'*iter* per l'approvazione definitiva dei due nuovi strumenti normativi ha comportato l'intervento congiunto di Parlamento europeo e Consiglio UE in base alla procedura detta di «codecisione» (ora definita dal Trattato di Lisbona «procedura legislativa»[176]). Il 18 dicembre 2015 è stato raggiunto un accordo sul testo del Regolamento e della Direttiva[177]. Il 14 aprile 2016 la plenaria del Parlamento Europeo ha adottato in seconda lettura i testi di Regolamento e Direttiva come approvati dal Consiglio[178]. Il 4 maggio 2016, sono stati pubblicati sulla Gazzetta Ufficiale dell'Unione Europea (GUUE) i testi del Regolamento europeo in materia di protezione dei dati personali e della Direttiva che regola i trattamenti di dati personali nei settori di prevenzione, contrasto e repressione dei crimini [179].

Il Presidente dell'Autorità Garante italiana per la protezione dei dati personali, dott. Antonello Soro, ha cosí commentato: «*Oggi è una giornata importante per i cittadini europei e per la tutela dei loro diritti. Con la pubblicazione in Gazzetta Ufficiale dell'Unione Europea dei testi del Regolamento in tema di protezione dei dati e della Direttiva nelle attività di polizia e giustizia, si conclude*

176 Art. 14 del Trattato sull'Unione Europea.
177 Vedi il comunicato stampa del Consiglio europeo del 18 dicembre 2015 «*Riforma della protezione dei dati nell'UE: il Consiglio conferma l'accordo con il Parlamento europeo*», consultabile sul sito *web* del Consiglio europeo alla pagina http://www.consilium.europa.eu/it/press/press-releases/2015/12/18-data-protection/in.
178 Vedi comunicato stampa del 14 aprile 2016.
179 Vedi il comunicato stampa del Garante *privacy*, del 4 maggio 2016, «*Pubblicato sulla Gazzetta Ufficiale Ue il nuovo Pacchetto protezione dati*», in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4964718.

uno dei più complessi, travagliati e rilevanti percorsi di riforma dell'Unione europea. Il Regolamento porta grandi novità sul piano della tutela dei diritti e degli strumenti previsti per responsabilizzare maggiormente le imprese stabilendo, al contempo, significative semplificazioni. Le nuove regole raccolgono certamente la sfida più importante: adeguare le norme di protezione dei dati ai cambiamenti determinati dall'incessante evoluzione delle tecnologie.».

Ma, soprattutto - aggiunge Soro - «*nel momento in cui si fanno sempre più forti le spinte anacronistiche a creare "barriere" alla libera circolazione di beni e persone, il Regolamento raggiunge l'ambizioso obiettivo di assicurare una disciplina uniforme ed armonizzata tra tutti gli Stati membri, eliminando definitivamente le numerose asimmetrie che si erano create nel tempo. L'Europa, per quanto debba ancora ampiamente esprimere le sue potenzialità nello sviluppo di un vero mercato digitale, ha oggi la straordinaria opportunità di dimostrare la propria capacità di evolvere e di esportare, su scala mondiale, il proprio modello di protezione dei dati capace di coniugare al punto più alto i diritti delle persone con le esigenze delle imprese e del mercato*».[180]

2.1. La Direttiva 95/46/CE e il trasferimento dei dati personali verso un paese «terzo».

Sebbene la Direttiva 95/46/CE sia stata abrogata e sostituita dal summenzionato Regolamento (UE) 2016/679, quest'ultimo sarà definitivamente applicabile, in via diretta in tutti i Paesi UE, solo a partire dal 25 maggio 2018 (quando dovrà essere garantito il perfetto allineamento fra la normativa nazionale e le disposizioni del Regolamento). Inoltre, non può, in ogni caso, non considerarsi la precedente normativa, di cui la presente trattazione non può prescindere. Lo richiede la instaurata fase di transizione in uno alla completezza della ricerca, nonché la correttezza dell'analisi e dell'interpretazione, non potendosi indagare il nuovo scenario che, in quanto ancora *in fieri*, necessita, appunto, di un'accurata, quanto dettagliata, ricostruzione del previgente quadro normativo che, come detto, esigenze di allineamento e recepimento, non consentono di relegarlo già nel dimenticatoio[181].

---

[180] Cfr. *«Pacchetto protezione dati in G.U.U.E.: Soro, giornata importante per i cittadini europei. Disciplina uniforme contro ogni barriera»*, Roma, 4 maggio 2016, commento del Presidente del Garante per la protezione dei dati personali, in http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4966337.

[181] Lo stesso Regolamento 2016/679, al considerando 9, specifica che gli obiettivi e i princípi della direttiva 95/46/CE rimangano tuttora validi. Tuttavia, evidenzia che la direttiva 95/46/CE non ha impedito la

La direttiva in parola è il principale strumento giuridico dell'UE in materia di protezione dei dati personali. Essa mira a proteggere le libertà e i diritti fondamentali delle persone fisiche (segnatamente il diritto alla vita privata) in occasione del trattamento dei dati personali, eliminando al tempo stesso gli ostacoli alla libera circolazione di tali dati. La stessa specifica (al secondo considerando) che i sistemi di trattamento dei dati sono al servizio dell'uomo[182] e che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse.

La Direttiva *de qua* viene anche definita «Direttiva madre», proprio in quanto costituisce il testo di riferimento, a livello europeo, in materia di protezione dei dati personali. A tal fine, la direttiva fissa limiti precisi per la raccolta e l'utilizzazione dei dati personali e chiede a ciascuno Stato membro di istituire un organismo nazionale indipendente incaricato della protezione di tali dati, il che ha condotto poi alla nascita delle Autorità nazionali di protezione dati. L'art. 29 della Direttiva 95/46 istituisce, inoltre, uno specifico Gruppo per la tutela delle persone (c.d. *Working Party* art. 29) che è composto da un rappresentante della Autorità di controllo designate da ciascuno Stato membro e da un rappresentante della Commissione. Il Gruppo, che si riunisce a *Bruxelles* ogni bimestre, ha un carattere consultivo nei confronti di tutti gli atti adottati a livello comunitario che possono incidere sulla protezione dei dati.

Poiché è stata adottata allo scopo di armonizzare[183] le normative nazionali sulla protezione dei dati, la direttiva sulla protezione dei dati è caratterizzata da un grado di specificità paragonabile a quella delle legislazioni nazionali (allora) vigenti in materia. Per la Corte di Giustizia dell'Unione europea «la direttiva 95/46 mira […] a rendere equivalente in tutti gli Stati membri il livello di tutela dei diritti e delle libertà delle persone riguardo al trattamento dei dati personali. […] Il ravvicinamento delle legislazioni nazionali applicabili in materia non deve avere per effetto un indebolimento della tutela da esse assicurata, ma deve, anzi, mirare a garantire un elevato grado di tutela nella Comunità. […]

---

frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche.» (cfr. 9° considerando Reg. 2016/679).

[182] Che il «trattamento dei dati personali dovrebbe essere al servizio dell'uomo» è espressamente sancito anche dal Regolamento (UE) 2016/679 al considerando 4, il quale sancisce altresí che «[i]l diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità».

[183] Cfr., per esempio, nella direttiva in disamina, i considerando 1, 4, 7 e 8.

L'armonizzazione delle suddette legislazioni nazionali non si limita quindi ad un'armonizzazione minima, ma sfocia in un'armonizzazione che, in linea di principio, è completa»[184]. Di conseguenza, gli Stati membri hanno solo una limitata libertà di manovra per quanto riguarda l'attuazione della direttiva. Se prima dell'entrata in vigore della direttiva uno Stato membro presentava già un livello di protezione più elevato ed ampio, detto *standard* poteva essere mantenuto.

Con particolare riferimento alla tematica del trasferimento dei dati personali, la Direttiva specifica che la tutela delle persone non deve essere impedita dal fatto che il responsabile del trattamento sia stabilito in un paese terzo, prevedendo che, in tal caso, è opportuno che i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva (ventesimo considerando).

Innanzitutto, occorre, distinguere il trasferimento dei dati verso un Paese non comunitario da quello intra-comunitario, il quale, proprio per l'esistenza di un adeguato livello di protezione discendente dalla implementazione della Direttiva sulla *data protection* in tutti i 28 Paesi membri, non pone alcun problema[185]: anzi, l'impostazione del legislatore è altamente «liberale» visto che le disposizioni del Codice *privacy* non possono essere applicate

---

184 CGUE, cause riunite C-468/10 e C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado,* 24 novembre 2011, punti 28 e 29.

185 La diversa questione della «trasmissione» di dati personali da un'impresa ad un'altra con sede in un altro Stato membro è stata affrontata dalla Corte di Giustizia, con la sentenza 15 marzo 2017 [c. 536/15, Tele2 (Netherlands) BV, Ziggo BV e Vodafone Libertel BV / Autoriteit Consument en Markt (ACM), in *www.curia.eu*]. In tale occasione una società belga, fornitrice di elenchi abbonati e servizi di consultazione telefonica accessibili dal proprio territorio, chiedeva alle imprese che attribuiscono numeri di telefono ad abbonati dei Paesi Bassi (vale a dire Tele2, Ziggo e Vodafone Libertel) di mettere a sua disposizione i dati relativi ai loro abbonati, avvalendosi a tale riguardo di un obbligo previsto dalla direttiva europea sul «servizio universale» (dir. 2002/22/CE). Ritenendo di non essere tenute a fornire i dati in questione a un'impresa avente sede in un altro Stato membro, le imprese suddette si rifiutavano di fornire i dati richiesti. Ebbene, la Corte ha dichiarato che la direttiva summenzionata si applica anche alle richieste provenienti da un'impresa che abbia sede in uno Stato membro diverso da quello in cui hanno sede le imprese che attribuiscono numeri di telefono agli abbonati, dal momento che tali imprese sono tenute a soddisfare, proprio in forza della direttiva sul «servizio universale» (*ex* art. 25, par. 2), «qualsiasi richiesta ragionevole di messa a disposizione». Pertanto, è stato statuito come la richiamata normativa non distingua a seconda che la richiesta sia formulata da parte di un'impresa con sede nello stesso Stato membro in cui ha sede l'impresa a cui tale richiesta è indirizzata o in un altro Stato membro. Tale assenza di distinzione è conforme allo scopo perseguito dalla direttiva, che mira, in particolare, a garantire la disponibilità in tutta l'Unione di servizi di buona qualità accessibili al pubblico attraverso una concorrenza efficace e un'effettiva possibilità di scelta. Inoltre, il rifiuto di mettere i dati relativi agli abbonati a disposizione dei richiedenti, per il solo motivo che questi ultimi avrebbero sede in un altro Stato membro, sarebbe incompatibile con il principio di non discriminazione.

in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni (art. 42[186]). In sostanza nemmeno è del tutto corretto parlare di «trasferimento», visto che lo spazio UE (e lo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è considerato un unico territorio.

Nel caso, invece, di trasferimenti di dati personali verso Paesi *extra*-UE - che ci interessa maggiormente, posto che spesso i *server* nei servizi *cloud* sono collocati nelle parti piú diverse del mondo - il discorso è diverso, vigendo un principio del tutto opposto.

Il Capo IV della Direttiva 95/46/CE è rubricato «Trasferimento dei dati personali verso paesi terzi», ove sono previsti i princípi (art. 25) e le deroghe (art. 26) in merito a siffatto trasferimento.

Pertanto, il trasferimento di dati personali da paesi appartenenti all'Unione europea verso Paesi «terzi» (non appartenenti all'UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) è vietato, in linea di principio (articolo 25, comma 1), a meno che il Paese in questione garantisca un «livello di protezione adeguato»[187]. L'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati, nel rispetto di determinate condizioni espressamente elencate al comma 2, dell'art. 25[188], in esame. La Commissione ha il potere di stabilire tale adeguatezza attraverso una specifica decisione (articolo 25, comma 6), c.d. «decisione di adeguatezza». In particolare, il paragrafo 6 dell'art. 25 attribuisce alla Commissione il potere di «constatare» che un paese terzo

[186] L'art. 42, D.lg. 30 giugno 2003, n. 196, prevede che: «Le disposizioni del presente codice non possono essere applicate in modo tale da restringere o vietare la libera circolazione dei dati personali fra gli Stati membri dell'Unione europea, fatta salva l'adozione, in conformità allo stesso codice, di eventuali provvedimenti in caso di trasferimenti di dati effettuati al fine di eludere le medesime disposizioni.».

[187] Ai sensi dell'art. 25, comma 1, della Direttiva 95/46/CE «Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.». È richiesto, dunque, un giudizio di adeguatezza, e non di uguaglianza, di protezione, nel senso che il paese importatore dei dati non deve garantire il medesimo livello di protezione offerto dalla legislazione europea, ma quelle garanzie, che ad un giudizio obiettivo, appaiano adeguate.

[188] L'art. 25, comma 2, Direttiva 95/46/CE, sancisce: «[l]'adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate.».

garantisce un livello di protezione adeguato, in virtú di parametri predeterminati, ossia «in considerazione della sua legislazione nazionale o i dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona». In tal modo, la disposizione in commento attua l'obbligo esplicito di protezione dei dati personali previsto all'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea e mira ad assicurare la continuità del livello elevato di tale protezione in caso di trasferimento di dati personali verso un paese terzo.

L'espressione «livello di protezione adeguato» deve essere inteso nel senso di esigere che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza della direttiva 95/46, letta alla luce della Carta[189]. Gli strumenti dei quali tale paese terzo si avvale, al riguardo, per assicurare un siffatto livello di protezione, se ben possono essere diversi da quelli attuati all'interno dell'Unione al fine di garantire il rispetto dei requisiti risultanti da tale direttiva, letta alla luce della Carta, devono tuttavia rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione[190].

Sulla base di questo meccanismo[191], ad oggi alcuni Stati *extra*-UE[192] sono stati ritenuti, con apposita «decisione di adeguatezza» ratificata da altrettanti provvedimenti dei Garanti nazionali, tali da garantire un adeguato livello di protezione dei dati personali nella rispettiva legislazione, con la conseguenza che trasferire i dati in tali Paesi è come trasferirli all'interno della UE.

Quella poc'anzi menzionata non è l'unica deroga al divieto di trasferimento dei dati, se ne rinvengono, infatti, altre che occorre passare in rassegna.

Innanzitutto, in deroga a tale divieto, il trasferimento verso Paesi terzi è consentito anche nei casi menzionati dall'articolo 26, comma 1, della Direttiva 95/46 (consenso della

189 Punto 73, Corte giust., 6 ottobre 2015, C-362/14, cit.
190 Punto 74, Corte giust., 6 ottobre 2015, C-362/14, cit.
191 Il procedimento in esame prevede, tra l'altro, il parere favorevole del Gruppo dei Garanti *privacy* UE.
192 Andorra; Argentina; Australia – PNR; Canada; Faer Oer; Guernsey; Isola di *Man*; Israele; *Jersey*; Nuova Zelanda; Svizzera; *Uruguay*; USA – *Safe Harbor* (ora dichiarato invalido dalla Corte di Giustizia, vedi Provvedimento del 22 ottobre 2015 e comunicato stampa del 6 novembre 2015 del Garante privacy italiano); USA – PNR.

persona interessata, necessità del trasferimento ai fini di misure contrattuali/precontrattuali, interesse pubblico preminente, salvaguardia dell'interesse vitale dell'interessato etc.), nonché sulla base di strumenti contrattuali che offrano garanzie adeguate (articolo 26, comma 2, della Direttiva 95/46).

Pertanto, il divieto in parola può essere superato dalle cosiddette «*clausole contrattuali standard*». La Commissione europea, ai sensi dell'articolo 26, comma 4, della Direttiva in disamina, può stabilire che determinati strumenti contrattuali consentono di trasferire dati personali verso Paesi terzi. Si tratta di una delle deroghe (stabilite nel comma 2, dell'articolo 26) al divieto di effettuare il trasferimento verso Paesi che non offrono garanzie «adeguate» ai sensi della Direttiva 95/46/CE. In pratica, incorporando il testo delle clausole contrattuali in questione in un contratto utilizzato per il trasferimento (*Data Transfer Agreement*), l'esportatore dei dati garantisce che questi ultimi saranno trattati conformemente ai princípi stabiliti nella Direttiva anche nel Paese terzo di destinazione. Sinora la Commissione ha adottato quattro decisioni in materia[193].

Altra deroga al divieto è rappresentata dalla procedura cosiddetta delle *BCR – Binding Corporate Rules*. Si tratta di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (*extra*-UE) tra società facenti parti dello stesso gruppo d'impresa. Le BCR si concretizzano in un documento contenente una serie di clausole (*rules*) che fissano i princípi vincolanti (*binding*) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (*corporate*). Le BCR costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali.

Il rilascio di un'autorizzazione al trasferimento di dati personali tramite BCR consente alle filiali della multinazionale che ne abbia fatto richiesta, anche se stabilite in diversi Paesi, di trasferire, all'interno del gruppo d'impresa, i dati personali oggetto delle BCR, senza ulteriori adempimenti (quali ad esempio la sottoscrizione di clausole contrattuali tipo, il rilascio di specifiche autorizzazioni ai sensi del Codice, etc). La procedura per la definizione

[193] Decisione Commissione, clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi, dir. 95-46-CE (5 febbraio 2010); Decisione della Commissione del 27 dicembre 2004 per l'introduzione di un insieme alternativo di clausole contrattuali tipo per il trasferimento di dati personali a paesi terzi (27 dicembre 2004); Decisione Commissione, clausole contrattuali tipo per trasferimento dati a carattere personale verso paesi terzi a norma dir. 95-46-CE (5 giugno 2001); Decisione Commissione, clausole contrattuali tipo per trasferimento dati personali a incaricati del trattamento residenti in paesi terzi, dir. 95-46-CE (27 dicembre 2001).

del testo delle BCR prevede una fase «europea» ed una fase «nazionale»; quest'ultima è finalizzata al rilascio dell'autorizzazione nazionale (ove necessaria, come in Italia).

Con riferimento alla procedura a livello europeo, e dal momento che le BCR hanno ad oggetto i flussi di dati personali tra società appartenenti a un unico gruppo di impresa e dislocate in diversi paesi del mondo, l'autorizzazione al trasferimento transfrontaliero di dati trova una sua utilità esclusivamente se rilasciata da tutte le Autorità di protezione dei dati competenti negli Stati Membri da cui hanno origine i trasferimenti.

Per questo motivo, il Gruppo dei Garanti UE ha elaborato una procedura di cooperazione a livello europeo in grado di assicurare la predisposizione di un testo di BCR condiviso da tutte le Autorità e valevole per tutti i trasferimenti oggetto delle BCR medesime. Tale procedura è condotta da una sola Autorità (c.d. «*lead Authority*») la quale dialoga, in rappresentanza di tutte le altre Autorità *privacy*, con la società capogruppo. In particolare, la *lead Authority* esamina la bozza di BCR presentata dalla società (c.d. «*consolidated draft*»), la invia alle altre Autorità per riceverne eventuali commenti (Fase 1) e dialoga con la società per la predisposizione di un testo che accolga tutte le osservazioni formulate (c.d. «*final draft*» - Fase 2).

Il documento cosí redatto è inviato alle Autorità partecipanti alla procedura, al fine di ottenerne una valutazione positiva in termini di adeguatezza del livello di protezione dei dati personali. Di recente, alcune Autorità (fra cui il Garante) hanno aderito ad una dichiara-zione di intenti, c.d. «*Dichiarazione di Mutuo riconoscimento*», al fine di semplificare la procedura di approvazione del testo di BCRa livello europeo, velocizzandone la relativa tempistica. Ai sensi di tale nuovo modello, la *lead Authority*, con il supporto di altre due Autorità, dialoga con la società capogruppo al fine di giungere alla predisposizione di un testo ritenuto in linea con i principi fissati dai documenti in materia di BCR emanati dai Garanti *privacy* UE. Il parere con il quale la *lead Authority* attesta la conformità del testo di BCR ai principi sopra indicati è considerato dalle altre Autorità aderenti al sistema di Mutuo riconoscimento quale fondamento sufficiente al rilascio della rispettiva autorizzazione nazionale. Qualora la singola Autorità si esprima a favore del testo di BCR, ovvero una volta raggiunta la definizione di un testo di BCR giudicato conforme dalla *lead Authority* in base alla procedura semplificata sopra descritta, l'Autorità nazionale potrà procedere al rilascio di un'autorizzazione nazionale al trasferimento dei dati personali oggetto del testo medesimo, ove prevista.

Sulla base di codesta normativa europea s'è modellata la normativa interna (Codice della *privacy*), la quale consente il trasferimento, anche temporaneo, fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea, solo se si verificano i presupposti fissati dall'art. 43[194] oppure in base ad una specifica autorizzazione del Garante da emettersi sulla base di adeguate garanzie per i diritti dell'interessato individuate secondo le specifiche di cui all'art. 44[195]. Lo stesso codice, nella disposizione di chiusura, art. 45, del Titolo VII (rubricato «Trasferimento dei dati all'estero») vieta poi i trasferimenti di dati verso quei Paesi di destinazione o di transito il cui ordinamento non assicura un livello di tutela delle persone adeguato.

---

[194] «Art. 43. Trasferimenti consentiti in Paesi terzi 1. Il trasferimento anche temporaneo fuori del territorio dello Stato, con qualsiasi forma o mezzo, di dati personali oggetto di trattamento, se diretto verso un Paese non appartenente all'Unione europea è consentito quando: a) l'interessato ha manifestato il proprio consenso espresso o, se si tratta di dati sensibili, in forma scritta; b) è necessario per l'esecuzione di obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato, ovvero per la conclusione o per l'esecuzione di un contratto stipulato a favore dell'interessato; c) è necessario per la salvaguardia di un interesse pubblico rilevante individuato con legge o con regolamento o, se il trasferimento riguarda dati sensibili o giudiziari, specificato o individuato ai sensi degli articoli 20 e 21; d) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; e) è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trasferiti esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; f) è effettuato in accoglimento di una richiesta di accesso ai documenti amministrativi, ovvero di una richiesta di informazioni estraibili da un pubblico registro, elenco, atto o documento conoscibile da chiunque, con l'osservanza delle norme che regolano la materia; g) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati; h) [soppressa]».

[195] «Art. 44. Altri trasferimenti consentiti 1. Il trasferimento di dati personali oggetto di trattamento, diretto verso un Paese non appartenente all'Unione europea, è altresì consentito quando è autorizzato dal Garante sulla base di adeguate garanzie per i diritti dell'interessato: a) individuate dal Garante anche in relazione a garanzie prestate con un contratto o mediante regole di condotta esistenti nell'ambito di società appartenenti a un medesimo gruppo. L'interessato può far valere i propri diritti nel territorio dello Stato, in base al presente codice, anche in ordine all'inosservanza delle garanzie medesime; b) individuate con le decisioni previste dagli articoli 25, paragrafo 6, e 26, paragrafo 4, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, con le quali la Commissione europea constata che un Paese non appartenente all'Unione europea garantisce un livello di protezione adeguato o che alcune clausole contrattuali offrono garanzie sufficienti.».

3. Tutela dei dati personali e loro libera circolazione su *internet*. Il caso *Lindqvist*.

La Corte di giustizia, come già visto[196], si era già pronunciata su questioni relative alla direttiva 95/46/CE, ma non in relazione al profilo della tutela della riservatezza in *internet* e al trasferimento di dati verso paesi terzi. Il giudice *a quo*, la *Göta hovrätt* (Corte d'appello della regione svedese del *Götaland*), sottopone all'attenzione della Corte di Giustizia sette questioni che offrono alla stessa la possibilità di definire la disciplina relativa al trattamento dei dati personali allorquando la stessa si interfaccia con le problematiche della rete. È il primo significativo intervento in materia, non esistendo precedenti in termini. La problematicità delle questioni, le piú critiche in tema di dati personali pubblicati in *internet*, impone di analizzarle tutte. Inoltre, le soluzioni offerte alle stesse, nella loro perduranza se non implementazione[197], dovranno poi essere confrontate con il Regolamento UE 2016/679, di recente approvato.

Occorre, allora, partire dalla vicenda - la cui protagonista può considerarsi una pioniera del *web* (all'epoca dei fatti non accessibile come oggi) - che ha generato il *dictum* giurisprudenziale, costituente senz'altro il «nocciolo duro» delle possibili interpretazioni successive (non a caso questa decisione viene citata anche nella decisione *Google Spain*[198]). Sicché, ricostruito il fatto, si potranno attentamente analizzare le questioni pregiudiziali vertenti sull'interpretazione della direttiva 95/46/CE.

La sig.ra *Lindqvist* era catechista nella parrocchia di *Alseda*, in Svezia. Ella, alla fine del 1998, creava, a casa sua e con un *personal computer*, alcune pagine *internet* allo scopo di consentire ai parrocchiani che si preparavano alla cresima di ottenere facilmente le informazioni che potevano essere loro utili. Tali pagine contenevano informazioni sulla sig.ra *Lindqvist* stessa e su diciotto suoi colleghi della parrocchia, compresi i loro nomi, accompagnati talvolta dai cognomi. La sig.ra *Lindqvist* descriveva, inoltre, in termini leggermente scherzosi, le mansioni dei colleghi e le loro abitudini nel tempo libero. In alcuni casi, era descritta la loro situazione familiare ed erano indicati i recapiti telefonici, nonché altre informazioni. Veniva altresí riferito il fatto che una collega, essendosi ferita ad un piede, era in congedo parziale per malattia.

---

[196] Sul punto si rinvia al § 2.1., Cap. II.

[197] Infatti, come chiarito al punto 58 della stessa sentenza sul caso *Lindqvist*, «le informazioni che si trovano su Internet possono essere consultate da un numero indefinito di persone residenti in molteplici luoghi e in qualsiasi momento. Il carattere ubiquitario di tali informazioni risulta in particolare dal fatto che i mezzi tecnici usati nell'ambito di Internet sono relativamente semplici e sempre meno costosi.».

[198] Cfr. ampiamente, *infra*, § 3.1., Cap. II.

La sig.ra *Lindqvist* veniva, quindi, accusata di aver utilizzato dati personali nell'àmbito di un trattamento automatizzato senza aver prima informato per iscritto la *Datainspektion* svedese (ente pubblico per la tutela dei dati trasmessi per via informatica), di averli trasferiti, senza autorizzazione, verso paesi terzi e di aver trattato, senza autorizzazione, dati personali sensibili (una ferita al piede ed un congedo parziale per malattia).

Condannata, dall'*Eksjö tingsrätt* (Tribunale di primo grado di *Eksjö*, Svezia), al pagamento di un'ammenda, la Sig.ra *Lindqvist* impugnava tale decisione dinanzi alla *Göta hovrätt* (Corte d'appello della regione del *Götaland*), che, dubitando sull'interpretazione della direttiva 95/46, applicabile in materia, sospendeva il procedimento e sottoponeva alla Corte di Giustizia sette questioni pregiudiziali, vertenti sull'interpretazione della predetta direttiva.

La Corte, innanzitutto, dichiara che l'operazione consistente nel fare riferimento, in una pagina *internet*, a diverse persone e nell'identificarle con il loro nome e cognome o con altri mezzi (numero di telefono o informazioni sulla loro situazione lavorativa e sui loro passatempi) costituisce un «trattamento di dati personali interamente o parzialmente automatizzato», ai sensi dell'art. 3, n. 1, della direttiva 95/46. Inoltre, quando viene menzionato lo stato di salute di una persona si tratta di un trattamento di dati relativi alla salute ai sensi dell'art. 8, n. 1, della stessa direttiva (quarta questione[199]).

La Corte richiama e analizza preliminarmente le nozioni di «dati personali» e «trattamento» (di siffatti dati) accolte dalla direttiva in analisi. La prima nozione - sostanziandosi in «qualsiasi informazione concernente una persona fisica identificata o identificabile»[200] - «ricomprende certamente il nome di una persona accostato al suo recapito telefonico o ad informazioni relative alla sua situazione lavorativa o ai suoi passatempo». Con riferimento alla seconda nozione[201], la Corte afferma che, gli tra i diversi esempi di operazioni, compiute con o senza l'ausilio di processi automatizzati, e applicate a dati personali, vi figurano la comunicazione mediante trasmissione, la diffusone o qualsiasi altra forma di messa a disposizione dei dati. È, allora, conseguenziale che l'operazione consistente nel far comparire in una pagina *internet* dati personali vada considerata come «trattamento» di tal genere.

---

[199] La quarta questione va quindi risolta nel senso che l'indicazione che una persona si è ferita ad un piede e si trova in congedo parziale per malattia costituisce un dato personale relativo alla salute ai sensi dell'art. 8, n. 1, della direttiva 95/46.
[200] Art. 2, lett. a), dir. 95/46/CE.
[201] Art. 2, lett. b), dir. 95/46/CE.

Ciò premesso, per affermare che tale trattamento è «automatizzato in tutto o in parte», la Corte rileva «che far apparire delle informazioni in una pagina Internet impone […] di realizzare un'operazione di caricamento di questa pagina su un server nonché le operazioni necessarie per rendere questa pagina accessibile a coloro che si sono collegati ad Internet. Tali operazioni vengono effettuate, almeno in parte, in modo automatizzato».

Risolvendo la terza questione[202] - con la quale il giudice *a quo* chiede se un trattamento come quello del caso concreto rientri, o meno, in una delle due eccezioni previste dall'art. 3, n. 2 (direttiva in commento) - la Corte statuisce che il trattamento di dati personali del caso di specie non rientra né nella categoria di quelle attività espressamente menzionate (di cui al «primo trattino» dell'art. 3, n. 2, ossia le attività previste nei titoli V e VI del Trattato sull'Unione europea nonché i trattamenti aventi ad oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività relative a settori del diritto penale), né nella categoria di attività a carattere esclusivamente personale o domestico («secondo trattino» dell'art. 3, n. 2), che esulano dall'àmbito d'applicazione della direttiva. La Corte, dunque, non accoglie la tesi della sig.ra *Lindqvist*, secondo la quale ella ha fatto uso della sua libertà di espressione creando pagine *internet* nell'àmbito di un'attività a scopo non lucrativo o del suo tempo libero e, pertanto, non avendo esercitato un'attività economica, tale sua attività esula dall'applicazione del diritto comunitario.

È il caso di analizzare in maniera piú specifica tale questione, concernente l'àmbito (*rectius*, campo) di applicazione (quello che viene definito oggi «ambito di applicazione materiale» dal Regolamento UE 2016/679, all'art. 2) della direttiva.

Ebbene, la Corte richiamato l'obiettivo essenziale della direttiva - cioè ravvicinare le disposizioni legislative, regolamentari ed amministrative degli Stati membri per eliminare gli ostacoli al funzionamento del mercato interno derivanti proprio dalle disparità esistenti tra le normative nazionali[203] - ritiene che «le attività menzionate a titolo esemplificativo nell'art. 3, n. 2, primo trattino, della direttiva 95/46 siano destinate a definire la portata dell'eccezione ivi prevista, di modo che detta eccezione si applica solo alle attività che vi sono così espressamente menzionate e che possono essere ascritte alla stessa categoria (*eiusdem generis*)». Sulla base di questa considerazione, la Corte statuisce che «attività a titolo

[202] La seconda, posta solo per il caso di soluzione negativa della prima, è assorbita e, pertanto, non occorre risolverla, proprio dalla risoluzione in senso affermativo della prima.
[203] Ciò, come precisa la Corte stessa, è stato già chiarito da Corte di Giustizia, sentenza 20 maggio 2003, cause riunite c. 465/00, c. 138/01 e c. 139/01, Österreichischer Rundfunk e a., Racc. pag. I-4989, punto 42.

religioso o di volontariato, come quelle esercitate dalla sig.ra *Lindqvist*, non sono equiparabili alle attività indicate nell'art. 3, n. 2, primo trattino, della direttiva 95/46 e non sono quindi comprese in tale eccezione».

Per quanto riguarda l'eccezione di cui all'art. 3, n. 2, secondo trattino, la Corte richiama il dodicesimo «considerando», relativo a tale eccezione, il quale menziona, a titolo di esempio di trattamento di dati effettuato da una persona fisica nell'esercizio di attività a carattere esclusivamente personale o domestico, la corrispondenza e la compilazione di elenchi di indirizzi. Tale esempio è indice del fatto che l'eccezione in parola deve interpretarsi nel senso che comprende unicamente le attività che rientrano nell'àmbito della vita privata o familiare dei singoli, il che manifestamente non avviene nel caso del trattamento di dati personali consistente nella loro pubblicazione su *internet* in modo da rendere tali dati accessibili ad un numero indefinito di persone.

La vicenda in esame affronta anche il tema del trasferimento transfrontaliero di dati personali sulle reti digitali (la quinta delle sette questioni sottoposte alla Corte di Giustizia). In buona sostanza, si chiede alla Corte se possa configurarsi trasferimento transfrontaliero di dati verso paesi terzi la semplice immissione di dati personali in *internet* - ospitati da un *web hosting provider* stabilito sul territorio comunitario - tale renderli accessibili a chiunque si colleghi ad *internet*, compresi coloro che si trovano in paesi terzi.

La Corte risolve la suddetta questione rilevando che la direttiva prevede anche norme specifiche[204] che mirano a garantire un controllo da parte degli Stati membri sul trasferimento di dati personali verso i paesi terzi. Tuttavia, alla luce dello stato di sviluppo di *internet* all'epoca dell'elaborazione della direttiva e della mancanza di criteri applicabili all'uso dello stesso, essa ritiene che il legislatore comunitario non avesse l'intenzione di includere nella nozione di «trasferimento verso un paese terzo di dati» l'inserimento di dati in una pagina *internet*, anche se questi in tal modo sono resi accessibili alle persone di paesi terzi.

La Corte, nel suo argomentare, consapevole del fatto che la direttiva non definisce, né all'art. 25 né in alcun'altra disposizione, in particolare al suo art. 2, la nozione di «trasferimento verso un paese terzo», non può che indagare sulle concrete modalità d'uso di *internet* (disponibili ai singoli, cosí come alla protagonista della vicenda), in quanto solo in

[204] Capo IV, Dir. 95/46/CE, rubricato «Trasferimento dei dati personali verso paesi terzi».

tale contesto è possibile accertare l'intenzione del legislatore comunitario e, quindi, qualificare le operazioni effettuate della sig.ra *Lindqvist*. Ebbene, la Corte evidenzia che quest'ultima, quale autrice di una pagina pubblicata in *internet*, trasmette i dati contenuti in tale pagina al suo fornitore di servizi di ospitalità (*web hosting provider*). Si descrive cosí l'attività di quest'ultimo, il quale gestisce l'infrastruttura informatica e la connessione del *server* che ospita il sito *internet*. In tal modo, i dati pubblicati giungono a chiunque sia collegato ad *internet* e chieda di ottenerli. La peculiarità di tale meccanismo consiste essenzialmente nel fatto che i *computer* che costituiscono questa infrastruttura informatica possono essere situati, e spesso lo sono, in uno o piú paesi diversi da quello del luogo in cui ha sede il *web hosting provider*.

Ciò premesso, la Corte evidenzia che, per ottenere le informazioni figuranti sulle pagine *internet* create dalla sig.ra *Lindqvist* e sulle quali la stessa aveva pubblicato dati relativi ai suoi colleghi, un utente di *internet* doveva non soltanto collegarsi al *web*, ma anche effettuare, con un procedimento personale, le azioni necessarie per consultare le suddette pagine. Ciò significa che le pagine *internet* create della sig.ra *Lindqvist* non contenevano quei meccanismi tecnici atti a consentire l'invio automatico di tali informazioni a persone che non avessero deliberatamente cercato di accedere a dette pagine.

Ne discende che, nel caso di specie, «i dati personali che giungono al computer di una persona che si trova in un paese terzo, provenienti da una persona che li ha caricati su un sito Internet, non sono stati trasferiti direttamente tra queste due persone, ma attraverso l'infrastruttura informatica del fornitore di servizi di ospitalità presso il quale la pagina è caricata.»[205].

Delineato, come sopra, il contesto in cui occorre accertare se il legislatore comunitario avesse l'intenzione, di ricomprendere nella nozione di «trasferimento verso un paese terzo di dati personali», operazioni come quelle effettuate dalla sig.ra *Lindqvist*, la Corte passa all'analisi del capo IV della direttiva 95/46, statuendo che esso «istituisce un regime complementare al regime generale attuato dal capo II della suddetta direttiva, riguardante la liceità di trattamenti di dati personali». Pertanto, sulla base di una puntuale ricostruzione dell'obiettivo e della *ratio* del citato capo IV, anche attraverso il richiamo ai «considerando»

[205] Punto 61 della sentenza in commento.

della direttiva ad esso relativi[206], dell'esigenza di garantire un controllo da parte degli Stati membri sul trasferimento di dati personali verso i paesi terzi[207] e preso atto che il capo IV della direttiva non contiene alcuna disposizione riguardante l'uso di *internet*[208], la Corte afferma che «[…], non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente nella nozione di «trasferimenti verso un paese terzo di dati personali» l'inserimento, da parte di una persona che si trovi nella situazione della sig.ra Lindqvist, di dati in una pagina Internet, anche se questi sono così resi accessibili alle persone di paesi terzi in possesso dei mezzi tecnici per consultarli».

Il ragionamento dei giudici comunitari fa essenzialmente perso sulla considerazione che, qualora il semplice caricamento di dati personali sul *server web* integrasse gli estremi per un trasferimento di dati personali verso un Paese terzo, l'applicazione del regime previsto dall'art. 25 della direttiva 96/46/CE produrrebbe un'*impasse*. L'operazione di caricamento, infatti, costituirebbe un trasferimento verso tutti i Paesi terzi, compresi quelli che non garantiscono un livello di tutela adeguato. Gli Stati membri, pertanto, si troverebbero a dover vietare l'inserimento dei dati in *internet* qualora anche solamente un Paese terzo non risultasse in grado di garantire tale livello di protezione.

