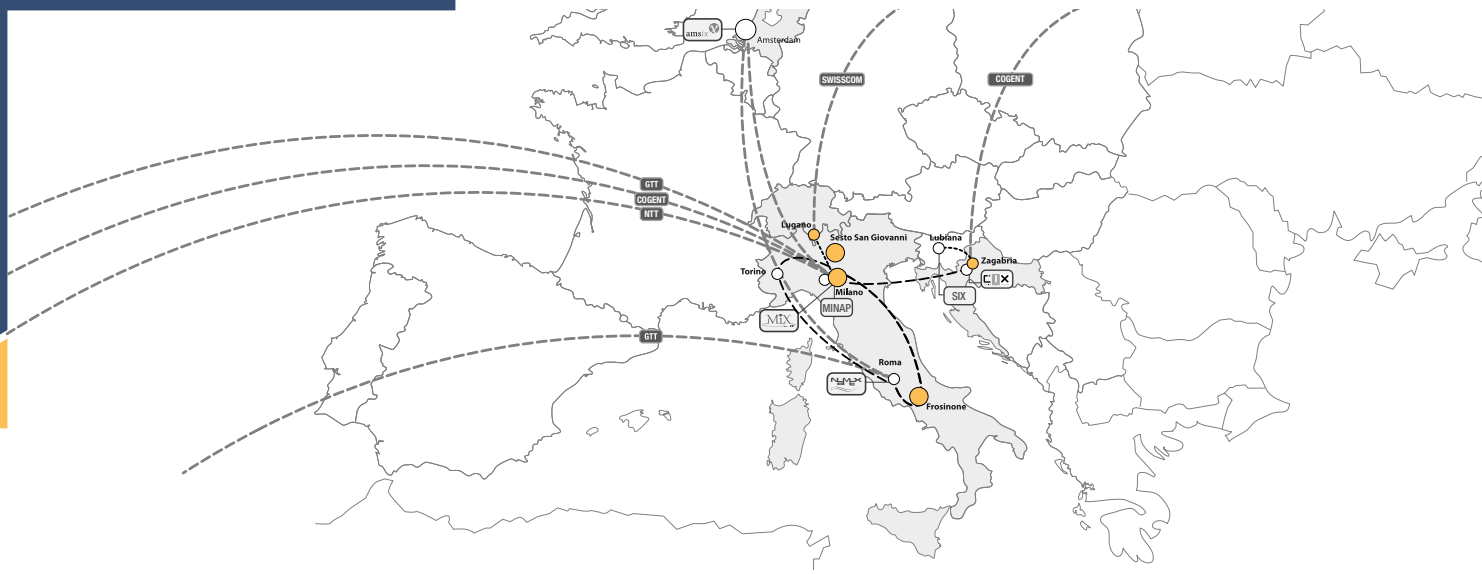
LA RAGGIUNGIBILITÀ GIURIDICA DEI DATI

Il cloud: rischi e regole di condotta nell'affidare i dati alla nuvola informatica

Ricerca a cura di:
Innocenzo Genna
Eugenio Prosperetti

hanno collaborato:
Giulio Pascali
Davide Tuzzolino

sponsored by DOMINION HOSTING HOLDING



Prefazione

Oggi si parla moltissimo dei dati: sappiamo come raccoglierli, usarli, derivarne di nuovi, aumentando l'efficienza delle aziende, migliorando i processi.

Ma cosa c'è dietro di essi? Dietro i dati ci sono le persone, le imprese e le responsabilità di chi è chiamato a ospitarli e gestirli: gli operatori dei servizi cloud.

Da sempre Seeweb è particolarmente sensibile a una gestione del dato in linea con i criteri europei di attenzione alla privacy, sempre più cruciale nell'era del multicloud di cui si parla molto come soluzione a problemi tecnologici o di lock-in. Appaiono invece meno chiare le implicazioni sulla protezione e sulla riservatezza dei dati a seguito dell'adozione del paradigma multicloud: sono tutti uguali i fornitori da questo punto di vista? Sono davvero intercambiabili con serenità e con la stessa facilità con la quale lo si fa a livello tecnologico? La risposta è no, i rischi sono complessi e non possono essere ignorati.

Oggi tutti i cloud provider si autopromuovono come porti sicuri per i dati dei loro clienti, ma c'è un tema rilevante: in un contesto globale che vede più della metà delle aziende e le organizzazioni europee adottare sistemi cloud USA (indipendentemente da dove poi siano collocati i data center) per ospitare i propri dati strategici, cosa dobbiamo sapere?

Il Privacy Shield è stato invalidato il 16 luglio 2020, quando la Corte di giustizia europea ha dichiarato inadeguata la protezione dei dati personali offerta dal regime dello scudo UE-USA. Alla luce del GDPR, non sembrano esserci garanzie adeguate a tutela dei dati europei in relazione ai programmi di sorveglianza del governo americano (si pensi al datagate e alle attività di indagine e intelligence svolte dall'agenzia governativa NSA). Da allora il trasferimento di dati verso operatori soggetti al diritto americano avviene sotto la responsabilità di chi la attua in uno scenario nel quale l'Europa la ritiene illegittima.

Grazie al lavoro degli esperti Eugenio Prosperetti e Innocenzo Genna, questo white paper approfondisce un tema complesso, pone quesiti e offre risposte, consente al lettore di conoscere scenari, rischi ed evoluzioni laddove si decida di affidare il proprio patrimonio informativo aziendale a player non europei. Lo studio affronta anche il tema inedito della "raggiungibilità giuridica" dei dati, che permane anche ove i data center del provider statunitense siano collocati in un qualsiasi stato dell'Unione Europea.

Antonio Baldassarra
CEO Seeweb

La Raggiungibilità Giuridica dei Dati

Il cloud: rischi e regole di condotta nell'affidare i dati alla nuvola informatica

Ricerca a cura di:
Innocenzo Genna
Eugenio Prosperetti

Hanno collaborato:
Giulio Pascali
Davide Tuzzolino

Il tema oggetto del presente Studio è quello della c.d. "raggiungibilità giuridica" dei dati.

La nozione giuridica di "raggiungibilità" è stata recentemente introdotta per indicare la possibilità per un soggetto di accedere e disporre, in maniera legittima, di dati memorizzati in un sistema cloud. Si tratta però di una nozione che può declinarsi a vari livelli: da un lato, esiste una "raggiungibilità" per l'utente originario titolare dei dati, così anche per coloro che eventualmente acquistano determinati diritti nell'ambito del servizio cloud; dall'altro lato, a questi soggetti si aggiunge un'ulteriore forma di "raggiungibilità" dei dati ad opera di entità - tipicamente istituzioni governative o autorità pubbliche - che, nell'esercizio delle proprie funzioni, potrebbero avere interesse ad accedere ai dati che si trovano in un cloud.

Infatti i dati, una volta esternalizzati, diventano "raggiungibili" in forza di un complesso coacervo di norme giuridiche provenienti da fonti diversificate (internazionali, europee e nazionali) e di disposizioni contrattuali, il cui peso complessivo e la cui articolazione non sono indifferenti per la strategia cloud di qualsiasi organizzazione, che sia cloud provider o cliente.

Il tema della "raggiungibilità giuridica" è teso così a valutare, nel concreto, l'accessibilità e disponibilità dei dati in un contesto di economia globalizzata, al fine di valutare il rischio derivante dalla possibilità che autorità governative estere, anche extra-europee, possano accedere oppure interdire l'accesso a dati immessi in cloud in forza di poteri autoritativi, o, financo, ordinarne la distruzione ad esempio a seguito di un embargo o per ragioni di sicurezza nazionale.

Lo Studio tiene in particolare considerazione il ruolo degli operatori USA nel settore europeo del cloud, sia per via della preponderante quota di mercato detenuta dagli stessi in Europa1[1], sia per via delle recenti implicazioni nate con l'annullamento del regime del Privacy Shield da parte della Corte Europea di giustizia.

1 Tra i dati più recenti, si veda Synergy Research Group, Primo trimestre 2020,
http://www.globenewswire.com/NewsRoom/AttachmentNg/5d1edd1e-dc3c-4847-9fc0-23a5e0eb20d5/en

Sintesi della ricerca

Quando i dati immessi nella nuvola rivestano particolare importanza, ad esempio se si tratta di dati personali oppure di dati aziendali o di rilevanza economica, la scelta del cloud provider deve essere attentamente ponderata. Non si tratta semplicemente di valutare l'offerta economica e tecnologica proposta dall'operatore, ma anche di considerare la sorte che i dati affidati in cloud possano avere a fronte di provvedimenti coercitivi da parte di autorità governative o giudiziarie, che ne potrebbero sancire l'accesso, l'interdizione o financo la distruzione. Si tratta del tema della raggiungibilità dei dati in ambiente cloud, oggetto del presente Studio.

Per effettuare tale valutazione, occorre tenere conto del sistema giuridico che sovrintende nel suo complesso il trattamento e l'accessibilità dei dati oggetto del contratto di cloud. In un contesto puramente europeo, cioè con cloud provider e server all'interno della UE, i dati di un cittadino o di una impresa europea appaiono sostanzialmente al sicuro grazie alle robuste garanzie fornite dalla legislazione dell'Unione, in primis il GDPR.

Ma occorre anche considerare la nazionalità del cloud provider, poiché questa può comportare la giurisdizione di paesi terzi e non europei che possono ritenersi autorizzati ad intervenire sulle proprie aziende, anche con riferimento a dati di cittadini europei da esse custoditi in server localizzati in Europa; pertanto la collocazione fisica dei server non attenua le cogenze derivanti dalla nazionalità del cloud provider. La fattispecie maggiormente diffusa, quella cioè del cloud provider di nazionalità statunitense, richiede di valutare l'applicabilità della legislazione USA, ed in particolare il Cloud Act, che può variare a seconda degli accordi assunti con i vari Stati europei. Con altre nazionalità e con paesi la cui normativa appare molto distante da quella europea, ad esempio la Cina come altri paesi dell'Asia, il caso appare ancora più complesso e delicato, per cui la raggiungibilità dei dati affidati in cloud deve essere attentamente valutata.