Al fine di evitare l'eventualità, con gli evidenti impatti sulla libera circolazione dei dati che la direttiva vuole salvaguardare, la Corte interpreta la direttiva sottolineando che il rendere accessibili dati personali, attraverso l'immissione di essi in una pagina *internet*, caricata presso un *provider* stabilito in uno Stato membro, non configura un «trasferimento di dati personali verso paesi terzi». In altri termini: l'inserimento in *internet* di dati personali

---

206 Punto 64, «L'obiettivo del capo IV viene definito nei 'considerando' da cinquantasei a sessanta della direttiva 95/46, i quali dispongono in particolare che, se la tutela delle persone garantita nella Comunità da questa direttiva non osta al trasferimento di dati personali verso paesi terzi che garantiscano un livello di protezione adeguato, l'adeguatezza deve essere valutata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti. Quando un paese terzo non offre un livello di protezione adeguato, il trasferimento di dati personali verso tale paese dev'essere vietato.

207 Punto 65, «L'art. 25 della direttiva 95/46 impone, da parte sua, agli Stati membri ed alla Commissione vari obblighi di controllo sui trasferimenti di dati personali verso i paesi terzi, tenuto conto del livello di protezione concesso a siffatti dati in ciascuno di tali paesi.». Punto 66, «In particolare, l'art. 25, n. 4, della direttiva 95/46 prevede che, qualora la Commissione constati che un paese terzo non garantisce un livello di protezione adeguato, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati personali verso il paese terzo in questione».

208 Punto 67, «[i]l capo IV della direttiva 95/46 non contiene alcuna disposizione riguardante l'uso di Internet. Esso non precisa in particolare i criteri che consentono di determinare se, per quanto riguarda le operazioni effettuate mediante fornitori di servizi di ospitalità, occorra basarsi sul luogo di stabilimento del fornitore o sul suo domicilio professionale ovvero sul o sui luoghi in cui sono situati i computer che costituiscono l'infrastruttura informatica del fornitore.».

rende gli stessi potenzialmente accessibili a chiunque si trovi in un paese terzo e abbia i mezzi tecnici per consultarli, ma ciò non implica, contrariamente a quanto ritenuto dalla Commissione, un trasferimento extracomunitario.

Se cosí non fosse, «[i]l regime speciale previsto dal capo IV della suddetta direttiva diverrebbe quindi necessariamente, per quanto riguarda le operazioni su Internet, un regime di applicazione generale».

Il sesto quesito del giudice nazionale concerne il bilanciamento tra libertà di espressione e diritto alla riservatezza. Il giudice svedese chiede alla Corte se, in un caso come quello di specie, la direttiva 95/46 CE sulla riservatezza incide sulla libertà di espressione in modo incompatibile con l'art. 10 CEDU e dunque se la definizione «trattamento di dati interamente o parzialmente automatizzato», prevista all'art. 3 (lettera b) della direttiva 95/46, soddisfa i criteri di precisione e prevedibilità.

L'art. 10 CEDU tutela la libertà di espressione, garantendo «la libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee»; e, in questo modo, sembra aver voluto comprendere una vasta gamma di forme di comunicazione. La norma convenzionale non considera, tuttavia, la libertà di espressione come un diritto illimitato. Al contrario, prevede la possibilità che questo venga sottoposto a determinate «formalità, condizioni, restrizioni o sanzioni», necessarie «in una società democratica […] per la protezione della reputazione o dei diritti altrui, per impedire la divulgazione di notizie riservate». Sul punto è il caso di ricordare che la giurisprudenza, nell'interpretare l'art. 10 CEDU, ha ravvisato nella libertà di espressione «uno dei fondamenti essenziali di una società democratica, una delle condizioni di base del suo progresso»[209].

I giudici di Lussemburgo osservano che le disposizioni della direttiva 95/46 non pongono alcun limite incompatibile con la libertà di espressione; che la medesima direttiva persegue due obiettivi inevitabilmente «confliggenti», precisamente quelli di una libera circolazione dei dati e della tutela della riservatezza delle persone; che la complessità della materia ha necessariamente portato la direttiva ad introdurre disposizioni relativamente «generiche» ed elastiche, in grado di tenere conto adeguatamente e di regolare «situazioni molto diverse»; che il compito di garantire il giusto equilibrio (e quindi di bilanciare gli interessi in gioco) spetta alle «autorità e ai giudici nazionali», incaricati di applicare la

[209] Sentenza *Handyside*, in *Europäische Grundrechte- Zeitschrift*, 1977, p. 38.

normativa statale emanata in esecuzione della direttiva europea. Di conseguenza, il «giusto equilibrio» tra libertà di espressione e riservatezza va verificato non già nella direttiva comunitaria, ma nella normativa nazionale. Per questa via il problema viene, piuttosto che risolto, spostato a livello «municipale». Secondo la Corte, la normativa nazionale sulla *privacy* può essere incompatibile con l'art. 10 CEDU se, operando, non garantisce il «giusto equilibrio». Nella sua decisione la Corte ha dunque affermato che, cosí formulate, le disposizioni generiche della direttiva 95/46 permettono un corretto bilanciamento tra la libertà di espressione e la riservatezza. A suo avviso, la direttiva lascia tuttavia «in numerosi casi» agli stati nazionali il compito di «decidere dei dettagli o di scegliere tra più opzioni» e quindi di individuare le modalità del bilanciamento.

L'ultima questione viene risolta nel senso che le misure adottate dagli Stati membri per garantire la protezione dei dati personali devono essere conformi tanto alle disposizioni della direttiva 95/46 quanto al suo obiettivo, consistente nel mantenere un equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata. Per contro, nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'àmbito di applicazione di quest'ultima, purché non vi osti alcun'altra disposizione del diritto comunitario.

3.1. ***Segue***. La sentenza «***Costeja***»[210].

Nel 2010, il sig. *Mario Costeja González*, cittadino spagnolo, presentava *all'Agencia Española de Protección de Datos* (Agenzia spagnola di protezione dei dati, AEPD) un reclamo contro *La Vanguardia Ediciones SL* (editore di un quotidiano largamente diffuso in Spagna, specialmente nella regione della Catalogna), nonché contro *Google Spain* e *Google Inc.* Il sig. *Costeja González* faceva valere che, allorché il proprio nome veniva introdotto nel motore di ricerca del gruppo *Google* («*Google Search*»), l'elenco di risultati mostrava dei *link* verso due pagine del quotidiano di *La Vanguardia*, datate gennaio e marzo 1998. Tali pagine annunciavano una vendita all'asta di immobili organizzata a seguito di un pignoramento

[210] Corte giust., 13 maggio 2014, C-131/12, Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González, in *www.curia.eu*.

effettuato per la riscossione coattiva di crediti previdenziali nei confronti del sig. *Costeja González*.

Mediante detto reclamo, il sig. *Costeja González* chiedeva, da un lato, che fosse ordinato a *La Vanguardia* di sopprimere o modificare le pagine suddette (affinché i suoi dati personali non vi comparissero piú) oppure di ricorrere a taluni strumenti forniti dai motori di ricerca per proteggere tali dati. Dall'altro lato, chiedeva che fosse ordinato a *Google Spain* o a *Google Inc.* di eliminare o di occultare i suoi dati personali, in modo che cessassero di comparire tra i risultati di ricerca e non figurassero piú nei *link* di *La Vanguardia*. Il sig. *Costeja González* affermava in tale contesto che il pignoramento effettuato nei suoi confronti era stato interamente definito da svariati anni e che la menzione dello stesso era ormai priva di qualsiasi rilevanza.

L'AEPD ha respinto il reclamo diretto contro *La Vanguardia*, ritenendo che l'editore avesse legittimamente pubblicato le informazioni in questione. Per contro, il reclamo è stato accolto nei confronti di *Google Spain* e *Google Inc.* L'AEPD ha chiesto a queste due società di adottare le misure necessarie per rimuovere i dati dai loro indici e per rendere impossibile in futuro l'accesso ai dati stessi. *Google Spain* e *Google Inc.* hanno proposto due ricorsi dinanzi all'*Audiencia Nacional* (Spagna), chiedendo l'annullamento della decisione dell'AEPD. È in tale contesto che il giudice spagnolo ha sottoposto una serie di questioni alla Corte di giustizia.

Con la sentenza in esame la Corte di Giustizia, similmente a quanto sostenuto dall'Avvocato generale, afferma che costituisce «trattamento di dati personali» l'attività di un motore di ricerca consistente nel trovare informazioni pubblicate o inserite da terzi su *internet*[211], nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di *internet* secondo un determinato ordine di preferenza, qualora tali informazioni contengano dati personali. Tuttavia, a differenza di quanto affermato dall'Avvocato generale, la Corte sostiene che il gestore del motore di ricerca deve essere considerato «responsabile» del menzionato trattamento, in quanto ne

[211] La Corte di Giustizia, nella sentenza in disamina, richiama al punto 26, quanto già affermato nel caso *Lindqvist*, ribadendo che: «per quanto riguarda in particolare Internet, la Corte ha già avuto modo di constatare che l'operazione consistente nel far comparire su una pagina Internet dati personali va considerata come un «trattamento» siffatto ai sensi dell'articolo 2, lettera b), della direttiva 95/46 (v. sentenza Lindqvist, C-101/01, EU:C:2003:596, punto 25).».

determina le finalità e gli strumenti del trattamento medesimo, ai sensi dell'art. 2, lett. d), dir. 95/46/CE[212].

Con riferimento all'àmbito di applicazione territoriale della normativa sulla protezione dei dati personali, la Corte osserva che *Google Spain* costituisce una filiale di *Google Inc.* nel territorio spagnolo e, pertanto, uno «stabilimento» ai sensi della Direttiva 95/46/CE sulla protezione dei dati. Al riguardo, la Corte considera che, quando dati siffatti vengono trattati per le esigenze di un motore di ricerca gestito da un'impresa che, sebbene situata in uno Stato terzo, dispone di uno stabilimento in uno Stato membro, il trattamento viene effettuato «nel contesto delle attività» di tale stabilimento, ai sensi della Direttiva, qualora quest'ultimo sia destinato ad assicurare, nello Stato membro in questione, la promozione e la vendita degli spazi pubblicitari proposti sul motore di ricerca al fine di rendere redditizio il servizio offerto da quest'ultimo[213].

Inoltre, sulla questione concernente l'estensione della responsabilità del gestore di un motore di ricerca ai sensi della direttiva 95/46, la Corte afferma che questi è obbligato a sopprimere, dall'elenco di risultati che appare a seguito di una ricerca effettuata a partire dal nome di una persona, alcuni *link* verso pagine *web* pubblicate da terzi e contenenti informazioni relative a questa persona, anche nel caso in cui tale nome o tali informazioni non vengano previamente o simultaneamente cancellati dalle pagine *web* di cui trattasi, e ciò anche nel caso in cui la loro pubblicazione su tali pagine *web* sia di per sé lecita[214].

Infine, interrogata sulla questione relativa alla portata del cd. «diritto all'oblio» degli interessati, la Corte afferma che occorre verificare, in particolare, se l'interessato abbia diritto a che informazioni riguardanti la sua persona non vengano piú, allo stato attuale, collegate al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome. Qualora si verifichi un'ipotesi siffatta, i *link* verso pagine *web* contenenti tali informazioni devono essere cancellati dall'elenco dei risultati di ricerca, a meno che sussistano ragioni particolari, come il ruolo ricoperto da tale persona nella vita

---

212 Punto 41, Corte giust., 13 maggio 2014, C-131/12, cit., in commento.

213 Punto 60, Corte giust., 13 maggio 2014, C-131/12, cit., in commento.

214 Punto 88, Corte giust., 13 maggio 2014, C-131/12, cit., in commento. In altri termini, a parere della Corte di Giustizia, al fine di salvaguardare al meglio il diritto fondamentale al rispetto della vita privata della persona interessata, è opportuno che il motore di ricerca non indicizzi piú le pagine sgradite, piuttosto che chiedere al c.d. sito sorgente di non pubblicare o rimuovere la notizia sgradita. La soluzione non convince F. DI CIOMMO, *Il diritto di accesso all'informazione in Internet*, in *Internet e Diritto civile*, a cura di C. Perlingieri e L. Ruggeri, Camerino-Napoli, 2015, p. 103, nota 46, ove l'a. evidenzia come sia ancor meno convincente «la veloce spiegazione con cui la Corte cerca di supportarla».

pubblica, giustificanti un interesse preminente del pubblico ad avere accesso a dette informazioni[215]. La Corte precisa che la persona interessata può rivolgere domande siffatte direttamente al gestore del motore di ricerca (anche quando nessun ordine di rimozione sia stato formulato nei confronti del gestore del sito) che deve in tal caso procedere ad un debito esame della loro fondatezza. In caso di mancato riscontro a tali richieste, l'interessato può adire l'autorità di controllo o l'autorità giudiziaria affinché queste effettuino le verifiche necessarie e ordinino al suddetto gestore l'adozione di misure precise conseguenti.

3.2. Casistica giurisprudenziale italiana dopo la sentenza «*Costeja*»: il Tribunale di Roma[216].

La notissima sentenza della Corte di giustizia europea del 13 marzo 2014, sopra analizzata, ha suscitato grande interesse e clamore sia tra gli addetti che ai lavori che presso l'opinione pubblica.

D'altronde non poteva essere altrimenti: la questione del «diritto all'oblio» o anche «diritto alla cancellazione»[217] di ciascuno di noi, a vedere cancellati i dati personali presenti in rete e che lo riguardano, è una di quelle che toccano chiunque, soprattutto nella attuale società in cui dati e informazioni personali sono presenti sul *web* ed il cui accesso è agevolato dal servizio di indicizzazione effettuato dai motori di ricerca.

Pertanto, sull'asserito presupposto dell'esistenza di un diritto all'oblio, un avvocato (che, nella specie, esercita la professione forense in Svizzera) conviene in giudizio dinanzi al Tribunale di Roma la società *Google Inc.*, chiedendo la deindicizzazione di alcuni *links* risultanti da una ricerca a proprio nome effettuata tramite il motore di ricerca *Google*.

---

[215] Punto 99, Corte giust., 13 maggio 2014, C-131/12, cit., in commento, ove si specifica la ragione giustificatrice di siffatta conclusione, in questi testuali termini: «i diritti fondamentali (dell'interessato derivanti dagli artt. 7 e 8 della Carta) […] prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico ad accedere all'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, in virtù dell'inclusione summenzionata, all'informazione di cui trattasi.».

[216] Trib. Roma, 3 dicembre 2015, n. 23771, in *www.iusexplorer.it*.

[217] Diritto oggi espressamente riconosciuto dal Regolamento europeo sulla *privacy* alla art. 17, rubricato appunto «Diritto alla cancellazione («diritto all'oblio»)». Sul punto v. *infra* § 4.1.2.

Tali *link* menzionavano il coinvolgimento del ricorrente in una vicenda giudiziaria, risalente al 2012/2013, nella quale era stato coinvolto - unitamente ad altri personaggi romani, alcuni esponenti del clero ed altri ricondotti alla criminalità della cd. banda della Magliana, relativamente a presunte truffe e guadagni illeciti realizzati dal sodalizio criminoso - senza peraltro riportare condanna alcuna.

Il Tribunale capitolino inquadra la vicenda nel trattamento dei dati personali e nel c.d. diritto all'oblio, il quale viene ritenuto configurabile «quale peculiare espressione del diritto alla riservatezza (privacy) e del legittimo interesse di ciascuno a non rimanere indeterminatamente esposto ad una rappresentazione non più attuale della propria persona derivante dalla reiterata pubblicazione di una notizia (ovvero nella specie il permanere della sua indicizzazione sui motori di ricerca), con pregiudizio alla propria reputazione e riservatezza (attesa l'attenuazione dell'attualità della notizia e dell'interesse pubblico all'informazione con il trascorrere del tempo dall'accadimento del fatto).».

Ebbene, secondo il Tribunale, il riconoscimento della sussistenza di un tale diritto in capo all'interessato impedisce il protrarsi del trattamento stesso e, con esso, l'indicizzazione, rendendo conseguentemente fondata la domanda di deindicizzazione spiegata nei confronti del gestore del motore di ricerca, cosí com'è stato statuito anche dalla recente pronuncia in materia resa dalla Corte di Giustizia del 13 marzo 2014 (causa C-131/12, sentenza «*Costeja*»), oltre che dalle, conformi, successive decisioni del Garante per la protezione dei dati personali.

Nel fare applicazione dei princípi contenuti nella sentenza della Corte di Giustizia, il Tribunale rinvia espressamente ad essa, evidenziando il reale ed effettivo *dictum* della stessa, ossia il bilanciamento[218] di interessi in conflitto, quindi tra *privacy* e altri diritti fondamentali,

[218] Sul tema del bilanciamento tra libertà di espressione, interessi individuali intaccati dall'esercizio di tale libertà e interesse pubblico alla conoscenza di una data notizia resa pubblica è intervenuta anche la Corte Europea dei Diritti dell'Uomo, con la sentenza del 16 luglio 2013 (caso *Wegrzybowski e Smolczewski vs. Polonia*, Rc. N. 33846/2007). La sentenza in parola offre una soluzione diversa da quella data dalla Corte di Giustizia del 13 marzo 2014 (causa c. 131/12, sentenza «*Costeja*»), disconoscendo, infatti, all'interessato il diritto ad ottenere la rimozione della notizia pubblicata in rete (peraltro non corretta e anche diffamatoria, poiché già acclarato dal giudice nazionale e, pertanto, come richiesto dal ricorrente, da rimuovere dal *web*) e individuando il punto di equilibrio tra interesse alla conservazione della notizia e interesse della persona interessata alla tutela della sua reputazione personale nell'eventuale obbligo, posto a capo dell'*editor*, di pubblicare un'aggiunta o una nota ad una fonte disponibile in *internet*, che specifichi la circostanza che l'informazione di cui si discute è stata reputata diffamatoria dall'Autorità giudiziaria. In tal modo, attraverso l'aggiornamento della notizia, il pubblico avrà una notizia contestualizzata alla luce degli avvenimenti storici successivi alla pubblicazione, quale, ad esempio, l'emissione di una sentenza che ne accerti il carattere diffamatorio. Per un'ampia disamina della pronuncia *de qua* si veda F. DI CIOMMO, *Il diritto di accesso all'informazione,* cit., p. 104 e s.

cosí rammentando che: «[s]econdo la citata pronuncia, in sintesi, gli utenti - in caso di ricerca nominativa su Google - non possono ottenere dal gestore del motore di ricerca la cancellazione dai risultati di una notizia che li riguarda se si tratta di un fatto recente e di rilevante interesse pubblico: il diritto all'oblio, infatti, deve essere bilanciato, ad avviso della corte, con il diritto di cronaca e con l'interesse pubblico alla conoscenza dei fatti acquisibili per il tramite dei links forniti dal motore di ricerca.».

Prosegue poi nel ricordare come la Corte europea, al fine di individuare quali possano essere i criteri idonei a ricercare il giusto equilibrio tra diritti fondamentali confliggenti, abbia evidenziato quello centrale assegnato, allo scopo, all'eventuale ruolo pubblico[219] rivestito dalla persona della cui *privacy* si tratta. È necessario per di piú, continua il Tribunale, citando testualmente la Corte di Giustizia, «verificare in particolare se l'interessato abbia diritto a che l'informazione riguardante la sua persona non venga più, allo stato attuale, collegata al suo nome da un elenco di risultati che appare a seguito di una ricerca effettuata a partire dal suo nome»[220].

Al fine di decidere la sussistenza, nel caso di specie, del paventato diritto «all'oblio» del ricorrente, il Tribunale ripercorre anche gli esiti degli approfondimenti svolti, a seguito della pronuncia della Corte di Giustizia, dalle autorità sovranazionali e nazionali deputate alla protezione dei dati personali, al fine di concretizzare quanto statuito dalla sentenza «*Costeja*» per quanto attiene all'individuazione dei parametri atti a orientare l'attività delle autorità nazionali nella gestione dei reclami degli interessati a seguito del mancato accoglimento, da parte del motore di ricerca, delle richieste di deindicizzazione.

In questo modo viene fatta menzione dell'importante lavoro svolto dal c.d. «Gruppo 29» (organo consultivo indipendente istituito in conformità all'articolo 29 della dir. 95/46/CE sulla protezione dei dati personali), evidenziandosi che esso, il 26 novembre 2014, ha

---

[219] Tal è l'avviso della Corte di Giustizia espresso nella sentenza «*Costeja*», richiamata dal Tribunale di Roma, ove, al punto 97, precisa che: «Dato che l'interessato può, sulla scorta dei suoi diritti fondamentali derivanti dagli articoli 7 e 8 della Carta, chiedere che l'informazione in questione non venga più messa a disposizione del grande pubblico mediante la sua inclusione in un siffatto elenco di risultati, occorre considerare – come risulta in particolare dal punto 81 della presente sentenza – che i diritti fondamentali di cui sopra prevalgono, in linea di principio, non soltanto sull'interesse economico del gestore del motore di ricerca, ma anche sull'interesse di tale pubblico a trovare l'informazione suddetta in occasione di una ricerca concernente il nome di questa persona. Tuttavia, così non sarebbe qualora risultasse, per ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi.».

[220] Il Tribunale di Roma richiama testualmente il punto 96 della sentenza «*Costeja*» in questione.

pubblicato delle linee guida per l'implementazione della menzionata pronuncia della Corte di Giustizia (causa C-131/12), le quali contengono una serie di criteri per orientare l'attività delle autorità nazionali nei casi di cui sopra, chiarendo che nessun criterio è di per sé determinante. In primo luogo tra i criteri in questione vi figura quello della natura del richiedente (in particolare, la circostanza per cui il richiedente rivesta un ruolo di rilievo pubblico, come nel caso di personaggi politici, dovrebbe tendenzialmente orientare verso il diniego della richiesta di deindicizzazione).

La sentenza in commento, al fine di pervenire ad una decisione sul caso sottopostogli, ricorda anche come i princípi esposti nelle linee guida emesse dal WP29, siano stati «integralmente recepiti dal Garante privacy nelle decisioni rese successivamente alla sentenza (*Costeja*)» e compie al riguardo espresso rinvio a due provvedimenti del nostro Garante, rispettivamente del 18 dicembre 2014 (n. 618) e 12 marzo 2015 (n. 153), precisando anche come quest'ultimo sia stato depositato agli atti dallo stesso gestore del motore di ricerca.

In particolare, la decisione del 18 dicembre 2014 sottolinea come nel caso di specie non sussistessero i presupposti per l'esercizio del diritto all'oblio contenuti nella sentenza «*Costeja*», «anche in considerazione del fatto che i medesimi risultavano essere assolutamente recenti, oltre che di pubblico interesse».

La decisione del Garante del 12 marzo 2015 evidenzia che tra i criteri che devono essere considerati per la disamina delle richieste di deindicizzazione ai motori di ricerca, vi è quello del ruolo pubblico dell'interessato nella vita pubblica e, correlativamente, quello della natura (pubblica o privata) delle informazioni allo stesso riferite. Di conseguenza, in tal caso, visto il ruolo che l'interessato riveste nella vita pubblica, prevale l'interesse della collettività ad accedere alle stesse rispetto al diritto dell'interessato alla protezione dei dati.

Pertanto, facendo applicazione dei princípi risultanti dalla sentenza della Corte di giustizia, del documento del WP29 e attraverso il richiamo a Cassazione n. 5525/2012[221]

[221] Cass., 05 aprile 2012, n. 5525, in *Foro it.*, 2013, I, c. 305. In questa occasione, la Cassazione, diversamente da quanto affermato dalla Corte di Giustizia dell'Unione Europea nel caso *Costeja*, ha affermato che l'interessato, al fine di tutelare il suo diritto alla riservatezza, e in particolare il suo (asserito) diritto all'oblio, anziché al motore di ricerca, è legittimato a rivolgersi direttamente al gestore del sito c.d. sorgente, che sarebbe quindi obbligato, se mantiene la notizia *on line*, ad aggiornare l'informazione cosí che risulti sempre attuale e completa; pertanto, la Suprema Corte evidenzia che è richiesta «la predisposizione di sistema idoneo a segnalare (nel corpo o a margine) la sussistenza di un seguito e di uno sviluppo della notizia, e quale esso sia stato […] consentendone il rapido ed agevole accesso da parte degli utenti ai fini del relativo adeguato

(per la quale il trascorrere del tempo, ai fini della sussistenza del diritto all'oblio, si configura quale elemento costitutivo), il Tribunale respinge la richiesta di *delisting*, affermando che debba ritenersi che le notizie individuate tramite il motore di ricerca risultino, nella specie, piuttosto recenti ed i fatti in esse narrati ancora attuali (dunque, insussistenza del presupposto del trascorrere del tempo). Inoltre, ad avviso del giudice capitolino, le notizie appaiono di «sicuro interesse pubblico, riguardando un'importante indagine giudiziaria che ha visto coinvolte numerose persone, seppure in ambito locale-romano». Ma ancora, sulla base del fatto che il ricorrente sia avvocato in Svizzera, libero professionista, si ritenere che questo «eserciti un "ruolo pubblico" proprio per effetto della professione svolta e dell'albo professionale cui è iscritto, laddove tale ruolo pubblico non è attribuibile al solo politico (cfr. linee guida del 26.11.20014) ma anche agli alti funzionari pubblici ed agli uomini d'affari (oltre che agli iscritti in albi professionali).»[222].

Ne consegue, cosí conclude la sentenza, che nell'ottica del bilanciamento tra diritti fondamentali, l'interesse pubblico a rinvenire sul *web* attraverso il motore di ricerca gestito dalla resistente notizie circa il ricorrente deve prevalere sul diritto all'oblio dal medesimo vantato.

3.3. La decisione «*Safe Harbour*» e il suo annullamento. Il caso *Maximillian Schrems*.

Con deliberazione n. 36 del 10 ottobre 2001, l'Autorità Garante italiana, vista la decisione della Commissione europea del 26 luglio 2000, n. 2000/520/CE, autorizzava il

approfondimento, giusta modalità operative stabilite, in mancanza di accordo tra le parti, dal giudice di merito.». Per note critiche v. F. DI CIOMMO e R. PARDOLESI, in *Danno resp.*, 2012, p. 701 ss.

[222] Sul «ruolo» dell'avvocato e sulla sua funzione sociale è interessante anche evidenziare il provvedimento n. 50/2017 de Garante della *Privacy*, con il quale si è stabilito che la *privacy* di un avvocato è fondamentale e prevale sull'interesse del pubblico alla visione degli atti di un procedimento disciplinare. Questi, infatti, sono preclusi all'accesso civico ai sensi della legge n. 241/1990, proprio in considerazione della particolare incidenza che avrebbe la loro visione sulla riservatezza degli interessati. Anche l'ispezione del conto corrente dell'avvocato viola la sua *privacy*, oltre che il segreto professionale al quale il professionista è tenuto; è quanto ritenuto dalla Corte EDU, sez. V, nel caso Sommer c. Germania (ric. 73607/13) del 27 aprile 2017 (in www.dirittoegiustizia.it, con nota di G. MILIZIA, *L'ispezione del conto corrente dell'avvocato viola il segreto professionale e la sua privacy*). Nella specie, la Corte di Strasburgo ha ravvisato una palese violazione dell'art. 8 CEDU nella prassi tedesca di ispezionare il conto bancario di un avvocato per il sospetto di un'infrazione penale, con conseguente accesso indiscriminato ad informazioni relative al titolare del conto ed a terzi, senza garanzie e alcun limite temporale.

trasferimento di dati personali dall'Italia verso organizzazioni aventi sede negli Stati Uniti secondo i «Principi di approdo sicuro in materia di riservatezza».

I giudici di Lussemburgo, nella vicenda *Maximillian Schrems/Data Protection Commissioner*[223], concludono per l'invalidità della summenzionata decisione 2000/520, che occorre brevemente passare in rassegna.

Essendo gli U.S.A. privi di un corpo normativo organico sulla tutela della *privacy* paragonabile a quello vigente in Europa, l'Unione Europea aveva previsto la possibilità, per le imprese americane, che intendevano utilizzare dati personali di cittadini europei per la loro attività, di aderire spontaneamente a determinati princípi fondamentali di tutela. Si tratta dei c.d. 7 princípi fondamentali e delle 15 «*Frequently Asked Questions*»[224] pubblicate dal

[223] Corte giust., 6 ottobre 2015, C-362/14, cit., il cui articolato percorso argomentativo si esporrà nel seguito del presente paragrafo.

[224] L'allegato II della decisione 2000/520 conteneva le «Domande più frequenti (FAQ)», qui di seguito riportate per estratto. FAQ 6 – Autocertificazione *D: Come può un'organizzazione autocertificare la propria adesione ai principi dell'approdo sicuro?* R: Un'organizzazione usufruisce dei vantaggi dell'approdo sicuro dalla data in cui autocertifica al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata l'adesione ai relativi principi, seguendo le indicazioni sotto riportate. Per autocertificare l'adesione all'approdo sicuro un'organizzazione può fornire al Dipartimento del commercio o ad una persona (fisica o giuridica) da esso designata una lettera, firmata da un proprio funzionario in nome dell'organizzazione che intende aderire all'approdo sicuro, contenente almeno le seguenti informazioni: 1) denominazione dell'organizzazione, indirizzo postale, indirizzo di posta elettronica, numero di telefono e fax; 2) descrizione delle attività dell'organizzazione in rapporto alle informazioni personali pervenute dall'UE; 3) descrizione della politica perseguita dall'organizzazione in merito a dette informazioni personali, che precisi tra l'altro: a) dove il pubblico può prenderne conoscenza; b) la data della loro effettiva applicazione; c) l'ufficio cui rivolgersi per eventuali reclami, richieste di accesso e qualsiasi altra questione riguardante l'approdo sicuro; d) lo specifico organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi a possibili pratiche sleali od ingannevoli e a violazioni delle norme legislative e regolamentari che disciplinano la tutela della sfera privata (ed elencati nell'allegato ai principi); e) il nome dei programmi concernenti la tutela della sfera privata cui partecipa l'organizzazione; f) il metodo di verifica (per esempio all'interno della società, effettuata da terzi) […] e g) il meccanismo di ricorso indipendente disponibile per indagare sui reclami non risolti. Le organizzazioni che intendono estendere i benefici dell'approdo sicuro alle informazioni riguardanti le risorse umane trasferite dall'UE per usi nel contesto di un rapporto di lavoro possono farlo qualora esista un organo statutario competente ad esaminare i ricorsi contro l'organizzazione relativi ad informazioni riguardanti le risorse umane, elencato nell'allegato "Principi di approdo sicuro". [...]. Il Dipartimento (o la persona da esso designata) conserverà un elenco di tutte le organizzazioni che inviano queste lettere, assicurando così la disponibilità dei vantaggi legati all'approdo sicuro, ed aggiornerà tale elenco in base alle lettere annuali ed alle notifiche ricevute secondo le modalità precisate nella FAQ 11. [...]. FAQ 11 – Risoluzione delle controversie e modalità di controllo dell'applicazione (enforcement). D: *Come si applicano le norme derivanti dal principio della garanzia di applicazione (enforcement) per la risoluzione delle controversie, e come si procede se un'organizzazione continua a non rispettare i principi?* R: Il principio della garanzia di applicazione (enforcement) stabilisce le norme per l'applicazione dell'approdo sicuro. Le modalità di applicazione delle norme di cui al punto b) di tale principio sono illustrate nella domanda sulla verifica (FAQ 7). La presente domanda interessa i punti a) e c), che prescrivono l'istituzione di dispositivi indipendenti di ricorso. Tali dispositivi possono assumere forme diverse, ma devono soddisfare le prescrizioni formulate nel contesto delle garanzie d'applicazione. Un'organizzazione può adempiere a tali prescrizioni nei modi seguenti: 1) applicando programmi di riservatezza elaborati dal settore privato nei quali siano integrati i principi dell'approdo sicuro e che contemplino dispositivi di attuazione efficaci, del tipo descritto dal principio delle garanzie d'applicazione; 2)

Governo degli Stati Uniti il 21 luglio 2000 e favorevolmente accolte dalla Commissione Europea con la decisione del 26 luglio 2000, n. 520. L'adesione al «*Safe Harbour*», facoltativa per le imprese americane, vincolava alle regole in esso contenute le imprese americane. Il loro rispetto era affidato alla *Federal Trade Commission* e, per le compagnie aeree, all'Amministrazione dei trasporti. I cittadini dell'Unione Europea che intendevano reclamare per il trattamento effettuato da un partecipante al «*Safe Harbour*» potevano rivolgersi ad un'istanza indipendente di composizione di controversie. A tale scopo, ogni organismo statunitense aderente al «*Safe Harbour*» indicava l'istanza con la quale si impegna a collaborare. In vari casi era pure possibile agire innanzi a giudici statunitensi, in base a norme di quell'ordinamento che non permettono dichiarazioni false, quali appunto quelle di un'impresa che dichiari di aderire ad una certa politica di protezione dei dati personali successivamente non rispettata[225]. In ogni caso, l'esportatore residente in Italia poteva previamente verificare, presso il Dipartimento del commercio americano o presso altri enti governativi competenti negli Stati Uniti, che l'importatore statunitense avesse aderito, mediante autocertificazione, ai princípi del «*Safe Harbour*».

È comunque opportuno osservare come, qualora l'operatore statunitense non avesse aderito al *Safe Harbour* (e il paese importatore non fosse stato ufficialmente riconosciuto come avente un adeguato livello di protezione) il trasferimento potesse (e possa a tutt'oggi) sempre essere possibile attraverso l'adozione e specifica sottoscrizione, da parte del soggetto importatore dei dati, delle c.d. «clausole contrattuali *standard*»[226].

---

uniformandosi a norme giurisdizionali o regolamentari emanate dalle corrispondenti autorità di controllo, che disciplinino il trattamento di reclami individuali e la soluzione delle controversie; oppure 3) impegnandosi a cooperare con le autorità di tutela dei dati aventi sede nella Comunità europea o loro rappresentanti autorizzati. Quest'elenco è fornito a titolo puramente esemplificativo e non limitativo. Il settore privato può indicare altri meccanismi di applicazione, purché rispettino il principio delle garanzie d'applicazione e le FAQ. Si noti che le citate garanzie d'applicazione si aggiungono a quelle di cui al paragrafo 3 dell'introduzione ai principi, in forza delle quali le iniziative di autoregolamentazione devono avere carattere vincolante in virtù dell'articolo 5 del Federal Trade Commission Act o analogo testo di legge. Meccanismi di ricorso: I consumatori dovrebbero essere incoraggiati a presentare gli eventuali reclami all'organizzazione direttamente interessata, prima di rivolgersi ai dispositivi indipendenti di ricorso. [...]. Attività della Commissione federale per il commercio (Federal Trade Commission, FTC): La Commissione federale per il commercio (FTC) si è impegnata ad esaminare in via prioritaria i casi trasmessi da organizzazioni di autoregolamentazione in materia di riservatezza (quali BBBOnline e TRUSTe) e dagli Stati membri dell'UE per denunciare la presunta non conformità ai principi dell'approdo sicuro, al fine di stabilire se vi siano state violazioni della sezione 5 del FTC Act, che vieta azioni o pratiche sleali od ingannevoli nel commercio. [...]».

[225] Con risoluzione del 5 luglio 2000, il Parlamento europeo ha manifestato l'esigenza di migliorare il testo dell'accordo in particolare sul punto dei ricorsi degli interessati relativi alla violazione dei princípi. La Commissione non ha negoziato tali modifiche, ma ha trasmesso questa risoluzione alle autorità americane.

[226] V. *retro* § 2.1. cap. II.

Decaduta, in virtú di Corte giust. 6 ottobre 2015, C-362/14, l'autorizzazione «Approdo Sicuro»[227], il Garante per la *privacy* ha comunicato (sul proprio sito *web*, in data 6 novembre 2015) che le imprese dovranno mettere in campo altri strumenti per tutelare i dati delle persone.

Pertanto, in attesa delle prossime decisioni che verranno assunte in sede europea, le imprese potranno dunque trasferire lecitamente i dati delle persone solo avvalendosi di strumenti quali, ad esempio, le *clausole contrattuali standard* o le regole di condotta adottate all'interno di un medesimo gruppo (le cosiddette BCR, *Binding Corporate Rules*). L'Autorità si è comunque riservata di effettuare controlli per verificare la liceità e la correttezza del trasferimento dei dati da parte di chi esporta i dati.

Occorre, a questo punto, analizzare il piú volte citato caso *Maximillian Schrems*, giunto all'attenzione dei giudici lussemburghesi. La Corte di Giustizia, con la sentenza nella causa C-362/14, *Maximillian Schrems/Data Protection Commissioner*[228], reputa che l'esistenza di una decisione della Commissione che dichiara che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti non può sopprimere e neppure ridurre i poteri di cui dispongono le Autorità nazionali di controllo in forza della Carta dei diritti fondamentali dell'Unione europea e direttiva sul trattamento dei dati personali[229] (dir. 95/46/CE).

La decisione in disamina nasce dalla vicenda del sig. *Maximillian Schrems*, cittadino austriaco, che, in quanto iscritto a *Facebook*, come tutti gli iscritti a tale *social network*, si vede trasferire i suoi dati su *server* situati nel territorio degli Stati Uniti. Occorre, allora,

---

[227] Il Garante per la *privacy* ha dichiarato decaduta l'autorizzazione emanata a suo tempo con la quale si consentivano i trasferimenti di dati verso gli Stati Uniti sulla base del cosiddetto accordo «*Safe Harbor*». Per poter trasferire dati oltreoceano, società multinazionali, organizzazioni e imprese italiane dovranno di conseguenza ricorrere alle altre possibilità previste dalla normativa sulla protezione dei dati personali. Il provvedimento (pubblicato sulla Gazzetta ufficiale) è stato adottato dal Garante a seguito della recente sentenza della Corte di Giustizia dell'Unione Europea, che ha dichiarato invalido il regime introdotto in virtú dell'accordo «Approdo sicuro» (*Safe Harbor*), facendo venire meno il presupposto di legittimità per il trasferimento negli Usa di dati personali dei cittadini europei per chi utilizzava questo strumento.

[228] Corte giust., 6 ottobre 2015, C-362/14, cit.

[229] V. punto 53 della decisone in commento «[…]una decisione della Commissione adottata sulla base dell'articolo 25, paragrafo 6, della direttiva 95/46, come la decisione 2000/520, non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un paese terzo di investire le autorità nazionali di controllo di una domanda, ai sensi dell'articolo 28, paragrafo 4, di tale direttiva, relativa alla protezione dei loro diritti e delle loro libertà con riguardo al trattamento di tali dati. Analogamente, una decisione di tale natura non può, come rilevato dall'avvocato generale, segnatamente, ai paragrafi 61, 93 e 116 delle sue conclusioni, né elidere né ridurre i poteri espressamente riconosciuti alle autorità nazionali di controllo dall'articolo 8, paragrafo 3, della Carta, nonché dall'articolo 28 di detta direttiva.».

controllare se il diritto e le prassi statunitensi offrano una adeguata tutela di protezione, alla luce della direttiva comunitaria, presupposto indispensabile affinché possa avvenire il trasferimento dei dati.

Infatti, il sig. *Maximillian Schrems* presenta una denuncia all'Autorità per la protezione dei dati personali irlandese (il *Data Protection Commissioner*), con la quale chiede di vietare a *Facebook Ireland* di trasferire i suoi dati personali verso gli Stati Uniti. In buona sostanza, egli ritiene - sulla base delle rivelazioni fatte dal sig. *Edward Snowden* in merito alle attività di *intelligence* degli Stati Uniti e in particolare a quelle della *National Security Agency* - che il quadro giuridico degli Stati Uniti non offrirebbe una protezione sufficiente dei dati personali.

Il commissario respinge la denuncia invocando una decisone della Commissione (Decisione 2000/520/CE, del 26/07/2000, c.d. *Decisione Safe Harbour*), con la quale si è ritenuto che Stati Uniti garantiscono un livello adeguato di protezione dei dati personali. Cosicché il sig. *Schrems* propone ricorso dinanzi alla *High Court* (Corte d'appello) avverso tale decisione, che decide quindi di coinvolgere la Corte di Giustizia UE chiedendo se una siffatta decisione della Commissione possa impedire che un'Autorità *Privacy* nazionale decida su una denuncia che un paese terzo non assicura un livello di protezione adeguato dei dati personali e, ove fondata, sospenda il trasferimento dei dati.

Sul punto, la Corte di Giustizia invalida[230] la Decisone *Safe Harbour*, con la conseguenza che l'autorità irlandese di controllo è tenuta ad esaminare la denunzia del sig. *Maximillian Schrems* e che ad essa spetta decidere se, sulla base della direttiva, occorre sospendere il trasferimento dei dati degli iscritti europei a *Facebook* verso gli Stati Uniti perché tale paese non offre un livello di protezione adeguato dei dati personali.

Questa sentenza, per la sua dirompente portata, non può che essere presa a riferimento nella presente ricerca, visti i suoi ulteriori e inevitabili risvolti effettivi sul sistema del trattamento dei dati personali, posto che occorrerà in futuro verificare in concreto se una decisione di adeguatezza della Commissione rispetti, o meno, i requisiti della normativa europea. Sul punto, i giudici di Lussemburgo offrono delle indicazioni importanti, non solo all'istituzione comunitaria, ma anche agli Stati nella predisposizione delle «*clausole contrattuali*

[230] La corte precisa (v. punto 61 della decisione in esame) che essa «è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione, quale una decisione della Commissione adottata in applicazione dell'articolo 25, paragrafo 6, della direttiva 95/46», precisando che «la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione […]».

standard», nei significativi passaggi in cui verificano la validità della decisione della Commissione del 26 luglio 2000, che poi dichiarano invalida. Un monito che non sembra essere stato recepito dagli operatori del *web*[231].

Innanzitutto, i giudici di Lussemburgo rilevano che l'adozione, da parte della Commissione, di una decisione in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 richiede la constatazione, debitamente motivata, da parte di tale istituzione, che il paese terzo di cui trattasi garantisce effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione. Pertanto, gli strumenti dei quali tale paese terzo si avvale per assicurare un «livello di protezione adeguato» ben possono essere diversi da quelli attuati all'interno dell'Unione, ma tali strumenti devono rivelarsi efficaci, nella prassi, al fine di assicurare una protezione sostanzialmente equivalente a quella garantita all'interno dell'Unione.[232]

Sulla base di questa necessaria premessa, la Corte analizza l'art. 1 della decisone 2000/520 evidenziando come l'adesione di un'organizzazione ai princípi dell'approdo sicuro avvenga sulla base di un sistema di autocertificazione e che questi sono applicabili alle organizzazioni americane autocertificate che ricevono dati personali dall'Unione, mentre dalle autorità pubbliche americane non si esige il rispetto di detti princípi. L'applicabilità degli stessi, per di piú, sottolinea la Corte, può essere limitata - in conformità all'allegato I, quarto comma, della decisione 2000/520 - «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]», nonché da «disposizioni legislative o regolamentari ovvero decisioni giurisdizionali quando tali fonti comportino obblighi contrastanti od autorizzazioni esplicite […]», cosí sancendosi il primato delle summenzionate esigenze sui princípi dell'approdo sicuro.

---

[231] *Facebook*, ad esempio, nelle impostazione sulla *privacy*, dopo la pronuncia in commetto, non ha smesso di dire che si applica il *Safe Harbour* testualmente riportando: «Facebook, Inc. rispetta il quadro Safe Harbor, in vigore tra Stati Uniti ed Unione Europea e tra Stati Uniti e Svizzera, in relazione alla raccolta, all'uso e al mantenimento dei dati provenienti dall'Unione Europea e dalla Svizzera, come stabilito dal Ministero dello Sviluppo Economico degli Stati Uniti. […]. Nel quadro della nostra partecipazione al programma *Safe Harbor*, ci impegniamo a risolvere mediante TRUSTe le eventuali dispute tra te e noi in relazione alle nostre normative e procedure. […]. Facebook può condividere le informazioni internamente con il nostro gruppo di aziende o con terzi per gli scopi descritti in questa normativa. Le informazioni raccolte all'interno dello Spazio Economico Europeo ("SEE") possono ad esempio essere trasferite a Paesi esterni al SEE per gli scopi descritti nella presente normativa.».

[232] Punti 71, 73 e 74.

Per la Corte, il carattere generale della citata deroga rende pertanto possibili ingerenze, fondate su esigenze connesse alla sicurezza nazionale e all'interesse pubblico o alla legislazione interna degli Stati Uniti, nei diritti fondamentali delle persone i cui dati personali sono o potrebbero essere trasferiti dall'Unione verso gli Stati Uniti. Pertanto, afferma la Corte «poco importa, per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza».

Non è dato, inoltre, rinvenire nella decisione 2000/520 alcuna dichiarazione quanto all'esistenza, negli Stati Uniti, di norme statali destinate a limitare le eventuali ingerenze nei diritti fondamentali delle persone i cui dati vengono trasferiti dall'Unione verso gli Stati Uniti. La decisione in parola, si aggiunge, neppure menziona l'esistenza di una tutela giuridica efficace nei confronti delle ingerenze di tale natura.

Estremamente importante è la considerazione di cui al punto 92 della decisione in commento, che demolisce definitivamente la decisione 2000/520, ove la Corte evidenzia che «[i]noltre, e soprattutto, la protezione del diritto fondamentale al rispetto della vita privata a livello dell'Unione richiede che le deroghe e le restrizioni alla tutela dei dati personali operino entro i limiti dello stretto necessario». Prosegue la Corte, al successivo punto, «in tal senso non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta».

È allora doveroso ritenere che una normativa: a) che consente alle autorità pubbliche di accedere in maniera generalizzata al contenuto di comunicazioni elettroniche pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata, come garantito dall'articolo 7 della Carta; b) che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta.

Sulla base di tali argomentazioni, la Corte conclude che l'articolo 1 della decisione oggetto del suo scrutinio viola i requisiti fissati all'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce della Carta, e che esso è, per tale motivo, invalido.

La Corte ritiene, poi, che l'art. 3, paragrafo 1, primo comma, della decisione in commento, privi le autorità nazionali di controllo dei poteri che esse traggono dall'art. 28 della direttiva 95/46, nel caso in cui una persona adduca elementi idonei a rimettere in discussione la decisone di adeguatezza della Commissione. In merito, si statuisce che il potere di esecuzione che il legislatore dell'Unione ha attribuito alla Commissione - con l'art. 25, par. 6, dir. 95/46 - non conferisce a tale istituzione la competenza di limitare i poteri delle autorità nazionali di controllo. Ciò posto, la Commissione, nell'adottare il summenzionato articolo 3, ha ecceduto la competenza attribuitale dall'art. 25, par. 6, dir. 95/46, letto alla luce della Carta, e per questo motivo esso è invalido.

Sulla base di tutte le considerazioni esposte, la Corte conclude per l'invalidità della decisione 2000/520.

3.4. Il nuovo «Scudo *Privacy*» per il trasferimento dei dati personali tra UE e USA.

Il 2 febbraio 2016, i rappresentanti delle autorità europee ed americane hanno annunciato il raggiungimento dell'accordo politico (cd. «Scudo *Privacy*» o «*Privacy Shield*»), che andrà a sostituire il cd. Approdo Sicuro («*Safe Harbor*»), invalidato, dalla Corte di Giustizia del Lussemburgo, con la sentenza di cui al paragrafo precedente.

Il menzionato accordo vuole assicurare che le società *extra* UE che importino dati personali dall'Unione europea forniscano maggiori garanzie nel trattamento dei dati personali. Esso, i cui dettagli sono ancora da definirsi dal Vice-Presidente Ansip e dalla Commissaria UE alla Giustizia Jourovà, include: a) obblighi in capo alle società americane che intendano importare dati personali dall'UE, incluso trattare i dati personali nel rispetto delle decisioni delle autorità *privacy* europee. Il Dipartimento del Commercio USA sarà poi incaricato di monitorare che le società interessate rendano pubblici i presidi a tutela della *privacy* posti in essere; b) garanzie ed obblighi di trasparenza in termini di accesso ai dati da parte del Governo USA. Le autorità americane hanno assicurato che l'accesso ai dati sarà limitato, in conformità ai princípi di necessità e proporzionalità. Saranno messi in piedi

degli strumenti di controllo che assicurino il rispetto del nuovo accordo ed in particolare la Commissione Europea ed il Dipartimento del Commercio USA condurranno annualmente controlli; c) effettiva protezione dei diritti dei cittadini europei, che potranno rivolgersi ad una pluralità di istituzioni ed istituti (le autorità *privacy* nazionali, il Dipartimento di Commercio USA, la *Federal Trade Commission*, *Alternative Dispute Resolution*, *Ombudsperson ad hoc*). In attesa della «decisione di adeguamento» in fase di redazione dalle istituzioni comunitarie, le autorità americane si sono impegnate a mettere in piedi gli strumenti di controllo e garanzia previsti dal nuovo accordo.

Lo Scudo *Privacy*, traguardo importante in tema di garanzia effettiva della protezione dei dati personali, ha probabilmente influenzato anche il nuovo Regolamento *Privacy* europeo.

4. Il trattamento dei dati personali alla luce del Regolamento europeo sulla *privacy*. Disposizioni generali.

«La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano» (1° considerando).

Il diritto alla protezione dei dati personali è un diritto[233] che dev'essere garantito a prescindere dalla nazionalità o dalla residenza delle persone fisiche (2° considerando), dovendo essere il trattamento dei dati personali al servizio dell'uomo (3° considerando). Tuttavia, il diritto in parola «non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità.»[234] (4° considerando, secondo periodo).

Il legislatore comunitario, consapevole del considerevole aumento dei flussi transfrontalieri di dati personali, evidenzia l'importanza, tra l'altro imposta dal diritto

[233] La tutela dei dati personali è un diritto riconosciuto ad «ogni persona», per garantire il rispetto della sua dignità, identità e riservatezza, anche dalla «Dichiarazione dei diritti in Internet», del 28 luglio 2015 (documento della Commissione per i diritti e i doveri in *internet*, istituita dalla Camera dei deputati) nel suo articolo 5, rubricato «Tutela dei dati personali».

[234] Il Regolamento in disamina recepisce quanto consolidatosi nella giurisprudenza della Corte di Giustizia e segnatamente espresso in: Corte giust., 9 novembre 2010, cause riunite C-92/09 e C-93/09, cit.; Corte giust., 12 giugno 2003, C-112/00, cit.; per una migliore disamina v. *retro*, nel presente Cap. II, § 1.1.

dell'Unione alle autorità nazionali degli Stati membri, di cooperare e scambiarsi dati personali «per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro» (5° considerando). Si pone in risalto, quindi, come la libera circolazione dei dati personali sia funzionale al progresso economico e sociale, al rafforzamento e alla convergenza delle economie nel mercato interno, ma in un'ottica compatibile con il benessere delle persone fisiche; realizzazione di uno spazio di libertà, di sicurezza e giustizia e, al contempo, di un'unione economica. Tutto questo il regolamento intende favorire.

In particolare, si è sentita l'esigenza di adattare la legislazione dell'Unione europea alle nuove tecnologie e all'uso sempre piú disparato che oggi si fa di *internet*[235]. I dati presenti nella rete, infatti, sono in continuo aumento e le connessioni tra diversi Paesi del mondo sempre piú fitte; in tale direzione si muove il considerando numero 6, per il quale: «[l]a rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.». Di qui l'esigenza, appunto, «di un quadro piú solido e coerente in materia di protezione dei dati personali, 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.» (7° considerando).

[235] Proprio la consapevolezza nel considerare *internet* una dimensione essenziale per il presente e il futuro delle nostre società, una dimensione diventata un immenso spazio di libertà, di crescita, di scambio e di conoscenza, è stata alla base, in Italia, della istituzione in sede parlamentare della Commissione di studio sui temi dei diritti e i doveri relativi ad *internet*, che ha portato alla approvazione e pubblicazione il 28 luglio 2015 - dopo una serie di audizioni di associazioni, esperti e soggetti istituzionali, oltre che a una consultazione pubblica durata cinque mesi - della «Dichiarazione dei diritti in Internet», che come si legge nel suo preambolo «è strumento indispensabile per dare fondamento costituzionale a principi e diritti nella dimensione sovranazionale.».

Si stabilisce, poi, che gli Stati membri, nella misura necessaria per la coerenza e per la comprensibilità delle disposizioni nazionali alle persone cui si applicano, possono «integrare elementi del (presente) regolamento nel proprio diritto nazionale», nel caso in cui lo stesso preveda specificazioni o limitazioni delle sue norme ad opera del diritto degli Stati membri (8° considerando).

Dopo aver premesso che gli obiettivi e princípi della direttiva 95/46/CE rimangano tuttora validi, se ne evidenziano i limiti della direttiva stessa, che «non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, […], che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche.». La causa di tutto ciò si rinviene nella compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, quale ostacolo alla libera circolazione dei dati personali all'interno dell'Unione. Differenze che possono costituire un freno all'esercizio delle attività economiche, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione (9° considerando). Pertanto, proprio al fine di «assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, […], offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri». (13° considerando).

È evidente, allora, quale sia l'oggetto e la finalità del regolamento in esame, ossia la protezione dei dati personali delle persone fisiche, stabilendosi norme per la loro protezione con riguardo al trattamento dei dati personali e norme per la libera circolazione di tali dati (art. 1, comma 1), che, nell'Unione europea, non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (art. 1, comma 3).

Il regolamento in disamina protegge le persone fisiche (a prescindere dalla nazionalità o dal luogo di residenza), identificate o identificabili, non decedute (27° considerando) e non

anche le persone giuridiche (14° e 26° considerando); e la protezione delle prime «dovrebbe applicarsi sia al trattamento automatizzato che al trattamento manuale dei dati personali» (15° considerando).

Il regolamento non si applica, inoltre: a) alle questioni di tutela dei diritti e delle libertà fondamentali o di libera circolazione dei dati personali riferite ad attività che non rientrano nell'ambito di applicazione del diritto dell'Unione, quali le attività riguardanti la sicurezza nazionale; b) al trattamento dei dati personali effettuato dagli Stati membri nell'esercizio di attività relative alla politica estera e di sicurezza comune dell'Unione (16° considerando); c) al trattamento di dati personali effettuato da una persona fisica nell'àmbito di attività a carattere esclusivamente personale o domestico (18° considerando); d) ai trattamenti effettuati per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, etc. (19° considerando). Inoltre, il presente regolamento non pregiudica pertanto l'applicazione della direttiva 2000/31/CE (21° considerando). Tutto ciò detto costituisce il c.d. «àmbito di applicazione materiale» del regolamento *ex* art. 2 dello stesso.

Al successivo art. 3, si prevede, invece, il c.d. «àmbito di applicazione territoriale», che rinviene i suoi presupposti già nei considerando 22, 23, 24 e 25. In virtú delle summenzionate disposizioni, il regolamento si applica anche in caso di trattamento dei dati personali effettuato nell'àmbito delle attività di uno stabilimento[236] da parte di un titolare del trattamento o di un responsabile del trattamento nel territorio dell'Unione, non rilevando pertanto il luogo in cui avvenga il trattamento (dunque, « indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione»). In altri termini, (anche) questo trattamento dev'essere conforme al regolamento in disamina (art. 3, comma 1). Si rivede, pertanto, la concezione tradizionale del principio di stabilimento nel territorio dell'Unione.

In buona sostanza ciò dovrebbe significare che se il titolare del trattamento 'o' il responsabile dello stesso (ossia uno dei due) ha uno stabilimento nell'Unione Europea, sarà applicabile, al trattamento dei dati effettuato, la normativa europea anche se il trattamento stesso avviene fuori dall'UE.

[236] Il considerando 22°, secondo periodo, chiarisce che «[l]o stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica.». Per la definizione di «stabilimento principale», v. art. 4, n. 16.

Il riferimento al titolare e al responsabile del trattamento con l'utilizzo, però, della disgiuntiva 'o' (ossia o l'uno o l'altro) non dovrebbe far sorgere problemi di sorta nel caso in cui uno dei due non sia stabilito nel territorio dell'Unione. In altri termini, ci si potrebbe interrogare sul cosa accada se il titolare sia stabilito nell'UE mentre il responsabile non lo sia e viceversa; occorrerà riferirsi al luogo di stabilimento dell'uno o dell'altro? In realtà, il dubbio è solo apparente, poiché è proprio l'uso della disgiuntiva 'o' tra le parole 'titolare del trattamento' 'responsabile del trattamento' che consente di affermare che è sufficiente che uno dei due sia situato nell'Unione, o meglio effettui il trattamento nell'àmbito delle attività di uno stabilimento nell'Unione.

Il paragrafo 2 dell'art. 3, introduce poi il criterio del luogo in cui gli interessati si trovano. Pertanto, se il trattamento dei dati personali di interessati che si trovano nell'Unione è effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, il regolamento si applicherà comunque, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Il paragrafo 3, prevede, poi, l'applicazione del regolamento al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtú del diritto internazionale pubblico. *Ergo*, in questi casi, la legge applicabile sarà quella del soggetto i cui dati vengono raccolti; *social network*, piattaforme *web* e motori di ricerca saranno quindi soggetti alla normativa europea anche se sono gestiti da società con sede fuori dall'UE[237].

4.1. ***Segue.*** **I Princípi del Regolamento europeo sulla *privacy*.**

Il capo II (artt. 5-11) del regolamento ribadisce i classici princípi da applicare al trattamento dei dati personali già propri della precedente normativa. Innanzitutto, circa il «modo» del trattamento, si prevede che questo si debba conformare ai princípi di «liceità, equità e trasparenza» (art. 5, lett. a). La loro «raccolta» sarà consentita solo per finalità

[237] In merito al tema «àmbito di applicazione territoriale» collegato all'aspetto della «conservazione» dei dati personali, v. *infra* Cap. III, § 2.

determinate, esplicite e legittime e il successivo trattamento deve svolgersi in modo che non sia incompatibile con tali finalità (art. 5, lett. b[238]); dev'essere, quindi, un trattamento a finalità limitata (principio di «limitazione della finalità»), nonché adeguato, pertinente e limitato a quanto necessario rispetto alle finalità dello stesso [c.d. «minimizzazione dei dati» (art. 5, lett. c)]. I dati personali devo essere esatti e, se necessario, aggiornati e devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati [principio di «esattezza» (art. 5, lett. d)] e conservati per un arco di tempo limitato, non superiore al conseguimento delle finalità per le quali sono trattati[239] [«limitazione della conservazione» (art. 5, lett. e)]. Il trattamento dovrà, inoltre, garantire un'adeguata sicurezza dei dati personali, nonché la protezione degli stessi - mediante la predisposizione di misure tecniche e organizzative adeguate - da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali [principio di «integrità e riservatezza» (art. 5, lett. f)]. In base al comma 2, dell'art. 5 in commento, competente per il rispetto del paragrafo 1 e in grado di comprovarlo è il titolare del trattamento (principio di «responsabilizzazione»).

Il principio di liceità del trattamento, già enunciato nei considerando 39, primo periodo (per il quale «[q]ualsiasi trattamento di dati personali dovrebbe essere lecito e corretto») e 40, trova la sua compiuta specificazione nel successivo art. 6. Pertanto, perché sia lecito, il trattamento di dati personali deve fondarsi sul consenso dell'interessato per una o piú specifiche finalità (lett. a) o su altra base legittima e, segnatamente, sulla necessità di salvaguardare specifici beni e interessi, come indicati nell'art. 6 medesimo, ovverosia: necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso (lett. b); necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto (lett. c); necessità di salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (lett. d); necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il

[238] Il secondo periodo della disposizione in commento, specifica che «un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali».

[239] Il secondo periodo della disposizione in commento prosegue specificando che «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».

titolare del trattamento (lett. e); necessità di perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (lett. f). Quest'ultima lettera non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti.

Il secondo comma dell'articolo in commento, attribuisce agli Stati membri la possibilità di mantenere o introdurre disposizioni piú specifiche per adeguare l'applicazione delle norme del regolamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto. Il comma 3 sancisce che la base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: dal diritto dell'Unione o dal diritto dello Stato membro cui è soggetto il titolare del trattamento. Il comma 4 prevede lo specifico caso del trattamento per una finalità diversa da quella per la quale i dati sono stati raccolti, prevedendo che per accertare se la finalità di un ulteriore trattamento sia compatibile con la finalità per la quale i dati personali sono stati inizialmente raccolti, il titolare del trattamento deve, dopo aver soddisfatto tutti i requisiti per la liceità del trattamento originario, tener conto tra l'altro di ogni nesso tra tali finalità e le finalità dell'ulteriore trattamento previsto, del contesto in cui i dati personali sono stati raccolti, in particolare le ragionevoli aspettative dell'interessato in base alla sua relazione con il titolare del trattamento con riguardo al loro ulteriore utilizzo; della natura dei dati personali; delle conseguenze dell'ulteriore trattamento previsto per gli interessati; e dell'esistenza di garanzie adeguate sia nel trattamento originario sia nell'ulteriore trattamento previsto.

Come detto, il consenso[240] è una (e non l'unica) delle condizioni di liceità del trattamento e, a mente del 32° considerando, esso deve esprimersi «mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale». Si evidenzia, inoltre, che il silenzio, l'inattività o la preselezione di caselle non dovrebbe configurare consenso e qualora il trattamento abbia piú finalità, il consenso dovrebbe

[240] La definizione di «consenso dell'interessato» si rinviene all'art. 4, n. 11, cosí intendendosi: «qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento».

essere prestato per tutte queste. Il legislatore comunitario si preoccupa anche di chiarire l'ipotesi del consenso richiesto attraverso mezzi elettronici, ove precisa che, in tal caso, la richiesta deve essere chiara, concisa e non interferire immotivatamente con il servizio per il quale il consenso è espresso (32° considerando). L'art. 7 sancisce, innanzitutto, che sarà onere del titolare del trattamento dimostrare che l'interessato ha prestato il proprio consenso al trattamento dei propri dati personali (comma 1). Se il consenso 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 (comma 2). È altresí espressamente prevista la possibilità per l'interessato di revocare il proprio consenso in qualsiasi momento, riconoscimento, dunque, di un vero e proprio diritto di revoca del consenso (comma 3).

Viene introdotta, all'art. 8, la categoria del trattamento dei dati dei minori, i quali, stante il disposto del 38° considerando, «meritano una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali.».

Gli artt. 9 e 10 del Regolamento, sulla scorta di quanto già determinato dalla precedente normativa, individuano rispettivamente i dati sensibili (e non solo) ed i dati giudiziari. L'art. 9 parte dalla premessa del divieto di trattamento dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, come pure trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona o dati relativi alla salute o alla vita sessuale e all'orientamento sessuale. Tale divieto, da considerare, quindi, come principio di carattere generale, non si applica quando ricorrono determinati casi previsti dalla disposizione in commento[241].

[241] Il paragrafo 2, art. 9, recita: «Il paragrafo 1 non si applica quando si verifica uno dei seguenti casi: a) l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1; b)il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato; c)il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso; d) il trattamento è effettuato, nell'ambito delle sue legittime attività e con

L'art. 10, invece, dispone che il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, può avvenire soltanto sotto il controllo dei pubblici poteri o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda adeguate garanzie per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali può essere tenuto soltanto sotto il controllo dei pubblici poteri

4.1.1. *Segue*. I princípi specifici di trasparenza, di *accountability*, di *privacy by design* e *privacy by default*.

Tra i princípi di maggiore rilevanza meritano un particolare approfondimento il principio di trasparenza, il principio di *accountability*, il principio della *privacy by design* e della *privacy by default*.

Il principio della trasparenza, cristallizzato nel 39° considerando, trova poi la sua specificazione nell'art. 12. Esso impone che le informazioni destinate al pubblico o all'interessato siano facilmente accessibili e di facile comprensione e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli

---

adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli *ex* membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato; e) il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato; f) il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali; g) il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato; h) il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità, fatte salve le condizioni e le garanzie di cui al paragrafo 3; i) il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale; j) il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.».

interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati piú a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.

Il Regolamento sancisce il principio di «*accountability*», per il quale il titolare del trattamento dovrà dimostrare l'adozione di politiche *privacy* e misure adeguate in conformità al Regolamento. Tale principio enunciato, già nel primo periodo del 78° considerando - secondo cui «la tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento» - viene recepito all'art. 24, il quale prevede che tenuto conto della natura, del campo di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento dei dati personali è effettuato conformemente al Regolamento. Dette misure sono riesaminate e aggiornate qualora necessario. Inoltre, se ciò è proporzionato rispetto alle attività di trattamento, le predette misure includono

l'attuazione di politiche adeguate in materia di protezione dei dati da parte del responsabile del trattamento.

Il Regolamento in disamina introduce il principio della «*privacy by design*» e quello della «*privacy by default*», come prevede il 78° considerando, secondo periodo, secondo cui «il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default».

Dal principio della «*privacy by design*» discende l'attuazione di adeguate misure tecniche e organizzative sia all'atto della progettazione che dell'esecuzione del trattamento, mentre in virtú del principio della «*privacy by default*», che ricalca il principio di necessità di cui all'attuale disciplina, si stabilisce che i dati personali vengano trattati solamente per le finalità previste e per il periodo strettamente necessario a tali fini.

Pertanto, l'art. 25, comma 1, prevede che: «[t]enendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'àmbito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati.».

Il principio della *privacy by default* è invece specificato al successivo comma 2, dell'art. 25, secondo cui: «[i]l titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica.».

4.1.2. *Segue*. Le principali novità.

A parte la, già segnalata, «novità» sul campo di applicazione territoriale, di cui all'art. 3, ove si rivede la concezione tradizionale del principio di stabilimento - ma, come evidenziato, non senza fugare dubbi circa la sua chiara ed univoca interpretazione - le nuove esigenze che hanno portato all'emanazione del Regolamento hanno favorito anche l'introduzione di alcune importanti novità rispetto alla normativa preesistente, che occorre passare in rassegna.

Il Regolamento riconosce espressamente il «diritto all'oblio»[242], ovvero la possibilità per l'interessato di decidere che siano cancellati e non sottoposti ulteriormente a trattamento i propri dati personali non piú necessari per le finalità per le quali sono stati raccolti, nel caso di revoca del consenso o quando si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al Regolamento (art. 17).

All'art. 20, si stabilisce il diritto alla «portabilità dei dati», in virtú del quale l'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti, qualora l'interessato abbia fornito il proprio consenso al trattamento o se questo sia necessario per l'esecuzione di un contratto.

Tra le novità di maggior rilievo, merita sicuramente un'attenzione particolare una nuova figura - e professionalità - che va ad affiancarsi alla nomenclatura già conosciuta nel nostro *Codice Privacy*, ovvero al «titolare» e al «responsabile» del trattamento. Tale nuova figura è quella del c.d. «*Data Protection Officer*» («DPO»), ossia il «responsabile della protezione dei dati». Il DPO dovrà essere obbligatoriamente presente: all'interno di tutte le aziende pubbliche, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni

[242] Diritto all'oblio che è espressamente riconosciuto anche «Dichiarazione dei diritti in Internet», del 28 luglio 2015, cit., all'art. 11, il quale prevede che: «1. Ogni persona ha diritto di ottenere la cancellazione dagli indici dei motori di ricerca dei riferimenti ad informazioni che, per il loro contenuto o per il tempo trascorso dal momento della loro raccolta, non abbiano più rilevanza pubblica. 2. Il diritto all'oblio non può limitare la libertà di ricerca e il diritto dell'opinione pubblica a essere informata, che costituiscono condizioni necessarie per il funzionamento di una società democratica. Tale diritto può essere esercitato dalle persone note o alle quali sono affidate funzioni pubbliche solo se i dati che le riguardano non hanno alcun rilievo in relazione all'attività svolta o alle funzioni pubbliche esercitate. 3. Se la richiesta di cancellazione dagli indici dei motori di ricerca dei dati è stata accolta, chiunque può impugnare la decisione davanti all'autorità giudiziaria per garantire l'interesse pubblico all'informazione.».

giurisdizionali (art. 37, comma 1, lett. a); nonché in tutte quelle ove i trattamenti presentino specifici rischi, come ad esempio le aziende nelle quali sia richiesto un monitoraggio regolare e sistematico degli «interessati» su larga scala (art. 37, comma 1, lett. b); e quelle che trattano i c.d. «dati sensibili» (art. 37, comma 1, lett. c). Le società facenti parte di uno stesso gruppo, a livello nazionale o transfrontaliero, potranno nominare un unico DPO, a condizione che lo stesso sia facilmente raggiungibile da ciascuna società del gruppo stesso (art. 37, comma 2). Un unico responsabile della protezione dei dati può essere designato anche per piú autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione (art. 37, comma 3).

Il «DPO» è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati e della capacità di assolvere i compiti dei quali è incaricato *ex* art. 39 (art. 37, comma 5). Egli, inoltre, potrà essere un dipendente della società titolare del trattamento o del responsabile del trattamento oppure, in alternativa, assolvere i propri compiti in base ad un contratto di servizi (art. 37, comma 6). Ad ogni modo, ogni azienda dovrà rendere noti i dati del proprio «DPO» – il quale dovrà essere contattabile da tutti i soggetti «interessati» – nonché comunicarli al locale «Garante per la protezione dei dati personali» (art. 37, comma 7).

Interessante, poi, è il ruolo che il Regolamento destina al «DPO». Leggendo l'art. 38, comma 3, si intuisce come il responsabile della protezione dei dati potrà avere, all'interno dell'azienda, una caratura che nulla avrà da invidiare a professionalità quali quella del «CFO», o del «*General Counsel*» o «HR *Manager*», in quanto, è stabilito, il «DPO» riferirà direttamente ai vertici gerarchici della società[243], senza intermediazioni, e con grande autonomia e indipendenza[244], rispetto agli altri dirigenti.

Per chiudere sul punto, di seguito i principali compiti (art. 39) cui sarà adibito il «DPO»:

a) informare e consigliare il titolare o il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento;

b) verificare l'attuazione e l'applicazione della normativa, oltre alla sensibilizzazione e formazione del personale e dei relativi *auditors*;

---

[243] Il comma 3, ultimo periodo, dell'art. 38 in commento, recita: «Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.».

[244] Il comma 3, dell'art. 38 in commento, recita: «Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti.».

c) fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;

d) fungere da punto di contatto per gli «interessati», in merito a qualunque problematica connessa al trattamento dei loro dati nonché all'esercizio dei loro diritti;

e) fungere da punto di contatto per il Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.

Altra novità di rilievo, è l'introduzione dell'obbligo, per ogni azienda titolare del trattamento dei dati, di tenere un «registro delle attività di trattamento» (art. 30), svolte sotto la propria responsabilità. Sul punto occorre, però, rilevare come il comma 5, dell'art. 30, esoneri dall'adempimento appena accennato le piccole e medie imprese, quelle dunque con meno di 250 dipendenti, a meno che, però, «[…] il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati […] o i dati personali relativi a condanne penali […]» (si vedrà, pertanto, come sarà interpretato ed applicato tale articolo nella prassi). Altro obbligo è quello di effettuare una «valutazione di impatto sulla protezione dei dati» (art. 35). Questo adempimento, in particolare, è richiesto in relazione: a) ai trattamenti automatizzati, ivi compresa la profilazione; b) con riguardo ai trattamenti su larga scala di categorie particolari di dati (sensibili); c) nonché relativamente ai dati ottenuti dalla sorveglianza sistematica, sempre su larga scala, di zone accessibili al pubblico. Sarà ad ogni modo il Garante *Privacy* (per quanto riguarda l'Italia), a redigere e rendere pubblico l'elenco delle tipologie di trattamenti soggetti al requisito della «valutazione d'impatto sulla protezione dei dati» (art. 35, comma 4).

L'art. 36 del Regolamento prevede, poi, la c.d. «consultazione preventiva» quando il titolare del trattamento, prima di procedere al trattamento dei dati personali, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. Se l'Autorità di controllo ritiene che il trattamento previsto non sia conforme al Regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, entro un periodo massimo di otto settimane dalla richiesta di consultazione, fornisce una consulenza per iscritto al titolare del trattamento dei dati, e ove applicabile al responsabile del trattamento. Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del

trattamento previsto. Qualora si applichi la proroga, il titolare del trattamento e, ove applicabile, il responsabile del trattamento ne sono informati, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta. Tali periodi possono essere sospesi fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

Tra i «nuovi» obblighi, a carico del titolare del trattamento, c'è anche quello di notifica della violazione dei dati personali all'autorità di controllo, di cui all'art. 33. Tale articolo dispone che «in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo» (*Data breach*).

La notifica in parola, in base al comma 3, dell'art. 33, deve almeno: «a) descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione; b) comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni; c) descrivere le probabili conseguenze della violazione dei dati personali; d) descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.».

Il successivo art. 34, invece, prevede un'altra importante incombenza collegata alla precedente e cioè la comunicazione di una violazione dei dati personali all'interessato. Difatti, quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo. La comunicazione deve descrivere con un linguaggio semplice e chiaro la natura della violazione dei dati personali e contiene almeno le informazioni e le raccomandazioni di cui all'art. 33.

A mente del comma 3, dell'articolo in esame, la comunicazione all'interessato non è richiesta se è soddisfatta una delle seguenti condizioni: «a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano

state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura; b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1; c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.».

Gli articoli 42 e 43 del Regolamento danno ampio spazio alla certificazione ed agli organismi di certificazione. In particolare l'art. 42 prevede che gli Stati membri, le autorità di controllo, il Comitato europeo per la protezione dei dati e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati, nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al Regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Si tiene conto delle esigenze specifiche delle micro, piccole e medie imprese. I meccanismi, i sigilli o i marchi approvati (ai sensi del comma 5) possono essere istituiti anche al fine di dimostrare la previsione di adeguate garanzie da parte dei titolari del trattamento o responsabili del trattamento non soggetti al Regolamento ai sensi dell'articolo 3, nel quadro dei trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali alle condizioni di cui all'articolo 46, paragrafo 2, lettera f). Detti titolari del trattamento o responsabili del trattamento assumono l'impegno vincolante ed esecutivo, mediante strumenti contrattuali o di altro tipo giuridicamente vincolanti, di applicare le stesse adeguate garanzie anche per quanto riguarda i diritti degli interessati. La certificazione è volontaria e accessibile tramite una procedura trasparente. La stessa non riduce la responsabilità del titolare del trattamento o del responsabile del trattamento riguardo alla conformità al Regolamento e lascia impregiudicati i compiti e i poteri dell'autorità di controllo competente. La certificazione è rilasciata dagli organismi di certificazione o dall'autorità di controllo competente in base ai criteri approvati dalla stessa o, ai sensi dell'articolo 63, dal Comitato europeo per la protezione dei dati. In quest'ultimo caso i criteri approvati dal Comitato possono risultare in una certificazione comune, il sigillo europeo per la protezione dei dati. Naturalmente il titolare del trattamento o responsabile del trattamento, che sottopone il trattamento effettuato al meccanismo di certificazione, fornisce all'organismo di certificazione o, se del caso, all'autorità di controllo

competente tutte le informazioni e l'accesso alle attività di trattamento necessarie a espletare la procedura di certificazione. La certificazione è rilasciata al titolare del trattamento o al responsabile del trattamento per un periodo massimo di tre anni e può essere rinnovata alle stesse condizioni purché continuino ad essere soddisfatti i requisiti pertinenti. È revocata, se del caso, dagli organismi di certificazione o dall'autorità di controllo competente, qualora non siano o non siano piú soddisfatti i requisiti per la certificazione.