La preliminare valutazione della normativa e della giurisdizione applicabili costituisce dunque un passaggio necessario ed irrinunciabile, accanto alle considerazioni economiche e tecnologiche. Le incertezze ed in rischi risultanti da tale valutazione possono peraltro essere compensati dalla predisposizione di modelli contrattuali e policy che disciplinino in anticipo ed in dettaglio il comportamento che il cloud provider deve tenere nel caso di provvedimenti di autorità di paesi terzi, con riferimento all'accessibilità ed alla conservazione dei dati.

INDICE

Capitolo 3- Il contesto giuridico che regola la raggiungibilità del dato nel cloud

Capitolo 4 - L'intervento delle autorità pubbliche sulla raggiungibilità del dato

Capitolo 5 - Conclusioni

CAPITOLO I
IL CLOUD ED I DATI

1.1. Definizione, modelli e diffusione dei servizi cloud

Definizione di cloud

Non esiste una definizione univoca, in linguaggio giuridico, tecnico o commerciale, di cloud o, come si usa dire in italiano, di "nuvola informatica". Infatti, la capacità del cloud di adattarsi in modo elastico alle esigenze del mercato suggerisce di utilizzare una nozione flessibile e la più onnicomprensiva possibile, pur con il rischio di qualche inesattezza.

Data questa premessa, il cloud può essere definito in prima battuta come una rete di server, ubicati ovunque e collegati tra loro, che lavorando come un unico ecosistema permettono di svolgere in modalità scalabile ed elastica una vasta serie di attività che, altrimenti, andrebbero eseguite con proprie e locali risorse hardware e software. Si tratta di attività quali, ad esempio, archiviare e gestire dati, eseguire applicazioni, fornire potenza di calcolo, distribuire contenuti o servizi tra cui video in streaming, posta elettronica Web, software o piattaforme di social media. Il cloud abilita inoltre attività che non potrebbero affatto essere eseguite in locale come, ad esempio, il lavoro condiviso sulla medesima piattaforma da luoghi diversi e l'accesso, con elaboratori di relativa potenza e piccole dimensioni ed anche in mobilità, a grandissime basi dati, potenti risorse di elaborazione e sistemi di intelligenza artificiale.

In coerenza con quanto sopra, l'Agenzia per l'Italia digitale (AgID), definisce il cloud come *"un modello di infrastrutture informatiche che consente di disporre, tramite internet, di un insieme di risorse di calcolo (ad es. reti, server, storage, applicazioni e servizi) che possono essere rapidamente erogate come un servizio. Questo modello consente di semplificare drasticamente la gestione dei sistemi informativi, trasformando le infrastrutture fisiche in servizi virtuali fruibili in base al consumo di risorse"*.[2]

La nozione di cloud appare ancor più chiara sottolineando i vantaggi che derivano dall'utilizzo di tale modello informatico ed organizzativo rispetto alle tradizionali soluzioni hardware. Il cloud infatti permette:

- accesso ad applicazioni da qualsiasi dispositivo ed in qualsiasi luogo, tramite Internet o connettività dedicata;
- rilevanti risparmi nell'utilizzo del software, grazie alla possibilità di pagare le risorse cloud in modalità "pay per use", cioè in base al consumo, con ciò evitando gli elevati investimenti fissi iniziali legati all'acquisto dell'infrastruttura ed alle licenze;
- riduzione dei costi relativi ai data center (affitto, consumi elettrici, manutenzione e pulizia, sicurezza, backup);
- maggiore flessibilità e minori costi nel testare nuovi servizi o apportarvi modifiche;
- aggiornamento continuo dell'infrastruttura e delle applicazioni;
- maggiore sicurezza.[3]

Modelli di cloud

All'interno della definizione complessiva di cloud possono essere ricondotti vari modelli, in funzione della distribuzione delle risorse cloud prescelta dalle aziende oppure delle macro-tipologie di servizi che possono essere forniti. Tali suddivisioni, per quanto tecnicamente complesse, riflettono comunque sempre il concetto di base, che identifica il cloud con una rete di server remoti i cui vari servizi sono accessibili tramite reti telematiche, che possono essere gestiti ed offerti sul mercato da attori e fornitori differenti e forniti su base contrattuale.

2 Definizione di cui a https://cloud.italia.it .
3 Una gestione dei dati in cloud può offrire la possibilità di ospitare i dati in infrastrutture con livelli di sicurezza altrimenti inaccessibili a piccole e medie imprese imprese/studi professionali, e gestita da personale specializzato.

Per quanto riguarda l'infrastruttura e la distribuzione delle risorse cloud, il mercato identifica al momento 4 modelli organizzativi principali:

- Il cloud pubblico, che opera attraverso la condivisione di risorse globali e offre servizi al pubblico tramite Internet o connettività dedicata;
- Il cloud privato, modello di cloud in cui i servizi sono offerti solo ad utenti previamente identificati e non al pubblico generale; può essere basato su server privati o su grandi server che vengono opportunamente configurati per separare le varie utenze cloud (normalmente utilizzando modelli Infrastructure-as-a-Service e Platform-as-a-Service) o, ancora, offrire servizi su una rete interna privata che ospita le risorse in locale;
- Il cloud ibrido, che condivide servizi tra cloud pubblici e privati a seconda dello scopo;
- Il community cloud, dove l'infrastruttura cloud è predisposta per fornire servizi cloud ad una specifica comunità di organizzazioni che hanno requisiti e obiettivi condivisi.

Dal punto di vista dei servizi usufruibili attraverso il cloud, la prassi commerciale tende a distinguere 3 principali tipologie:

- Infrastructure-as-a-Service (IaaS), ovvero la fornitura di una infrastruttura tecnologica fisica in forma virtuale come il servizio di accesso (anche on-demand) a risorse informatiche quali reti, memoria e server da remoto mediante apposito software ed Application Programming Interfaces (API), in forma scalabile e senza la necessità di acquistare hardware e licenze;
- Platform-as-a-Service (PaaS), ovvero la fornitura in forma di servizio di un ambiente informatico per testare, sviluppare e gestire applicazioni;
- Software-as-a-Service (SaaS), e cioè servizi erogati tramite l'elaborazione di dati mediante applicazioni software installate ed eseguite sui server del cloud provider, ed accessibili tramite Internet sfruttando diverse tipologie di dispositivi (Desktop, Mobile, etc).

Le definizioni tecniche del modello cloud e le proprietà specifiche dei servizi possono essere consultate presso il NIST.[4]

Il cloud in Italia

In Italia i servizi cloud si sono diffusi in tempi abbastanza recenti. La diffusione è stata all'inizio condizionata da vari fattori quali, ad esempio, la dimensione delle aziende e le loro caratteristiche di crescita, la necessità o meno di disporre di dati distribuiti sul territorio, nonché dalla disponibilità di capacità informatiche interne. Il mercato è però ora in forte crescita, in parte anche in virtù della formidabile spinta venuta, nel 2020, dalla situazione di emergenza scaturita dalla pandemia da Covid-19, che ha richiesto ad aziende e collettività di riorganizzare in modalità "agile" attività e processi[5]. Alla fine del 2020, il 59% delle imprese italiane faceva uso di servizi di cloud computing.[6]

Secondo le stime dell'Osservatorio Cloud del Politecnico di Milano[7], nel 2020 il mercato cloud italiano ha raggiunto i 3,34 Miliardi di euro, in crescita del + 21% rispetto al consuntivo del 2019, pari a 2,77 Miliardi di euro. In termini di spesa assoluta i primi tre settori merceologici per rilevanza sono il Manifatturiero (24%), il settore Bancario (21%) ed il Telco/Media (15%).

I servizi cloud maggiormente diffusi in Italia sono i seguenti:

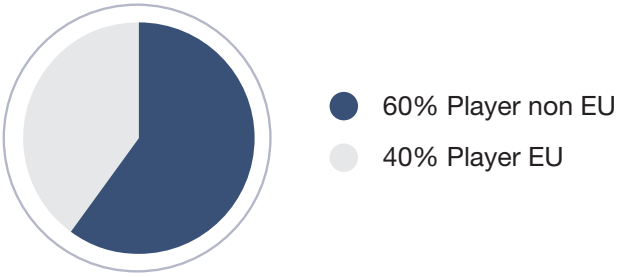
- IaaS: comprende servizi di cloud storage, cloud backup e sincronizzazione, website hosting, cloud drive, server virtuale, tra cui IBM Cloud, Google Cloud, Amazon AWS, Seeweb Cloud Server, Aruba, Irideos, ecc.

4 National Institute of Standards and Technology, US Department of Commerce; The Nist Definition of Cloud computing, Special Publication 800-145, settembre 2011. Disponibile al seguente link https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
5 Il "balzo in avanti" accaduto in Italia dovuto al Covid è ben rappresentato dalle statistiche Eurostat, Cloud computing - statistics on the use by enterprises, 19 gennaio 2021.
6 Dati Eurostat: Use of cloud computing services in enterprises, 2020.
7 Edizione 2019-2020 dell'Osservatorio Cloud Transformation dell'ottobre 2020; si veda il comunicato stampa accessibile al seguente link:https://www.osservatori.net/it/ricerche/comunicati-stampa/cloud-italia-mercato-2020

- servizi PaaS: si tratta di un mercato molto frammentato in cui operano, tra gli altri, Amazon, SAP, Google, Oracle, Microsoft ed IBM.
- servizi di elaborazione SaaS: comprende servizi estremamente diversificati tra cui caselle di posta elettronica, sistemi operativi (ad esempio GSuite e Office 365), servizi di fatturazione elettronica di provider quali Infocert, Aruba, gestionali per ufficio in cloud quali Zucchetti e Team System, ed inoltre servizi molto popolari quali Dropbox, Onedrive, SugarSync, Google Drive, ICloud solo per fare alcuni esempi

Secondo dati del Ministero dell'Innovazione, il 60% del mercato italiano del cloud è fornito da operatori non europei[8].