Infine, per quanto concerne il «sistema sanzionatorio», il Regolamento ha aumentato l'ammontare delle sanzioni amministrative pecuniarie (art. 83), che potranno arrivare fino ad un massimo di 20 milioni di Euro o fino al 4% del fatturato mondiale totale annuo, lasciando peraltro ciascuno Stato membro libero di adottare norme relative ad altre sanzioni.

4.1.3. *Segue*. Le garanzie sul trasferimento di dati personali al di fuori dell'UE.

Il Regolamento dedica particolare attenzione al trasferimento dei dati personali verso paesi terzi o organizzazioni internazionali, stabilendo le norme disciplinanti tale trasferimento nel Capo V, appunto rubricato «Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali» (artt. 44-50). I trasferimenti in parola sono possibili a patto che siano soddisfatte un certo numero di condizioni e garanzie, che di seguito si analizzano.

In primis, viene dettato, all'art. 44, il principio generale per un siffatto trasferimento. Si sancisce, dunque, che «[q]ualunque 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.».

Per quanto concerne le specifiche condizioni di ammissibilità del trasferimento in esame, la prima di esse è la «decisone di adeguatezza» Commissione (art. 45). In buona sostanza, il trasferimento è consentito quando la Commissione ha deciso che il paese terzo, un territorio o uno o piú settori specifici all'interno del paese terzo, o l'organizzazione internazionale garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche.

La Commissione, nel valutare l'adeguatezza del livello di protezione, prende in considerazione, in particolare, una serie di elementi espressamente indicati al comma 2 dell'art. 45. In buona sostanza - in linea con i valori fondamentali su cui è fondata l'Unione, in particolare la tutela dei diritti dell'uomo - la Commissione, nella sua valutazione, tiene conto: *i)* del modo in cui tale paese rispetta lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, nonché la legislazione generale e settoriale riguardante segnatamente la sicurezza pubblica, la difesa e la sicurezza nazionale, come pure l'ordine pubblico e il diritto penale, nonché i diritti effettivi e azionabili dagli interessati e un mezzo di ricorso effettivo in sede amministrativa e giudiziale; *ii)* dell'esistenza, nel paese terzo, di un effettivo controllo indipendente della protezione dei dati e della previsione di meccanismi di cooperazione con autorità di protezione dei dati degli Stati membri, in modo tale da assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti; *iii)* degli impegni internazionali che il paese terzo o l'organizzazione internazionale hanno assunto, nonché gli obblighi derivanti dalla partecipazione del paese terzo o dell'organizzazione internazionale a sistemi multilaterali o regionali, soprattutto in relazione alla protezione dei dati personali, nonché all'attuazione di tali obblighi (in particolare, a mente del 105° considerando, «si dovrebbe tenere in considerazione l'adesione dei paesi terzi alla convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale e relativo protocollo addizionale»).

Di notevole importanza è la previsione contenuta nel 104° considerando, ove si specifica che il paese terzo «dovrebbe offrire garanzie di un adeguato livello di protezione sostanzialmente equivalente a quello assicurato all'interno dell'Unione, segnatamente quando i dati personali sono trattati in uno o più settori specifici.». Si recepisce, pertanto, il *dictum* della Corte di Giustizia nel caso *Maximilliam Schrems*, circa l'esatta portata e interpretazione dell'espressione «livello di protezione adeguato» - figurante all'art. 25,

paragrafo 6, dir. 95/46 - che se, da un lato, non esige che il paese terzo assicuri un livello di protezione identico, dall'altro, sta a significare che il medesimo paese deve però assicurare un livello di protezione sostanzialmente equivalente a quello garantito nell'Unione Europea[245].

La Commissione, dopo aver valutato l'adeguatezza del livello di protezione, sulla base di quanto testé detto, può decidere, mediante atti di esecuzione, che un paese terzo, un territorio o uno o piú settori specifici all'interno di un paese terzo, o un'organizzazione internazionale garantiscono un livello di protezione adeguato (comma 3).

Questo atto di esecuzione (adottato secondo la procedura d'esame di cui all'articolo 93, paragrafo 2 e che specifica il proprio àmbito di applicazione geografico e settoriale e, ove applicabile, identifica la o le autorità di controllo) non è perpetuo, né immodificabile. Esso, infatti, prevede un meccanismo di riesame periodico, almeno ogni quattro anni, che tenga conto di tutti gli sviluppi pertinenti nel paese terzo o nell'organizzazione internazionale. Se poi risulta dalle informazioni disponibili, in particolare in seguito al riesame di cui prima, che un paese terzo, un territorio o uno o piú settori specifici all'interno di un paese terzo, o un'organizzazione internazionale non garantiscono piú un livello di protezione adeguato, la Commissione revoca, modifica o sospende, nella misura necessaria, la decisione adottata mediante atti di esecuzione senza effetto retroattivo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 93, paragrafo 2, o, in casi di estrema urgenza, secondo la procedura di cui all'articolo 93, paragrafo 3 (comma 5).

La Commissione pubblica nella Gazzetta ufficiale dell'Unione europea e sul suo sito *web* l'elenco dei paesi terzi, dei territori e settori specifici all'interno di un paese terzo, e delle organizzazioni internazionali per i quali ha deciso che è o non è piú garantito un livello di protezione adeguato (comma 8).

Le decisioni e autorizzazioni di adeguatezza esistenti, ossia quelle adottate dalla Commissione *ex* articolo 25, paragrafo 6, dir. 95/46/CE, restano in vigore fino a quando non vengono modificate, sostituite o abrogate da una decisione della Commissione adottata conformemente al comma 3 o 5 dell'art. 45 in commento (comma 9).

In mancanza di una valutazione di adeguatezza il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o

[245] V. punto 73, Corte giust., 6 ottobre 2015, C-362/14, cit., già analizzato *infra* 3.3. cap. II.

un'organizzazione internazionale solo se ha offerto garanzie adeguate[246] e a condizione che siano disponibili diritti azionabili degli interessati e mezzi di ricorso effettivi per gli stessi (art. 46).

Costituiscono garanzie adeguate, ad esempio, le norme vincolanti d'impresa approvate in conformità dell'art. 47. Infatti, il trasferimento dei dati vero un paese terzo può altresí avvenire quando vi siano norme vincolanti d'impresa che però devono essere approvate dall'Autorità di controllo e purché: a) siano giuridicamente vincolanti e si applichino a tutti i membri interessati del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, compresi i loro dipendenti; b) conferiscano espressamente agli interessati diritti azionabili in relazione al trattamento dei loro dati personali; e c) soddisfino i requisiti di cui al paragrafo 2[247].

---

[246] Il comma 2, dell'art. 46, specifica che: Possono costituire garanzie adeguate di cui al paragrafo 1 senza necessitare di autorizzazioni specifiche da parte di un'autorità di controllo: a) uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici; b) le norme vincolanti d'impresa in conformità dell'articolo 47; c) le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2; e) un codice di condotta approvato a norma dell'articolo 40, unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati; o f) un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati. Il successivo comma 3, prevede che: Fatta salva l'autorizzazione dell'autorità di controllo competente, possono altresì costituire in particolare garanzie adeguate di cui al paragrafo 1: a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale; o b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

[247] Il paragrafo 2 in questione sancisce che: Le norme vincolanti d'impresa di cui al paragrafo 1 specificano almeno: a) la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri; b) i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione; c) la loro natura giuridicamente vincolante, a livello sia interno che esterno; d) l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa; e) i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa; f) il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in

L'art. 49 del Regolamento prevede anche diverse deroghe all'applicazione dei princípi generali in tema di trasferimento dei dati verso paese terzi specificati in precedenza. Varie sono le ipotesi prese in considerazione, tra le principali si annoverano i casi in cui l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per sé stesso, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate, oppure il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali prese su istanza dell'interessato, oppure il trasferimento sia necessario per importanti motivi di interesse pubblico, oppure il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria, etc.

Con i trasferimenti transfrontalieri di dati personali al di fuori dell'Unione potrebbe aumentare il rischio che la persona fisica non possa esercitare il proprio diritto alla protezione dei dati, in particolare per tutelarsi da usi o comunicazioni illeciti di tali informazioni. Allo stesso tempo, le autorità di controllo possono concludere di non essere in grado di dar corso ai reclami o svolgere indagini relative ad attività condotte oltre frontiera. I loro sforzi di collaborazione nel contesto transfrontaliero possono anche essere ostacolati dall'insufficienza di poteri per prevenire e correggere, da regimi giuridici incoerenti e da difficoltà pratiche quali la limitatezza delle risorse disponibili. Pertanto, vi è

---

parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione; g) le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14; h) i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 35 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami; i) le procedure di reclamo; j) i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente; k) i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo; l) il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j); m) i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e n) l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali.

la necessità di promuovere una piú stretta cooperazione tra le autorità di controllo della protezione dei dati affinché possano scambiare informazioni e condurre indagini di concerto con le loro controparti internazionali. Tal è la finalità e la *ratio* dell'art. 50, rubricato, appunto, «Cooperazione internazionale per la protezione dei dati personali». In particolare, la Commissione e le autorità di controllo adottano misure adeguate : *i)* atte a sviluppare meccanismi di cooperazione internazionale per agevolare e prestare mutua assistenza a livello internazionale nell'applicazione della legislazione sulla protezione dei dati personali; *ii)* prestare assistenza reciproca a livello internazionale in particolare mediante notificazione, deferimento dei reclami, assistenza alle indagini e scambio di informazioni; *iii)* coinvolgere le parti interessate in discussioni e attività dirette a promuovere la cooperazione internazionale nell'applicazione della legislazione in materia di protezione dei dati personali; *iv)* promuovere lo scambio e la documentazione delle legislazioni e delle prassi *in subiecta* materia, compresi i conflitti di giurisdizione con paesi terzi.

4.1.4. ***Segue*. Il comitato europeo per la protezione dei dati.**

L'art. 68 prevede il «Comitato europeo per la protezione dei dati» che è istituito come organismo dell'Unione ed è dotato di personalità giuridica. Esso è rappresentato dal suo presidente ed è composto dalla figura di vertice di un'autorità di controllo di ciascuno Stato membro e dal garante europeo della protezione dei dati, o dai rispettivi rappresentanti. La Commissione, attraverso un proprio rappresentante all'uopo designato, ha il diritto di partecipare alle attività e alle riunioni del comitato senza diritto di voto; ha altresí il diritto a che le vengano comunicate, da parte del presidente del comitato, le attività del comitato stesso.

Il comitato viene concepito dal legislatore europeo come organismo di garanzia e nomofilattico, vista la sua finalità precipua di assicurare «l'applicazione coerente» del regolamento (art. 70, comma 1). Nell'adempimento dei suoi compiti o nell'esercizio dei suoi poteri il Comitato europeo per la protezione dei dati opera con indipendenza. Gli

innumerevoli compiti del Comitato sono elencati nell'art. 70[248], mentre il successivo articolo 71 richiede al comitato la redazione di una relazione annuale sulla protezione delle persone

[248] L'art. 70 recita: 1. Il comitato garantisce l'applicazione coerente del presente regolamento. A tal fine, il comitato, di propria iniziativa o, se del caso, su richiesta della Commissione, in particolare: a) sorveglia il presente regolamento e ne assicura l'applicazione corretta nei casi previsti agli articoli 64 e 65 fatti salvi i compiti delle autorità nazionali di controllo; b) fornisce consulenza alla Commissione in merito a qualsiasi questione relativa alla protezione dei dati personali nell'Unione, comprese eventuali proposte di modifica del presente regolamento; c) fornisce consulenza alla Commissione sul formato e le procedure per lo scambio di informazioni tra titolari del trattamento, responsabili del trattamento e autorità di controllo in merito alle norme vincolanti d'impresa; d) pubblica linee guida, raccomandazioni e migliori prassi in materia di procedure per la cancellazione di link, copie o riproduzioni di dati personali dai servizi di comunicazione accessibili al pubblico di cui all'articolo 17, paragrafo 2; e) esamina, di propria iniziativa o su richiesta di uno dei suoi membri o della Commissione, qualsiasi questione relativa all'applicazione del presente regolamento e pubblica linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del presente regolamento; f) pubblica linee guida, raccomandazioni e migliori pratiche conformemente alla lettera e) del presente paragrafo, per specificare ulteriormente i criteri e le condizioni delle decisioni basate sulla profilazione ai sensi dell'articolo 22, paragrafo 2; g) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per accertare la violazione di dati personali e determinare l'ingiustificato ritardo di cui all'articolo 33, paragrafi 1 e 2, e le circostanze particolari in cui il titolare del trattamento o il responsabile del trattamento è tenuto a notificare la violazione dei dati personali; h) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, relative alle circostanze in cui una violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche di cui all'articolo 34, paragrafo 1; i) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali basati sulle norme vincolanti d'impresa applicate, rispettivamente, dai titolari del trattamento e dai responsabili del trattamento, nonché gli ulteriori requisiti per assicurare la protezione dei dati personali degli interessati di cui all'articolo 47; j) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, al fine di specificare ulteriormente i criteri e i requisiti dei trasferimenti di dati personali sulla base dell'articolo 49, paragrafo 1; k) elabora per le autorità di controllo linee guida riguardanti l'applicazione delle misure di cui all'articolo 58, paragrafi 1, 2 e 3, e la previsione delle sanzioni amministrative pecuniarie ai sensi dell'articolo 83; l) valuta l'applicazione pratica delle linee guida, raccomandazioni e migliori prassi di cui alle lettere e) e f); m) pubblica linee guida, raccomandazioni e migliori prassi conformemente alla lettera e) del presente paragrafo, per stabilire procedure comuni per le segnalazioni da parte di persone fisiche di violazioni del presente regolamento ai sensi dell'articolo 54, paragrafo 2; n) incoraggia l'elaborazione di codici di condotta e l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati ai sensi degli articoli 40 e 42; o) effettua l'accreditamento di organismi di certificazione e il suo riesame periodico a norma dell'articolo 43 e tiene un registro pubblico di organismi accreditati a norma dell'articolo 43, paragrafo 6, e dei titolari o responsabili del trattamento accreditati, stabiliti in paesi terzi a norma dell'articolo 42, paragrafo 7; p) specifica i requisiti di cui all'articolo 43, paragrafo 3, ai fini dell'accreditamento degli organismi di certificazione ai sensi dell'articolo 42; q) fornisce alla Commissione un parere in merito ai requisiti di certificazione di cui all'articolo 43, paragrafo 8; r) fornisce alla Commissione un parere in merito alle icone di cui all'articolo 12, paragrafo 7; s) fornisce alla Commissione un parere per valutare l'adeguatezza del livello di protezione in un paese terzo o in un'organizzazione internazionale, così come per valutare se il paese terzo, il territorio o uno o più settori specifici all'interno di tale paese terzo, o l'organizzazione internazionale non assicurino più un livello adeguato di protezione. A tal fine, la Commissione fornisce al comitato tutta la documentazione necessaria, inclusa la corrispondenza con il governo del paese terzo, con riguardo a tale paese terzo, territorio o settore specifico, o con l'organizzazione internazionale; t) emette pareri sui progetti di decisione delle autorità di controllo conformemente al meccanismo di coerenza di cui all'articolo 64, paragrafo 1, e sulle questioni presentate conformemente all'articolo 64, paragrafo 2, ed emette decisioni vincolanti ai sensi dell'articolo 65, anche nei casi di cui all'articolo 66; u) promuove la cooperazione e l'effettivo scambio di informazioni e prassi tra le autorità di controllo a livello bilaterale e multilaterale; v) promuove programmi comuni di formazione e facilita lo scambio di personale tra le autorità di controllo e, se del caso, con le autorità di controllo di paesi terzi o di

fisiche con riguardo al trattamento nell'Unione e, se del caso, nei paesi terzi e nelle organizzazioni internazionali.

4.1.5. *Segue*. Reclamo e ricorso giurisdizionale.

L'art. 77 del Regolamento stabilisce come principio generale che, fatto salvo ogni altro ricorso amministrativo o giurisdizionale, l'interessato che ritenga che il trattamento dei dati personali che lo riguardano non sia conforme al Regolamento ha il diritto di proporre reclamo a un'autorità di controllo, segnatamente nello Stato membro in cui risiede abitualmente, lavora oppure nel luogo della presunta violazione. Si prevede, quindi, un rimedio amministrativo dinanzi all'Autorità garante come alternativo rispetto agli altri rimedi giurisdizionali. Il reclamante, peraltro, dev'essere informato, dall'autorità di controllo cui è stato proposto il reclamo, dello stato o dell'esito dello stesso, compresa la possibilità di un ricorso giurisdizionale ai sensi dell'articolo 78 (comma 2, art. 77).

Ampio spazio è poi dedicato all'esercizio del ricorso giurisdizionale sia contro l'Autorità di controllo (art. 78) che contro il titolare del trattamento o del responsabile del trattamento (art. 79). Il legislatore comunitario, in entrambi i casi, individua anche l'autorità giurisdizionale presso la quale promuovere le azioni anzidette, in un'ottica di favore per l'interessato.

Per quanto concerne le azioni nei confronti dell'autorità di controllo, esse sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'autorità di controllo è stabilita (art. 78, comma 3). Viene adottato, pertanto, il criterio del foro «esclusivo domestico».

Per le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono, invece, previsti due criteri alternativi tra loro. Infatti, è stabilito che tali controversie

---

organizzazioni internazionali; w) promuove lo scambio di conoscenze e documentazione sulla legislazione e sulle prassi in materia di protezione dei dati tra autorità di controllo di tutto il mondo; x) emette pareri sui codici di condotta redatti a livello di Unione a norma dell'articolo 40, paragrafo 9; e y) tiene un registro elettronico, accessibile al pubblico, delle decisioni adottate dalle autorità di controllo e dalle autorità giurisdizionali su questioni trattate nell'ambito del meccanismo di coerenza. 2. Qualora chieda consulenza al comitato, la Commissione può indicare un termine, tenuto conto dell'urgenza della questione. 3. Il comitato trasmette pareri, linee guida, raccomandazioni e migliori prassi alla Commissione e al comitato di cui all'articolo 93, e li pubblica. 4. Se del caso, il comitato consulta le parti interessate e offre loro la possibilità di esprimere commenti entro un termine ragionevole. Fatto salvo l'articolo 76, il comitato rende pubblici i risultati della procedura di consultazione.

sono promosse: o dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento oppure, in alternativa, dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri (comma 2, art. 79). È quindi espressamente sancito il criterio dell'alternatività tra il foro dello stabilimento titolare del trattamento o del responsabile del trattamento e il foro della residenza abituale dell'interessato, che presumibilmente consentirà a quest'ultimo di optare per questo foro.

L'art. 80 del Regolamento chiarisce, inoltre, che l'interessato, qualora ritenga che siano stati violati i diritti di cui gode a norme del regolamento (142° considerando), ha il diritto di dare mandato a un organismo, un'organizzazione o un'associazione, che siano debitamente costituiti secondo il diritto di uno Stato membro, che non abbiano scopo di lucro, i cui obiettivi statutari siano di pubblico interesse e che siano attivi nel settore della tutela dei diritti e delle libertà degli interessati con riguardo alla protezione dei dati personali, di proporre il reclamo per suo conto a un'autorità di controllo e di esercitare per suo conto i diritti a un ricorso giurisdizionale o esercitare il diritto di ottenere il risarcimento del danno, se quest'ultimo è previsto dal diritto degli Stati membri (142° considerando).

4.1.6. *Segue*. Diritto al risarcimento e responsabilità.

Il Regolamento ribadisce i princípi propri della Direttiva 95/46/CE in merito al risarcimento del danno a favore dell'interessato. Difatti l'art. 82 prevede che chiunque subisca un danno materiale o immateriale cagionato da una violazione del Regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento. Un titolare del trattamento coinvolto nel trattamento risponde per il danno cagionato dal suo trattamento non conforme al Regolamento. Un responsabile del trattamento risponde per il danno cagionato dal trattamento solo se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario alle legittime istruzioni del titolare del trattamento.

Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, se dimostra che l'evento dannoso non gli è in alcun modo imputabile (*probatio diabolica*).

Qualora piú titolari del trattamento o responsabili del trattamento oppure entrambi siano coinvolti nello stesso trattamento e siano responsabili dell'eventuale danno cagionato dal trattamento, ogni titolare del trattamento o responsabile del trattamento risponde in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.

Qualora, poi, un titolare del trattamento o un responsabile del trattamento abbia pagato l'intero risarcimento del danno, tale titolare del trattamento o responsabile del trattamento ha il diritto di reclamare dagli altri titolari o responsabili del trattamento coinvolti nello stesso trattamento la parte del risarcimento corrispondente alla loro parte di responsabilità per il danno.

Le azioni legali per l'esercizio del diritto di ottenere il risarcimento del danno sono naturalmente promosse dinanzi alle autorità giurisdizionali competenti a norma del diritto nazionale dello Stato membro.

CAPITOLO III

La tutela dei dati personali nell'era del *cloud computing*

Sommario: 1. La conservazione dei documenti informatici in *cloud computing*. - 2. La conservazione dei dati personali nella giurisprudenza della Corte di giustizia. - 3. Principio dell'interoperabilità e diritto alla portabilità dei dati. - 4. I ruoli dei diversi operatori nei sistemi *cloud*. Il fornitore: titolare o responsabile? - 5. Obblighi di protezione dei dati nella relazione cliente-fornitore. - 6. Responsabilità in àmbito *cloud*. - 7. Il primo codice di condotta per garantire la protezione dei dati personali dei clienti di *provider* di infrastrutture *cloud*.

1. La conservazione dei documenti informatici in *cloud computing*.

I sistemi di *cloud computing* sono diventati determinanti in relazione ai processi di condivisione e conservazione dei dati, sviluppando flussi e archivi documentali gestiti completamente *on line*.

I vantaggi sono evidenti e comprovati, ma non si possono nascondere gli aspetti negativi[249], anzi, la loro valutazione costituisce una necessaria attività per creare maggiore affidamento e consapevolezza negli utenti[250].

La specifica natura del *cloud computing* comporta infatti che le informazioni vengano trattate e conservate al di là del perimetro della propria rete aziendale e del proprio dispositivo elettronico, per cui, i rischi devono essere attentamente valutati in relazione ai modelli di servizio che s'intende adottare e, in particolar modo, se si coinvolgono dati di soggetti terzi nell'esercizio di un'attività professionale.

Come spesso accade, l'innovazione dirompente che il *cloud computing* sta producendo, «genera processi non sempre di facile leggibilità e comprensibilità»[251]. Proprio per questo motivo, nel valutare il passaggio a questo nuovo modello, è fondamentale che ogni

[249] Sul punto v. *supra* cap. I, §§ 7 e 7.1.

[250] L'educazione all'uso consapevole di *internet* costituisce un diritto fondamentale della persona rimesso alla promozione delle istituzioni pubbliche, in particolare attraverso il sistema dell'istruzione e della formazione, oltre che al loro intervento per rimuovere ogni forma di ritardo culturale che precluda o limiti l'utilizzo di internet da parte delle persone (art. 3, comma 4, «Dichiarazione dei diritti in Internet», cit.). Con particolare riguardo all'uso consapevole del sistema *cloud computing*, in àmbito nazionale, il Garante per la protezione dei dati personali è intervenuto piú volte al fine di favorire un utilizzo consapevole e corretto del detto sistema, in particolare, dettando accurate informazioni per l'utilizzo dello stesso in modo da tutelare al meglio i dati personali degli utenti che si affidano a un contratto di *cloud computing*. In tal senso, di notevole rilevanza è la Scheda di documentazione del 23 giugno 2011 "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi"*, alla la quale si rinvia al § 2.1, Cap. I.

[251] E. CARLONI, *Tendenze recenti e nuovi principi della digitalizzazione pubblica*, in *Gior. dir. amm*., 2015, 4, p. 307.

organizzazione valuti attentamente le numerose criticità, *in primis* per quanto riguarda la protezione dei dati personali trattati attraverso questi sistemi. Come ricordato dal Garante per la protezione dei dati personali «prima di esternalizzare la gestione di dati e documenti o adottare nuovi modelli organizzativi è necessario porsi alcune domande, scegliendo con cura la soluzione più sicura per le attività istituzionali o per il proprio business»[252].

Le problematiche che il fenomeno in esame sottende pongono a confronto due aspetti, al contempo connessi tra loro seppur a volte antitetici, della protezione dei dati personali: da un lato, l'opportunità di utilizzare, nell'àmbito del trattamento, sofisticate ed efficienti piattaforme tecnologiche a costi decisamente competitivi; dall'altro, la necessità di garantire la sicurezza dei dati trattati[253]. Questo importante bilanciamento non è privo di rischi. Una riflessione sul tema è sicuramente utile, anche se scarsi, sul piano italiano ed europeo, sono i contributi rilevanti[254].

D'altra parte, salvo il caso in cui si tratti di una società altamente specializzata che ha predisposto clausole contrattuali *ad hoc* per l'offerta di un servizio specifico di conservazione, appare assai difficile far rientrare la complessa relazione tra azienda e *outsourcer* nei generici e standardizzati contratti di servizi di *cloud computing* che il mercato offre. Per cui occorre cautela nella scelta del fornitore del servizio.

La disciplina dei documenti informatici e la loro conservazione è contenuta nel Codice dell'Amministrazione Digitale[255] (CAD), che prescrive le norme di carattere generale, e nelle regole tecniche[256] predisposte dal CNIPA[257]. Ai sensi dell'art. 2, lett. p), del CAD il documento informatico è «il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti[258]».

---

252 Garante per la protezione dei dati personali, *Cloud computing - Proteggere i dati per non cadere dalle nuvole*, Doc-Web n. 1895296.

253 Per una disamina della questione del trasferimento dei dati personali dei cittadini europei verso gli Stati Uniti, v. *retro*, cap. II, § 2.1.

254 Un'importante rassegna delle problematiche emerse in sede europea è contenuta in P. KITSOS, P. PAPPA, *Surveillance in the Clouds. The emergence of Cloud Computing and the Reshaping of Data Protection Lagislation*, in Clavell W. et al. (eds.), "Living in Surveillance Societies: The State of Surveillance. Proceedings of LISS conference 3", 2013, p. 281 ss.

255 Trattasi del d.lg. 7 marzo 2005 n. 82, intitolato «Codice dell'amministrazione digitale», pubblicato nella Gazz. Uff. 16 maggio 2005, n. 112, S.O.

256 d.P.C.M. del 22 febbraio 2013; d.P.C.M. 13 novembre 2014.

257 Poi DigitPA e Agenzia per l'Italia Digitale.

258 Lettera cosí sostituita dall' art. 1, comma 1, lett. d), D.Lgs. 26 agosto 2016, n. 179, a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall' art. 66, comma 1, del medesimo D.Lgs. n. 179/2016.

L'articolo 3 del CAD rubricato «Diritto all'uso delle tecnologie» prevede, al comma 1, che «chiunque ha il diritto di usare le soluzioni e gli strumenti di cui al presente Codice nei rapporti con i soggetti di cui all'articolo 2, comma 2[259], anche ai fini della partecipazione al procedimento amministrativo, fermi restando i diritti delle minoranze linguistiche riconosciute»[260].

L'art. 3, comma 1, lett. b), d.lg. 26 agosto 2016, n. 179*,* a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall' art. 66, comma 1, del medesimo d.lg. n. 179/2016, ha aggiunto, all'articolo in parola, i comma 1-*quater*, 1-*quinquies* e 1-*sexies*[261].

Il Capo III del CAD è intitolato «Formazione, gestione e conservazione dei documenti informatici» e all'art. 43 (Riproduzione e conservazione dei documenti), prevede che i documenti degli archivi, le scritture contabili, la corrispondenza ed ogni atto, dato o documento di cui è prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se la riproduzione e la conservazione nel tempo sono effettuate in modo da garantire la conformità dei documenti agli originali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71.

Al successivo comma 1-*bis* è sancito che se il documento informatico è conservato per legge da uno dei soggetti di cui all'articolo 2, comma 2, cessa l'obbligo di conservazione a carico dei cittadini e delle imprese che possono in ogni momento richiedere accesso al documento stesso.

---

[259] L'art. 2, comma 2, recita: Le disposizioni del presente Codice si applicano alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, nonché alle società a controllo pubblico, come definite nel decreto legislativo adottato in attuazione dell'articolo 18 della legge n. 124 del 2015, escluse le società quotate come definite dallo stesso decreto legislativo adottato in attuazione dell'articolo 18 della legge n. 124 del 2015.

[260] Comma modificato dall'art. 3, comma 1, d.lg. 4 aprile 2006, n. 159 e dall'art. 3, comma 1, lett. a), d.lg. 30 dicembre 2010, n. 235 e, successivamente, cosí sostituito dall' art. 3, comma 1, lett. a), d.lg. 26 agosto 2016, n. 179, a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall'art. 66, comma 1, del medesimo d.lg. n. 179/2016.

[261] Il comma 1-*quater* recita: «La gestione dei procedimenti amministrativi è attuata dai soggetti di cui all'articolo 2, comma 2, in modo da consentire, mediante strumenti informatici, la possibilità per il cittadino di verificare anche con mezzi telematici i termini previsti ed effettivi per lo specifico procedimento e il relativo stato di avanzamento, nonché di individuare l'ufficio e il funzionario responsabile del procedimento. 1-quinquies. Tutti i cittadini e le imprese hanno il diritto all'assegnazione di un'identità digitale attraverso la quale accedere e utilizzare i servizi erogati in rete dai soggetti di cui all'articolo 2, comma 2, alle condizioni di cui all'articolo 64. 1-sexies. Tutti gli iscritti all'Anagrafe nazionale della popolazione residente (ANPR) hanno il diritto di essere identificati dalle pubbliche amministrazioni tramite l'identità digitale di cui al comma 1-quinquies, nonché di inviare comunicazioni e documenti alle pubbliche amministrazioni e di riceverne dalle stesse tramite un domicilio digitale, alle condizioni di cui all'articolo 3-bis.».

Conservare è un'attività polifunzionale, poiché strumentale ad una pluralità di obiettivi, tutti indispensabili e da preservare.

Infatti conservare è, innanzitutto, proteggere nel tempo gli archivi digitali prodotti dalle pubbliche amministrazioni, impedendone il danneggiamento, la perdita o la distruzione. Allo stesso tempo, significa anche consentire l'accesso controllato a dati, documenti e informazioni e la diffusione degli stessi per fini amministrativi e di ricerca, nonché tutelare e valorizzare la memoria storica. È, inoltre, garantire autenticità, integrità, leggibilità e reperibilità dei documenti e predisporre idonee misure per la qualità e la sicurezza fisica, logica e tecnologica dei sistemi.

Come definito dall'art. 44 del d.lg. 82/2005 (CAD), rubricato «Requisiti per la gestione e conservazione dei documenti informatici»[262], il sistema di gestione informatica e conservazione dei documenti informatici della pubblica amministrazione assicura: l'identificazione certa del soggetto che ha formato il documento e dell'amministrazione o dell'area organizzativa omogenea di riferimento[263]; la sicurezza e l'integrità del sistema e dei dati e documenti presenti; la corretta e puntuale registrazione di protocollo dei documenti in entrata e in uscita; la raccolta di informazioni sul collegamento esistente tra ciascun documento ricevuto dall'amministrazione e i documenti dalla stessa formati; l'agevole reperimento delle informazioni riguardanti i documenti registrati; l'accesso, in condizioni di sicurezza, alle informazioni del sistema, nel rispetto delle disposizioni in materia di tutela dei dati personali; lo scambio di informazioni, ai sensi di quanto previsto dall'articolo 12, comma 2, con sistemi di gestione documentale di altre amministrazioni al fine di determinare lo stato e l'*iter* dei procedimenti complessi; la corretta organizzazione dei documenti nell'àmbito del sistema di classificazione adottato; l'accesso remoto, in condizioni di sicurezza, ai documenti e alle relative informazioni di registrazione tramite un identificativo univoco; il rispetto delle regole tecniche di cui all'articolo 71.[264]

L'art. 44, dopo aver individuato gli obiettivi del sistema di conservazione, testé descritti, obbliga altresí l'ente a nominare un proprio «Responsabile della conservazione», che

[262] Rubrica così sostituita dall'art. 36, comma 1, lett. a), d.lg. 26 agosto 2016, n. 179, a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall' art. 66, comma 1, del medesimo d.lg. n. 179/2016.
[263] Ossia quella di cui all'articolo 50, comma 4, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
[264] Comma modificato dall'art. 30, comma 1, lett. a), D.Lgs. 30 dicembre 2010, n. 235 e, successivamente, così sostituito dall' art. 36, comma 1, lett. b), D.Lgs. 26 agosto 2016, n. 179, a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall' art. 66, comma 1, del medesimo D.Lgs. n. 179/2016.

secondo la previsione di cui al comma 1-*bis*[265], gestisce il sistema di gestione e conservazione dei documenti informatici. Il successivo comma 1-*ter* attribuisce la facoltà al medesimo di delegare la conservazione ad altri soggetti pubblici o privati, sempre che offrano idonee garanzie organizzative e tecnologiche[266].

Per le regole tecniche in materia di sistema di conservazione previste dal presente articolo occorre vedere il d.P.C.M. 3 dicembre 2013[267].

Quest'ultimo descrive il sistema di conservazione, definendo: le fasi del processo i soggetti coinvolti[268] i modelli organizzativi i compiti del «Responsabile». Impone alle Pubbliche Amministrazioni, anche in caso di affidamento all'esterno, di designare come proprio Responsabile della conservazione un dirigente o un funzionario. Esso ha definito le misure attuative degli obblighi di conservazione, in forma digitale, dei documenti della P.A. come prescrive il CAD. L'art. 3[269] (rubricato «Sistema di conservazione») individua con

---

[265] Il comma 1-*bis*, recita: Il sistema di gestione e conservazione dei documenti informatici è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti conclusi. Tale comma è stato aggiunto dall'art. 30, comma 1, lett. b), D.Lgs. 30 dicembre 2010, n. 235 e, successivamente, così sostituito dall' art. 36, comma 1, lett. c), D.Lgs. 26 agosto 2016, n. 179, a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall' art. 66, comma 1, del medesimo D.Lgs. n. 179/2016.

[266] Cosí testualmente il comma 1-*ter*: Il responsabile della conservazione può chiedere la conservazione dei documenti informatici o la certificazione della conformità del relativo processo di conservazione a quanto stabilito nel presente articolo ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche. Anche codesto comma è stato aggiunto dall'art. 30, comma 1, lett. b), D.Lgs. 30 dicembre 2010, n. 235 e, successivamente, cosí modificato dall' art. 36, comma 1, lett. d), D.Lgs. 26 agosto 2016, n. 179, a decorrere dal 14 settembre 2016, ai sensi di quanto disposto dall' art. 66, comma 1, del medesimo D.Lgs. n. 179/2016.

[267] Regole tecniche in materia di sistema di conservazione ai sensi degli articoli 20, commi 3 e 5-bis, 23-ter, comma 4, 43, commi 1 e 3, 44, 44-bis e 71, comma 1, del Codice dell'amministrazione digitale di cui al decreto legislativo n. 82 del 2005. Pubblicato nella Gazz. Uff. 12 marzo 2014, n. 59, S.O. Vedi anche il d.P.C.M. 13 novembre 2014, il quale indica le tipologie di oggetti da inviare in conservazione (documenti, fascicoli, aggregazioni documentali, registri, repertori informatici).

[268] I soggetti coinvolti nell'attività di conservazione sono: a) il produttore: ovverosia la persona fisica o giuridica che trasmette i documenti da conservare mediante pacchetti di versamento. Nelle P.A. solitamente si identifica con il Responsabile della gestione documentale; b) il responsabile della Conservazione: colui che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità e autonomia, in relazione al modello organizzativo adottato; c) l'utente: la persona fisica o giuridica che richiede l'accesso ai documenti presenti nel sistema di conservazione al fine di acquisire dati, documenti e informazioni.

[269] L'art. 3 del d.P.C.M. 3 dicembre 2013, recita: 1. In attuazione di quanto previsto dall'art. 44, comma 1, del Codice, il sistema di conservazione assicura, dalla presa in carico dal produttore di cui all'art. 6 fino all'eventuale scarto, la conservazione, tramite l'adozione di regole, procedure e tecnologie, dei seguenti oggetti in esso conservati, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

buona precisione l'oggetto della conservazione: i documenti informatici e i documenti amministrativi informatici con i metadati a essi associati.

L'ampiezza di questo provvedimento è facilmente desumibile dall'art. 40 del CAD: «le pubbliche amministrazioni formano gli originali dei propri documenti con mezzi informatici». Dunque, pressoché l'intero patrimonio informativo pubblico rientra nella disciplina in commento.

Il collegamento con i sistemi di *cloud computing* appare chiaramente dalla proposta di modelli organizzativi[270] definiti dall'art. 5 del d.P.C.M.[271], implementabili negli enti pubblici assoggettati alla disciplina. I modelli organizzativi possibili per le pubbliche amministrazioni sono fondamentalmente due: *in house*, ove quindi la conservazione è svolta all'interno della struttura organizzativa e, pertanto, senza avvalersi di fornitori di servizi in *cloud computing*; *in outsorurcing*, ove la conservazione è affidata, in modo totale o parziale, esclusivamente a conservatori accreditati inseriti nell'elenco di AgID (attualmente 25 soggetti), e cioè tramite piattaforme *cloud*. *In house* o *in outsorcing*, il sistema di conservazione deve rispettare le regole tecniche del d.P.C.M. 3 dicembre 2013.

Può accreditarsi presso l'Agenzia il soggetto pubblico e privato che possieda i requisiti amministrativi, organizzativi, tecnologici adeguati a garantire qualità e sicurezza della conservazione, mentre è obbligato a richiedere l'accreditamento il soggetto pubblico e privato che vuole erogare servizi di conservazione rivolti alle pubbliche amministrazioni.

---

a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati di cui all'allegato n. 5 al presente decreto;
b) i fascicoli informatici ovvero le aggregazioni documentali informatiche con i metadati ad essi associati di cui all'allegato n. 5 al presente decreto, contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che appartengono al fascicolo o all'aggregazione documentale.
2. Le componenti funzionali del sistema di conservazione assicurano il trattamento dell'intero ciclo di gestione dell'oggetto conservato nell'ambito del processo di conservazione.
3. Il sistema di conservazione garantisce l'accesso all'oggetto conservato, per il periodo prescritto dalla norma, indipendentemente dall'evolversi del contesto tecnologico.

[270] In merito, si veda G. TROIANO, *La conservazione dei documenti in* "cloud computing", in *Cib. dir.*, 2013, p. 265.

[271] L'art. 5 del d.P.C.M., rubricato «Modelli organizzativi della conservazione» recita: «1. Il sistema di conservazione opera secondo modelli organizzativi esplicitamente definiti che garantiscono la sua distinzione logica dal sistema di gestione documentale, se esistente. 2. Ai sensi dell'art. 44 del Codice, la conservazione può essere svolta: a) all'interno della struttura organizzativa del soggetto produttore dei documenti informatici da conservare; b) affidandola, in modo totale o parziale, ad altri soggetti, pubblici o privati che offrono idonee garanzie organizzative e tecnologiche, anche accreditati come conservatori presso l'Agenzia per l'Italia digitale. 3. Le pubbliche amministrazioni realizzano i processi di conservazione all'interno della propria struttura organizzativa o affidandoli a conservatori accreditati, pubblici o privati, di cui all'art. 44-bis, comma 1, del Codice, fatte salve le competenze del Ministero dei beni e delle attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42, e successive modificazioni.

Per garantire un sistema di conservazione affidabile, l'Agenzia individua i requisiti per l'accreditamento. Per i soggetti privati è richiesta l'affidabilità organizzativi, tecnologica e finanziaria e segnatamente: a) forma giuridica di società di capitali e capitale sociale versato non inferiore a 200.000 euro; b) requisiti di onorabilità dei rappresentati legali, dei soggetti preposti all'amministrazione e degli organi di controllo. In ogni caso il soggetto che voglia accreditarsi deve dimostrare l'adozione procedure conformi a *standard* e disposizioni legislative vigenti e l'impiego di specifiche figure professionali, quali: Responsabile del servizio di conservazione; Responsabile della funzione archivistica di conservazione; Responsabile del trattamento dei dati personali; Responsabile della sicurezza dei sistemi per la conservazione; Responsabile dei sistemi informativi per la conservazione; Responsabile dello sviluppo e della manutenzione del sistema di conservazione.

Per quanto piú specificamente attiene al trattamento dei dati personali contenuti in questi documenti e fascicoli informatici e vista la mole di dati personali giornalmente trattati dalle P.A. e costantemente archiviati in questi sistemi, è evidente come il legislatore abbia dovuto predisporre alcune specifiche regole inerenti al corretto trattamento di questi dati.

È proprio il d.P.C.M. in questione a inquadrare il fornitore del servizio di conservazione come responsabile esterno del trattamento dei dati personali nell'art. 6, comma 8[272]. «Questa netta presa di posizione può essere fuorviante: occorre limitare questa regola ai soli servizi di conservazione, senza estenderla genericamente a tutti i servizi offerti con il paradigma del *cloud computing*.»[273]. Questi, infatti, sul piano tecnico, sono differenti dai

[272] L'art. 6, comma 8, del sopra citato d.P.C.M., stabilisce che «[i]l soggetto esterno a cui è affidato il processo di conservazione assume il ruolo di responsabile del trattamento dei dati come previsto dal Codice in materia di protezione dei dati personali.»

[273] Cosí testualmente S. LEUCCI, S. GIRELLA, J.L. LOUIS A BECCARA, *Pubblica amministrazione e protezione dei dati personali nelle "nuvole": criticità e soluzioni*, in *Inf. dir.*, 2014, p. 42. Gli a. invitano a non «cadere nella trappola della confusione terminologica» adducendo interessanti motivazioni. Innanzitutto, il fatto che non sia corretto limitarsi alla mera nomina di ogni fornitore di servizi *cloud* a responsabile del trattamento emerge dalla considerazione per la quale, a differenza dei servizi di *email* e collaborazione d'ufficio, la conservazione digitale dei documenti è un'attività prevista e imposta a norma di legge (dal CAD e dal d.P.C.M. attuativo), «certificando tale disciplina normativa la totale soggezione del settore alle dinamiche e alle piú elevate garanzie pubblicistiche.». Inoltre, proseguono gli a., il controllo sui sistemi e sui dati è reso agevole dal requisito previsto dall'art. 9, comma 2, del d.P.C.M. in parola, per il quale il sistema di conservazione delle PPAA e i sistemi di conservazione dei conservatori accreditati prevedono la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale e garantiscono un accesso ai dati presso la sede del produttore e misure di sicurezza conformi a quelle previste dal decreto; pertanto, «questa disposizione agevola i controlli del titolare-cliente sul responsabile-fornitore, permettendone così una più semplice divisione degli incarichi privacy.». Molto interessante, poi, è la circostanza per la quale il servizio di email e collaborazione prevede il

sistemi di conservazione che rispondono ad esigenze diverse degli enti pubblici. La grande «diversità risiede negli aspetti funzionali: i sistemi di posta elettronica e di collaborazione offerti dalla "nuvola" non si limitano ad offrire solo servizi di conservazione/memorizzazione (incluse tutte le attività propedeutiche e correlate), ma estendono il campo di operatività a funzionalità ulteriori e completamente diverse (gestione di posta elettronica, scambi di messaggi, redazioni di documenti ecc.); solo una minima parte di informazioni, in particolare quelle destinate a costituire il contenuto degli atti, sarà oggetto di conservazione.».[274] Inoltre, mentre nel *cloud computing* i dati vengono costantemente trasferiti anche nelle piú remote località del mondo, nella conservazione digitale una simile situazione non potrebbe riproporsi, come emerge dalla lettura del citato provvedimento presidenziale (art. 9, comma 2).

Pertanto, qualora i due servizi fossero davvero sovrapponibili risulta difficile giustificare il ricorso ad un servizio di *email* e collaborazione offerto secondo il paradigma del *cloud computing*; diversamente, anche qualora il servizio di conservazione digitale potesse essere svolto con le modalità di *cloud computing*, dovrà tenersi presente la strutturale e congenita diversità tra le due attività[275].

2. La conservazione dei dati personali nella giurisprudenza della Corte di giustizia.

La Corte di giustizia, con sentenza dell'8 aprile 2014 (cause C-293/12 e C-594/12)[276], dichiara invalida la direttiva sulla conservazione dei dati[277] ritenendo che la stessa, poiché

---

trasferimento dei dati a soggetti non accreditati presso le AgID, che potrebbero utilizzarli per finalità proprie, ovvero con strumenti su cui la P.A. cliente non riesce ad avere alcun controllo effettivo.

274 S. LEUCCI, S. GIRELLA, J.L. LOUIS A BECCARA, *Pubblica amministrazione* cit., p. 43 s., ove si evidenzia, quindi, come nella conservazione digitale permanga alla P.A. il controllo sui propri dati, mentre, nel quotidiano utilizzo di altre tipologie di servizi (quali quelli offerti attraverso il paradigma del *cloud*) è alquanto evidente il rischio di perdere definitivamente tali dati. Infatti, gli aspetti tecnici della conservazione digitale sono normativamente disciplinati e in capo all'ente pubblico (titolare) rimangono i poteri di determinare le finalità (conservazione), le modalità e le misure di sicurezza del sistema; il fornitore, quale responsabile, avrà chiare responsabilità legate all'oggetto del processo di cui si farà carico.

275 S. LEUCCI, S. GIRELLA, J.L. LOUIS A BECCARA, *o.c.*, p. 44.

276 Corte di Giustizia, 8 aprile 2014, cause riunite c. 293/12 e c. 594/12, Digital Rights Ireland e Seitlinger e a., in *www.curia.eu*. Per un commento esaustivo si veda M. MESSINA, *La Corte di Giustizia UE si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità*, in *Ordine internazionale e diritti umani*, 2014, p. 396 ss.

277 Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE (GU L

impone la conservazione di tali dati e ne consente l'accesso alle autorità nazionali competenti, si ingerisca in modo particolarmente grave nei i diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale. Inoltre, il fatto che la conservazione ed il successivo utilizzo dei dati avvengano senza che l'abbonato o l'utente registrato ne siano informati può ingenerare negli interessati la sensazione che la loro vita privata sia oggetto di costante sorveglianza.

La Corte esamina, quindi, se un'ingerenza siffatta nei diritti fondamentali in questione sia giustificata. Sicché essa constata che la conservazione dei dati imposta dalla direttiva non è idonea ad arrecare pregiudizio al contenuto essenziale dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati di carattere personale. Infatti, la direttiva non consente di prendere conoscenza del contenuto delle comunicazioni elettroniche in quanto tale e prevede che i fornitori di servizi o di reti debbano rispettare determinati princípi di protezione e di sicurezza dei dati. Inoltre, la conservazione dei dati ai fini della loro eventuale trasmissione alle autorità nazionali competenti risponde effettivamente a un obiettivo di interesse generale, vale a dire la lotta alla criminalità grave nonché, in definitiva, la pubblica sicurezza.

Tuttavia, la Corte ritiene che il legislatore dell'Unione, con l'adozione della direttiva sulla conservazione dei dati, abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità.

A tale riguardo, la Corte osserva che, in considerazione, da un lato, dell'importante ruolo svolto dalla protezione dei dati personali nei confronti del diritto fondamentale al rispetto della vita privata e, dall'altro, della portata e della gravità dell'ingerenza in tale diritto che la direttiva comporta, il potere discrezionale del legislatore dell'Unione risulta ridotto e che occorre quindi procedere a un controllo rigoroso.

Anche se la conservazione dei dati imposta dalla direttiva può essere considerata idonea a raggiungere l'obiettivo perseguito dalla medesima, l'ingerenza vasta e particolarmente

---

105, pag. 54). Essa ha per obiettivo principale l'armonizzazione delle disposizioni degli Stati membri sulla conservazione di determinati dati generati o trattati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione. Essa è quindi volta a garantire la disponibilità di tali dati a fini di indagine, accertamento e perseguimento di reati gravi, come in particolare i reati legati alla criminalità organizzata e al terrorismo. In tal senso, la direttiva dispone che i suddetti fornitori debbano conservare i dati relativi al traffico, i dati relativi all'ubicazione nonché i dati connessi necessari per identificare l'abbonato o l'utente. La direttiva non autorizza, invece, la conservazione del contenuto della comunicazione e delle informazioni consultate.

grave di tale direttiva nei diritti fondamentali in parola non è sufficientemente regolamentata in modo da essere effettivamente limitata allo stretto necessario.

In primo luogo, infatti, la direttiva trova applicazione generalizzata all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi.

In secondo luogo, la direttiva non prevede alcun criterio oggettivo che consenta di garantire che le autorità nazionali competenti abbiano accesso ai dati e possano utilizzarli solamente per prevenire, accertare e perseguire penalmente reati che possano essere considerati, tenuto conto della portata e della gravità dell'ingerenza nei diritti fondamentali summenzionati, sufficientemente gravi da giustificare una simile ingerenza. Al contrario, la direttiva si limita a fare generico rinvio ai «reati gravi» definiti da ciascuno Stato membro nella propria legislazione nazionale. Inoltre, la direttiva non stabilisce i presupposti materiali e procedurali che consentono alle autorità nazionali competenti di avere accesso ai dati e di farne successivo uso. L'accesso ai dati, in particolare, non è subordinato al previo controllo di un giudice o di un ente amministrativo indipendente.

In terzo luogo, quanto alla durata della conservazione dei dati, la direttiva impone che essa non sia inferiore a sei mesi, senza operare distinzioni tra le categorie di dati a seconda delle persone interessate o dell'eventuale utilità dei dati rispetto all'obiettivo perseguito. Inoltre, tale durata è compresa tra un minimo di sei ed un massimo di ventiquattro mesi, senza che la direttiva precisi i criteri oggettivi in base ai quali la durata della conservazione deve essere determinata, in modo da garantire la sua limitazione allo stretto necessario.

La Corte constata, peraltro, che la direttiva non prevede garanzie sufficienti ad assicurare una protezione efficace dei dati contro i rischi di abusi e contro qualsiasi accesso e utilizzo illeciti dei dati. Essa rileva, tra l'altro, che la direttiva autorizza i fornitori di servizi a tenere conto di considerazioni economiche in sede di determinazione del livello di sicurezza da applicare (in particolare per quanto riguarda i costi di attuazione delle misure di sicurezza) e non garantisce la distruzione irreversibile dei dati al termine della loro durata di conservazione.

La Corte censura, infine, il fatto che la direttiva non impone che i dati siano conservati sul territorio dell'Unione. La direttiva non garantisce, quindi, il pieno controllo da parte di un'autorità indipendente del rispetto delle esigenze di protezione e di sicurezza, come è

invece espressamente richiesto dalla Carta dei diritti fondamentali dell'Unione europea (art. 8). Orbene, un controllo siffatto, compiuto sulla base del diritto dell'Unione, costituisce un elemento essenziale del rispetto della protezione delle persone con riferimento al trattamento dei dati personali.

La pronuncia, pertanto, ha affermato un importante principio: i dati relativi alle comunicazioni elettroniche devono essere conservati nel territorio dell'Unione, anche al fine di prevenire e contrastare reati gravi.

Alla luce del nuovo Regolamento UE sulla *Privacy*, può dirsi che il problema della conservazione dei dati personali (*rectius*, non conservazione degli stessi all'interno dell'Unione europea), non è poi cosí drammatico come può sembrare e ciò in base alla specificazione, nella nuova normativa europea, dell'àmbito di applicazione territoriale della stessa (art. 3). In altri termini, quand'anche i dati personali venissero conservati in un Paese terzo, tale pratica non sempre varrebbe (nel senso che non automaticamente sarebbe sufficiente) ad escludere l'applicabilità del Regolamento in discorso.

La conservazione è essa stessa un trattamento (di dati personali), consistendo quest'ultimo in «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali», come, ad esempio, «la conservazione» (art. 4, n. 2).

Adesso, si ipotizzi che il trattamento di dati personali, *sub specie* di operazione di conservazione degli stessi, avvenga al di fuori dell'Unione. Siffatta conservazione determinerebbe automaticamente la non applicabilità del Regolamento UE? La risposta giusta dovrebbe essere negativa, anche se la formulazione dell'art. 3, par. 1, non sembra la migliore possibile.

Secondo la citata disposizione, ai fini dell'applicabilità o meno del diritto dell'Unione, non rileva il luogo in cui si realizza la conservazione dei dati personali, ma occorrerà far riferimento all'àmbito delle attività di uno stabilimento di un titolare del trattamento 'o' di un responsabile dello stesso nell'Unione. In breve, se un titolare 'o' un responsabile è stabilito nell'Unione allora il regolamento si applica «indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione» (criterio dello stabilimento nell'Unione di un titolare 'o' di un responsabile che effettua il trattamento).

Pertanto, il criterio di riferimento, per radicare l'applicabilità dello stesso, è lo stabilimento nell'Unione delle attività del titolare del trattamento 'o' del responsabile del

medesimo, nel senso che se queste attività - ossia le decisioni sulle finalità e sui mezzi del trattamento (*rectius*, sulla conservazione) dei dati personali o comunque le principali attività del trattamento stesso - sono poste in essere in un suo stabilimento sito in uno Stato membro ciò farà sí che sarà applicabile il Regolamento.

Per il concetto stabilimento, non espressamente definito nel Regolamento, occorre far riferimento al considerando 22°, il quale specifica come lo stabilimento prescinda da una determinata forma giuridica, essendo suo elemento qualificante «l'effettivo e reale svolgimento di un'attività nel quadro di un'organizzazione stabile.».

In altri termini, in base al criterio dello stabilimento nell'Unione di un titolare 'o' di un responsabile che effettua il trattamento dei dati personali di una persona fisica identificata o identificabile (*rectius*, l'interessato), non rileva il luogo in cui sono conservati i dati personali, che potrebbe, ad esempio, situato anche al di fuori dell'Unione, occorrendo, invece, fare riferimento all'effettivo e reale svolgimento di un'attività di un titolare o di un responsabile nel quadro di un'organizzazione stabile all'interno dell'Unione.

Altro caso: titolare o responsabile del trattamento non stabiliti nell'Unione, ma gli interessati si trovano nell'Unione (art. 3, par. 2). Si applicherà il Regolamento in discorso quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Emerge chiaramente la portata innovativa del criterio in parola, consistente nel fatto che l'elemento che determina l'applicabilità del Regolamento europeo è legato al luogo in cui è situato l'interessato (criterio del luogo in cui l'interessato si trova); se questi si trova nell'Unione, si applicherà il regolamento anche se titolare o responsabile del trattamento non sono stabiliti nell'Unione.

Inoltre il regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico (art. 3, par. 3).

3. Principio dell'interoperabilità e diritto alla portabilità dei dati.

Nel corso del tempo può presentarsi la necessità di cambiare fornitore, determinata da una serie indeterminata di ipotesi relative alle variabili esigenze e/o scelte del fruitore del servizio, quali ad esempio: cambiamenti strutturali (fusioni o acquisizioni societarie), modifiche normative, etc. Ciò richiede di preoccuparsi – alla stipula di un contratto per servizi di *cloud computing* - della portabilità dei dati, sotto il duplice profilo del loro recupero (che richiede la conoscibilità dei sistemi) e della loro piena riutilizzabilità. Tali aspetti sono connessi da un lato con le caratteristiche tecniche, dall'altro con le licenze d'uso delle applicazioni informatiche utilizzate dal fornitore.

Il ricorso a un diverso fornitore o a una diversa infrastruttura potrebbe essere agevolato dall'utilizzo di un *open cloud* (in sintesi un *cloud* realizzato con tecnologia *open source*) che, per le sue caratteristiche di flessibilità (sotto il profilo *hardware* e *software*) e conoscibilità, può facilitare il processo di migrazione[278].

I fautori dell'*open cloud* evidenziano che le infrastrutture di *cloud computing* fornite come *close source* oppure come *open source* interni non permettono alla comunità di contribuire al loro sviluppo, rendendo complicate convergenza e interoperabilità, anche perché le tecnologie sono conosciute solo da alcuni professionisti specializzati. L'utilizzo dell'*open cloud*, consentirebbe invece di ovviare al problema, permettendo inoltre di individuare facilmente professionisti competenti.

Nell'*open cloud*, in primo luogo, il fatto che i fornitori lavorino insieme assicura che le caratteristiche del servizio scelto (sicurezza, integrazione, portabilità, interoperabilità, *governance*/*managment*, monitoraggio) sono indirizzate verso una collaborazione aperta e verso l'uso appropriato degli *standard*. In secondo luogo, i fornitori non utilizzano la propria posizione di mercato per vincolare gli utilizzatori a particolari piattaforme, né limitano la loro scelta tra fornitori. In terzo luogo, i fornitori devono, e possono, utilizzare e adottare

[278] È evidente il vantaggio, per l'utente, di un utilizzo di servizi che favoriscono la portabilità dei dati. È chiaro, infatti, che il ricorso a servizi di *cloud computing* basati su formati e *standard* aperti, facilita la transizione da un sistema *cloud* ad un altro, anche se gestiti da fornitori diversi. Ciò consente di scongiurare il rischio che eventuali modifiche unilaterali dei contratti di servizio, da parte di uno qualunque degli operatori che intervengono nella catena di fornitura, si traducano in condizioni peggiorative vincolanti o, comunque, facilita eventuali successivi passaggi da un fornitore all'altro. Privilegiare i servizi che favoriscono la portabilità dei dati è una delle indicazioni che il Garante Privacy italiano ha voluto fornire agli utenti dei servizi in questione nella Scheda di documentazione del 23 giugno 2011 "*Cloud computing: indicazioni per l'utilizzo consapevole dei servizi"*, alla quale si rinvia al § 2.1, Cap. I, per una migliore disamina.

standard esistenti e appropriati: non hanno la necessità di duplicare né di reinventare tecnologie; quando si rende necessario l'utilizzo di nuovi *standard* o la modifica di quelli esistenti, gli sviluppatori si assicurano di non crearne troppi e del fatto che i nuovi *standard* promuovono e non inibiscono l'innovazione. In quarto luogo, lo sforzo della comunità che si muove intorno a un *open cloud* è diretta a perseguire i bisogni degli utilizzatori e dovrebbe essere verificata rispetto alle loro reali esigenze.

Qualunque sia la scelta dell'utente, i criteri enunciati possono essere tenuti presenti per assicurarsi che un'infrastruttura di *cloud computing* sia aperta e consenta la scelta, la flessibilità e l'agilità richieste dall'utilizzatore.

Nella pratica, dalle statistiche pubblicate sui siti *web* delle comunità *open source* emerge che l'utilizzo di infrastrutture di *open cloud* non è esclusivamente limitato all'utilizzo nelle comunità di ricerca per la pubblicazione dei risultati di progetto, ma è anche destinato agli utilizzatori finali. Anche le pubbliche amministrazioni europee fanno ricorso a soluzioni *open source* a supporto delle proprie attività.

In Europa vi sono anche ampie comunità di sviluppo e un forte *background* nello sviluppo e nell'utilizzo dell'*open source*. Tuttavia, molte tecnologie sviluppate in Europa sono sfruttate da società statunitensi: stando alle stime, il 90% del volume di affari derivante da sistemi *open source* è generato da utenti non europei; ancora, molti consorzi che si occupano dello sviluppo e della commercializzazione dell'*open source* hanno sede negli Stati Uniti e sono state fondate da società IT statunitensi (come *Sourceforge* e *Code Plex*).

Se la ricerca sul *cloud computing* ha come obiettivo la realizzazione di un'opportunità economica europea sostenibile è opportuno un maggiore sviluppo delle aziende europee con diversi modelli imprenditoriali, volte a sviluppare al meglio questo patrimonio tecnologico.

Per superare gli ostacoli derivanti dall'adozione di *standard* diversi nella produzione informatica, è stato adottato dall'Unione Europea con proprie definizioni istituzionali, il principio dell'interoperabilità, già contenuto nella Direttiva 91/250/CEE per la quale nei considerando 10, 11 e 12 si prevede che «i programmi per elaboratore svolgono la funzione di comunicare e operare con altri componenti di un sistema informatico e con gli utenti; che a tale scopo è necessaria un'interconnessione e un'interazione logica e, ove opportuno, materiale per consentire a tutti i componenti software e hardware di operare con altri software e hardware e con gli utenti in tutti i modi in cui sono destinati a funzionare;

considerando che le parti del programma che assicurano tale interconnessione e interazione fra gli elementi del software e dell'hardware sono generalmente denominate «interfacce»; considerando che tale interconnessione e interazione funzionale è generalmente denominata «interoperabilità»; che tale interoperabilità può essere definita come la capacità di due o più sistemi di scambiare informazioni e di usare reciprocamente le informazioni scambiate».

Il Regolamento UE sulla *privacy* qualifica la portabilità dei dati come un diritto dell'interessato (art. 20), non a caso inserito nel Capo III, appunto rubricato «Diritti dell'interessato». Lo stesso Regolamento chiarisce la portata e l'essenzialità del diritto in parola, con il dichiarato obiettivo di assicurare piú tutele e libertà per i cittadini, al considerando 68 ove si specifica come sia «opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati» indicando quando il medesimo diritto dovrebbe applicarsi[279].

Pertanto, con il diritto alla portabilità dei dati si è liberi di trasferire i propri dati in un mercato digitale piú aperto alla concorrenza. Diritto alla «portabilità» dei propri dati personali che quindi significa diritto di trasferirli da un titolare del trattamento ad un altro. Ad esempio, si potrà cambiare il *provider* di posta elettronica senza perdere i contatti e i messaggi salvati. È chiaro che ci sono, però, alcune eccezioni che non consentono l'esercizio del diritto: in particolare, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi[280].

---

[279] Cfr. Considerando 68 del Regolamento in disamina «Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto. Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche. Non dovrebbe pertanto applicarsi quando il trattamento dei dati personali è necessario per l'adempimento di un obbligo legale cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento».

[280] L'art. 20 in commento recita: «1. L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora: a) il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e b) il trattamento sia effettuato con mezzi automatizzati. 2. Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile. 3. L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento necessario per l'esecuzione di un compito di interesse pubblico o connesso

Il legislatore europeo ha, quindi, non solo recepito che i *software* utilizzati nel *cloud*, data la rilevanza che esso ha per il futuro dello sviluppo della società dell'informazione, devono poter essere capaci di scambiarsi i dati, leggendo e scrivendo sullo stesso *file* e usando lo stesso protocollo per farlo, ma anche che occorreva rafforzare ulteriormente il controllo da parte dell'interessato sui propri dati personali. Di talché ha attribuito allo stesso il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile, i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento. Peraltro, un ulteriore riferimento esplicito alla tecnologia *cloud* può rinvenirsi nella circostanza per la quale il diritto in parola è attribuito all'interessato qualora, tra le altre ipotesi, il trattamento si basi «su un contratto ai sensi dell'art. 6, paragrafo 1, lettera b)».

In altri termini, trattamento effettuato con mezzi automatizzati e basato su un contratto di cui l'interessato è parte, quali condizioni per l'operatività del diritto alla portabilità dei dati, possono considerarsi indici espliciti di riferibilità del diritto medesimo anche alla fattispecie del *cloud computing*, considerato che alla base dei servizi di *cloud* v'è pur sempre un contratto e che costituisce un «processo automatizzato» inserire dei dati nella «nuvola» (tramite, beninteso, l'utilizzo della rete *internet*), poiché ciò realizza un'operazione di caricamento delle stesse su un *server* unitamente alle operazioni necessarie per renderli poi accessibili a coloro che alla «nuvola» si collegano[281].

Ciò posto, anche se alcuni fornitori di servizi *cloud* non hanno ben compreso (o non vogliono comprendere) l'importanza dell'utilizzo di *standard* aperti, continuando a definire - indipendentemente l'uno dall'altro - formati ai quali attenersi e che l'utente adotta pedissequamente, con il nuovo Regolamento UE *privacy* (che, si ricorda, sarà direttamente applicabile in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018) questa riluttanza verso la previsione di protocolli di standardizzazione per i sevizi *cloud* sembra giunta al capolinea, cosí aprendosi una nuova era nella fase di progettazione dei programmi volta a garantirne la capacità di scambiarsi le informazioni e di usare reciprocamente le informazioni scambiate.

---

all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. 4. Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui.».

[281] Sulla specificazione della nozione di trattamento automatizzato vedi la sentenza sul caso *Lindqvist*, già analizzata al § 3, cap. II.

4. I ruoli dei diversi operatori nei sistemi *cloud*. Il fornitore: titolare o responsabile?

Come piú volte accennato, il *cloud computing* coinvolge una serie di diversi operatori ed è importante valutare e chiarire il ruolo di ciascuno di essi al fine di stabilire i rispettivi obblighi specifici per quanto concerne l'attuale legislazione in materia di protezione dei dati.

Va ricordato che, in tema di compiti e responsabilità di diversi attori[282], il Gruppo di lavoro «Articolo 29», nel suo parere 1/2010[283] sui concetti di «responsabile del trattamento» e «incaricato del trattamento», rileva che «il concetto di responsabile del trattamento serve a determinare in primissimo luogo chi risponde dell'osservanza delle norme relative alla protezione dei dati, e il modo in cui gli interessati possono esercitare in pratica i loro diritti - serve, in altre parole, ad attribuire responsabilità». Si evidenziano, dunque, due criteri generali di responsabilità: osservanza delle norme e attribuzione della responsabilità, da tener presente dalle parti interessate.

Il cliente *cloud* determina la finalità ultima del trattamento e decide in merito all'esternalizzazione di tale trattamento e alla delega ad un'organizzazione esterna delle attività di trattamento, in tutto o in parte. Il cliente *cloud* agisce pertanto in qualità di titolare del trattamento dei dati, alla luce della nuova normativa europea.

Il Regolamento UE 2016/679 sulla protezione dei dati definisce il «titolare del trattamento» come «la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali» (art. 4, n. 7). Il cliente *cloud*, in quanto titolare del trattamento, deve accettare la responsabilità dell'osservanza della legislazione sulla protezione dei dati ed è soggetto a tutti gli obblighi di cui al Regolamento *privacy*.

Quest'ultimo prevede, fra i suoi pilastri, il principio di *accountability* (che potrebbe essere tradotto in «responsabilizzazione e obbligo di rendicontazione»).

---

[282] Relativamente alla corretta attribuzione dei ruoli *privacy*, occorre rammentare la discrepanza terminologica utilizzata dalla Direttiva 95/46/CE e, di conseguenza, nei pareri del Gruppo di Lavoro Articolo 29 per la protezione dei dati personali, oltre che nelle indicazioni del Garante Europeo, rispetto alla normativa nazionale (d.lg. 196/03) e rispetto al Regolamento UE 2016/679 sulla protezione dei dati. Pertanto, il «responsabile» di cui alla dir. 95/46/CE è il «titolare» per il d.lg. 196/03 e per il Regolamento UE 2016/679, mentre l'«incaricato» è il «responsabile» per la medesima legislazione nazionale e per la «nuova» europea.

[283] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, Parere 1/2010, WP 169, adottato il 16 febbraio 2010.

Si tratta di un forte riconoscimento a livello normativo di un principio già riconosciuto dal Gruppo di lavoro «Articolo 29»[284], per il quale il titolare del trattamento dei dati deve essere in grado di dimostrare di avere adottato un processo complessivo di misure giuridiche, organizzative, tecniche, per la protezione dei dati personali, anche attraverso l'elaborazione di specifici modelli organizzativi: deve dimostrare in modo positivo e proattivo trattamenti di dati effettuati sono adeguati e conformi al regolamento europeo in materia di *privacy*.

Il regolamento prevede, già nel considerando n. 74, che è opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto: in particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare il proprio grado di conformità delle attività di trattamento con il regolamento, compresa l'efficacia delle misure.

Nell'art. 24 del Regolamento, rubricato «Responsabilità del titolare del trattamento» viene previsto che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento sia effettuato conformemente al presente regolamento, tenuto conto della natura, dell'àmbito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche. L'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento (art. 24, comma 3).

Il summenzionato principio di *accountability* è strettamente connesso con le misure di sicurezza e con l'analisi del rischio, con la valutazione di impatto *privacy* e con i princípi *privacy by design*, *privacy by default* che devono essere presenti nella progettazione di servizi e programmi[285].

---

[284] Per approfondimenti sul principio di *accountability*: Gruppo Art. 29, *Opinion 3/2010 on the principle of accountability*; *Linee guida Privacy OCSE del 2013*; 32 esima Conferenza mondiale dei Garanti europei a Gerusalemme del 2010 Secondo il sopra citato parere n. 3 del 2010 del Gruppo art. 29 i titolari del trattamento devono adottare misure in grado che le norme in materia di protezione dei dati siano rispettate nel contesto delle operazioni di trattamento e disporre di documentazione finalizzata a dimostrare agli interessati e alle autorità di controllo le misure adottate per garantire il rispetto delle norme di protezione dei dati.

[285] M. ALOVISIO, F. DI RESTA, *Norme* privacy *UE, ecco tutto ciò che bisogna sapere su* accountability *e sicurezza*, in www.agendadigitale.eu reperibile all'indirizzo http://www.agendadigitale.eu/infrastrutture/norme-privacy-ue-

Viene specificato che le sopra citate misure sono riesaminate e aggiornate qualora necessario (art. 24, comma 1, ultimo periodo)[286]. Le sopra citate misure includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento, se ciò è proporzionato rispetto alle attività di trattamento[287].

Il cliente *cloud* può incaricare il fornitore *cloud* della scelta dei metodi e delle misure tecniche e organizzative da utilizzare per conseguire gli scopi del titolare del trattamento.

Il fornitore *cloud* è l'entità che fornisce i servizi di *cloud computing* nelle varie forme precedentemente discusse. Quando fornisce gli strumenti e la piattaforma, agendo per conto del cliente *cloud*, il fornitore *cloud* è considerato alla stregua di un responsabile del trattamento, ossia, secondo il regolamento UE «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento»[288].

Come affermato nel parere 1/2010, per valutare la responsabilità del trattamento si possono utilizzare alcuni criteri[289]. In effetti, si possono presentare situazioni in cui un fornitore di servizi *cloud* può essere considerato contitolare o titolare a pieno titolo[290], a seconda delle circostanze concrete. Ad esempio, potrebbe trattarsi del caso in cui il fornitore procede al trattamento di dati per scopi propri.

---

ecco-tutto-cio-che-bisogna-sapere-suaccountability-e-sicurezza_2279.htm, per i quali l'«*accountability* costituisce una delle principali sfide per le pubbliche amministrazioni ed aziende: un notevole cambio culturale e di approccio, come è possibile dimostrare per le organizzazioni di essere compliance rispetto agli obblighi previsti dal regolamento europeo in materia di protezione dei dati personali? cosa devono fare le imprese e le pubbliche amministrazioni nelle more dell'entrata in vigore del regolamento? L'accountability costituisce una delle principali sfide per le pubbliche amministrazioni ed aziende: un notevole cambio culturale e di approccio, come è possibile dimostrare per le organizzazioni di essere compliance rispetto agli obblighi previsti dal regolamento europeo in materia di protezione dei dati personali? cosa devono fare le imprese e le pubbliche amministrazioni nelle more dell'entrata in vigore del regolamento?». In senso critico gli autori evidenziano che «l'attuale codice della *privacy* non prevede in modo diretto il principio di accountability, prevede un sistema di responsabilità civili, penali e amministrative e una serie di adempimenti formali (informativa, consenso, notificazione al Garante, misure minime e idonee) ma non un approccio di responsabilizzazione.».

286 M. ALOVISIO, F. DI RESTA, *Norme* privacy *UE*, *o.c.*, per i quali «si tratta di un principio del miglioramento continuo, di sicurezza come processo e non come prodotto che è emerso nelle best practice aziendali».

287 Condividono il riferimento alla proporzionalità rispetto alle attività di trattamento M. ALOVISIO, F. DI RESTA, *Norme* privacy *UE*, o.c., per i quali tale riferimento è «ottimo al fine di evitare sistemi ridondanti».

288 In questo senso, al di là della discrepanza terminologica - da cui l'utilizzo del termine di «incaricato del trattamento», secondo quella che è la terminologia propria della direttiva 95/46/CE - il GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, Parere 5/2012, WP 196, adottato il 1° luglio 2012.

289 Ad es. livello di istruzioni, controllo da parte del cliente *cloud*, competenza delle parti.

290 Cosí, sempre al di là della discrepanza terminologica di cui prima, il GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit.

Il Gruppo di lavoro Articolo 29 per la protezione dei dati personali ebbe a precisare che «[n]ell'attuale scenario del *cloud computing*, i clienti di servizi di *cloud computing* potrebbero non avere margine di manovra nel negoziare i termini contrattuali dell'uso dei servizi *cloud,* che in molti casi sono caratterizzati da offerte standardizzate. In ogni caso, alla fine è il cliente che decide in merito all'assegnazione di parte o della totalità del trattamento a servizi *cloud* per scopi specifici; il punto fondamentale in questo caso è che il ruolo del fornitore *cloud* sarà quello di un contraente nei confronti del cliente. Come affermato nel parere 1/201012 sui concetti di "responsabile del trattamento" e "incaricato del trattamento" del Gruppo di lavoro articolo 29 *"lo squilibrio fra il potere contrattuale di un piccolo responsabile del trattamento rispetto a un grosso fornitore di servizi non può giustificare il fatto che il primo accetti clausole e condizioni non conformi alla normativa sulla protezione dei dati"*. Per questo motivo, il responsabile del trattamento deve scegliere un fornitore *cloud* che garantisca l'osservanza della normativa in materia di protezione dei dati.».[291]

Anche se con una terminologia diversa, il Regolamento UE prevede un meccanismo analogo che recepisce quando espresso dal Garante europeo, stabilendo che il «titolare del trattamento» (quindi il «vecchio» responsabile per la direttiva 95/46/CE e, di conseguenza, per i Pareri del Garante europeo), allorquando un trattamento venga effettuato per suo conto, «ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato.» (art. 28, par. 1).

Pertanto il cliente (titolare del trattamento) potrà scegliersi solo (*rectius*, «unicamente») quel fornitore (responsabile del trattamento) che presenti quelle «garanzie sufficienti» testé indicate. È chiaro, allora, il monito del legislatore europeo, sulla scia degli interventi del Garante, agli utenti di servizi *cloud* che, nel decidere in merito all'assegnazione di parte o della totalità del trattamento a servizi *cloud* per scopi specifici, devono prestare un'attenzione particolare, che si traduce nell'obbligo di ricorrere unicamente a quei

[291] Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit., ove si specifica altresí che «Un'enfasi particolare va posta sulle caratteristiche dei contratti applicabili, che devono prevedere una serie di garanzie standard per la protezione dei dati, ivi comprese quelle descritte dal Gruppo di lavoro nelle sezioni 3.4.3 (Misure tecniche e organizzative) e 3.5 (Trasferimenti internazionali), nonché su meccanismi aggiuntivi che si possono dimostrare adeguati per agevolare la *due diligence* e la responsabilità (quali *audit* di terzi indipendenti e certificazioni dei servizi di un fornitore – cfr. sezione 4.2).».

fornitori in grado di garantire l'osservanza della normativa in materia di protezione dei dati.