MERCATO CLOUD EUROPEO



Percentuale di utilizzo di operatori cloud europei e USA da dati del Ministero dell'innovazione

Il cloud e la pubblica amministrazione italiana

Il Piano Triennale per l'informatica nella Pubblica Amministrazione[9], adottato nell'ambito della "Strategia per la Crescita digitale del Paese"[10], ha previsto una strategia per l'adozione del cloud computing nella Pubblica Amministrazione che si articola attraverso 3 elementi principali:[11]

- il principio Cloud First secondo il quale le PA devono, in via prioritaria, adottare il paradigma cloud (in particolare i servizi SaaS) prima di qualsiasi altra opzione tecnologica tradizionale, normalmente basata su housing o hosting;
- il modello cloud della PA, cioè il modello strategico che si compone di infrastrutture e servizi qualificati da AgID sulla base di un insieme di requisiti volti a garantire elevati standard di qualità e sicurezza per la PA. In funzione di questo modello è stata creata un'apposita piattaforma, il Cloud Marketplace di AgID12[12], che consente di visualizzare la scheda di ogni servizio mettendo in evidenza le caratteristiche, il costo e i livelli di servizio dichiarati dal fornitore. Le PA possono così confrontare servizi analoghi e decidere, in base alle loro esigenze, le soluzioni più adatte.[13]
- Il programma di abilitazione al cloud (cloud enablement program), vale a dire l'insieme di attività, risorse, metodologie da mettere in campo per rendere le pubbliche amministrazioni capaci di migrare e mantenere in efficienza i propri servizi informatici (infrastrutture e applicazioni) all'interno del modello cloud della PA.

A decorrere dal 1° aprile 2019, le Amministrazioni Pubbliche possono acquisire esclusivamente servizi IaaS,

8 Intervento del Ministro Paola Pisano, al Summit Gaia-X online, 19 ottobre 2020, disponibile al seguente link qui: https://innovazione.gov.it/assets/docs/2020-11-19-intervento-ministra-pisano-a-gaia-x-summit.pdf
9 Adottato con DPCM del 17 luglio 2020 e disponibile al seguente link: https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_l_informatica_nella_pa_2020_2022.pdf
10 Versione adottata nel 2016, e seguito delle osservazioni della Commissione Europea, e disponibile al seguente link: https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf
11 I 3 elementi della strategia sono disponibili al seguente link: https://cloud.italia.it
12 Si vedano le Circolari AgID n. 2 e n.3 del 9 aprile 2018. Si veda anche: https://cloud.italia.it/marketplace/
13 Il Marketplace indica anche le modalità di acquisizione con cui uno specifico servizio potrà essere acquisito da una amministrazione rimandando allo strumento di procurement disponibile (il portale www.acquistinretepa.it) per procedere con l'acquisizione.

PaaS e SaaS qualificati da AgID e pubblicati nel Catalogo dei servizi cloud per la PA qualificati.

Dopo un'iniziale situazione di stallo dovuta alla difficoltà di gestire a livello individuale le complessità delle gare per questa tipologia "immateriale" di servizi, il mercato cloud della P.A. è decollato ed è attualmente caratterizzato dalla fornitura di servizi attraverso la gara CONSIP denominata "SPC Cloud". Tale modello di gara pubblica ha aggiudicato, come previsto dal Piano Triennale sopra citato, nella forma di contratti quadro ad adesione aperta ed obbligatoria da parte delle Pubbliche Amministrazioni, quattro "lotti" (categorie) di servizi cloud a favore della P.A.[14].

L'arrivo dei cloud provider globali, ed in particolare di quelli statunitensi, ha contributo alla crescita del mercato italiano ed all'automatizzazione dei processi della P.A. (così come dei privati). Attualmente tali operatori globali sono ben presenti nel panorama italiano dei servizi cloud, benché siano più attivi verso i privati che verso la P.A., in quanto la gara SPC comporta dei complessi vincoli contrattuali ed amministrativi specifici verso gli aggiudicatari dei lotti sopra citati. Tuttavia, anche nel mercato privato i cloud provider globali tendono ad adottare un modello che li vede affiancati a dei partner locali, in quanto i modelli contrattuali adottati da tali operatori internazionali sono fortemente standardizzati e difficilmente si adeguano ad oneri e condizioni locali, così come all'assunzione di rischi verso entità locali pubbliche o private (es. prestazione di fideiussioni, negoziazione di contratti specifici che prevedono diritti di verifica o obblighi di gestione dell'infrastruttura cloud ad hoc, penali, ecc.). I cloud provider globali preferiscono dunque essere "intermediati" e fornire un servizio standard, rimandando a contrattualizzazioni con un reseller locale eventuali specificità ed oneri richiesti dal singolo progetto.[15]

Va inoltre ricordato il recente Piano Nazionale di Ripresa e Resilienza[16] (c.d. Recovery Fund - Next Generation EU) in discussione al momento della stesura del presente lavoro, il quale prevede la creazione di un cloud italiano della Pubblica Amministrazione da svilupparsi in coerenza con il progetto UE "Gaia X". Il progetto prevede la sostituzione, in maniera organica, dei CED locali sul territorio, standardizzando e rendendo efficiente l'archiviazione ed elaborazione del patrimonio di dati della P.A. italiana.

1.2. Dati, informazioni e relative categorie

Ai fini del presente Studio, occorre chiarire cosa si intenda giuridicamente per "dati", termine che normalmente ricopre i segni, le parole e le immagini trasmessi attraverso dei bit, e se anche questi ultimi, i bit, abbiano una qualche rilevanza giuridica. Occorre inoltre stabilire se e per quali motivi i dati debbano essere distinti dalle informazioni.

I bit

I bit sono il risultato della conversione in impulsi elettromagnetici, tramite un codice binario, di dati intelligibili all'uomo. Il codice binario si fonda sull'utilizzo di due soli segni, lo 0 e l'1, corrispondenti a due stati elettrici, ai quali viene dato appunto il nome di bit, termine risultante dalla crasi di binary digit. Delle sequenze ordinate di bit permettono di visualizzare sul monitor dell'elaboratore delle rappresentazioni (segni grafici, foto o immagini in movimento).

Il valore giuridico dei bit è discutibile a seconda che lo si approcci nel campo dell'informatica (quindi come semplice cifra binaria) oppure nell'ambito della teoria dell'informazione (cioè come l'unità di misura definita della quantità minima di informazione). Ai fini del nostro Studio, i bit assumono valore giuridico solo nella mi-

14 Cfr. https://www.consip.it/attivita/gara-spc-cloud-disponibile-la-documentazione e siti tematici dei contratti quadro aggiudicati: lotto1: https://www.cloudspc.it/ lotto 2: https://www.spc-lotto2-sicurezza.it/ lotto 3: https://www.spclotto3.it lotto 4: https://www.spclotto4.it

15 Al di là dei menzionati compiti contrattuali verso la PA, il principale scopo di questi reseller locali è quello di fornire forza commerciale sul territorio ed assicurare l'integrazione dei servizi (sia cloud che altri). Tuttavia, può essere scarsa la possibilità per tali reseller, se di piccole dimensioni, di influire su policy, tecnologia e governance dei servizi cloud (ad esempio per quanto riguarda le policy di sicurezza, la distribuzione territoriale dei dati, la configurazione dei servizi), elementi che rimangono prevalentemente nelle mani dell'operatore globale. Si tratta di un aspetto da valutare caso per caso. Si nota peraltro, nel contesto nazionale, ad indicare la crescente importanza di realtà nazionali in grado di interloquire con i grandi operatori cloud (in questo caso Google), la recentissima costituzione della nuova società Noovle Spa dedicata alle attività di cloud enabling in cui è confluita la rete data center del gruppo Telecom. Italia.

16 Cfr. http://www.politicheeuropee.gov.it/it/comunicazione/approfondimenti/pnrr-approfondimento/

sura in cui arrivino, attraverso un sistema di codifica, a rappresentare idee o concetti che siano giuridicamente o economicamente rilevanti: in tal caso, parleremo più propriamente di dato o informazione. Il bit che non sia dotato di questa capacità di rappresentazione non è pertinente ai fini del presente Studio, benché possa sempre avere rilevanza giuridica per altri scopi (ad esempio, in tema di cybersecurity).

I dati

Il concetto di dato e la sua regolamentazione in diritto è fondamentale ai fini del nostro Studio, in quanto il concreto assetto contrattuale e regolamentare del rapporto di cloud è certamente influenzato dall'opinione su cosa costituisca un "dato" suscettibile di produrre effetti giuridici nell'ordinamento che regola il rapporto tra cliente e provider.

I dati sono delle rappresentazioni intellegibili all'uomo e possono essere definiti, in particolare, come "*rappresentazioni originarie, cioè non interpretate, di un fenomeno, evento, o fatto, effettuate attraverso simboli o combinazioni di simboli, o di qualsiasi altra forma espressiva legate a un qualsiasi supporto*"[17]. Tale capacità di rappresentazione deriva dalla codifica che permette di convertire - in caso di dati in formato elettronico - i bit in simboli, immagini e suoni.

I dati hanno una indubbia rilevanza giuridica ed economica ed in quanto tali sono oggetto di specifica protezione secondo discipline via via applicabili.

La principale disciplina che sancisce tali effetti giuridici è quella europea sul "documento elettronico", introdotta con il Regolamento (UE) 2014/910[18] (c.d. "Regolamento EIDAS"). In base all'art. 43 del regolamento non si possono negare effetti giuridici ai "dati" contenuti in un documento elettronico per il motivo della forma elettronica. Pertanto, un giudice non può rifiutarsi di tenere in considerazione i documenti elettronici ed i dati ivi contenuti, e ne deve esaminare il merito.

> *"Una notevole fetta del mercato cloud è in mano a grossi player USA: di qui la necessità di comprendere a fondo gli aspetti giuridici al di là della collocazione fisica dei loro data center"*

Il documento elettronico è definito dal regolamento europeo come: "*qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva*". Di conseguenza, ai sensi della normativa UE il tema della raggiungibilità riguarda quei dati che rispondono alla definizione di documento elettronico appena menzionata, in quanto possono essere oggetto di provvedimenti giuridici. A completamento del quadro normativo europeo, vanno anche ricordati il Regolamento 2016/679 sulla protezione dei dati personali (il c.d. GDPR) nonché la Direttiva 2016/680 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[19]; non vanno inoltre dimenticate le norme che regolano la proprietà intellettuale sui dati stessi e, come si dirà nei paragrafi successivi, le nuove previsioni riguardanti la circolazione, accesso e portabilità dei dati "non personali".