Il cliente-titolare del trattamento potrà ricorrere ad un responsabile del trattamento che abbia aderito a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 potendo essere questo elemento utilizzato per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 dell'articolo in parola (par. 5).

Venendo poi agli obblighi propri del fornitore-responsabile, a costui non è consentito il ricorso ad altro responsabile (e, quindi, delegare i suoi compiti) senza previa autorizzazione scritta, specifica o generale, del titolare - *ex* par. 2, art. 28 - e alle condizioni di cui al paragrafo 4[292] del medesimo art. 28. I trattamenti operati dal responsabile sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri[293]- stipulato in forma scritta, anche in formato elettronico (par. 9) - che preveda, in particolare, che il responsabile: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento[294]; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza[295]; c) adotti tutte le misure richieste ai sensi dell'articolo 32 («sicurezza del trattamento»); d) rispetti le condizioni di cui ai paragrafi 2 e 4

---

[292] Il paragrafo 4, dell'art. 28, recita: «Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile.».

[293] Contratto o atto «che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento.» (art. 28, par. 3)

[294] Sul punto anche il GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit., ebbe a precisare che la «direttiva 95/46/CE stabilisce che: "*L'incaricato del trattamento o chiunque agisca sotto la sua autorità o sotto quella del responsabile del trattamento, non deve elaborare i dati personali ai quali ha accesso, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi legali*". Anche l'accesso ai dati da parte del fornitore *cloud* durante la prestazione del servizio è fondamentalmente disciplinato dall'obbligo di rispettare le disposizioni dell'articolo 17 della direttiva (cfr. sezione 3.4.2.).».

[295] Sul punto anche il GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit., ebbe a precisare che i «fornitori di servizi di *cloud computing* (in quanto incaricati del trattamento) hanno il dovere di garantire la riservatezza.

per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato.

Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui sopra può basarsi, in tutto o in parte, su clausole contrattuali tipo - anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43 - stabilite dalla Commissione - secondo la procedura d'esame di cui all'art. 93, paragrafo 2 - o da un'autorità di controllo - in conformità del meccanismo di coerenza di cui all'articolo 63 (paragrafi 6, 7 e 8, art. 28).

Vi è un preciso obbligo giuridico del titolare del trattamento di impartire istruzioni documentate al responsabile (art. 28, par. 3, lett. a), cui corrisponde un dovere di quest'ultimo (o di chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento) nel momento in cui abbia accesso ai dati personali, di trattarli secondo le istruzioni ricevute dal titolare del trattamento, tanto che non può trattare tali dati se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o degli Stati membri (art. 29).

Caso quest'ultimo decisamente inverosimile quando si parla di un grande *cloud provider*, da un lato, e di piccola e media impresa-*buyer*, dall'altro, mentre è verosimile asserire che, nella maggior parte dei casi, nemmeno *buyer* come una grande impresa o una P.A. riescano di fatto ad impartire istruzioni dettagliate al *cloud provider* e ad esercitare quel controllo tipico

del rapporto titolare-responsabile, ne deriva che la soluzione di fatto piú aderente alla normativa *privacy* odierna è quella di una titolarità autonoma in capo al *cloud provider*.[296]

A bene vedere, al di là degli apprezzabili sforzi interpretativi[297] volti a superare le facili e apodittiche soluzioni[298] atte ad attribuire al cliente il ruolo di titolare e al fornitore quello di responsabile, alla luce del nuovo Regolamento *privacy* si può dar per assodato che il fornitore che si spinga sino al punto di determinare ulteriori finalità del trattamento rispetto a quelle fissate dal cliente assuma la qualifica di titolare. Ciò è detto espressamente nel comma 10 dell'art. 28 in disamina, ove è sancito che «fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.».

Ciò che rileva, pertanto, è chi in concreto ha determinato le finalità e i mezzi del trattamento, cosí assumendo di diritto quella qualifica che corrisponde alla sua attività di fatto realizzata. Questo può considerarsi un chiaro intervento teso ad ampliare i casi in cui un fornitore di servizi di *cloud* può essere definito titolare del trattamento.

---

[296] Si evidenziano questi aspetti in S. LEUCCI, S. GIRELLA, J.L. LOUIS A BECCARA, *Pubblica amministrazione* cit., p. 26 s., ove gli autori si rifanno alle raccomandazioni di DIGITPA, *Raccomandazioni e proposte sull'utilizzo del* cloud computing *nella pubblica amministrazione*, in *www.agid.gov.it/sites/default/files/.../raccomandazioni_cloud_e_pa_-_2.0_0.pdf*.

[297] S. LEUCCI, S. GIRELLA, J.L. LOUIS A BECCARA, *o.c.*, p. 24 ss., per i quali limitarsi a sostenere che, per individuare correttamente nel fornitore il ruolo di responsabile, «è sufficiente che il cliente abbia stabilito "quali dati trattare", "per quanto tempo", nonché "quali terzi avranno accesso ai dati", potrebbe essere, se non fuorviante, quanto meno foriero di eccessive semplificazioni.». Pertanto, proseguono gli a. - richiamando il Parere del GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sui concetti di "responsabile del trattamento" e "incaricato del trattamento"*, cit. - «se il cliente non è realmente in grado di valutare il rispetto degli obblighi (contrattualmente previsti) di verifica periodica, di *reporting* e, più generalmente, di adeguatezza e conformità del servizio offerto dal fornitore, è davvero sufficiente aver predisposto analoghe clausole contrattuali per inquadrare quest'ultimo quale mero responsabile? O, piuttosto, secondo un sano criterio di prevalenza della sostanza sulla forma (principio "di effettività", … le clausole di un contratto non sono sempre decisive, poiché ciò consentirebbe alle parti di assegnare le responsabilità nel modo loro più conveniente? Ad ogni modo […] sarà gioco forza attribuire al cliente i più ampi poteri d'azione e, correlativamente, privare il fornitore di eccessivi spazi di determinazione. […] Qualora, invece, il fornitore ritenesse di non voler accettare simili restrizioni al proprio "libero arbitrio", coerenza vuole che il ruolo più adeguato allo stesso sarà quello di titolare (co-titolare, o autonomo titolare, si valuterà poi nello specifico), con ogni relativa assunzione di responsabilità.».

[298] Cosí come descritto in G. NOTO LA DIEGA, *o.c.*, p. 577.

5. Obblighi di protezione dei dati nella relazione cliente-fornitore.

La legittimità del trattamento di dati personali in servizi di *cloud computing* dipende dall'osservanza dei princípi fondamentali della legislazione UE in materia di protezione dei dati. Occorrerà, allora, anche in questo caso, risolvere le problematiche proprie del fenomeno in esame alla luce del nuovo Regolamento UE sulla *privacy*, applicabile anche alle fattispecie future che l'evoluzione tecnologica può presentare. In particolare, dev'essere garantita la trasparenza nei confronti degli interessati, dev'essere rispettato il principio della specificazione e limitazione delle finalità e i dati personali devono essere cancellati non appena la loro conservazione non è piú necessaria. Inoltre, devono essere attuate opportune misure tecniche e organizzative per garantire un livello adeguato di protezione e sicurezza dei dati.

La trasparenza[299] è fondamentale per il trattamento equo e legittimo dei dati personali. Il Regolamento UE, *ex* art. 12, obbliga il cliente *cloud* (o anche il fornitore se determina le finalità e i mezzi del trattamento[300]) a fornire all'interessato, presso il quale raccoglie dati che lo riguardano, le informazioni di cui agli artt. 13 e 14 e quindi, qualora i dati personali siano raccolti presso l'interessato: la sua identità, i suoi dati di contatto e quelli del responsabile della protezione dei dati (ove ricorre tale figura), le finalità del trattamento e la base giuridica dello stesso, i legittimi interessi perseguiti dal titolare del trattamento o da terzi [qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f)], gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali e ove applicabile, la sua intenzione di trasferire dati personali a un paese terzo o a un'organizzazione internazionale (inclusa: l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il

[299] Si ricorda che come principio di carattere generale il diritto alla trasparenza indica il diritto di ogni cittadino-consumatore a ricevere informazioni, comprensibili, chiare e trasparenti in ogni fase del suo rapporto con l'erogatore del servizio. La trasparenza dallo stesso d.lg. n. 33/2013 è stata intesa come accessibilità totale delle informazioni concernenti l'organizzazione e l'attività delle pubbliche amministrazioni, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche. Ovviamente tale accessibilità è da intendersi anche attraverso lo strumento della pubblicazione on line di dati ed informazioni su siti istituzionali, nonché il loro trattamento secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca *web* ed il loro riutilizzo (*open data*) nel rispetto dei principi sul trattamento dei dati personali.

[300] Ciò in base al disposto del comma 10, dell'art. 28, cfr. § 3. Pertanto, ogni qualvolta ci si riferisce al «cliente *cloud*» il riferimento è da intendersi anche al «fornitore *cloud*», là dove abbia, in concreto, determinato «le finalità e i mezzi del trattamento», comportandosi, dunque, quale titolare del trattamento medesimo.

riferimento alle garanzie appropriate o opportune e i mezzi per ottenere una copia di tali dati o il luogo dove sono stati resi disponibili).

Il cliente *cloud* sarà inoltre tenuto a fornire ulteriori informazioni, nella misura in cui esse siano necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato[301] (art. 13, comma 2[302]). È poi previsto che, nel caso in cui il titolare del trattamento intendesse trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento, debba fornire all'interessato informazioni in merito a tale diversa finalità e ogni ulteriore informazione pertinente di cui al paragrafo 2 dell'art. 13 (art. 13, comma 3).

Qualora i dati personali non siano stati ottenuti presso l'interessato, troverà applicazione l'art. 14[303] con il relativo obbligo in capo al cliente *cloud* di fornire all'interessato le informazioni ivi specificate.

---

[301] Già la direttiva 95/46/CE obbliga(va) il cliente *cloud* a fornire all'interessato, presso il quale raccoglie dati che lo riguardano, informazioni sulla sua identità e sulla finalità del trattamento. Il cliente *cloud* è inoltre tenuto a fornire ulteriori informazioni, ad esempio relative ai destinatari o alle categorie di destinatari dei dati, che possono anche comprendere incaricati e subincaricati del trattamento nella misura in cui tali ulteriori informazioni siano necessarie per garantire un trattamento leale nei confronti dell'interessato (cfr. articolo 10 della direttiva). Un obbligo corrispondente di informare l'interessato sussiste quando dati che non sono stati ottenuti dallo stesso interessato, bensì da fonti diverse, vengano registrati o divulgati a un terzo (cfr. articolo 11). Sul punto, vedi GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit.

[302] L'art. 13, comma 2, recita: «In aggiunta alle informazioni di cui al paragrafo 1, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti ulteriori informazioni necessarie per garantire un trattamento corretto e trasparente: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca; d) il diritto di proporre reclamo a un'autorità di controllo; e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati; f) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.».

[303] L'art. 14, rubricato «Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato», recita: «1. Qualora i dati non siano stati ottenuti presso l'interessato, il titolare del trattamento fornisce all'interessato le seguenti informazioni: a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante; b) i dati di contatto del responsabile della protezione dei dati, ove applicabile; c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento; d) le categorie di dati personali in questione; e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali; f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un destinatario in un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione o, nel caso dei trasferimenti di cui all'articolo 46 o 47, o all'articolo 49, secondo comma, il riferimento alle garanzie adeguate o opportune e i mezzi per ottenere una

Il cliente *cloud* deve fornire all'interessato anche le comunicazioni di cui agli articoli da 15 a 22 - ossia rendere edotto l'interessato dei suoi diritti di accesso, di rettifica, di cancellazione, di limitazione del trattamento, di portabilità, di opposizione, di cui ne agevola l'esercizio (art. 12, comma 2) - e quella di violazione dei dati personali *ex* articolo 34. Tali informazioni e comunicazioni sono fornite, di regola, in modo gratuito, salvo che siano manifestamente infondate o eccessive, in particolare perché ripetitive (art. 12, comma 5).

Il cliente *cloud* dovrà fornire all'interessato le informazioni e le comunicazioni relative al trattamento di cui prima «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.» (art. 12). Circa la forma, il Regolamento UE prevede che le stesse siano fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici e,

---

copia di tali dati o il luogo dove sono stati resi disponibili. 2. Oltre alle informazioni di cui al paragrafo 1, il titolare del trattamento fornisce all'interessato le seguenti informazioni necessarie per garantire un trattamento corretto e trasparente nei confronti dell'interessato: a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo; b) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f), i legittimi interessi perseguiti dal titolare del trattamento o da terzi; c) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento dei dati personali che lo riguardano e di opporsi al loro trattamento, oltre al diritto alla portabilità dei dati; d) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a), l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prima della revoca; e) il diritto di proporre reclamo a un'autorità di controllo; f) la fonte da cui hanno origine i dati personali e, se del caso, l'eventualità che i dati provengano da fonti accessibili al pubblico; g) l'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato. 3. Il titolare del trattamento fornisce le informazioni di cui ai paragrafi 1 e 2: a) entro un termine ragionevole dall'ottenimento dei dati personali, ma al più tardi entro un mese, in considerazione delle specifiche circostanze in cui i dati personali sono trattati; b) nel caso in cui i dati personali siano destinati alla comunicazione con l'interessato, al più tardi al momento della prima comunicazione all'interessato; oppure c) nel caso sia prevista la comunicazione ad altro destinatario, non oltre la prima comunicazione dei dati personali. 4. Qualora il titolare del trattamento intenda trattare ulteriormente i dati personali per una finalità diversa da quella per cui essi sono stati ottenuti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità e ogni informazione pertinente di cui al paragrafo 2. 5.I paragrafi da 1 a 4 non si applicano se e nella misura in cui: a) l'interessato dispone già delle informazioni; b) comunicare tali informazioni risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, fatte salve le condizioni e le garanzie di cui all'articolo 89, paragrafo 1, o nella misura in cui l'obbligo di cui al paragrafo 1 del presente articolo rischi di rendere impossibile o di pregiudicare gravemente il conseguimento delle finalità di tale trattamento. In tali casi, il titolare del trattamento adotta misure appropriate per tutelare i diritti, le libertà e i legittimi interessi dell'interessato, anche rendendo pubbliche le informazioni; c) l'ottenimento o la comunicazione sono espressamente previsti dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento e che prevede misure appropriate per tutelare gli interessi legittimi dell'interessato; oppure d) qualora i dati personali debbano rimanere riservati conformemente a un obbligo di segreto professionale disciplinato dal diritto dell'Unione o degli Stati membri, compreso un obbligo di segretezza previsto per legge.

ove richiesto dall'interessato, possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato (art. 12, ultimo periodo).

Il cliente *cloud* fornirà all'interessato le informazioni relative all'azione intrapresa riguardo a una richiesta ai sensi degli articoli da 15 a 22 senza ingiustificato ritardo e, comunque, entro un mese dal ricevimento della richiesta stessa (art. 12, comma 3[304]). Se non ottempera a codesta richiesta, il titolare del trattamento informa l'interessato senza ritardo (o comunque entro massimo un mese dal ricevimento della richiesta) dei motivi dell'inottemperanza e della possibilità di proporre reclamo a un'autorità di controllo e di proporre ricorso giurisdizionale.

La trasparenza dev'essere garantita anche nel rapporto tra cliente *cloud*, fornitore *cloud* e (eventuali) subcontraenti. Il cliente *cloud* è in grado di valutare la legittimità del trattamento di dati personali nei servizi *cloud* solo se il fornitore del servizio lo informa in merito a tutte le questioni pertinenti. Un titolare del trattamento che preveda di ingaggiare un fornitore *cloud* dovrebbe verificare attentamente i termini e le condizioni di tale fornitore e valutarli dal punto di vista della protezione dei dati.

Ai fini della trasparenza nel *cloud computing* occorre che il cliente *cloud* sia a conoscenza di tutti i subcontraenti che contribuiscono all'erogazione del servizio *cloud,* nonché dell'ubicazione di tutti i centri presso i quali può essere effettuato il trattamento dei dati personali[305]. Se l'erogazione di un servizio richiede l'installazione di *software* sui sistemi del cliente *cloud* (ad es. *browser plug-in*), il fornitore *cloud* è tenuto, a titolo di buona prassi, ad informare il cliente di questa circostanza e in particolare delle sue implicazioni dal punto di vista della protezione e della sicurezza dei dati. Viceversa, il cliente *cloud* dovrebbe sollevare la questione *ex ante*, se non è affrontata in misura sufficiente dal fornitore *cloud*[306].

Il principio della specificazione e limitazione della finalità[307] richiede che i dati personali siano raccolti per finalità determinate, esplicite e legittime e successivamente trattati

---

304 Il comma 3, dell'art. 12, in commento, prosegue prevedendo che: «Tale termine può essere prorogato di due mesi, se necessario, tenuto conto della complessità e del numero delle richieste. Il titolare del trattamento informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta. Se l'interessato presenta la richiesta mediante mezzi elettronici, le informazioni sono fornite, ove possibile, con mezzi elettronici, salvo diversa indicazione dell'interessato.».

305 Solo in tal caso sarà in grado di valutare se i dati personali possono essere trasferiti a un cosiddetto paese terzo al di fuori dello Spazio economico europeo (SEE) che non garantisce un adeguato livello di protezione ai sensi della normativa comunitaria.

306 Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit.

307 Già la direttiva 95/46/CE, all'articolo 6, paragrafo 1, lettera b) prevede(va) tale principio.

(sempre in maniera da garantirne un'adeguata sicurezza) in modo non incompatibile con tali finalità, nonché conservati limitatamente al conseguimento delle finalità per le quali sono trattati. Sul rispetto di tali princípi applicabili al trattamento dei dati personali (meglio specificati all'art. 5 del Reg. UE) è competente il titolare del trattamento, il quale dovrà essere in grado di comprovarne il detto rispetto (principio di «responsabilizzazione»).

Ne discende, allora, che il cliente *cloud* dovrà determinare la finalità del trattamento prima di procedere alla raccolta di dati personali dall'interessato, informandolo in proposito. Il cliente *cloud* non deve trattare dati personali per finalità diverse che non siano compatibili con quelle originali.

Inoltre, occorre garantire che i dati personali non siano (illegalmente) trattati per ulteriori finalità dal fornitore del servizio *cloud* o da uno dei suoi subcontraenti. Poiché un tipico scenario di servizi *cloud* può facilmente coinvolgere un maggior numero di subcontraenti, il rischio del trattamento di dati personali per ulteriori finalità incompatibili dev'essere considerato particolarmente alto. Per ridurre al minimo tale rischio, il contratto tra fornitore e cliente *cloud* dovrebbe prevedere misure tecniche e organizzative intese a mitigarlo e fornire garanzie in merito alla registrazione (*logging*) e all'*audit* di operazioni di trattamento di dati personali eseguite da dipendenti del fornitore *cloud* o subcontraenti. Il contratto dovrebbe prevedere sanzioni contro il fornitore o il subcontraente in caso di violazione della legislazione sulla protezione dei dati.

Già a norma dell'articolo 6, paragrafo 1, lettera e), della direttiva 95/46/CE, i dati personali devono essere conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. I dati personali che non sono piú necessari devono essere cancellati o resi anonimi. Ove non sia possibile cancellarli a causa di norme di legge sulla conservazione (ad es. normative fiscali), l'accesso a tali dati personali dev'essere bloccato.

In merito, anche il Garante europeo[308] ammoniva che spetta al cliente *cloud* garantire che i dati personali siano cancellati non appena non siano piú necessari nel senso sopra indicato. Il principio della cancellazione dei dati si applica ai dati personali a prescindere dal fatto che siano memorizzati su disco rigido o altri supporti per la conservazione dei dati (ad

[308] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit.

es. nastri per *backup*). Poiché i dati personali possono essere conservati in sovrabbondanza su diversi *server* in diversi luoghi, occorre garantire che in ciascun caso siano cancellati in modo irrecuperabile (vale a dire che devono essere cancellati anche versioni precedenti, *file* temporanei e persino frammenti di *file*).

I clienti *cloud* devono essere consapevoli del fatto che i dati di *log* che agevolano la verifica, la conservazione, la modifica o la cancellazione dei dati possono anch'essi essere qualificati come dati personali relativi all'interessato che ha avviato la relativa operazione di trattamento[309]. La cancellazione sicura dei dati personali impone che i supporti di memorizzazione vengano distrutti o smagnetizzati o che i dati personali conservati siano effettivamente cancellati mediante sovrascrittura. Per la sovrascrittura di dati personali si dovrebbero utilizzare speciali strumenti *software* che sovrascrivono piú volte i dati, conformemente a specifiche riconosciute. Il cliente *cloud* dovrebbe assicurarsi che il fornitore *cloud* garantisca la cancellazione sicura nel senso sopra citato e che il contratto tra il fornitore e il cliente contenga chiare disposizioni per la cancellazione dei dati personali. Lo stesso vale per i contratti tra fornitori *cloud* e subcontraenti.

Oggi, con il Regolamento UE, il diritto alla cancellazione ha assunto il rango «di diritto dell'interessato», consacrato nell'art. 17.

Il cliente *cloud* (titolare) ha, pertanto, l'obbligo di cancellare senza ingiustificato ritardo i dati personali dell'interessato, se sussiste (almeno) «uno» dei motivi espressamente indicati nel testo dell'articolo e segnatamente: i dati personali non sono piú necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato revoca il consenso [prestato *ex* articolo 6, paragrafo 1, lettera a), o in base all'articolo 9, paragrafo 2, lettera a)] e se non sussiste altro fondamento giuridico per il trattamento; l'interessato si oppone al trattamento ai sensi dell'articolo 21; i dati personali sono stati trattati illecitamente; 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; i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Basta la ricorrenza di *uno solo dei motivi* testé indicati per essere obbligati alla cancellazione dei dati personali, alla quale si deve provvedere senza ingiustificato ritardo.

---

[309] Questo significa che occorre definire i periodi ragionevoli di conservazione per *file* di *log* e stabilire le procedure per garantire la cancellazione puntuale o l'anonimizzazione di tali dati.

Il paragrafo 2[310] dovrebbe, invece, trovare applicazione ai casi di «contitolarità del trattamento», di cui all'art. 26.

Sembrerebbe questa la lettura piú in linea con il senso logico della disposizione, altrimenti letteralmente si dovrebbe dire che il titolare del trattamento sia tenuto ad adottare le misure ragionevoli, anche tecniche, per informare se stesso della richiesta di cancellazione dell'interessato. Allora, sembra corretto affermare che, nel caso in disamina, il titolare del trattamento informa gli «altri» titolari della richiesta di cancellazione.

Ovviamente, il «diritto all'oblio» non è senza limiti, è il legislatore europeo se ne avvede al paragrafo 3, stabilendo che i precedenti paragrafi non si applicano nella misura in cui il trattamento sia necessario: per l'esercizio del diritto alla libertà di espressione e di informazione; b) per l'adempimento di un obbligo legale che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento; c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3; d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento; o e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

Pertanto, le limitazioni all'operatività del diritto all'oblio, prima rimesse all'elaborazione pretoria, sono state adesso tipizzate dal legislatore europeo.

Infatti, che il diritto in parola necessitasse di un giudizio di bilanciamento era stato già chiarito sia dalla giurisprudenza nostrana che da quella di Lussemburgo.

Quest'ultima nel famoso caso *Costeja*[311], nell'affermare che i diritti fondamentali dell'interessato (di cui agli articoli 7 e 8 della Carta) prevalgono anche sull'interesse del pubblico a trovare le informazioni in occasione di una ricerca concernente il nome dell'interessato stesso, ebbe tuttavia a precisare che «così non sarebbe qualora risultasse, per

[310] Il paragrafo 2, dell'articolo in esame, recita: «Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, 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.»

[311] Per una completa disamina della questione, si rinvia al Cap. II, § 3.1.

ragioni particolari, come il ruolo ricoperto da tale persona nella vita pubblica, che l'ingerenza nei suoi diritti fondamentali è giustificata dall'interesse preponderante del pubblico suddetto ad avere accesso, mediante l'inclusione summenzionata, all'informazione di cui trattasi.».

Devono quindi sussistere ragioni particolari giustificanti un interesse preponderante del pubblico ad avere accesso alle informazioni, in mancanza la persona interessata può esigere[312] la soppressione di qualsiasi *link*, copia o riproduzione dei suoi dati personali.

Il riferimento al ruolo ricoperto da una persona nella vita pubblica, quale ragione particolare giustificante un interesse preponderante del pubblico ad avere accesso alle informazioni, è utilizzato anche dal Tribunale di Roma per escludere la sussistenza dell'asserito diritto all'oblio del ricorrente, considerato quindi recessivo rispetto all'interesse pubblico a rinvenire sul *web*, attraverso il motore di ricerca gestito dalla resistente, notizie circa lo stesso[313].

Con riferimento alla libertà di espressione e di informazione, Cassazione penale n. 45051/2009[314] ebbe modo di affermare che «il servizio giornalistico televisivo, realizzato dopo diversi anni dall'accaduto, su un grave e clamoroso fatto di cronaca nera giudiziaria per porlo alla riflessione del pubblico, costituisce legittimo esercizio della libertà di manifestazione del pensiero e del diritto di cronaca, sempre nell'osservanza dei limiti di verità e continenza, se si fonda su un persistente o rivitalizzato interesse pubblico che va, peraltro, contemperato con il diritto all'oblio nel senso di legittima aspettativa della persona coinvolta ad essere dimenticata dall'opinione pubblica e rimossa dalla memoria collettiva.». Sulla stessa lunghezza d'onda il Garante protezione dati personali che, con propria

---

[312] La Corte di Giustizia richiama gli articoli 12, lettera b) e 14, primo comma, lettera a), della direttiva 95/46/CE. Con l'applicazione del Regolamento UE sulla *privacy* si dovrà richiamare il suo art. 17.

[313] Trib. Roma, cit. «[…] risulta che l'odierno ricorrente è avvocato in Svizzera, libero professionista, circostanza che consente di ritenere che questo eserciti un "ruolo pubblico" proprio per effetto della professione svolta e dell'albo professionale cui è iscritto, laddove tale ruolo pubblico non è attribuibile al solo politico (cfr. linee guida del 26.11.20014) ma anche agli alti funzionari pubblici ed agli uomini d'affari (oltre che agli iscritti in albi professionali). In conclusione, nell'ottica del sopra menzionato bilanciamento, l'interesse pubblico a rinvenire sul web attraverso il motore di ricerca gestito dalla resistente notizie circa il ricorrente deve prevalere sul diritto all'oblio dal medesimo vantato.».

[314] Cass. pen., 17 luglio 2009, n. 45051, in *Riv. pen.*, 2010, 273, con nota di PALERMO. Sul diritto all'oblio e sui suoi primi riconoscimenti in giurisprudenza v. Cass., 09 aprile 1998, n. 3679, in *Foro it.*, 1998, I, 1834, con nota di LAGHEZZA, per tale intendendosi «il legittimo interesse di ogni persona a non restare indeterminatamente esposta ai danni ulteriori che arreca al suo onore ed alla sua reputazione la reiterata pubblicazione di una notizia, in passato legittimamente divulgata».

decisione del 6 maggio 2009[315], chiarì che la diffusione dei dati personali, nell'àmbito dell'attività giornalistica, sebbene possa avvenire anche senza il consenso degli interessati, esige tuttavia, non solo il rispetto dei limiti del diritto di cronaca, ed in particolare quello della essenzialità dell'informazione riguardo a fatti di interesse pubblico, ma anche nel rispetto di alcuni princípi generali applicabili a qualunque tipo di trattamento, tra i quali il dovere di trattare i dati personali in modo corretto, verificando anzitutto la loro esattezza.

Ecco emergere un sistema di limiti al diritto all'oblio e contro limiti agli altri interessi costituzionalmente protetti che con esso devono bilanciarsi, allorché si specifica che libertà di manifestazione del pensiero e del diritto di cronaca se, da un lato è costituzionalmente garantita, dall'altro deve esercitarsi sempre nell'osservanza dei limiti di verità e continenza e fondarsi su un persistente o rivitalizzato interesse pubblico.

Di recente anche il Tribunale di Napoli Nord (Aversa)[316], nel premettere che «il diritto all'oblio è la naturale conseguenza di una corretta e logica applicazione dei principi generali del diritto di cronaca», ha affermato che «come non va diffuso il fatto la cui diffusione (lesiva) non risponda ad un reale interesse pubblico, così non va riproposta la vecchia notizia (lesiva) quando ciò non sia più rispondente ad una attuale esigenza informativa».

Anche il fattore tempo gioca un ruolo decisivo nella fattispecie in disamina, occorre infatti rammentare che, come risultante dalla sentenza n. 5525/2012[317] della Suprema Corte di Cassazione, il trascorrere del tempo, ai fini della configurazione del diritto all'oblio - configurato, dalla sentenza stessa, quale diritto «a che non vengano ulteriormente divulgate notizie che per il trascorrere del tempo risultino oramai dimenticate o ignote alla generalità dei consociati» - si configura quale elemento costitutivo.

Il giudice, pertanto, sarà chiamato a considerare il tempo trascorso e, qualora, tale presupposto, nel caso concreto, risulti essere assolutamente insussistente, risalendo i fatti ad un periodo non lontano ed essendo, quindi, gli stessi ancora attuali, dovrà giocoforza rigettare la richiesta di deindicizzazione di *links* risultanti da una ricerca a nome del richiedente.

---

315 Garante protezione dati personali, 6 maggio 2009, in *Resp. civ.*, 2009, 2349, con nota di PERON (nella specie, si ritenne la concretizzazione di illecito trattamento di dati personali la diffusione su alcuni quotidiani, a corredo della notizia di un incidente stradale mortale, della fotografia di un omonimo della vittima, tratta da un *social network* senza verificare la corrispondenza di identità tra la persona ritratta e quella coinvolta nel fatto di cronaca).

316 Trib. Napoli Nord (Aversa), 10 agosto 2016, in *Rep. Foro it.*, 2016, *Merito extra*, n. 2016.1952.37.

317 Cass., 05 aprile 2012, n. 5525, in *Foro it.*, 2013, I, c. 305, con nota di TUCCI.

6. Responsabilità in àmbito *cloud*.

Nelle tecnologie informatiche, si può definire la responsabilità come la capacità di stabilire che cosa ha fatto un'entità in un determinato momento nel passato e come lo ha fatto. Nel campo della protezione dei dati spesso assume un significato più ampio e descrive la capacità delle parti di dimostrare di aver preso misure adeguate per garantire l'attuazione dei principi di tutela dei dati.

La responsabilità nelle tecnologie informatiche assume una particolare importanza per indagare su violazioni dei dati personali, dove clienti *cloud*, fornitori e subcontraenti possono avere ciascuno un certo grado di responsabilità operativa. La capacità della piattaforma *cloud* di fornire meccanismi di monitoraggio e *logging* affidabili e completi riveste un'importanza fondamentale a questo proposito.

Inoltre, i fornitori di servizi *cloud* dovrebbero fornire prove documentali di misure opportune ed efficaci per la realizzazione dei principi di protezione dei dati delineati nelle sezioni precedenti. Esempi di simili misure sono le procedure per garantire l'identificazione di tutte le operazioni di trattamento dei dati e per rispondere a richieste di accesso, la distribuzione di risorse tra cui la designazione di funzionari addetti alla protezione dei dati e responsabili dell'osservanza dei principi di protezione dei dati, ovvero procedure di certificazione indipendenti. Inoltre, i responsabili del trattamento dovrebbero garantire di essere pronti a dimostrare l'istituzione delle misure necessarie, su richiesta delle autorità di vigilanza competenti[318].

Il Gruppo di lavoro Articolo 29 formula osservazioni dettagliate sull'argomento della responsabilità nel parere 3/2010[319], ove evidenzia che nel suo documento sul futuro della *privacy* (WP168) del dicembre 2009[320], esso stesso ha ritenuto che l'attuale quadro giuridico non sia riuscito appieno a garantire che gli obblighi in materia di protezione dei dati si traducano in meccanismi efficaci atti a fornire una protezione reale. Per migliorare la situazione, il Gruppo di lavoro proponeva, pertanto, che la Commissione esaminasse l'opportunità di introdurre meccanismi basati sulla responsabilità, con un particolare accento sulla possibilità di includere un principio di «responsabilità» nella versione riveduta

---

[318] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul cloud computing*, cit.

[319] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul principio di responsabilità*, Parere 3/2010, WP 173, adottato il 13 luglio 2010. Il documento si occupa fondamentalmente delle misure che dovrebbero essere adottate o previste per garantire la conformità nel settore della protezione dei dati.

[320] Documento sul futuro della *privacy* (WP168) del dicembre 2009.

della direttiva sulla protezione dei dati. Tale principio, secondo il Gruppo di lavoro, rafforzerebbe il ruolo del responsabile del trattamento (beninteso, oggi titolare del trattamento) e ne aumenterebbe la responsabilità.

«Un principio di responsabilità vincolante imporrebbe esplicitamente ai responsabili del trattamento di attuare misure appropriate ed efficaci per dare applicazione ai principi e agli obblighi della direttiva, e per dimostrarne su richiesta l'osservanza. In pratica, ciò dovrebbe concretarsi in programmi improntati all'adattabilità mirati ad attuare i principi esistenti di protezione dei dati (talvolta denominati "programmi di conformità"). Quale complemento a tale principio, potrebbero essere istituiti obblighi aggiuntivi diretti ad attuare garanzie di protezione dei dati o ad assicurarne l'efficacia. Potrebbe trattarsi, per esempio, di una disposizione che obbliga a effettuare una valutazione d'impatto sulla privacy per le operazioni di trattamento di dati a più alto rischio.»[321].

Il Regolamento UE 2016/679 sembra aver recepito i suggerimenti del Gruppo di lavoro, prevedendo, al paragrafo 2 dell'art. 5, in capo al titolare del trattamento il principio di «responsabilizzazione», sicché questi sarà tenuto, poiché soggetto competente, al rispetto dei princípi applicabili al trattamento dei dati personali e dovrà essere in grado di comprovarne l'osservanza.

Il principio di responsabilità trova poi la sua consacrazione nell'art. 24, ove si prevede che il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al regolamento (c.d. principio di «*accountability*»[322]).

---

321 GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul principio di responsabilità*, cit.

322 Il GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul principio di responsabilità*, cit., al fine di evitare probabili incomprensioni sul significato del termine inglese «*accountability*» (responsabilità) - a differenza di quanto accade nel mondo anglosassone (dal quale il termine stesso proviene), dove il suo significato è ampiamente compreso e condiviso - e consapevole che «risulta complesso definire che cosa esattamente significhi "accountability" in pratica», chiarisce che «responsabilità e obbligo di rendere conto sono due facce della stessa medaglia ed entrambe sono elementi essenziali di una buona governance. Solo quando si dimostra che la responsabilità funziona effettivamente nella pratica può instaurarsi una fiducia sufficiente.». Il Garante europeo, quindi, si premura di precisare che «il documento si occupa quindi delle misure che dovrebbero essere adottate o previste per garantire la conformità nel settore della protezione dei dati. I riferimenti alla responsabilità devono pertanto essere intesi nel senso utilizzato nel presente parere, fatta salva la possibilità di trovare un'altra formulazione che meglio rispecchi il concetto qui esposto. È per questo che il documento non è incentrato sui termini, ma si concentra pragmaticamente sulle misure da adottare, piuttosto che sul concetto in sé.». Il Gruppo di lavoro articolo 29 formulava una disposizione sostanziale che, a suo avviso, avrebbe potuto essere introdotta in un quadro legislativo globale, il cui testo è il seguente: «"*Articolo X - Applicazione dei principi di protezione dei dati 1. Il responsabile del trattamento attua misure*

Questa nuova disposizione sembra in linea con le disposizioni specifiche già esistenti nel quadro legislativo attuale. Si può citare in particolare l'articolo 6 della direttiva 95/46/CE, che al paragrafo 1 fa riferimento ai principi relativi alla qualità dei dati e al paragrafo 2 stabilisce che «[i]l responsabile del trattamento - (*rectius*, il titolare per il Reg. UE) - è tenuto a garantire il rispetto delle disposizioni del paragrafo 1». La nuova disposizione sembrerebbe conforme anche all'articolo 17, paragrafo 1, in cui si stabilisce che il responsabile del trattamento (*rectius*, il titolare per il Reg. UE) deve attuare misure tecniche ed organizzative. In effetti, una norma generale sulla responsabilità rafforza la necessità che i titolari del trattamento applichino le norme sulla sicurezza di cui all'articolo 17, in aggiunta a quanto previsto nelle rimanenti disposizioni.

Mettere in atto «misure tecniche e organizzative adeguate» per garantire il trattamento conforme al regolamento *privacy* e obbligo di rendere conto sono due facce della stessa medaglia. Il primo elemento dell'obbligo imporrebbe ai titolari del trattamento di attuare misure appropriate. Questi tipi di misure non sono specificati nel testo della norma generale sulla responsabilità. Tuttavia, interventi da parte dalle autorità nazionali di protezione dei dati, del Gruppo di lavoro articolo 29 o dalla Commissione potrebbero indicare, in determinati casi, un insieme minimo di misure specifiche costituenti misure appropriate[323].

Nel caso di trattamenti di dati di maggiori dimensioni, piú complessi o ad alto rischio, l'efficacia delle misure adottate dovrebbe essere verificata periodicamente. In merito, il Regolamento UE è ancora piú incisivo, prevedendo il riesame e l'aggiornamento, delle misure in questione, ogniqualvolta ciò sia necessario. Esistono diversi modi per valutare l'efficacia (o inefficacia) delle misure: monitoraggio, *audit* interni ed esterni, ecc. Per quanto riguarda i trasferimenti di dati personali al di fuori dell'Unione europea, i titolari o i responsabili del trattamento dovrebbero adottare ed attuare misure appropriate per ottemperare all'obbligo della presentazione di «garanzie adeguate» di cui all'articolo 46 del Regolamento UE, quali, ad esempio, le «norme vincolanti d'impresa» e sempre che risulti che «gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi».

---

appropriate ed efficaci per garantire che i principi e gli obblighi stabiliti nella direttiva siano rispettati. 2 Su richiesta dell'autorità di vigilanza, il responsabile del trattamento dimostra la conformità con il paragrafo 1.»

323 Un esempio di tali misure sarebbe l'adozione in alcuni casi di politiche e processi interni necessari per l'attuazione dei principi di protezione dei dati, che rispecchino le leggi e i regolamenti vigenti, V. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, *Sul principio di responsabilità*, cit.

A ben vedere, una disposizione sulla responsabilità non rappresenta una grande novità e per la maggior parte non impone obblighi che non fossero già impliciti nella normativa vigente. In sintesi, la nuova disposizione non mira ad assoggettare i titolari del trattamento a nuovi princípi, ma piuttosto a garantire di fatto l'effettiva osservanza di quelli esistenti[324].

A questo punto, occorre indagare sulle conseguenze connesse al rispetto (o al mancato rispetto) del principio di responsabilità. Il Gruppo di lavoro articolo 29 evidenzia che osservare il principio di responsabilità non significa necessariamente agire in conformità ai princípi sostanziali enunciati nella normativa sulla *privacy*, cioè esso non fornisce una presunzione legale di conformità, né sostituisce tali princípi. Il titolare del trattamento, e se del caso il responsabile dello stesso, possono avere attuato e verificato le misure che hanno posto in essere e tuttavia trovarsi coinvolti in irregolarità. Di conseguenza, l'adozione di misure volte al rispetto dei princípi non deve in nessun caso esonerare titolare e responsabile del trattamento dalle azioni di verifica dell'applicazione delle autorità di protezione dei dati. In pratica, titolari e responsabili del trattamento del settore pubblico e privato che abbiano adottato misure nell'àmbito di robusti programmi di conformità hanno maggiori probabilità di essere in regola con la legge. In effetti, poiché hanno predisposto misure efficaci dirette al rispetto dei princípi sostanziali di protezione dei dati, dovrebbe essere meno probabile per loro incorrere in violazioni. Pertanto, nel valutare sanzioni relative a violazioni della *privacy*, le autorità di protezione dei dati potrebbero considerare rilevanti l'attuazione (o la mancata attuazione) delle misure e la loro verifica.

In linea con quanto testé detto è la previsione di cui all'ultimo paragrafo dell'art. 24, ove si dice che «l'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 può essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento.».

Il Regolamento UE prevede anche l'obbligo, sempre in capo al titolare del trattamento, di effettuare una valutazione d'impatto sulla *privacy* (art. 35) e, qualora questa indichi che il

[324] Uno sviluppo legislativo in qualche modo simile è avvenuto nel 2009 in occasione della modifica della direttiva 2002/585, che ha imposto l'obbligo di attuare una politica di sicurezza, in particolare di "*garanti[re] l'attuazione di una politica di sicurezza in ordine al trattamento dei dati personali*". Così, per quanto riguarda le disposizioni di sicurezza di tale direttiva, il legislatore ha deciso che era necessario introdurre l'obbligo esplicito di predisporre e attuare una politica di sicurezza. Inoltre, l'articolo 18 della direttiva 95/46, che fa riferimento alla designazione di incaricati della protezione dei dati, accanto al sistema di regole d'impresa vincolanti di cui sopra, offrono già esempi di misure pratiche che possono essere adottate dai responsabili del trattamento.

trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio, l'obbligo, per il medesimo titolare, di consultare l'autorità di controllo (art. 36).

Il richiamato art. 35 del Regolamento parla di valutazione d'impatto sulla protezione dei dati che deve essere effettuata dal responsabile del trattamento - il quale si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno (par. 2) - quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, il campo di applicazione, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche.

La valutazione d'impatto sulla protezione dei dati è richiesta in particolare nei seguenti casi: una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche; b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati. La stessa Autorità comunica tali elenchi al Comitato europeo per la protezione dei dati. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (anche tali elenchi sono comunicati dall'Autorità al Comitato europeo per la protezione dei dati). Prima di adottare tali elenchi l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 del Regolamento (che richiede una cooperazione delle

Autorità di controllo e, se del caso, con la Commissione, per un'applicazione coerente del Regolamento) se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili si tiene debito conto, anche, del rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

L'art. 36 del Regolamento prevede la c.d. «consultazione preventiva» quando il titolare del trattamento, prima di procedere al trattamento dei dati personali, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio. Se l'Autorità di controllo ritiene che il trattamento previsto non sia conforme al Regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, entro un periodo massimo di otto settimane dalla richiesta di consultazione, fornisce una parere per iscritto al titolare del trattamento dei dati, e ove applicabile al responsabile del trattamento. Questo periodo può essere prorogato di ulteriori sei settimane, tenendo conto della complessità del trattamento previsto. Qualora si applichi la proroga, l'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. Tali periodi possono essere sospesi fino all'ottenimento da parte dell'autorità di controllo delle informazioni eventualmente richieste ai fini della consultazione. Tale consultazione presenta caratteri comuni con quella che noi conosciamo come verifica preliminare disciplinata dall'art. 17[325] del Codice in materia di protezione dei dati personali, anche se è prevista in un contesto senz'altro diverso.

[325] L'art. 17, rubricato «Trattamento che presenta rischi specifici», recita: «1. Il trattamento dei dati diversi da quelli sensibili e giudiziari che presenta rischi specifici per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato, in relazione alla natura dei dati o alle modalità del trattamento o agli effetti che può

7. Il primo codice di condotta per garantire la protezione dei dati personali dei clienti di *provider* di infrastrutture *cloud*.

Il CISPE (*Cloud Infrastructure Services Providers in Europe*) ha presentato, nel mese di settembre 2016, il primo codice di condotta per garantire la protezione dei dati personali dei clienti di *provider* di infrastrutture *cloud*. Il CISPE ha voluto regolamentare per la prima volta l'intero settore dei servizi *cloud* per i clienti e i loro utenti, in vista dell'entrata in vigore del nuovo Regolamento UE 2016/679 per la protezione dei dati personali, basandosi su *standard* di sicurezza riconosciuti a livello internazionale.

Il codice in commento, partendo dal (necessario) presupposto secondo cui v'è una vasta gamma di fornitori di servizi *cloud* che fornisce una varietà di differenti modelli di *cloud computing*, evidenzia subito che la disciplina in tema di protezione dei dati non si applica a tutti i modelli di *cloud* nello stesso modo, ma dipenderà necessariamente dal tipo di servizi di *cloud computing* che viene offerto e dalla categoria dei dati che vengono trattati. Tali fornitori di diversi tipi di servizi di *cloud computing* hanno necessariamente ruoli e responsabilità diverse, in particolare in relazione alla protezione e alla sicurezza dei dati.

Pertanto, si chiarisce immediatamente che «[*t*]*his Code of Conduct (Code) focusses on IaaS providers. IaaS providers are referred to in this Code as Cloud Infrastructure Services Providers (CISPs).* Lo scopo che il codice persegue «*is to guide customers in assessing whether cloud infrastructure services are suitable for the processing of personal data that the customer wishes to perform. The very*

---

determinare, è ammesso nel rispetto di misure ed accorgimenti a garanzia dell'interessato, ove prescritti. 2. Le misure e gli accorgimenti di cui al comma 1 sono prescritti dal Garante in applicazione dei principi sanciti dal presente codice, nell'ambito di una verifica preliminare all'inizio del trattamento, effettuata anche in relazione a determinate categorie di titolari o di trattamenti, anche a seguito di un interpello del titolare.». Con tale disposizione si prevedono accorgimenti nel caso in cui il trattamento dei dati diversi da quelli sensibili e giudiziari, c.d. «dati quasi-sensibili» implichi o determini specifici rischi per i diritti e le libertà fondamentali, nonché per la dignità dell'interessato. Come sottolineato da G. ALPA, *La disciplina dei dati personali*, in *Atti del Convegno ITA*, Roma, 1998, c'è da chiedersi se i diritti e le libertà fondamentali siano soltanto quelli risultanti dalla Costituzione ovvero si faccia riferimento anche ai trattati e alle Convenzioni (ad esempio la Convenzione europea sui diritti dell'uomo e i princípi generali del diritto comunitario). Il quesito, nel contesto di un'interpretazione sistematica e assiologica, deve trovare risposta affermativa nel senso che i diritti e le libertà fondamentali derivanti da tali fonti, contribuiscono alla formazione e al completamento di un quadro di princípi di rango costituzionale. L'art. 17 rappresenta un tentativo di adeguamento all'art. 20 della direttiva 95/46/CEE, poiché essa prevedrebbe che gli Stati, dapprima individuino i casi in cui adottare tali specifiche garanzie, eventualmente anche in sede di esame preliminare di una nuova normativa (e si suppone quindi lo facciano per legge) e, in seguito, che l'Autorità di controllo (ovvero il Garante) ne sorvegli l'attuazione, secondo le misure indicate, prima che il trattamento venga posto in essere. Per approfondimenti sul punto, si veda AAVV., *Codice in materia di protezione dei dati personali*, *Commento articolo per articolo al testo unico sulla* privacy *d.lgs. 30 giugno 2003, n. 196*, G. CASSANO e S. FADDA (a cura di), 2004, p. 134 e ss.

different nature of cloud infrastructure services compared to other types of cloud computing services – means that a specific Code tailored for IaaS is required.»[326].

Il codice è costituito da una serie di requisiti per i *processors* di dati CISPs con una particolare attenzione per la sicurezza. Questi sono riportati nella sezione 5 (Requisiti protezione dei dati) e la Sezione 6 (requisiti di trasparenza). Questi requisiti sono indicati collettivamente nel Codice come i requisiti del codice.

Qualsiasi CISP può dichiarare la sua adesione ai requisiti del codice per qualsiasi servizio *cloud* di infrastrutture se: a) il servizio è conforme ai requisiti del codice; b) nei confronti di tale servizio, il CISP si conforma a tutte le leggi sulla protezione dei dati dell'UE applicabili e vincolanti su di esso, tra cui la direttiva sulla protezione dei dati (e le eventuali trasposizioni nazionali di esse applicabili) e al regolamento generale sulla protezione dei dati (GDPR) quando sarà applicabile; c) il servizio offre al cliente la possibilità di scegliere di utilizzare il servizio per memorizzare ed elaborare i dati interamente all'interno del SEE.

Qualsiasi CISP dichiarando la sua adesione al Codice deve essere in grado di soddisfare tutti i requisiti del codice. Per quanto riguarda i dati trattati per conto di un cliente che utilizza il servizio di infrastruttura *cloud*, il CISP: a) non ha l'accesso (o non può utilizzare) a tali dati ad eccezione di quanto necessario per fornire i servizi al cliente; b) non può trattare tali dati per propri scopi, tra cui, in particolare, ai fini di *data mining*, profilazione o di *marketing* diretto. Il CISP può agire come un responsabile del trattamento nei confronti di alcuni dati personali forniti dal cliente al CISP. Questo include, per esempio, informazioni sul conto (come ad esempio nomi utente, indirizzi email e dati di fatturazione), che il cliente fornisce al CISP in connessione con la creazione o gestione del conto del cliente utilizzato per accedere al servizio del CISP. Il presente Codice non si applica quando il CISP elabora tali dati come un responsabile del trattamento.

La sezione 5 - sulla premessa che la normativa UE sulla protezione dei dati fa una distinzione tra il «titolare» (*controller*), ossia chi determina le finalità e gli strumenti del trattamento di dati personali e il «responsabile» (*processor*), ossia chi elabora dati personali per conto del *controller* - evidenzia come il codice intervenga per definire il ruolo del cliente, come *controller* o come *processor*, prevedendo che i servizi di infrastruttura *cloud* vengono

[326] Lo scopo del Codice è quello di guidare i clienti a valutare se i servizi di infrastruttura di *cloud* sono adatti per il trattamento dei dati personali che il cliente desidera eseguire. La diversa natura dei servizi infrastruttura *cloud* rispetto ad altri tipi di servizi di *cloud computing* significa che è richiesto un codice specifico su misura per i servizi offerti in modalità IaaS.

utilizzati come parte di una varietà di diverse operazioni di *business* e ci possono essere molteplici parti coinvolte in una catena di approvvigionamento. Pertanto, come guida generale, si chiarisce che:

• il cliente sarà il *controller* (titolare) in relazione ai dati personali se è egli stesso a determinare le finalità per le quali i dati saranno elaborati e ha scelto come saranno elaborati;

• il cliente sarà, invece, un mero *processor* (responsabile) in relazione ai dati personali se si limiterà ad una attività di mero trattamento (*merely processing*) dei dati personali sul servizio del CISP per conto e secondo i desideri di una terza parte (che può essere il titolare o altri terzi in una catena di fornitura).

Qualora il cliente scelga di archiviare o comunque trattare i dati personali utilizzando i servizi di un CISP, questo sarà il responsabile.

Lo scopo della sezione 5 in commento è quello di chiarire il ruolo del CISP come responsabile del trattamento in base al diritto sulla protezione dei dati dell'UE nel contesto dei servizi di infrastruttura *cloud*. Il Codice persegue questo obiettivo attraverso: a) l'individuazione dei requisiti dei responsabili (*processors*) del trattamento dei dati in base alla normativa europea sulla protezione (DP *requirement*); e b) applicando il requisito DP nel contesto servizi di infrastruttura di *cloud*, assegnando la responsabilità per questi requisiti tra il CISP e il cliente e definire i requisiti specifici per il CISP ai sensi del Codice (*requirement for* CISP)[327].

Il titolare deve assicurare che i dati personali vengono trattati in modo lecito. Il trattamento è lecito solo se si applicano determinate condizioni. Salvi i casi in cui sia richiesto di rispettare altre disposizioni di diritto, il responsabile può trattare dati personali solo su istruzioni documentate del titolare [Art 28, par. 3, lett. a), GDPR].

Il CISP tratterà i dati personali in conformità alle istruzioni del cliente. Il contratto di servizio e l'utilizzo da parte del cliente delle caratteristiche e funzionalità messe a

[327] Oltre al Codice, CISPs e i clienti sono incoraggiati a prendere in considerazione tutti i requisiti di legge sulla protezione dei dati dell'UE rispettivamente nella loro fornitura e nell'uso dei servizi di infrastruttura di cloud, rispettivamente. Un obiettivo chiave del codice è che affronterà i requisiti fondamentali per CISPs di diritto allora vigente sulla protezione dei dati dell'UE. In particolare, questo include la GDPR quando si sarà in vigore e requisiti del codice sono definiti con riferimento al GDPR. Il Codice sarà rivisto e aggiornato, se necessario, in considerazione cambiamenti nella legge sulla protezione dei dati dell'UE, in conformità con la Sezione 7 (Governance) (comprese tutte le specifiche vincolanti che possa essere fornite dalle autorità di controllo competenti in materia di GDPR).

disposizione dal CISP come parte del servizio è dato dalle istruzioni complete e finali del cliente al CISP in relazione al trattamento dei dati personali.

I CISPs non hanno alcun controllo sui contenuti che il cliente sceglie di caricare sul servizio (tra cui se essi includano, o meno, dati personali). I CISPs non hanno alcun ruolo nel decidere se il cliente utilizza il servizio di infrastruttura *cloud* per il trattamento dei dati personali, a quale scopo e sul se o sul come essi vengano protetti. Pertanto, i CISPs non sono in grado di verificare se ci può essere una base legale per il trattamento. Come tale, la loro responsabilità è limitata: a) alla conformità con le istruzioni del cliente, come previsto o riflessa nel contratto di servizio; e b) a fornire informazioni sul servizio ai sensi della Sezione 6 (obblighi di trasparenza) del Codice.

Il trattamento da parte di un *processor* è disciplinato da un contratto scritto che è vincolante tra *processor* e *controller* e che definisce l'oggetto e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e categorie di dati soggetti e gli obblighi e i diritti del *controller*. Il contratto può essere in forma elettronica (art. 28, par. 3 GDPR). Il CISP definisce le caratteristiche del servizio e come viene consegnato e i diritti e gli obblighi del cliente nel Contratto di Servizio di cui alle sezioni (a) e (b)[328].

I CISPs forniscono infrastrutture. I clienti hanno la possibilità di scegliere come utilizzare questa infrastruttura e possono anche scegliere di cambiare il modo e per quale scopo essi utilizzano questa infrastruttura quando vogliono.

Previsioni specifiche sono dettate anche in tema di sicurezza del trattamento dei dati personali ove, al paragrafo 5.3 della sezione 5ª in analisi, si premette innanzitutto che sia *controller* che *processor* devono, tenendo conto dello stato dell'arte, i costi di attuazione e la natura, la portata, il contesto e le finalità del trattamento, nonché il rischio di varia probabilità e la gravità per i diritti e le libertà delle persone fisiche, implementare adeguate

[328] a) Descrizione del trattamento. Per facilitare queste caratteristiche di servizi di infrastruttura *cloud* e per evitare la necessità di modificare l'accordo di servizio o di entrare in un nuovo accordo di servizio ogni volta che il cliente o qualsiasi utente finale sceglie di cambiare il modo in cui utilizza il servizio, la descrizione del trattamento nell'accordo (contratto) deve essere redatta in un modo che può ospitare i cambiamenti che clienti che vogliono applicare. Per una maggiore flessibilità, contratti di assistenza possono riguardare la descrizione del trattamento utilizzando i servizi di infrastruttura *cloud* su base generica, ad esempio, "elaborazione, *storage* e distribuzione di contenuti sulla rete del CISP"; b)Forma del contratto. A condizione che sia per iscritto (anche in forma elettronica) e giuridicamente vincolante tra il CISP e il cliente, il contratto di servizio può assumere qualsiasi forma, tra cui: un unico contratto; una serie di documenti come un contratto di servizi di base con relativi allegati (accordi di elaborazione dati, SLA, i termini di servizio, le politiche di sicurezza, etc.); o termini e condizioni *standard online*.

misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio (Art 32, par. 1, GDPR).

Si specifica, poi, che, per quanto concerne le misure di sicurezza, che il CISP dovrà porre in essere (*Requirement for* CISP), il codice prevede che questi implementerà e adotterà adeguate misure tecniche e organizzative per le strutture di *data center* del CISP, *server*, apparecchiature di rete e sistemi *software host* che si trovano sotto il controllo del CISP e che sono utilizzati per fornire il servizio del CISP (Rete CISP). Tali misure tecniche e organizzative devono essere progettate per aiutare i clienti a proteggere i dati personali contro il trattamento non autorizzato, la perdita accidentale o illecita, l'accesso o la divulgazione.

I servizi di infrastruttura *cloud* hanno agnostici contenuti. Essi offrono le stesse misure tecniche e organizzative e livello di sicurezza a tutti i clienti, indipendentemente dal fatto che riguardino il trattamento dei dati personali o meno, o la natura, la portata, il contesto e le finalità del trattamento che il cliente vuole che il servizio esegua.

Il codice chiaramente evidenzia che il CISP non è l'unico responsabile per la sicurezza nel contesto dell'uso di un cliente del servizio di infrastruttura *cloud* e, pertanto, specifica che ci sono alcuni aspetti chiave della sicurezza che sono a carico del cliente (e non sotto la responsabilità del CISP). Ad esempio, il cliente (e non il CISP) è responsabile per la sicurezza dei sistemi operativi ospitati, le applicazioni ospitate sul servizio, i dati in transito e a riposo, il servizio di accesso all'Area Clienti (le credenziali) e le autorizzazioni per il personale cliente che utilizza il servizio.

I clienti dovrebbero rivedere: a) le informazioni messe a disposizione da parte del CISP in materia di sicurezza dei dati per quanto riguarda i servizi[329]; b) la configurazione scelta dal cliente del servizio di infrastruttura *cloud* e l'utilizzo delle funzioni e i controlli disponibili in connessione con il servizio di infrastruttura *cloud*; e c) le misure di sicurezza che il cliente dovrà mettere in atto per gli aspetti della sicurezza sotto la sua responsabilità, e determinarsi, in modo indipendente, sul se, tutte insieme, queste misure forniscano un adeguato livello di sicurezza del trattamento che il servizio va ad eseguire. Questa determinazione dovrebbe essere basata sulla natura, la portata, il contesto e le finalità del trattamento previsto del cliente.

[329] Si v. la Sezione 6 (obblighi di trasparenza), del codice in commento.

Poiché è il cliente che decide cosa trattare (cioè quali dati e per quali scopi), solo il cliente può determinare il livello di sicurezza «appropriato» per memorizzare i dati personali e dei processi il servizio che utilizza. Il CISP non è in grado di fare questa valutazione perché il CISP non controlla, non limita o comunque non controlla quello che è il trattamento da eseguire dal cliente che utilizza il servizio.

Il CISP, da parte sua, manterrà un programma di sicurezza delle informazioni con l'obiettivo di: a) identificare i rischi ragionevolmente prevedibili e interni alla sicurezza della rete CISP; e b) ridurre al minimo i rischi di sicurezza, anche attraverso valutazioni del rischio e *test* regolari. Il CISP designerà uno o piú personale CISP per coordinare e rendere conto per il programma di sicurezza delle informazioni.

Il CISP effettuerà verifiche periodiche della sicurezza della rete CISP e sull'adeguatezza del programma di sicurezza delle informazioni del CISP. Questi può scegliere di rivedere il suo programma di sicurezza delle informazioni nei confronti di uno o piú *standard* di sicurezza del settore; valuterà costantemente la sicurezza della rete CISP per determinare se sono necessarie ulteriori misure di sicurezza o diversi per rispondere ai nuovi rischi per la sicurezza oi risultati generati dalle proprie revisioni periodiche del CISP; può modificare gli *standard* di sicurezza del CISP di tanto in tanto, ma continuerà per tutta la durata del Contratto di servizi a fornire almeno lo stesso livello di sicurezza come descritto negli *standard* di sicurezza del CISP alla data di efficacia del Contratto di servizi.

Previsioni specifiche sono dettate anche in tema di trasferimento dei dati personali verso paesi terzi (par. 5.4). Innanzitutto, si richiama l'art. 44 del GDPR, per il quale sia il *controller* che il *processor* devono garantire che qualsiasi trasferimento di dati personali oggetto di trattamento a un paese terzo deve avvenire solo se determinate condizioni ai sensi del diritto sulla protezione dei dati dell'UE siano rispettate.

Si individuano cosí i *requirement for* CISP e segnatamente: a) *location*. Il servizio di infrastruttura *cloud* fornirà al cliente la possibilità di scegliere di utilizzare il servizio per memorizzare ed elaborare i dati interamente all'interno del SEE; b) *information*. Il CISP fornirà le informazioni ai clienti sulla regione e il paese in cui i dati vengono memorizzati ed elaborati da o per conto del CISP, compreso se il CISP subappalta parte del trattamento

a terzi[330]; c) *level of protection*. Il CISP implementerà o altrimenti renderà disponibile ai clienti un livello di conformità riconosciuta ai sensi del diritto sulla protezione dei dati dell'UE per il trasferimento legittimo dei dati personali al paese in questione (tra cui, ad esempio, la norma UE contrattuali clausole, norme vincolanti d'impresa o UE -US *Privacy Shield* per i trasferimenti di dati personali verso gli Stati Uniti d'America), se: *i*) il cliente trasferisce i dati dall'interno del SEE da memorizzare utilizzando il servizio del CISP in qualsiasi paese al di fuori del SEE che non è riconosciuto dalla Commissione europea in grado di fornire un livello di protezione adeguato dei dati personali; o *ii*) il CISP è autorizzato ad accedere ai dati memorizzati utilizzando il servizio del CISP all'interno del SEE da questo paese di cui al punto (i) di cui sopra.

In attuazione dell'art. 28, par. 3, lett. e) GDPR - per il quale, tenuto conto della natura del trattamento, il *processor* deve assistere il *controller* con adeguate misure tecniche e organizzative, nella misura in cui ciò sia possibile, per l'adempimento dell'obbligo del *controller* di rispondere alle richieste di esercizio dei diritti della persona interessata - il CISP (v. paragrafo 5.7., intitolato «Data Subject requests») fornirà al cliente la possibilità di rettificare, cancellare, limitare o recuperare i dati dei clienti. Il cliente può utilizzare questa capacità per aiutare cliente nell'adempimento dei suoi obblighi per rispondere alle richieste di esercizio dei diritti della persona interessata. Il CISP può fornire al cliente la possibilità di rettificare, cancellare, limitare o recuperare i dati del cliente: a) come parte del servizio; o b) permettendo ai clienti di progettare e implementare le proprie soluzioni utilizzando il servizio.

Oltre a fornire al cliente la possibilità di rettificare, cancellare, limitare o recuperare i dati dei clienti, il codice di condotta in disamina specifica in maniera molto chiara che il CISP non è tenuto a fornire ulteriore assistenza al cliente con richieste di dati dei soggetti. Questo perché è il cliente (e non il CISP) il responsabile della gestione dati trattati

[330] Per motivi di sicurezza, solo una posizione generale (ad esempio un'area di città o l'area di una regione) deve essere fornito. Questa descrizione generale deve, almeno, permettere al cliente di identificare quale Stato membro dell'Unione europea ha giurisdizione sull'elaborazione effettuata dal cliente che sta utilizzando il servizio. Se necessario per assolvere obblighi di un'autorità di vigilanza competente secondo la legge vigente in materia di utilizzo del cliente del servizio e purché le informazioni sono protette da adeguati obblighi di riservatezza vincolanti per l'autorità, il CISP comunica alla competente autorità di vigilanza l'indirizzo esatto delle strutture competenti. Per i servizi che possono essere eseguiti indifferentemente all'interno di diversi luoghi della Rete CISP, CISPs renderà le informazioni facilmente accessibili al cliente e consentirà ai clienti di selezionare la posizione/i all'interno della rete CISP in cui verranno trattati i loro dati.

utilizzando il servizio. Pertanto, il CISP non sa ciò (*rectius*, i dati) che i clienti stanno caricando sul servizio e, in particolare, chi sono le persone interessate di tali dati.

Precise regole di condotta sono dettate per consentire l'attuazione degli obblighi di riservatezza in capo al *processor ex* art. 28, par. 3, lett. b (v. paragrafo 5.8) e al fine di garantire il rispetto dell'art. 48, per il quale i responsabili del trattamento (ma anche i titolari) possono dare esecuzione ad una sentenza o decisione amministrativa di un paese terzo che necessita di dati personali da trasferire o divulgare soltanto in base a un accordo internazionale in vigore tra il paese terzo richiedente e l'Unione europea o uno Stato membro.

Particolarmente importanti sono le regole di condotta relative al «data breach» (paragrafo 5.10) e a quelle dettate per la cancellazione o la restituzione dei dati personali (paragrafo 5.11).

Per quanto concerne la prima tematica, sul presupposto per il quale il *processor* devono notificare una violazione dei dati al *controller* senza indebito ritardo dopo essere venuto a conoscenza di essa (art. 33, par. 2) e in ossequio all'art. 28, par. 3, lett. f) - per il quale tenuto conto della natura del trattamento e delle informazioni disponibili al *processor*, questi deve assistere il *controller* nel garantire il rispetto agli obblighi di cui agli artt. da 32 a 36 - il CISP attua una politica di gestione degli incidenti di sicurezza che specifica le procedure per l'identificazione e la risposta agli incidenti di sicurezza di cui il CISP venga a conoscenza. Questa politica comprende: linee guida per decidere quale tipo di incidenti devono essere notificati al cliente sulla base del potenziale impatto sui dati; guida su come incidenti dovrebbero essere affrontati; e un insieme di informazioni da mettere a disposizione del cliente dopo l'incidente violazione dei dati.

Per quanto riguarda la notifica delle violazioni di sicurezza, se il CISP viene a conoscenza di un accesso non autorizzato ai dati personali dei clienti sulle apparecchiature del CISP questi le notificherà al cliente senza indebito ritardo.

La notifica descriverà: la natura della violazione della sicurezza, le conseguenze della violazione, le misure adottate o proposte da adottare da parte del CISP in risposta all'incidente e fornirà un punto di contatto presso il CISP.

Per quanto concerne il tema «*deletion or return of personal data*», sul presupposto di cui all'art. 28, par. 3, lett. g) - secondo cui a discrezione del *controller*, il *processor* deve cancellare o restituire tutti i dati personali al *controller* (e cancellare le copie esistenti) alla fine della

prestazione di servizi - il CISP fornirà al cliente la possibilità di recuperare ed eliminare i dati dei clienti. Il cliente può utilizzare questa capacità per recuperare o cancellare i dati del cliente al termine della fornitura del servizio.

A seconda del tipo di servizio, il CISP può fornire al cliente la possibilità di recuperare ed eliminare i dati del cliente o come parte del servizio oppure permettendo ai clienti di progettare e implementare le proprie soluzioni di eliminazione e recupero utilizzando il servizio.

Il CISP non può gestire o scegliere di eliminare i dati di un cliente. Né è il CISP che può fornire al cliente assistenza per l'eliminazione dei dati al di là della concessione della possibilità al cliente di recuperare o cancellare i dati stessi. Pertanto, è responsabilità del cliente di gestire l'eliminazione e il recupero dei dati sul servizio tenendo conto di qualsiasi processo innescato dalla risoluzione o della scadenza del contratto di assistenza.

Osservazioni conclusive.

Le tecnologie informatiche sono il cuore della società moderna. Attraverso tecnologie digitali è svolta l'attività sociale ed è diffusa l'essenza di persone fisiche e giuridiche. Il Regolamento europeo 2016/679 (che, si ricorda, sarà direttamente applicabile, in base al suo art. 99, in tutti gli Stati dell'Unione europea a partire dal 25 maggio 2018) rappresenta lo strumento atto a formalizzare il nuovo corso digitale della tutela dei dati personali, a livello comunitario ed extracomunitario. Questo mostra peculiarità rilevanti di tipo tecnico-giuridico: è obbligatorio e direttamente applicabile in tutti gli Stati membri senza necessità di recepimento; ha un'essenza informatico giuridica spiccata; implica tutele verso i cittadini dell'Unione europea anche da parte di nazioni *extra* UE; mira a responsabilizzare utenti e aziende sulle attività digitali che concedono e/o dispongono.

Gli aspetti di interesse per l'interprete, introdotti dal nuovo Regolamento, sono molteplici. Si pensi alla disciplina su *social* e minori (art.8), al diritto di accesso dell'interessato (art. 15), al diritto all'oblio (art.17), al diritto alla portabilità dei dati (art. 20), al principio di *accountabilty* (art. 5, comma 2 e art. 24), ai princípi di *privacy by design* e *privacy by default* (art. 25), ai requisiti del responsabile del trattamento e alla disciplina dei trattamenti da parte del medesimo (art. 28), al registro delle attività di trattamento (art.30),

alla *data breach notification* (art. 33) in uno alla valutazione d'impatto sulla protezione dei dati, espressamente prevista allorché il trattamento preveda «l'uso di nuove tecnologie» (art. 35), all'incoraggiamento verso l'elaborazione di codici di condotta destinati a contribuire alla corretta applicazione del regolamento (art. 40), la cui adesione da parte del *processor* può essere utilizzata come elemento per dimostrare la sussistenza in capo allo stesso delle garanzie sufficienti richieste per il trattamento (art. 28, comma 5), al meccanismo dello sportello unico (art. 60), al nuovo impianto sanzionatorio (art. 83), etc.

Si possono, in sintesi, evidenziare cinque assi portanti del Regolamento UE in parola: principio dell'*accountability*, *data protection impact assessment*, *data breach notification*, *privacy by design* e *by default*, *data protection officer*. Sono questi, appunto, gli architravi su cui poggia tutto il sistema del nuovo Regolamento e che sono alla base di una corretta configurazione di un sistema di gestione *privacy*. La lettura combinata e disposta degli articoli sulla sicurezza dei dati (dall'art. 24 all'art. 39) mostra la strategia di difesa dei dati concepita dal legislatore comunitario, la *Governance*, fondata su princípi di buon senso tecnico-giuridico e propri di una disciplina già conosciuta e spesso non chiaramente compresa: la *Cyber Security*.

Le tecnologie *cloud* consentono di trattare e conservare i dati su sistemi di *server* dislocati nelle diverse parti del pianeta e sottoposti, nella loro inevitabile materialità, a molti rischi, da quelli sismici a quelli legati a fenomeni di pirateria, non solo «informatica», o ad atti di terrorismo o a rivoluzioni imprevedibili.

Crescono i pericoli legati alla perdita e al furto di enormi quantità di dati e si amplia il numero dei soggetti che intervengono nell'àmbito di trattamenti cosí complessi e disarticolati.

Neutralità della rete, obbligo di denunciare le *serious breaches*, necessità di ridefinire le responsabilità nell'àmbito di catene complesse di trattamento dei dati: ecco alcuni titoli di una tematica sempre piú vitale per le nostre società, per il nostro sviluppo economico, per la nostra libertà e convivenza democratica. Le imprese e gli operatori a cui il mercato offre questi nuovi servizi pensano soprattutto alla diminuzione di costi o alle opportunità di costante ammodernamento che queste tecnologie consentono, prestando scarsa attenzione al fatto che comportano la perdita del possesso fisico dei dati e dei programmi operativi che utilizzano.

Di quanto sopra ne è consapevole il legislatore europeo che evidenzia le problematiche legate alla rapidità dell'evoluzione tecnologica già nel considerando n° 6 e, in particolare,

sottolinea come la portata della condivisione e della raccolta di dati personali sia aumentata in modo significativo e come la tecnologia attuale consenta, tanto alle imprese private quanto alle autorità pubbliche, di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. È un chiaro riferimento alla tecnologia *cloud*.

Occorre, *in primis*, informare sui rischi. L'avanzata delle nuove tecnologie non può e non deve essere fermata né ostacolata, ma deve essere regolata a garanzia di tutti. Per questo il Garante per la protezione dei dati personali ha lanciato un segnale forte a tutti, agli operatori istituzionali, alle imprese, agli utenti affinché aumenti la consapevolezza nell'uso delle tecnologie.

È sempre piú urgente però che gli utenti siano informati dagli stessi fornitori dei rischi connessi ai servizi offerti. Dall'attuale informativa «statica» su come sono trattati i nostri dati, si deve allora passare rapidamente a un'informativa «dinamica» sui rischi che i trattamenti comportano. Anche in quest'àmbito è necessaria un'«informativa di rischio» analoga, per esempio, a quelle sull'uso dei farmaci o sui pericoli dell'eccessiva velocità.

La prevenzione, dunque, assurge al rango di connotato imprescindibile e ineludibile della tematica *de qua* e 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*) sembra essere stata delineata dal Regolamento *privacy* 2016 con la codificazione del principio di *accountability* e con le previsioni di cui all'art. 28. Ripartizione meglio specificata con il *Code of Conduct*, 26 *September* 2016 del CISPE, il cui scopo dichiarato è quello di guidare i clienti nel valutare se il servizio di infrastruttura *cloud* che si intende usare è adatto per le attività di trattamento dei dati che essi desiderano eseguire e aiutare gli stessi a scegliere il servizio di infrastruttura *cloud* giusta per le loro esigenze specifiche.

È ammesso, da parte del titolare del trattamento - obbligato alla messa in atto di quelle misure tecniche e organizzative «adeguate», per garantire e dimostrare che il trattamento è effettuato conformemente al normativa regolamentare (art. 24) - il ricorso «unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate» (art. 28, comma 1). I trattamenti da parte di tali responsabili sono disciplinati da un contratto o da altro atto giuridico (che dev'essere stipulato in forma scritta, anche in formato elettronico *ex* comma 9, art. 28) a norma del diritto dell'Unione o degli Stati membri. Tali atti devono vincolare il responsabile del

trattamento al titolare del trattamento e prevedere tutto quanto espressamente indicato al comma 3 dell'art. 28. Assume particolare rilevanza l'adesione da parte del responsabile a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42, poiché essa adesione può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui all'articolo in parola.

L'oggettiva difficoltà nel negoziare ruoli e responsabilità con il *cloud service provider*, che spesso è una organizzazione molto piú grande del cliente, poi oggi rileggersi proprio alla luce dell'art. 28 in commento. Tale articolo attribuisce un preciso obbligo giuridico al titolare del trattamento di impartire istruzioni documentate al responsabile (art. 28, par. 3, lett. a), cui corrisponde un dovere di quest'ultimo (o di chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento) nel momento in cui abbia accesso ai dati personali, di trattarli secondo le istruzioni ricevute dal titolare del trattamento, tanto che non può trattare tali dati se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o degli Stati membri (art. 29).

Caso quest'ultimo decisamente inverosimile quando si parla di un grande *cloud provider*, da un lato, e di piccola e media impresa-*buyer*, dall'altro; mentre è verosimile asserire che, nella maggior parte dei casi, nemmeno *buyer* come una grande impresa o una P.A. riescano di fatto ad impartire istruzioni dettagliate al *cloud provider* e ad esercitare quel controllo tipico del rapporto titolare-responsabile. Ne deriva che la soluzione di fatto piú aderente alla normativa *privacy* odierna è quella di una titolarità autonoma anche in capo al *cloud provider*.