In ordinamenti extra-UE quali gli USA le definizioni di documento elettronico tendono ad essere più ampie e meno dettagliate. Ad esempio, negli USA lo Uniform Electronic Transactions Act (UETA) definisce "*Electronic record*" come "*a record created, generated, sent, communicated, received, or stored by electronic means*" indicando dunque qualsiasi possibile formato e contenuto.

In proposito, va però ricordato che negli USA non esiste una normativa federale avente ad oggetto la tutela dei "dati" o dei "dati personali" sulla base di un modello comparabile a quello europeo. La tutela è soprattutto indiretta, in quanto basata sulle norme a tutela dei consumatori, ad esempio mediante il Federal Trade Commission Act del 1914, ma vi sono anche leggi dei singoli stati (es. la California) a tutela dei dati personali. La conseguenza di ciò è che diversamente dalla UE, basata su di un sistema più rigido e garantistico, in USA la semplice raccolta dei dati, anche massiva, non è di regola soggetta ad autorizzazione preventiva (cioè al consenso del data subject), mentre ad essere regolato, caso per caso e in funzione del territorio in cui avviene,

17 Definizione tratta da http://www.dei.unipd.it/~dinunzio/fdi-2014-2015/04_dati_informazioni.pdf
18 Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, art. 3 comma
19 Cfr. capitolo 2 dello Studio.

è solamente l'uso dei dati.

Le informazioni

Il dato va distinto, in linea di principio, dall'informazione, in quanto l'informazione è il risultato di una particolare sequenza temporale e spaziale di dati che rende possibile un processo di interpretazione significativa per il destinatario - mentre non tutti i dati possono detenere tale "contenuto informativo" ma, come si è detto, sono giuridicamente rilevanti solo quelli che sono in grado di esprimerlo. Tuttavia, le discipline giuridiche si riferiscono prevalentemente al concetto di dato/informazione nel suo complesso, piuttosto che dare rilevanza alla distinzione tra i due concetti. Ad esempio, la Direttiva Open Data considera il dato come sinonimo di documento[20], mentre la recente proposta di Data Governance Act adotta anch'essa una definizione complessiva per cui il dato è definito come "*any digital representation of acts, facts or information*".[21] Anche il GDPR, riferendosi ai dati personali, sposa una definizione complessiva di dato ed informazione.[22] Pertanto, alla luce di quanto sopra, ai fini del nostro Studio non sarà necessario distinguere sistematicamente tra dato ed informazione, salvo quando ciò sia richiesto da circostanze specifiche. Quindi, quando si farà riferimento al concetto di "dati", si intenderanno anche i dati avente un contenuto informativo interpretabile, e cioè anche le informazioni.

Il termine informazione viene inoltre sovente utilizzato nel linguaggio giuridico in abbinamento a "confidenziali" o "riservate" per definire quella particolare tipologia di dati che fa parte del patrimonio aziendale e viene resa oggetto di particolari obblighi di confidenzialità nel corso di un rapporto contrattuale. In questo senso il termine "informazioni" indica sia dati personali che dati non personali e si riferisce alla univocità della titolarità/provenienza dell'insieme di dati.

Categorie di dati: personali e non personali

Benché il concetto di dato sia fortemente legato alla nozione di dato personale ai sensi del GDPR, trattandosi del corpus giuridico che per primo ne ha esaltato il valore giuridico in senso generale, questa non è l'unica accezione di dato rilevante ai fini del nostro Studio. I dati possono infatti anche essere non personali, cioè non associabili ad una persona identificata o identificabile in base ai dati stessi. Il regime e la circolazione dei dati non personali è oggetto, inter alia, della citata normativa di cui al Regolamento (UE) 2018/1807[23] che riguarda l'accessibilità e la portabilità dei dati non personali e che meglio si descriverà nel capitolo 4.

I dati non personali possono essere qualificati come segue:

(i) dati che già in origine non si riferiscono ad una persona fisica identificata o identificabile, ad esempio dati statistici, meteorologici, industriali o commerciali. Tra questi dati assumono una valenza importante i dati provenienti dai dispositivi e dalla robotica che costituiscono l'infrastruttura dell'Internet of Things (ad es.: dati di traffico; meteo) e quelli relativi alle aziende (dati commerciali come liste clienti, dati vendite e costi, segreti industriali non ancora oggetto di IP, know-how, testi contrattuali, codice sorgente, brevetti in corso di studio, ecc.);

(ii) dati che inizialmente erano dati personali, ma che poi sono stati resi anonimi in quanto sottoposti ad un processo di anonimizzazione;

(iii) dati misti, cioè un insieme di dati sia personali che non personali (ad esempio i dati di documenti fiscali o pubblici di un'impresa, che indicano nome ed altre informazioni sui dirigenti).

Il cloud non è infatti composto di soli dati personali ed in questo senso, nel corso dello Studio, ove appro-

20 Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019, articoli 1 e 2
21 Articolo 2 (1) della "Proposal for a Regulation of the European Parliament and of the Council on European data (Data Governance Act) {SEC(2020) 405 final}: "*data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording*;".
22 Articolo 4(1) del GDPR in relazione alla definizione di dato personale: "*«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)*"
23 Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea

priato si distingueranno "dati non personali e aziendali" da "dati personali", mentre con il termine "dati" senza ulteriore specificazione si intenderanno entrambi.

1.3. La "localizzazione" dei dati

Il concetto di localizzazione dei dati deve misurarsi con la natura immateriale degli stessi e, pertanto, non corrisponde al medesimo concetto utilizzato nell'ambito dei beni fisici. Nei confronti dei dati tale concetto deve tenere conto della loro natura composita: da un lato, la natura elettronica dei bit, dall'altro il software che permette di controllare tali bit e, in ultima analisi, di produrre, partendo dai bit, un risultato intellegibile per il destinatario (attraverso la codifica).

Localizzazione e bit

La natura elettronica dei bit complica il concetto classico di localizzazione. I bit infatti sono localizzati in dispositivi hardware collegati a dei server su cui sono installate le applicazioni e che svolgono le funzioni di calcolo ed elaborazione. Per ragioni di semplicità, tuttavia, si usa dire che i bit sono localizzati nei server ed anche questo Studio adotterà questa affermazione, pur sapendo che si tratta di una semplificazione.

I dati possono tuttavia essere frammentati (attraverso il c.d. *striping*) ed i relativi bit distribuiti attraverso vari server, che possono trovarsi in data center distinti e persino localizzati in differenti paesi (ad esempio per fornire un backup efficiente). Inoltre, per evitare problemi derivanti dal malfunzionamento di un singolo server, un cloud provider può scegliere di usare policy di ridondanza per cui il medesimo dato è allo stesso momento frammentato in più server, posti anche in differenti Paesi e dunque non si può esattamente determinare quale sia la sua esatta localizzazione. Allocazione e distribuzione dei bit/dati può inoltre variare nel corso del tempo, anche molte volte al giorno, all'ora o anche al minuto, per effetto di politiche di management del cloud provider. I data center ed i server possono appartenere anche ad operatori diversi rispetto al cloud provider, una pratica abbastanza comune per permettere l'elasticità del servizio cloud. La contrattualizzazione di tali fattispecie può essere complessa, andando dalla co-locazione presso data center esterni fino all'outsourcing vero e proprio.

> *"La localizzazione giuridica dei dati è un concetto fondamentale che regola il trasferimento dei dati. Oggi, se non in casi tassativamente definiti, con il GDPR i dati non possono essere trasferiti all'infuori della UE"*

Nonostante la complessità appena descritta, l'operatore cloud dovrebbe in qualsiasi momento essere sempre in grado, in principio, di sapere dove si trovano i dati, cioè in quali server sono distribuiti i relativi bit in un dato momento, poiché tale conoscenza è necessaria, ad esempio, per poter adempiere ad una richiesta giudiziaria. Tale conoscenza della localizzazione da parte dell'operatore non corrisponde però, generalmente, alla possibilità di tenere informato il proprio cliente su dove siano residenti i dati, se non in termini generali, indicando, ad esempio, la macro-area geografica in cui sono ubicati i server dove saranno gestiti i dati.

Localizzazione e software

La codifica ed i processi informatici che portano a risolvere degli impulsi elettrici in un contenuto intelligibile aggiungono un ulteriore livello di complessità. Colui che controlla il software necessario a governare tali processi e le regole di governance del sistema che ne gestisce la localizzazione e sicurezza è il reale dominus dei dati, ma può essere soggetto distinto dal cloud provider o dal proprietario dei server o, ancora, dalla parte con cui il titolare dei dati ha acceso un rapporto contrattuale (l'intermediario, il rivenditore, l'aggregatore, ecc.). Pertanto, il concetto di localizzazione non può prescindere dal tenere conto di questa complessità giuridica. Così, ai fini del GDPR il soggetto responsabile dei dati è il "titolare" (ed in subordine il "responsabile del trattamento"), mentre ai sensi della normativa sul commercio elettronico, il soggetto responsabile è colui che gestisce il sito o una piattaforma online e che quindi ha gli strumenti per effettuare la rimozione di contenuti dichiarati illegittimi. Pertanto, in alcune circostanze il controllo sui dati esercitato, attraverso dei programmi

software, da un cloud provider che fornisce un servizio SaaS può essere più penetrante, in termini di effettività, di quello del loro effettivo titolare, cioè il cliente[24].

La localizzazione giuridica dei dati

Il concetto di localizzazione dei dati è pertanto complesso e, ai fini giuridici, deve tener conto sia della localizzazione dei server, sia della localizzazione del soggetto che esercita il software che controlla i dati. La giurisdizione applicabile deve pertanto tenere conto di entrambi i fattori, a seconda dello scopo che si intende perseguire. In un giudizio di responsabilità appare determinante la localizzazione del titolare/controller, ma per eseguire un sequestro (ad esempio per bloccare un sito) diventa fondamentale anche il luogo dove si trovano i server e, prima ancora, la sede legale del responsabile del trattamento/processor incaricato di gestirli.