A bene vedere, alla luce del nuovo Regolamento *privacy*, si può sostenere che il fornitore che si spinga sino al punto di determinare ulteriori finalità del trattamento rispetto a quelle fissate dal cliente assuma la qualifica di titolare. Ciò è espressamente detto nel comma 10 dell'art. 28 in disamina, ove è sancito che «fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione.». Ciò che rileva, pertanto, è chi in concreto ha determinato le finalità e i mezzi del trattamento, cosí assumendo di diritto quella qualifica che corrisponde alla sua attività di fatto realizzata. Questo può considerarsi un chiaro intervento teso ad ampliare i casi in cui un fornitore di servizi *cloud* può essere definito titolare del trattamento.

In ogni caso, sia il *cliente* che il *cloud provider* dovranno, tenendo conto dello stato dell'arte, i costi di attuazione e la natura, la portata, il contesto e le finalità del trattamento, nonché il

rischio di varia probabilità e la gravità per i diritti e le libertà delle persone fisiche, implementare «adeguate misure tecniche e organizzative» per garantire un livello di sicurezza adeguato al rischio (art. 32).

Omissioni informative del gestore del servizio e inconsapevolezza dell'utente sono destinate al tramonto alla luce degli «obblighi di trasparenza» contenuti nella Sezione 6, (*Transparency Requirement*) del *Code of Conduct*, 26 *September* 2016 del CISPE, che appunto obbligano il *cloud provider* a informare l'utente-titolare del trattamento per un utilizzo consapevole del servizio e, quindi, per consentirgli quella «valutazione di impatto» sulla protezione dei dati personali che egli è tenuto ad effettuare in base all'art. 35.

Il cliente, infatti, dev'essere in grado di effettuare affidabili valutazioni d'impatto dei trattamenti sulla sicurezza e protezione dei dati, compiuti sui servizi di infrastruttura *cloud*. Il *cloud provider*, stabilisce il *Code of Conduct*, può aiutare il cliente a raggiungere questo obiettivo, fornendo la trasparenza circa le misure di sicurezza attuate dallo stesso per i suoi servizi; e per fornire un'adeguata trasparenza il fornitore del servizio perseguirà i seguenti sei obiettivi: *i*) un *service agreement* che affronta la ripartizione delle responsabilità tra il CISP e il cliente per la sicurezza del servizio; *ii*) una dichiarazione di alto livello (*high level statement*) sugli obiettivi di sicurezza e le norme che si applicano al servizio per quanto riguarda almeno riservatezza, disponibilità, integrità; *iii*) informazioni sulla progettazione e la gestione del servizio per aiutare i clienti a comprendere le potenziali minacce e le vulnerabilità dell'uso del servizio; *iv*) informazioni dei processi di gestione del rischio e criteri del CISP per il servizio; *v*) informazioni sulle misure di sicurezza attuate dal *cloud provider* per il servizio; *vi*) documentazione di assicurazione sul sistema di gestione della sicurezza delle informazioni del fornitore del servizio.

Con riferimento al tema della conservazione dei dati in *cloud computing* è chiaro che essi potrebbero essere dislocati ovunque, il che pone (per la *privacy*) importanti questioni di esportazione dati all'estero. Detta tematica è balzata agli onori delle cronache dopo la pubblicazione della sentenza della Corte di Giustizia dell' 8 aprile 2014. La pronuncia, nel dichiarare invalida la direttiva 2006/24/CE, ha affermato un importante principio: i dati relativi alle comunicazioni elettroniche devono essere conservati nel territorio dell'Unione, anche al fine di prevenire e contrastare reati gravi. Per quanto concerne la conservazione dei documenti informatici richiama occorre richiamare il CAD (codice dell'amministrazione digitale, d.lg. 82/2005) e, in particolare, quanto contenuto nel suo art. 44, nonché il

d.P.C.M. 3 dicembre 2013 che definisce le misure attuative degli obblighi di conservazione, in forma digitale, dei documenti della P.A., come previste dal CAD. In tale contesto si evidenzia come il controllo sui sistemi e sui dati è reso agevole dal requisito previsto dall'art. 9, co. 2, del d.P.C.M. in disamina che, ai fini di vigilanza da parte di AgID, impone ai sistemi di conservazione delle pubbliche amministrazioni e ai conservatori accreditati la materiale conservazione dei dati e delle copie di sicurezza sul territorio nazionale per garantire l'accesso ai dati presso la sede del produttore e misure di sicurezza adeguate.

Alla luce del nuovo Regolamento UE sulla *privacy*, può dirsi che il problema della conservazione dei dati personali (*rectius*, non conservazione degli stessi all'interno dell'Unione europea), non è poi cosí drammatico come può sembrare e ciò in base alla specificazione, nella nuova normativa europea, dell'àmbito di applicazione territoriale della stessa (art. 3). In altri termini, quand'anche i dati personali venissero conservati in un Paese terzo tale pratica non sempre varrebbe (nel senso che non automaticamente sarebbe sufficiente) ad escludere l'applicabilità del Regolamento in discorso.

La conservazione è essa stessa un trattamento (di dati personali), consistendo quest'ultimo in «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme di dati personali», come, ad esempio, «la conservazione» (art. 4, n. 2).

Adesso, si ipotizzi che il trattamento di dati personali, *sub specie* di operazione di conservazione degli stessi, avvenga al di fuori dell'Unione. Siffatta conservazione determinerebbe automaticamente la non applicabilità del Regolamento UE? La risposta giusta dovrebbe essere negativa, anche se la formulazione dell'art. 3, par. 1, non è la migliore possibile.

Secondo la citata disposizione, ai fini dell'applicabilità o meno del diritto dell'Unione, non rileva il luogo in cui si realizza la conservazione dei dati personali, ma occorrerà far riferimento all'àmbito delle attività di uno stabilimento di un titolare del trattamento o di un responsabile dello stesso nell'Unione. In breve, se un titolare 'o' un responsabile è stabilito nell'Unione (*rectius*, ha uno stabilimento nell'Unione e il trattamento è effettuato nell'àmbito delle attività dello stesso) allora il regolamento si applica «indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione».

Pertanto, il criterio di riferimento, per radicare l'applicabilità dello stesso, è lo stabilimento nell'Unione delle attività del titolare del trattamento 'o' del responsabile del

medesimo, nel senso che se queste attività - ossia le decisioni sulle finalità e sui mezzi del trattamento (*rectius*, sulla conservazione) dei dati personali o comunque le principali attività del trattamento stesso - sono poste in essere in un suo stabilimento sito in uno Stato membro ciò farà sí che sarà applicabile il regolamento.

Altro caso: titolare e responsabile del trattamento non stabiliti nell'Unione, ma gli interessati si trovano nell'Unione (art. 3, par. 2). Si applicherà il Regolamento in discorso quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Pertanto, il *cloud provider* statunitense (o comunque extraeuropeo) che offra il proprio servizio a persona fisica identificata o identificabile - *rectius*, l'«interessato», cui i dati personali, oggetto di trattamento, lo riguardano - che si trova nell'Unione e indipendentemente dall'obbligatorietà di un suo pagamento per il servizio reso (che può, dunque, essere offerto anche gratuitamente), dovrà rispettare la normativa *privacy* europea e, segnatamente, il regolamento *de quo*.

Il regolamento, inoltre, si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtú del diritto internazionale pubblico (art. 3, comma 3).

Anche la questione portabilità dei propri dati su altro Csp (problema del c.d. «*vendor lock-in*») può essere affrontata e, auspicabilmente, risolta alla luce del Regolamento. Viene in rilievo il principio dell'interoperabilità, già contenuto nella Direttiva 91/250/CEE nei considerando 10, 11 e 12. Sul punto, poi, il Regolamento UE sulla *privacy* qualifica la portabilità dei dati come un diritto dell'interessato (art. 20), non a caso inserito nel Capo III, appunto rubricato «Diritti dell'interessato». Lo stesso Regolamento chiarisce la portata e l'essenzialità del diritto in parola, con il dichiarato obiettivo di assicurare piú tutele e libertà per i cittadini, al considerando 68 ove si specifica come sia «opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati» indicando quando il medesimo diritto dovrebbe applicarsi.

Pertanto, con il diritto alla portabilità dei dati si è liberi di trasferire i propri dati in un mercato digitale piú aperto alla concorrenza. Diritto alla «portabilità» dei propri dati personali che quindi significa diritto di trasferirli da un titolare del trattamento ad un altro.

Ad esempio, si potrà cambiare il *provider* di posta elettronica senza perdere i contatti e i messaggi salvati. È chiaro che ci sono, però, alcune eccezioni che non consentono l'esercizio del diritto: in particolare, quando si tratta di dati contenuti in archivi di interesse pubblico, come ad esempio le anagrafi.

Ciò posto, anche se alcuni fornitori di servizi *cloud* non hanno ben compreso (o non vogliono comprendere) l'importanza dell'utilizzo di *standard* aperti, continuando a definire - indipendentemente l'uno dall'altro - formati ai quali attenersi e che l'utente adotta pedissequamente, con il nuovo Regolamento UE *privacy* questa riluttanza verso la previsione di protocolli di standardizzazione per i sevizi *cloud* sembra giunta al capolinea, cosí aprendosi una nuova era nella fase di progettazione dei programmi volta a garantirne la capacità di scambiarsi le informazioni e di usare reciprocamente le informazioni scambiate.

Per quanto riguarda il diritto in parola, il Gruppo dei Garanti UE (WP 29) - che ha approvato lo scorso 13 dicembre tre documenti con indicazioni e raccomandazioni su: «responsabile per la protezione dei dati» (*Data Protection Officer*-DPO); diritto alla portabilità dei dati; e «autorità capofila» (che fungerà da «sportello unico» per i trattamenti transnazionali) - evidenzia il suo valore di strumento per l'effettiva libertà di scelta dell'utente, che potrà decidere di trasferire altrove i dati personali forniti direttamente al titolare del trattamento (piattaforma di *social network*, fornitore di posta elettronica etc.) oppure generati dall'utente stesso navigando o muovendosi sui siti o le piattaforme messe a sua disposizione. Il documento esamina proprio gli aspetti tecnici legati soprattutto ai requisiti di interoperabilità fra i sistemi informatici e alla necessità di sviluppare applicazioni che facilitino l'esercizio del diritto.

È nell'art. 35 del Regolamento (valutazione di impatto *privacy*), scritto espressamente per quel tipo di trattamento che prevede in particolare «l'uso di nuove tecnologie», che il riferimento al *cloud* appare oltremodo chiaro e univoco.

È chiaro, infatti, che il profilo della riservatezza rappresenta la maggiore sfida da affrontare sul versante della *data protection*. Il titolare del trattamento che utilizzi servizi *cloud* perde di fatto il controllo dei propri dati. Proprio la necessità di adottare un *privacy impact assessment* (valutazione dell'impatto-*privacy*), che consenta di valutare i rischi derivanti dall'uso di tali sistemi ed individuare meglio le forme di tutela, aveva indotto i rappresentanti dei Garanti Europei, riuniti nel c.d. «Gruppo di Berlino», nel corso di una riunione del 2011, ad individuare nella perdita di controllo (c.d. *loss of control*) da parte del

titolare, il principale problema per l'introduzione su larga scala di questo nuovo servizio. Pertanto, secondo l'Autorità garante, sarà compito dell'utente porre in essere tutti gli accorgimenti previsti per garantire il corretto trattamento dei dati immessi nel *cloud*, iniziando da un'attenta verifica del grado di affidabilità del fornitore di servizi al quale ci si intende affidare, tenendo in considerazione le proprie esigenze imprenditoriali o istituzionali, la quantità e la tipologia di dati da migrare su *cloud*, i rischi e le misure di sicurezza. Sotto questo profilo è raccomandabile la scelta di fornitori *cloud* dotati di certificazioni ampiamente riconosciute a livello internazionale, come avviene per lo specifico *standard* previsto per il settore *cloud*: l'Iso 27018. Si tratta di un *set* di regole costruito sugli *standards* Iso 27001 e 27002 per garantire il rispetto dei princípi e delle norme *privacy* dettate dalla direttiva 95/46/CE, da parte dei *providers* di *public cloud* che se ne dotano. L'idea di base è quella di realizzare un tipico esempio di *privacy by design*, non a caso, altro architrave del Regolamento in disamina.

Sul versante della *data breach notification*, il *cloud provider* sarà tenuto a notificare una violazione dei dati personali al cliente-*controller*, senza indebito ritardo, dopo aver avuto conoscenza di essa violazione (art. 33, par. 2). Rientra, infatti, tra i suoi compiti - tenuto conto della natura del trattamento e delle informazioni a sua disposizione - quello di assistere il *controller* nel garantire il rispetto agli obblighi di sicurezza dei dati personali, di cui alla Sezione 2 del Capo IV (art 28, par. 3, lett. f). Pertanto, il *cloud provider* dovrà attuare una politica di gestione degli incidenti di sicurezza che specifichi le procedure per l'identificazione e la risposta agli incidenti di sicurezza di cui venga a conoscenza. Sul punto, il *Code of Conduct*, 26 *September* 2016 del CISPE, ha specificato (paragrafo 5.10) che questa politica comprende: linee guida per decidere quale tipo di incidenti devono essere notificati al cliente sulla base del potenziale impatto sui dati; guida su come incidenti dovrebbero essere affrontati; e un insieme di informazioni da mettere a disposizione del cliente dopo l'incidente violazione dei dati. Il medesimo codice specifica anche che la notifica deve descrivere la natura della violazione della sicurezza, le conseguenze della violazione, le misure adottate o proposte da adottare da parte del *cloud provider* in risposta all'incidente e deve fornire un punto di contatto con lo stesso.

Non è stata poi trascurata la questione degli obblighi di protezione dei dati nella relazione cliente-fornitore. In base al principio di trasparenza (che è fondamentale per il trattamento equo e legittimo dei dati personali), il Regolamento UE, *ex* art. 12, obbligherà il

cliente *cloud* - o anche il fornitore se determina le finalità e i mezzi del trattamento, in virtú del comma 10, dell'art. 28 - a fornire all'interessato, presso il quale raccoglie dati che lo riguardano, le informazioni di cui agli artt. 13 e 14. Inoltre, si dovranno fornire all'interessato anche le comunicazioni di cui agli articoli da 15 a 22 - ossia rendere edotto l'interessato dei suoi diritti di accesso, di rettifica, di cancellazione, di limitazione del trattamento, di portabilità, di opposizione, di cui ne agevola l'esercizio (art. 12, comma 2) - e quella di violazione dei dati personali *ex* articolo 34. Tali informazioni e comunicazioni sono fornite, di regola, in modo gratuito, salvo che siano manifestamente infondate o eccessive, in particolare perché ripetitive (art. 12, comma 5) e «in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori» (art. 12). Circa la forma, il Regolamento UE prevede che le stesse siano fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici e, ove richiesto dall'interessato, possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato (art. 12, ultimo periodo). La trasparenza dev'essere garantita anche nel rapporto tra cliente *cloud*, fornitore *cloud* e (eventuali) subcontraenti.

In virtú del principio della specificazione e limitazione della finalità, il cliente *cloud* dovrà determinare la finalità del trattamento prima di procedere alla raccolta di dati personali dall'interessato, informandolo in proposito. Il cliente *cloud* non deve trattare dati personali per finalità diverse che non siano compatibili con quelle originali. Inoltre, occorre garantire che i dati personali non siano (illegalmente) trattati per ulteriori finalità dal fornitore del servizio *cloud* o da uno dei suoi subcontraenti.

Per quanto concerne la cancellazione, invece, anche il Garante europeo Art. 29 (Parere 5/2012, WP 196, adottato il 1° luglio 2012) ammoniva che spetta al cliente *cloud* garantire che i dati personali siano cancellati non appena non siano piú necessari nel senso sopra indicato. Oggi, con il Regolamento UE, il diritto alla cancellazione ha assunto il rango «di diritto dell'interessato», consacrato nell'art. 17. Il cliente *cloud* (titolare) ha, pertanto, l'obbligo di cancellare senza ingiustificato ritardo i dati personali dell'interessato, se sussiste (almeno) «uno» dei motivi espressamente indicati nel summenzionato articolo. Tuttavia, il «diritto all'oblio» non è senza limiti, è il legislatore europeo se ne avvede al paragrafo 3 dell'articolo in questione. Pertanto, le limitazioni all'operatività del diritto all'oblio, prima rimesse all'elaborazione pretoria, sono state adesso tipizzate dal legislatore europeo. Infatti,

che il diritto in parola necessitasse di un giudizio di bilanciamento era stato già chiarito sia dalla giurisprudenza nostrana che da quella di Lussemburgo. Ecco emergere un sistema di limiti al diritto all'oblio e contro limiti agli altri interessi costituzionalmente protetti che con esso devono bilanciarsi, allorché viene piú volte specificato che libertà di manifestazione del pensiero e del diritto di cronaca se, da un lato è costituzionalmente garantita, dall'altro deve esercitarsi sempre nell'osservanza dei limiti di verità e continenza e fondarsi su un persistente o rivitalizzato interesse pubblico.

Di recente, la *Wikimedia Foundation*, organizzazione *no-profit* che gestisce *Wikipedia*, ha presentato una petizione al Consiglio di Stato francese per «sostenere l'accesso alla conoscenza». L'enciclopedia *online* si è schierata a sostegno di *Google* nel caso che vede la compagnia contrapposta alla Commissione nazionale per l'informatica e la libertà (Cnil), il garante francese per la *privacy*, sul diritto all'oblio davanti ai giudici d'oltralpe. In buona sostanza il Garante *Privacy* francese sostiene che il diritto all'oblio per essere efficace deve essere globale, mentre *Google* e *Wikipedia* si oppongono proclamando il primato del diritto di libero accesso alla conoscenza, del diritto all'informazione e alla libertà di espressione; la questione dovrà essere risolta dal Consiglio di Stato.

Al di là della soluzione che proporrà il Consiglio di Stato francese, a parere di chi scrive, problematiche di tal genere, vedendo contrapposti interessi costituzionalmente garantiti, non possono che essere affrontate sulla base delle peculiarità del caso concreto ricostruendo, nel complesso sistema italo-comunitario delle fonti, quei valori/princípi idonei a costruire, di volta in volta, la disciplina piú congrua. Si tratta, quindi, di effettuare un non sempre agevole bilanciamento di interessi in conflitto e, in tale ottica, verificare la sussistenza di ragioni di interesse pubblico che, nella mutata realtà sociale e in quel singolo peculiare caso, possano consacrare il primato del diritto di libero accesso alla conoscenza, del diritto all'informazione e alla libertà di espressione sul diritto all'oblio.

BIBLIOGRAFIA

AA.VV., *Manuale di diritto dell'informatica*, a cura di D. VALENTINO, 3ª ed., Napoli, 2016.

ALPA G., BESSONE M., BONESCHI L. e CAIAZZA G. (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983; ID., «*Privacy*» *e statuto dell'informazione*, in *Riv. dir. civ.*, 1979, I, p. 72 ss.

ARIETA G., *Il problema della tutela della vita privata e le nuove leggi sulle intercettazioni telefoniche*, in *Temi Romana*, 1974, p. 532 ss.

AULETTA T.A., *Riservatezza e tutela della personalità*, Milano, 1978.

BELISARIO E., *"Diritto sulle nuvole – Profili giuridici del* cloud computing*"*, in *Altalex*, 2011.

BOBBIO N., *Diritto e logica*, in *Riv. int. fil. dir.*, 1962, p. 25 ss.

BOCCHINI R. e GENOVESE A., *Il contratto di* outsourcing, in R. BOCCHINI e A.M. GAMBINO (a cura di), *I contratti di somministrazione e di distribuzione*, Torino, 2011, p. 141 ss.

BRADSHAW S., MILLARD C. e WALDEN I., *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*, in *International Journal of Law and Information Technology*, 2011, p. 187 ss.

BUSNELLI F.D., *Spunti per un inquadramento sistematico, in Tutela della* privacy. *Commentario*, a cura di M.C. BIANCA e F.D. BUSNELLI, in *Nuove leggi civ.*, 1999, p. 230 ss.

BUTTARELLI G., *Banche dati e tutela della riservatezza*, Milano, 1997, p. 377, ss.

CARELLA G., *La scelta della legge applicabile da parte dei contraenti*, in AA.Vv., *Il nuovo diritto europeo dei contratti: dalla Convenzione di Roma al Regolamento Roma I,* Milano*,* 2007.

CARLEO R., *Il contratto di* outsourcing, in R. BOCCHINI (a cura di), *I contratti di somministrazione di servizi*, Torino, 2006, p. 549 ss.

CATAUDELLA A., *La tutela civile della vita privata*, Milano, 1972; ID., *Riservatezza (diritto alla)*, in *Enc. giur.* Treccani, XXVII, Roma, 1990.

CERRI A., *Libertà negativa di manifestazione del pensiero e di comunicazione. Diritto alla riservatezza: fondamento e limiti*, in *Giur. cost.*, 1974, p. 610 ss.

CIPRIANI N., *Dall'identità personale all'identità commerciale*, in *Riv. dir. comm.*, 1997, II, p. 267 ss.

COLANGELO G., *L'enforcement del diritto d'autore nei servizi cloud computing*, in *Dir. aut.*, 2012.

CORTESI A.D., *I contratti e l'informatica*, in M. MEGALE (a cura di), *ICT e diritto nella società dell'informazione*, Torino, 2012, p. 80 s.

CRYSTAL N., GIANNONI-CRYSTAL F., Something's got to give: *breve comparazione tra l'approccio americano ed europeo al* cloud computing, *soluzioni pratiche*, in *Cultura dir.*, 2014, p. 27 ss.

CUFFARO V. e RICCIUTO V. (a cura di), *La disciplina di dati personali*, Torino, 1997.

D'AMBROSIO M., Social network *e diritti della personalità. Considerazioni in tema di* privacy *e responsabilità civile*, in *Riv. giur. Mol. Sannio*, 2012, p. 330 ss.; ID., D*iritto all'immagine e utilizzo (in)consapevole della rete internet*, nota a Trib. Napoli 15 luglio 2014, in *Foro nap.*, 2016, 1, pp. 153 ss.; ID., *Cloud computing*, in *Manuale di diritto dell'informatica*, 3ª ed., a cura di D. Valentino, Napoli, 2016, p. 413 ss.

DE CUPIS A., *Il diritto all'identità personale*, Milano, 1949; ID., *I diritti della personalità*, 2ª ed., Milano, 1982.

DE VIVO M.C., *Il contratto ed* il cloud computing, in *Rass. dir. civ.*, 2013, p. 1001 ss.

ESPOSITO C., *La libertà di manifestazione del pensiero nell'ordinamento italiano*, Milano, 1958;

FABIANO N., *Approvata dalla Conferenza mondiale dei Garanti la risoluzione sulla* Privacy by Design, in http://www.istitutoitalianoprivacy.it/it/2010/11/02/approvata-dalla-conferenza-mondiale-dei-garanti-la-risoluzione-sulla-privacy-by-design/.

FALCE V., Standard *e* Cloud computing, in *Dir. ind.*, 2015, p. 155 ss.

FERRI G.B., *Diritto all'informazione e diritto all'oblio*, in *Riv. dir. civ.*, 1990, I, p. 801; ID., *Privacy e libertà informatica,* in *Banche dati telematica e diritti della persona*, a cura di Alpa Bessone, Padova, 1984, p. 47 ss.

FLICK V. e AMBRIOLA C., *Dati nelle nuvole: aspetti giuridici del cloud computing e applicazione alle amministrazioni pubbliche*, in *federalismi.it*, 2013, n. 6, p. 2 ss.

FOGGETTI N., *Privacy Protection, applicable Law and Jurisdiction Issues in Cloud Computing: an Internationl and EU prospective*, in *Cib. dir.*, 2014, p. 207 ss.

GIOVA S., *Introduzione*, in *Tutela della persona, beni comuni e valorizzazione dei nuovi diritti* (a cura di), Napoli, 2008, p. 9 ss.; ID., *Tutela della persona beni comuni e valorizzazione dei nuovi diritti. Atti del convegno di Campobasso e Isernia, 14-15 novembre 2007*, Napoli, 2008, p. 1 ss; ID., *La tutela del consumatore telematico nel D.lgs. n. 21 del 2014*, in *Rivista giuridica del Molise e del Sannio*, Napoli, 2014, p. 109 ss.

GUZZO A., *Il concetto di* Privacy Enhancing Technologies (PET), in *Sicurezza informatica e tutela della* privacy del 26/02/2009 e consultabile sulla pagina *web http://www.diritto.it/docs/27375-il-concetto-di-privacy-enhancing-technologies-pet*.

LAMETTI D., Cloud computing*: verso il terzo* Enclosures Movement?, in *Riv. crit. dir. priv.*, 2012, p. 363 ss.

LILLÀ MONTAGNANI M., *Primi orientamenti in materia di responsabilità dei fornitori di servizi* cloud *per violazione del diritto d'autore in rete*, in *Riv. dir. ind.*, I, 2014, p. 177 ss.

LÓPEZ JIMÉNEZ D., *La "computación en la nube" o "cloud computing" examinada desde el ordenamiento jurídico español*, in *Rev. de Derecho de la Pontificia Universidad Católica de Valparaíso XL*, 2013, p. 694 ss.

MANTELERO A., *Il contratto per l'erogazione alle imprese di servizi di* cloud computing, in *Contr. impr.*, 2012, p. 1216 ss; ID, *Processi di outsourcing informatico e* cloud computing*: la gestione dei dati personali ed aziendali*, in *Dir. inf.*, 2010, pp. 673 ss.

MANTOVANI F., *Mezzi di diffusione e tutela dei diritti umani*, in *Arch. giur.*, 1968, p. 390.

MELL-T. GRANCE P., *The NIST Definition of Cloud Computing*, 2011, disponibile al sito *Internet* «http://esre.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

MESSINA M., *La Corte di Giustizia UE si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità*, in *Ordine internazionale e diritti umani*, 2014, p. 396 ss.

MESSINETTI D*., voce* Personalità *(diritti della)*, in *Enc. dir.*, XXXIII, Milano, 1983, p. 355; ID., *Circolazione dei dati personali e dispositivi di regolazione dei poteri individuali*, in *Riv. crit. dir. priv.*, 1999, p. 339;

MILETTI A., *La protezione dei dati nella rete tra* cloud computing *e diritto all'oblio: questioni di riservatezza e responsabilità*, in *Corti salernitane*, 2012, p. 259 ss.

MORTATI C., *Istituzioni di diritto pubblico*, II, 2ª ed., Padova, 1967.

MULA D., *Il contratto di fornitura di servizi* cloud, in AA.VV., Internet *e diritto civile*, a cura di C. Perlingieri e L. Ruggeri, Camerino-Napoli, 2015, p. 549 ss.

NOTO LA DIEGA G., *Il* cloud computing*. Alla ricerca del diritto perduto nel web 3.0*, in *Eur. dir. priv.*, 2014, p. 577 ss.

PALMIRANI M., MARTONI M., *Informatica giuridica per le relazioni aziendali*, Torino, 2012.

PARDOLESI R., *Dalla riservatezza alla protezione dei dati personali: una storia di evoluzione e discontinuità,* in ID. (a cura di), *Diritto alla riservatezza e circolazione dei dati personali*, Milano, 2003, p. 1 ss.

PERLINGIERI P., *La personalità umana nell'ordinamento giuridico,* Camerino-Napoli, 1972; ID., *L'interpretazione della legge come sistematica ed assiologica. Il broccardo* in claris non fit interpretatio*, il ruolo dell'art. 12 disp. prel. c.c. e la nuova scuola dell'esegesi*, (1985), in ID., *Scuole tendenze e metodi. Problemi del diritto civile*, Napoli, 1989; ID., *La persona e i suoi diritti - Problemi del diritto civile*,

Napoli, 2005; ID., *Complessità e unitarietà dell'ordinamento giuridico vigente,* in *Rass. dir. civ.*, 2005, p. 188 ss.; ID., *Il diritto civile nella legalità costituzionale secondo il sistema italo-comunitario delle fonti*, Napoli, 2006; ID., *La contrattazione tra imprese*, in *Riv. dir. impr.*, 2006, 3, p. 330 ss.; ID., *Fonti del diritto e "ordinamento del caso concreto"*, in *Riv. dir. priv.*, 2010, p. 7 ss.; ID., *Il diritto privato europeo tra riduzionismo economico e dignità della persona*, in *Eur. dir. priv.*, 2010, p. 345 ss.

PIZZETTI F., *Dati e diritti nell'epoca della comunicazione elettronica*, in ID., *Il caso del diritto d'autore*, 2ª ed., Torino, 2013; ID., *Uomini e dati. Evoluzione tecnologica e diritto alla riservatezza*, in *Foro it.*, 2011, V, c. 230.

POIER S., *As blurred as a cloud. Preliminary notes questioning some social-legal aspects of cloud computing*, in *Cib. dir.*, 2010, p. 319 ss.

PROSPERETTI E., *Gli obblighi di assicurare la custodia e la sicurezza dei dati in un sistema* cloud, in G. Cassano (a cura di), *Trattato di diritto dell'*internet, Padova, 2012, p. 680 ss.

RAVÀ A., *Istituzioni di diritto privato,* Padova, 1938.

RENGIFO GARCÍA E., *Computaciòn en la nube*, in *Revista la propiedad inmaterial*, 17, 2013.

RESCIGNO P., voce *Personalità (diritti della)*, in *Enc. giur.*, XXIV, Roma, 1991.

RICCI A., *L'*outsourcing *e* cloud computing, in G. FINOCCHIARO e F. DELFINI, *Diritto dell'informatica*, Torino, 2014, p. 664 ss.

RODOTÀ S., *La* «privacy» *tra individuo e collettività*, in *Politica del diritto,* 1974, p. 545; ID., *Repertorio di fine secolo*, Bari, 1992; ID., *Tecnologie e diritti*, Bologna, 1995; ID., *Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali*, in *Riv. crit. dir. priv.*, 1997; ID., *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione*, Roma-Bari, 1997; ID., *Verso una Dichiarazione dei diritti di Internet*, in www.camera.it.

ROTENBERG M., *Diritti e libertà civili nell'era tecnologica: social network, Facebook, body scanning, cloud computing, geotagging e behavioral privacy*, in *Cib. dir*, 2010, Vol. 11, n. 1, p. 173 ss.

RUGGERI L., *I Domain names*, *Manuale di diritto dell'informatica*, 3ª ed., a cura di D. Valentino, Napoli, 2016, p. 81 ss.

SARZANA C., *Nuove applicazioni informatiche: ido e cloud computing – nuovi problemi per la sicurezza, la privacy, l'ambiente ed il diritto*, in *www.diritto.it.*

SCODITTI E., *Il diritto dei contratti fra costruzione giuridica e interpretazione adeguatrice,* in *Foro it.*, 2014, I, c. 2036;

STAZI A., MULA D., *Titolarità e contitolarità dei diritti IP nei sistemi di* crowdsourcing, open source *e* cloud computing, in *Dir. ind.*, p. 149 ss.

TOSI E., *Natura e qualificazione dei contratti di fornitura di sistemi informatici*, in *Dir. inf.*, 1995, II, p. 386 e ss.

TROIANO G., *Profili civili e penali del* cloud computing *nell'ordinamento giuridico nazionale: alla ricerca di un equilibrio tra diritti dell'utente e doveri del fornitore*, in *Cib. dir.*, 2011, Vol. 12, n. 3, p. 233; ID., *La conservazione dei documenti in* cloud computing, *ivi*, 2013, p. 265 ss.

UBERTAZZI B., *Il regolamento Roma I sulla legge applicabile alle obbligazioni contrattuali,* Milano, 2008, p. 121 ss.

UBERTAZZI T. M., *Sul bilanciamento tra libertà di espressione e* privacy, in *Danno resp.*, 4, 2004, p. 386 ss.

VALENTINO D., *Obblighi di informazione, contenuto e forma negoziale*, Napoli, 1999. ID., *La fornitura di servizi informatici e l'informatizzazione delle imprese*, in ID. (a cura di), *Manuale di diritto dell'informatica*, 3ª ed., Napoli, p. 235-263;

WARREN S.D., BRANDEIS L.D., *The right of privacy,* in *Harv. L. Rev.*, 1890, p. 193 ss.

ZALLONE R., *Informatica e telematica: i nuovi contratti di servizi*, in *Diritto delle nuove tecnologie*, collana diretta da V. Franceschelli e E. Tosi, Milano, 2003, p. 63 ss.

ZENO-ZENCOVICH V., *Onore e reputazione nel sistema del diritto civile*, Napoli, 1985; ID., voce *Personalità (diritti della)*, in *Dig. disc. priv., sez. civ.*, XII, Torino, 1995, p. 456; ID., voce *Onore e reputazione*, in *Dig. disc. priv., sez. civ.*, XIII, Torino, 1995, p. 91; ID., *I diritti della personalità dopo la legge sulla tutela dei dati personali*, in *Studium Juris*, 1997, p. 466 ss.

GIURISPRUDENZA.

CORTE EUROPEA DEI DIRITTI DELL'UOMO (CEDU)

Corte EDU, 2 agosto 1984, n. 8691/79, Malone c. Regno Unito; Corte EDU, 3 aprile 2007, C-62617/00, Copland c. Regno Unito

Corte EDU, 6 settembre 1978, n. 5029/71, Klass e a. c. Germania; Corte EDU, 2 settembre 2010, n. 35623/05, Uzun c. Germania

Corte EDU, 11 luglio 1985, n. 9248/81, Leander c. Svezia; Corte EDU, 4 dicembre 2008, n. 30562/04, S. e Marper c. Regno Unito

Corte EDU, 17 luglio 2008, n. 20511/03, I. c. Finlandia

Corte EDU, 2 dicembre 2008, n. 2872/02, K.U. c. Finlandia

Corte EDU, 7 febbraio 2012, nn. 40660/08 e 60641/08, *Von Hannover c. Germania (n. 2)*

Corte EDU, 10 maggio 2011, *Mosley c. Regno Unito*, n. 48009/08

Corte EDU, 16 luglio 2013, Rc. n. 33846/2007, *Wegrzybowski e Smolczewski c. Polonia*

CORTE DI GIUSTIZIA DELL' UNIONE EUROPEA (CGUE)

Corte giust., 6 novembre 2003, c. 101/01, Göta hovrätt (Svezia) c. Bodil Lindqvist, in *www.curia.eu*.

Corte giust., 16 dicembre 2008, c. 73/07, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy e Satamedia Oy, punti 56, 61 e 62, in *www.curia.eu*.

Corte giust., 9 novembre 2010, cause riunite C-92/09 e C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert/Land Hessen, in *www.curia.eu*

Corte giust., 13 maggio 2014, C-131/12, Google Spain SL, Google Inc./Agencia Española de Protección de Datos, Mario Costeja González, in *www.curia.eu*

Corte giust., 8 aprile 2014, cause riunite C-293/12 e C-594/12, Digital Rights Ireland e Seitlinger e a., in *www.curia.eu*

Corte giust., 6 ottobre 2015, C-362/14, Maximillian Schrems c. Data Protection Commissioner, in *www.curia.eu*

Corte giust., 15 marzo 2017, C-536/15, Tele2 (Netherlands) BV, Ziggo BV e Vodafone Libertel BV c. Autoriteit Consument en Markt (ACM), in *www.curia.eu*

SUPREMA CORTE DI CASSAZIONE

Cass., 27 maggio 1975 n. 2129, in *Foro it.*, 1976, I, c. 2895

Cass., 25 maggio, 2000, 6877, in *Danno e resp.*, 2000, p. 974, con nota di CASSANO

Cass., 25 giugno 2004, n. 11864, in *Foro it.*, 2004, I, c. 3380, con nota di A. PALMIERI

Cass., 20 febbraio 2006, n. 3651, in *Foro it.*, 2006, I, c. 2801, con nota di LAGHEZZA

Cass., 27 ottobre 2006, n. 23273, in *Rep. Foro it.*, 2006, voce *Contratto in genere*, 1740, n. 491

Cass., 15 febbraio 2007, n. 3462, in *Rep. Foro it.*, 2007, voce *Contratto in genere*, 1740, n. 560

Cass. pen., 05 marzo 2008, n. 16145, in *Corr. giur.*, 2008, 9, p. 1228, con nota di S. SICA

Cass. pen., 24 aprile 2008, n. 23086, in CED *on line*, 2008

Cass., 24 aprile 2008, n. 10690, in *Nuova giur. civ.*, 2008, I, p. 1309, con nota di ANZANI

Cass., 4 gennaio 2011, n. 186, in *Foro it.*, 2011, I, c. 1128

Cass., 05 aprile 2012, n. 5525, in *Foro it.*, 2013, I, c. 305

Cass., 01 settembre 2015, n. 17399, in *CED on line*, 2015

TRIBUNAL SUPREMO DE ESPAÑA

Tribunal Supremo, Sala de lo Civil, Pleno, *Sentencia núm*. 91/2017, in Instituto del Derecho Iberoamericano (Idibe).

GIURISPRUDENZA DI MERITO ITALIANA

Trib. Napoli, 15 luglio 2014, n. 12749, in *Foro nap.*, 2016, p. 153 ss., con nota di D'AMBROSIO

Trib. Roma, 03 dicembre 2015, n. 23771, in *Utet on line*

Trib. Napoli Nord, 10 agosto 2016, in *Rep. Foro it.*, 2016, *Merito extra*, n. 2016.1952.37

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 piú 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 tecnologia. 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: *Lindquist*, *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 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'àmbito 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 giocoforza 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. Departement 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 rapidely 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 define 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 lies in the current context of. Some fundamental judgments of European jurisprudence are reviewed (judgments: *Lindquist*, *Costeja*, *Scherm*s) 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 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 interfere 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 constumer and provider.