La localizzazione giuridica dei dati è inoltre un concetto fondamentale per le discipline che regolano il trasferimento dei dati. I dati soggetti all'ambito di applicazione del GDPR[25] non possono essere trasferiti all'infuori della UE se non in casi tassativamente definiti, mentre nel caso dei dati non personali il Regolamento 2018/1807 prevede che "*gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità*".

La cifratura

Nell'ambito dei processi che controllano i dati deve anche essere considerata la cifratura, cioè il processo che, attraverso l'utilizzo di chiavi private, mira a garantire la confidenzialità dei dati. Nell'ambito dei servizi cloud la crittografia è normalmente fornita per la trasmissione e lo storage dei dati, ma non per la fase di elaborazione e calcolo, che deve invece avvenire in chiaro perché il dato deve essere "a disposizione" di chi lo elabora (ad esempio per essere oggetto di arricchimento che lo renda idoneo ad alimentare un sistema di intelligenza artificiale).

La fornitura di una cifratura end-to-end è ancora in parte un processo complesso da gestire dal punto di vista tecnologico, ed inoltre inidonea a mettere in sicurezza la totalità delle fasi tecnologiche che riguardano i servizi cloud perché, come detto, alcune di esse prevedono proprio la condivisione dei dati tra cliente e cloud provider.

Peraltro, anche qualora i dati possano essere cifrati, non si può escludere l'accesso da parte di agenzie governative che possano imporre l'installazione di backdoor.

Il routing

Per completezza, e per gli aspetti di sicurezza dei dati che saranno analizzati nel presente Studio, occorre tenere conto del routing che attualmente avviene, in via prevalente, negli Stati Uniti.

24 Interessante la norma italiana prevista dall'art. 64 comma 2-quinquies del CAD (Codice dell'Amministrazione Digitale approvato con D.Lgs. 82/2005 successivamente modificato e integrato) che prevede l'esenzione di responsabilità derivanti dall'obbligo generale di sorveglianza per le attività sui propri siti laddove si preveda l'accesso con il sistema di identità digitale SPID. Ciò perché gli utenti sono in questo caso identificati con certezza e dunque le attività compiute su siti in hosting sono ascrivibili con certezza a utenti identificati e non ricadono in nessun caso sul hosting provider.
25 Art. 3 GDPR

CAPITOLO 2
PROPRIETÀ, TITOLARITÀ ED ALTRI DIRITTI SUI DATI

L'esame sulla raggiungibilità giuridica dei dati presuppone che si qualifichi la relazione giuridica che intercorre tra essi e coloro che sui medesimi vantano delle pretese. Tale relazione è argomento complesso e disciplinato da un articolato coacervo normativo. Focalizzando l'analisi ai fini del presente Studio, si tratta di stabilire se i dati, come definiti nel precedente capitolo, possano essere oggetto di diritti tipicamente qualificati (con i relativi corollari) ai sensi della normativa vigente, oppure se occorra ipotizzare delle nuove figure giuridiche.

2.1. I diritti sui dati

Proprietà, possesso e titolarità dei dati

Dal punto di vista giuridico si parla di "proprietà" nel momento in cui un soggetto (il proprietario, appunto) abbia il diritto di godere e disporre delle cose in modo pieno ed esclusivo, entro i limiti e con l'osservanza degli obblighi stabiliti dall'ordinamento giuridico[26].

Generalmente, possono essere oggetto di diritti i c.d. "beni"[27] che sono nella disponibilità del proprietario e dei quali egli può dunque disporre pienamente ed indiscriminatamente. In tale definizione non sembra possano rientrare a pieno titolo i bit, mentre è dato certo ed incontestabile che possano esserlo i dati e le informazioni con essi rappresentati. A dimostrazione di ciò si rileva - a titolo d'esempio - che proprio tali dati ed informazioni possono essere oggetto di diritti di proprietà intellettuale ed industriale[28], mentre non possano esserlo i bit, che sono in effetti un mero "veicolo" tramite il quale le informazioni ed i dati possono circolare. Non a caso, se un bit viene eliminato non è detto che l'informazione o il dato in esso codificati vengano per tale ragione a mancare, anzi è ragionevole presumere che essi esistano ancora, sebbene codificati in altro mezzo (informatico od analogico che possa essere).

Pertanto, è opportuno circoscrivere l'analisi ai fini del presente Studio ai soli dati o tutt'al più a dati ed informazioni, e con riferimento agli stessi esaminare la potenziale applicazione delle categorie generali di "titolarità", "controllo" o "possesso" ai fini della qualificazione giuridica dei vari soggetti che esercitano potestà e diritti.

Cominciando proprio dal "possesso", non sembra che la definizione dello stesso possa del tutto risolvere l'incertezza, in quanto trattasi di concetto eccessivamente generico, utile solo in parte per l'analisi che si sta svolgendo[29]. Quanto al "controllo", la definizione giuridica dello stesso ci porta fortemente fuori tema, e non sembra adeguata al contesto[30].

Per quanto riguarda la definizione di "titolarità", sebbene essa non sia propriamente oggetto di codifica normativa, si intende con la stessa - per unanime ricostruzione di giurisprudenza e dottrina, nonché per ricostruzione ex adverso dalle molteplici norme che vi fanno riferimento - sostanzialmente la particolare relazione di appartenenza che lega una situazione giuridica soggettiva al rispettivo soggetto di diritto[31]. Si vede dunque che la titolarità non necessariamente coincide con la proprietà e può sorgere a prescindere.

La definizione sembrerebbe, dunque, particolarmente adatta alla disciplina del bit, soprattutto se si considera

26 Così, infatti, dispone l'art. 832 del Codice civile, in una definizione rimasta sostanzialmente immutata dalla sua codificazione.
27 A mente dell'art. 810 del Codice civile, infatti, "sono beni le cose che possono formare oggetto di diritti".
28 Caso emblematico, con riferimento alle informazioni, è ad esempio rappresentato dalla tutela giuridica attribuita dall'ordinamento alle c.d. "Banche Dati", definite dall'art. 2, n.9 della L. 633/1941 come "*raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo*", e reputate degne di tutela da abusi di terzi in ragione del loro valore economico.
29 Ex art. 1140 del Codice civile, "*il possesso è il potere sulla cosa che si manifesta in un'attività corrispondente all'esercizio della proprietà o di altro diritto reale. Si può possedere direttamente o per mezzo di altra persona, che ha la detenzione della cosa*". Come è agevole notare, la definizione può forse giovare a ricostruzioni sul "possesso" di un bit da parte dei vari soggetti coinvolti, ma non aiuta del tutto a definire se chi possiede tali bit possa o debba esserne responsabile a monte.
30 Il "controllo" è infatti oggetto di molteplici definizioni normative, tutte però a tema squisitamente societario.
31 Senza voler qui scendere troppo nel dettaglio delle ricostruzioni giuridiche, l'etimologia stessa della parola spinge a considerare il "titolo" di un diritto, dunque l'atto o fatto giuridicamente rilevante, al ricorrere del quale un soggetto acquista il diritto medesimo (es.: per regola generale, ai sensi dell'art. 2 del Codice civile, una persona acquista la capacità di agire – e dunque di compiere con coscienza negozi giuridicamente rilevanti – non appena compiuti 18 anni).

che, in un campo decisamente complementare a quello dell'informatica giuridica come quello dell'energia elettrica, le varie normative disciplinano la "titolarità" degli impianti che la producono in capo a vari soggetti, che a loro volta ne rendono "disponibile" l'accesso e la fruizione ad altri, tramite sistemi di "connessione"[32]. Del pari, l'utilizzo del concetto di "titolarità", in rapporto al contenuto dei bit (sfruttando in tal senso anche la disciplina sul commercio elettronico[33] e quella sulla protezione dei dati personali) è di indubbio aiuto per l'identificazione delle responsabilità e dei ruoli dei vari soggetti coinvolti nello scambio, detenzione e controllo degli stessi.

In conclusione, ai fini dell'analisi in corso occorrerà considerare la peculiare relazione giuridica (rectius: le peculiari relazioni giuridiche) che intercorrono tra il titolare del dato, il cloud provider ed il dato stesso, una volta che questo viene trasferito all'interno di sistemi in cloud.

La titolarità dei dati nel cloud

Come si è scritto nei paragrafi che precedono, un dato può essere oggetto di titolarità da parte di un soggetto giuridico non appena si verificano le condizioni che la legge pone perché tale titolarità venga in essere. Tale titolarità, una volta sorta, può così tradursi in un diritto di proprietà sull'informazione contenuta nel dato stesso, ma non necessariamente implica l'esercizio di un diritto di medesima ampiezza sui bit che costituiscono il dato e sulle infinite possibili copie degli stessi, una volta che lo stesso è stato oggetto di digitalizzazione. Ciò emerge vieppiù con forza nel momento in cui il dato, codificato in bit, è oggetto di diffusione a terzi tramite sistemi in cloud: si pensi, ad esempio, alla diffusione di un file di testo online: il fatto che l'autore di tale testo ne sia titolare non comporta automaticamente che chiunque ne venga in possesso tramite una condivisione online ne diventi a sua volta "titolare", né - d'altra parte - che l'originario "titolare" abbia sempre e comunque il diritto di vietarne la diffusione. Può così anche esistere la situazione in cui il titolare delle "informazioni" rappresentate dai bit non sia il titolare materiale dei bit, intesi come contenitore, attraverso cui le informazioni circolano (es. una copia non autorizzata).

Il beneficiario della condivisione, a sua volta, potrà esserne tutt'al più un astratto "possessore", sino a che esso non faccia qualcosa di giuridicamente rilevante sul dato, tale da far sì che possa configurarsi a suo beneficio una autonoma titolarità dello stesso[34].

Diverso è, però, evidentemente il ruolo del fornitore tecnico che, grazie ai suoi sistemi, intermedia e consente la circolazione e condivisione del file e il passaggio dello stesso tra titolare e successivi possessori, vale a dire il cloud provider.

In proposito, è opportuno ricordare - tema che verrà meglio approfondito nei paragrafi che seguono - come il cloud sia un contratto di natura mista, e per tale sua natura abbia caratteristiche del tradizionale contratto di deposito, ma anche dell'appalto di servizi, del contratto di licenza e di quello di somministrazione[35]. Ciò rende particolarmente complessa non solo la sua disciplina (che dovrà necessariamente seguire una logica "caso per caso"), ma anche e soprattutto comporta estrema difficoltà nel disciplinare un rapporto giuridico spesso tra soggetti residenti in Stati differenti (e diversi sistemi giuridici).

Deve inoltre considerarsi con attenzione la tripartizione delle tipologie di manifestazioni del cloud (SaaS, IaaS e PaaS) già evidenziata al §1.1, ed operata in ragione delle loro finalità e funzionalità, che aggiunge un ulteriore livello di problematica, laddove ciascuna macrocategoria di fattispecie contrattuale presuppone differenti obblighi e regimi di responsabilità per il provider dei servizi[36].

---

32 Il D.lgs. 115/2008 e s.m.i., preposto alla definizione delle reti elettriche e dei sistemi semplici di produzione e consumo dell'energia stessa, parla infatti a più riprese di "titolarità" delle unità di produzione e di consumo di energia elettrica in capo a più soggetti giuridici.
33 Prima fra tutte la disciplina di cui al D.lgs. 70/2003 e s.m.i., attuazione della Direttiva 2000/31/CE sull'e-commerce.
34 Tale status giuridico è suffragato dalle innumerevoli norme Italiane ed internazionali in materia di opere derivate, che tutelano il creatore delle stesse, senza dimenticare perciò - perlomeno a livello morale se non addirittura sostanziale - i diritti delle opere originali dalle quali le stesse derivano.
35 Emblematico, sul punto, il dettato dell'art. 1677 del Codice civile, a mente del quale "*se l'appalto ha per oggetto prestazioni continuative o periodiche di servizi, si osservano, in quanto compatibili, le norme di questo capo [n.d.r.: cioè quelle dell'appalto] e quelle relative al contratto di somministrazione*".
36 Mentre, ad esempio, il provider di sistemi cloud in modalità SaaS offre servizi applicativi software e dovrà presumibilmente garantirne il corretto funzionamento, un provider cloud in modalità IaaS avrà, invece, perlomeno il diverso obbligo di mettere a disposizione dei propri clienti le sole risorse hardware virtualizzate.

Il cloud provider, peraltro, potrebbe non essere il solo soggetto coinvolto nel regime gestionale dei dati, in quanto tra esso e il proprio cliente possono potenzialmente trovare collocazione numerosi altri soggetti, a seconda della tipologia dei contenuti dei dati medesimi, della natura del cloud provider, della collocazione dei suoi server e molteplici altre variabili. A titolo d'esempio, nel rapporto tra il cloud provider e il cliente/titolare dei dati potrebbe subentrare il licenziatario della particolare tecnologia grazie alla quale il contenuto è stato creato, oppure - ipotesi non così avulsa dalla realtà come si potrebbe pensare - il creatore/licenziatario di una porzione di codice integrata in un contenuto memorizzato in cloud. Ancora: potrebbe frapporsi tra il titolare del dato e il cloud provider il fornitore di una specifica licenza proprietaria per un sistema di codifica dei dati, nel caso della violazione, della modifica o addirittura della cessazione della propria licenza.

> *"Tra cloud provider e cliente possono essere coinvolti nella gestione del dato svariati altri soggetti, a seconda della tipologia dei dati medesimi, della natura del cloud provider, della collocazione dei suoi server e altro".*

Il ruolo del software

Proseguendo proprio sul tema della tecnologia, impatta notevolmente sui regimi di responsabilità tra il titolare dei dati e il provider dei sistemi cloud anche la tipologia di software utilizzato nei sistemi cloud (preminentemente nei sistemi SaaS, ma non solo) e la licenza tramite la quale detto software viene utilizzato.

La maggior parte dei sistemi utilizzati per lo sviluppo, la gestione e l'allocazione dei bit relativi ai dati archiviati sul cloud sono, infatti, concessi sotto licenza proprietaria; ciò non toglie che esistano anche sistemi di content management service ed architetture di virtualizzazione in cloud progettati su licenze c.d. "open source". A seconda della tipologia di licenza dei software gestionali cloud, dunque, potrebbe variare il regime di gestione dei dati veicolati tramite gli stessi e, pertanto, anche le responsabilità del provider coinvolto. Su questo si dirà nel successivo paragrafo come le previsioni contrattuali possano e debbano giocare un ruolo determinante.

2.2. L'impatto del GDPR sulla disciplina contrattuale

La titolarità del dato tra cliente e cloud provider

Nell'ottica di meglio chiarire il concetto di "titolarità" del dato, quanto stabilito fino ad ora deve anche confrontarsi con la disciplina del GDPR, e della speculare Direttiva (UE) 2016/680, che si sovrappongono ed intersecano la disciplina strettamente contrattuale per assicurare la tutela dei dati personali e regolamentarne l'uso. Infatti, in virtù del GDPR, al contratto cloud si affianca, per quanto riguarda gli aspetti strettamente relativi alla gestione dei dati personali, un contratto di evidente natura atipica e mista, il c.d. Data Processing Agreement (DPA) espressamente previsto dalla vigente normativa a tutela dei dati personali. Tale contratto chiarisce ruoli e responsabilità, in particolare con riferimento alla ripartizione delle responsabilità tra il "Titolare del trattamento dei dati personali" e il c.d. "Responsabile (esterno) del trattamento dei dati personali" (dualismo che, in lingua inglese, è ancor più suggestivo, parlandosi, rispettivamente, di "Data Controller" e di "Data Processor"), che corrispondono rispettivamente al cliente del cloud provider che conferisce i dati ed il cloud provider che è chiamato a gestirli.

Tale distinzione di ruoli è fondamentale per delineare responsabilità ed obbligazioni che il cloud provider (tipicamente Responsabile del trattamento, cioè Processor) assume verso il cliente (tipicamente Titolare del trattamento, cioè Controller) in relazione al trattamento ed alla sicurezza dei dati immessi nel cloud[37].

37 La nozione di Responsabile del trattamento dei dati personali, originariamente riferibile a soggetti ed entità che trattano dati personali su incarico del Titolare e che potevano o meno essere presenti anche all'interno dell'organizzazione stessa del Titolare, è stata modificata a seguito del Parere 1/2010 - WP 169 dell'Art. 29 Working Party sui concetti di "responsabile del trattamento" e "incaricato del trattamento" (https://www.garanteprivacy.it/documents/10160/10704/wp169+-+Parere+1+2010+sui+concetti+di+responsabile+del+trattamento+e+incari.pdf/64cd4700-f0d4-4c04-b834-9c3da69a93ea?version=1.1), i cui concetti sono stati poi trasposti nel GDPR. Ad oggi, la nozione di Responsabile del Trattamento, definito all'art. 4, paragrafo 1, n.8) del GDPR come "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*", disciplina espressamente – unitamente a quanto all'art. 28 GDPR – il ruolo di un soggetto esclusivamente esterno all'organizzazione del Titolare.

Tuttavia, si osserva che la complessità organizzativa di alcune piattaforme cloud, specie delle più grandi, di regola porta verso la standardizzazione delle previsioni dei DPA, sicché il titolare viene chiamato a conferire al proprio neo-nominato "responsabile" un incarico basato su prescrizioni standard decise da quest'ultimo, e normalmente poco negoziabili, ritagliate sui servizi di gestione dei dati che vengono attivati.

La portata del GDPR non si limita tuttavia solamente di certo alla previsione della necessità di un DPA.

Sin dalle sue definizioni il GDPR contribuisce infatti a delineare alcuni fenomeni di importanza cruciale, non solo per quel che riguarda la tipologia dei dati che possono essere oggetto di condivisione e scambio, ma anche nella qualificazione stessa delle attività che possono essere poste in essere, con specifico riferimento a quella particolare tipologia di dati[38].

Come già evidenziato al §1.2. *supra*, la definizione stessa di "dato personale" codificata all'art. 4, n.1), del GDPR, espande in maniera esponenziale la dimensione operativa della tutela dei dati personali, andando per la prima volta in ambito europeo a ricomprendervi "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*". Com'è agevole notare, si tratta di una definizione ampia, quasi sproporzionata rispetto all'ambito del regolamento, della quale non può non tenersi conto anche al di fuori del novero applicativo dello stesso.

La definizione delle attività di "trattamento" al n.2) del medesimo articolo 4 completa il cerchio, andando a ricomprendervi "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*". Tali definizioni impongono di considerare attentamente qualsiasi attività svolta nei confronti di dati potenzialmente personali, in locale od in cloud che esse siano realizzate, proprio perché trattasi di attività a loro volta potenzialmente rientranti nel novero del concetto di "trattamento".

Il GDPR, infatti, prevede conseguentemente una serie di obblighi e di diritti in capo al Titolare del trattamento, il quale determina modalità e finalità di tali attività nei confronti del dato, diversi da quelli spettanti al Responsabile, il quale a propria volta effettua attività di trattamento dei dati su espresso mandato del Titolare, ed anzi conformandosi alle istruzioni che quest'ultimo gli fornisce[39]. Si tratta, a ben vedere, del conferimento della più ampia gamma di poteri in capo al Titolare, e ciò sembra in realtà in aperto contrasto con la disciplina contrattuale del cloud, laddove è in realtà il Responsabile, e cioè il cloud provider a "dettar legge" circa le condizioni alle quali conserva i file per conto del Titolare. È infatti il cloud provider a decidere le condizioni entro le quali il cliente può utilizzare i vari servizi acquistati, ed il cliente - salvi rari casi - non può far altro che conformarvisi, accettando spesso più di un DPA in proposito[40]. La conseguenza paradossale è che a livello contrattuale, ed in particolare nei termini e condizioni dei servizi cloud, si stabilisce un assetto di data protection in base al quale il cliente, che si assume Titolare del trattamento, va spesso a nominare il cloud provider prescelto quale suo Responsabile esterno, per le attività di espressa competenza, limitate in relazione ai Service Level Agreement (SLA) del caso.

Quel che è certo e comune alle due (evidentemente diverse, sebbene affini) situazioni, è però che solo il Titolare dei dati sia per legge l'unico soggetto che può compiere tutte le operazioni sui dati che siano proprie del

38 È opportuno sin d'ora precisare che, nonostante il GDPR faccia espressamente riferimento a specifiche tipologie di dati (delle quali si dirà a breve), esso fornisce una disciplina di carattere generale appropriata all'utilizzo per una gamma ben più ampia di generici "dati".

39 Questo assetto, previsto dall'interazione tra gli artt. 24 e 28 del GDPR, è in realtà delineato dalle stesse definizioni dei due soggetti, nn.7) ed 8) dell'art. 3 GDPR, ed è codificato come "*accountability*" (responsabilizzazione); esso si traduce in un maggior carico di responsabilità a carico del Titolare, che determina mezzi e modalità di trattamento a proprio integrale rischio e responsabilità), ma che può poi riversare responsabilità specifiche a carico del Responsabile esterno cui affida i dati, e su cui può poi rivalersi a livello contrattuale, in caso di inottemperanza.

40 Ai sensi dell'art. 28, comma 3, del GDPR, "*i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*." Tale specifico atto, i cui specifici contenuti sono ulteriormente disciplinati nel prosieguo del comma in questione, prende spesso le forme di un Data Processing Agreement, spesso in congiunzione alle clausole ed alle previsioni richieste per trattamenti extra-UE, in ossequio agli artt. 44-49 del GDPR in materia.

suo ruolo; e che egli ne sia effettivamente il solo responsabile, in punto di contenuto, demandando al cloud provider (suo Responsabile) un più limitato corpus di potestà circa i dati affidatigli, specificamente funzionale alla tipologia di servizio sottoscritto.

Il problema del trasferimento dei dati all'estero

Tra le previsioni fondamentali del GDPR, come noto, vi è il divieto[41] di trasferire dati personali al di fuori dell'Unione Europea in assenza di una decisione di adeguatezza della Commissione che certifichi che il Paese o organizzazione internazionale destinataria del trasferimento garantisce un livello adeguato di protezione dei dati personali in questione.

Ove mancasse la suddetta decisione di adeguatezza, il Regolamento consente al Titolare o al Responsabile del trattamento comunque il trasferimento solo in presenza di "garanzie adeguate" e tassativamente previste[42], tra le quali hanno particolare importanza, ai fini della presente trattazione, le c.d. "clausole contrattuali tipo" adottate dalla Commissione europea, le "norme vincolanti d'impresa" e, in subordine, le clausole contrattuali tra il Titolare del trattamento o il Responsabile del trattamento e le loro controparti (o il destinatario) nel Paese terzo dove devono essere trasferiti i dati.

Dal 16 luglio 2020, con riferimento ai trasferimenti verso gli USA, solamente il secondo ordine di strumenti è utilizzabile per effettuare i trasferimenti dei dati personali in cloud (e non), poiché con una dirompente sentenza (la c.d. decisione "Schrems II"), la Corte di Giustizia UE ha invalidato l'accordo di adeguatezza c.d. "Privacy Shield" che dal 2016 regolava e consentiva i trasferimenti di dati personali tra UE e USA, consentendo di trasferire i dati in regime analogo a quello del GDPR, senza dunque particolari formalità.

Il risultato pratico è che, dal luglio 2020 in poi, ogni trasferimento di dati personali verso gli USA, per essere effettuato legittimamente, deve essere assistito da una delle ulteriori garanzie previste dal GDPR che, inoltre, possono essere soggette a ulteriori specifiche da parte dell'European Data Protection Board (EPDB).

Gli ulteriori limiti imposti dal GDPR

Altro tema da non trascurare, sempre con specifico riferimento alla normativa sulla tutela dei dati personali, è quello della effettiva limitazione per legge degli utilizzi "automatizzati" e "per progettazione" dei dati personali: come noto, ai sensi dell'art. 25 del GDPR tutti i soggetti che trattano dati personali devono fare in modo che i loro sistemi di trattamento siano sin dalla loro progettazione strutturati per trattare solo i dati personali realmente necessari in relazione al servizio (c.d. "minimizzazione" o "privacy by design") e, ai sensi dell'art. 5 GDPR, trattino per impostazione predefinita i dati in maniera sicura e rispettosa dei diritti alla riservatezza (c.d. "privacy by default"). A tali obblighi si aggiunge l'oggettiva impossibilità, per un qualsivoglia Titolare o Responsabile del trattamento, di operare trattamenti basati esclusivamente su logiche automatizzate (primo fra tutti quello che porta alla profilazione degli interessati sulla base di specifiche informazioni ad essi pertinenti), in difetto dell'espresso consenso dell'interessato o di apposite previsioni di legge, di cui all'art. 22 GDPR[43]. I margini di operatività del cloud provider cui i dati vengono affidati dal Titolare incontrano, quindi, ulteriori restrizioni all'accesso ed all'utilizzo, delle quali non potrà non tenersi conto, nell'ambito dell'esame del regime delle responsabilità.

Va detto che tali limitazioni non sono assolute poiché il GDPR:

- riguarda solo i dati personali, e quindi restano fuori dal suo raggio d'azioni quelli non personali, tra cui quelle aziendali (di cui *supra*, § 1.2.);
- consente agli Stati membri dell'UE di introdurre limitazioni ove ritenute necessarie per conciliare la protezione dei dati personali con la libertà di informazione ed espressione (art. 85) o per ragioni relative ad esigenze di archiviazione (art. 89).
- consente altresì limitazioni alla sua efficacia ed applicazione per ragioni di sicurezza nazionale, difesa,

41 Il divieto in questione si ricava dall'art. 45 del GDPR
42 Si veda art. 46, commi 2 e 3, GDPR.
43 La norma è posta specificamente a tutela del diritto degli interessati a che i loro dati personali non siano sottoposti a trattamenti particolarmente "invasivi" della loro sfera personale, in quanto suscettibili di incidere in maniera significativa sulla stessa.

sicurezza pubblica e la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica (art. 23), purché necessarie e proporzionate in una società democratica e rispettose dell'essenza dei diritti e libertà fondamentali.

- oltre a tali specifiche disposizioni, all'art. 2§2 esclude interamente dal perimetro di applicazione le materie del controllo frontiere, asilo, immigrazione e la co-operazione tra forze di polizia e giudiziale sulle indagini criminali.

Si noti, inoltre, che per quanto invece attiene al trattamento dei dati personali in materia di prevenzione del crimine, investigazioni, indagini e procedimenti penali, esso è regolato non dal GDPR, ma dalla Direttiva 2016/680, trasposta in Italia dal D.Lgs. 51/2018. La differente impostazione tra le due normative lascia peraltro alcuni margini di intervento agli Stati: il GDPR non si applica ai casi di sicurezza nazionale, e neppure la Direttiva 2016/680 (salvo vi siano indagini su crimini o esigenze di prevenzione di minacce alla sicurezza).

In conclusione, gli Stati membri della UE mantengono un certo margine per intervenire sui dati personali quando vi siano esigenze di sicurezza nazionale, considerate a prescindere da una concreta minaccia. In tal caso il GDPR non offre protezione ai dati personali. Ovviamente i generali principi UE in tema di trasparenza dell'azione amministrativa e diritto al contraddittorio rimangono vigenti e, dunque, qualsiasi cessione ed uso dei dati non potrebbe avvenire in assenza di notifica all'interessato ma il consenso potrebbe in questi casi non essere elemento necessario affinché vi sia un accesso o una cessione dei dati personali.

CAPITOLO 3
IL CONTESTO GIURIDICO CHE REGOLA LA RAGGIUNGIBILITÀ DEL DATO NEL CLOUD

3.1 Il contratto cloud e la rilevanza della tipologia contrattuale

Avendo stabilito nel capitolo che precede la relazione che intercorre tra dati ed i loro titolari, alla luce sia del diritto civile che del GDPR, occorre ora analizzare come tale relazione giuridica si esplica nel contesto dei contratti che regolano il rapporto di "cloud".

La problematica generale: limiti ed effetti della "negoziabilità" del contratto di cloud

Il contratto con il quale vengono acquistati e forniti i servizi cloud è un aspetto fondamentale e dirimente per il tema della raggiungibilità giuridica del dato. Infatti, a seconda del tipo di contratto predisposto è possibile - nelle varie fattispecie che si presentano - confrontarsi con differenti assetti di disponibilità/accessibilità del dato tra cliente (cioè il titolare originario dei dati) e cloud provider che, a seconda del servizio reso, può (o meno), come si è detto, divenire anch'esso un titolare dei dati, ovvero limitarsi a elaborarli secondo le istruzioni ricevute, a volte in forma criptata ed inaccessibile.

Si tratta di un'analisi delicata perché, come accennato *supra*, il tipo di contratto che regola il rapporto è prevalentemente scelto dal provider di servizi cloud, mentre la capacità negoziale del cliente appare spesso limitata (quanto meno per la tipologia di contratto, mentre maggiore autonomia può esercitarsi per talune condizioni economiche e tecniche). Inoltre, i diversi ordinamenti in cui operano i vari cloud provider attivi in Europa (alcuni anche in più giurisdizioni) possono prevedere regole differenti per le varie tipologie contrattuali.

Il quadro risulta ulteriormente complicato dal fatto che il diritto internazionale permette di determinare convenzionalmente la legge contrattuale applicabile al contratto, per cui un atto sottoscritto in Italia potrebbe essere assoggettato, per volontà delle parti espressa in contratto, ad una legge di uno Stato terzo (ad esempio, secondo le fattispecie più diffuse, alle leggi del Regno Unito o dell'Irlanda del Nord, oppure persino di Stati federati degli USA quali New York, New Delaware o California). Nella prevalenza dei casi si tratta di discipline completamente diverse da quella italiana e, tranne rari casi, non note alle parti straniere che si trovano ad accettarle.

Le parti potrebbero inoltre stabilire (o, meglio, trovarsi a dover accettare) una giurisdizione ad hoc per eventuali controversie, con il risultato che eventuali azioni giudiziali verso il cloud provider dovrebbero essere giudicate da un tribunale extra-europeo (negli USA ad esempio) oppure via arbitrato internazionale, con costi ed oneri anche molto diversi da quelli che la parte sopporterebbe per una analogia controversia domestica.

Peraltro, anche nei casi in cui il contratto sia regolato dalla legge italiana e il foro delle liti rimanga in Italia, si osserva come il tema del cloud, ed in particolare le relative configurazioni contrattuali, non sia ancora consolidato presso molti tribunali italiani. La giurisprudenza (peraltro in permanente ritardo a causa dello storico arretrato degli uffici giudiziari) si è sino ad ora occupata per lo più di questioni relative a progettazioni software da eseguire in loco, mentre non si rinvengono sentenze recenti a livello nazionale che chiariscano gli aspetti fondamentali dei rapporti all'interno del contratto di cloud per i quali, dunque, ci si affida soprattutto all'elaborazione della dottrina giuridica.

Regolamentazione contrattuale ed impatto sulla raggiungibilità dei dati

Rispetto ad un iniziale fiorire di contratti "cloud" piuttosto generici e che non descrivevano gli aspetti caratterizzanti del servizio, ben presto si è compresa la necessità di una specificità di questa tipologia contrattuale.

È infatti particolarmente importante che il contratto per servizi cloud chiarisca gli aspetti fondamentali del rapporto tra cloud provider e cliente/titolare dei dati e, altresì, sia particolarmente esplicito quanto alla sua

qualificazione. Solo in tal modo si potranno determinare con facilità le regole applicabili alla fattispecie, soprattutto in relazione all'affidamento di dati a un terzo che, in base al disposto contrattuale, non ne diviene titolare o, meglio, normalmente non dovrebbe divenirne titolare salvo che ci siano esigenze specifiche che trovino giustificazione in contratto.

Infatti, dal momento in cui i dati iniziano ad essere esternalizzati al terzo e non risiedono più sull'infrastruttura locale del cliente, e sebbene l'utente percepisca solo in misura minima che i dati sono stati memorizzati su di un server remoto, dal punto di vista giuridico si verifica una trasformazione fondamentale del rapporto tra titolare e dati che può essere sintetizzata nel modo che segue:

- disponibilità ed accessibilità dei dati in capo al cliente/titolare continuano ad esistere, ma solo in quanto il terzo, cioè il cloud provider, fornisce il servizio nelle forme disciplinate e regolate dal contratto;
- il cliente/titolare dispone dei dati non perché accede a qualcosa in proprio possesso, ma semmai perché fruisce - ventiquattro ore al giorno - di un servizio reso dal cloud provider che, tuttavia, potrebbe a un certo punto trovarsi nella condizione di non adempiere al contratto, volutamente o per cause di forza maggiore (con conseguenze, anche serie, sulla disponibilità dei dati per il proprio cliente)[44].

Quindi, il contratto gioca un ruolo fondamentale, soprattutto in presenza di criticità e fattori imprevisti: qualora esso non fosse sufficientemente chiaro, dettagliato ed idoneo circa il tipo di esigenze e tutela richieste dallo specifico contraente (es. un ospedale, uno studio legale, un'assicurazione, ecc.), un qualsiasi evento pregiudizievole per le parti, incluse controversie ed incomprensioni, potrebbe causare conseguenze devastanti, con prolungata inaccessibilità dei dati o, addirittura, perdite dei medesimi.

Altrettanto è importante che il contratto disciplini le misure che il cloud provider adotterà in relazione alla tipologia di dati da gestire (sensibili, personali, segreti aziendali, ecc.) e che il cliente, a monte di ciò, informi correttamente il cloud provider di quali siano le suddette tipologie e il livello di sicurezza atteso. Infatti, non tutti i dati richiedono le stesse misure di sicurezza e hanno la stessa disciplina per quanto riguarda tempi e modalità di conservazione e, nel momento in cui a gestire i dati è un'entità terza (il cloud provider), sarà questa a dover assicurare il rispetto degli obblighi di legge conseguenti.

Ricapitolando, il contratto di cloud costituisce il fondamentale strumento giuridico che regola la fornitura del servizio di cloud in tutti i suoi aspetti. In base ad esso viene determinata la specifica natura del servizio prestato dal cloud provider, il regime della responsabilità dell'operatore sui dati affidati e quindi, in ultima analisi, il tema della raggiungibilità.

Alcuni esempi possono meglio chiarire le criticità che si possono presentare in caso di contratti redatti in modo impreciso o con scarso dettaglio:

- sul piano tecnico:
  - il passaggio da un cloud provider ad un altro potrebbero determinare difficoltà nell'ottenere l'esportazione dei dati in formato standard;
  - il cliente potrebbe trovarsi a dover ripristinare dal cloud grandi quantità di dati senza però aver concordato con il cloud provider tempistiche certe di ripristino (in assenza di SLA adeguati);
- sul piano contrattuale:
  - ai termini di contratto potrebbero non essere stati definiti gli obblighi del cloud provider relativamente alla riconsegna/cancellazione dei dati che, invece, dovrebbero trovare puntuale definizione in ogni contratto cloud;
  - eventi quali il fallimento del cliente[45] (con conseguenze sui pagamenti), una procedura concorsuale e persino il semplice mancato/ritardato pagamento dei servizi potrebbero determinare il rifiuto del cloud provider di concedere l'accesso ai dati;

44 Cfr. ad esempio https://www.corrierecomunicazioni.it/digital-economy/blackout-mondiale-per-google-services-tutto-risolto-in-poche-ore/ ; https://st.ilsole24ore.com/art/tecnologie/2011-04-29/incendio-server-arubait-tilt-121947.shtml?refresh_ce=1 ; https://www.bbc.com/news/technology-36460328
45 Si veda https://www.hostingtalk.it/cloud-computing-quando-il-provider-fallisce_-c0000067g/

- laddove il contratto cloud preveda il trattamento di dati al di fuori della UE occorre assicurare contrattualmente, per mezzo di apposite "clausole contrattuali tipo"[46] approvate dall'Unione UE (generalmente incorporate in un annesso DPA) che il cloud provider rispetterà le pertinenti previsioni del GDPR, ad esempio assicurando adeguata sicurezza ai dati e notificando tempestivamente il titolare in caso di data breach;

- alcune tipologie di titolari (ad esempio banche ed istituzioni finanziarie) sono soggette a obblighi regolamentari specifici quanto alla gestione dei dati in cloud, tra i quali assume rilevanza il diritto di audit periodico da parte del titolare presso il cloud provider, ed inoltre la previsione che eventuali richieste di accesso di terzi ai dati vengano prontamente notificate[47];
- in caso di subappalto (qualora non vietato dal contratto) le garanzie fornite dal cloud provider devono essere le medesime che il cloud provider imporrà ai terzi subappaltatori, ed il loro ambito territoriale dovrebbe essere previamente reso noto ed autorizzato dal cliente. Infatti, qualora il cliente commissioni servizi a un cloud provider in ragione di specifiche garanzie ed ambiti territoriali su come e dove conservare i dati, occorre certezza che l'operatore non eluda tali pattuizioni affidando i dati a terzi (e così determinando la possibilità di ulteriori "raggiungibilità" dei dati da parte di Stati terzi).

I temi suddetti hanno evidentemente un impatto fondamentale sulla generale "raggiungibilità" dei dati affidati in cloud e, pertanto, possono (e dovrebbero) trovare definizione nell'ambito di un contratto ben strutturato. Nel prosieguo si osserverà, tuttavia, che la contrattualistica standard sovente non consente di negoziare il contenuto ad hoc di un contratto cloud ma che, al contempo, esistono raggiungibilità "imperative" che non possono essere escluse per via contrattuale. La conseguenza di ciò può persino essere che la scelta del contratto avverrà cambiando (o scegliendo a monte) il cloud provider che presenti il miglior compromesso dal punto di vista contrattuale. Un accorto affidamento dei dati in cloud deve dunque, nel valutare eventuali criticità derivanti dalla raggiungibilità del dato, contemperare:

- i fattori che possono essere gestiti per via contrattuale, in quanto dipendenti dalla tipologia di contratto sottoscritto tra titolare del dato e cloud provider, tenendo ovviamente conto della legge applicabile al contratto stesso;
- la giurisdizione in cui operano il cloud provider medesimo ed i propri subappaltatori, nonché quella del luogo in cui intendono ospitare i dati che saranno gestiti ed elaborati nel corso delle attività contrattuali.

Si vedrà ora quali siano le caratteristiche specifiche del contratto cloud nell'ordinamento italiano, valevoli, in generale, in tutti gli ordinamenti europei di identica matrice, ma decisamente differenti in ordinamenti anglosassoni come UK e USA.

3.2. Il contratto di cloud nell'ordinamento italiano

Il contratto di cloud come contratto atipico

Il contratto cloud per il diritto è quel che si dice un contratto "atipico", nel senso che non esiste in Italia una norma che regola lo specifico contratto "cloud". Ma da ciò non deriva che la tipologia di obblighi ivi contenuti sia sconosciuta al diritto. Infatti, il contratto per servizi cloud, a prescindere dalla espressa qualificazione come tale, può infatti essere ricondotto ad alcune tipologie già regolate dal Codice civile e dal diritto dei contratti e, soprattutto, non sconosciute alla Giurisprudenza.

Questa operazione è particolarmente importante già in sede di negoziato/conclusione del contratto, poiché quanto più un contratto cloud contiene all'origine le caratteristiche di contratti c.d. "tipici", tanto più le eventuali criticità che potranno sorgere saranno risolvibili secondo criteri e interpretazioni giuridiche consolidate e facilmente rintracciabili. Parimenti si potranno individuare più chiaramente la ripartizione delle responsabilità

46 Cfr. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

47 Si vedano ad esempio le Linee Guida EBA sull'outsourcing a cloud provider, vincolanti per l'industria finanziaria ed assicurativa: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers

legate alla conservazione ed elaborazione dei dati tra cliente e cloud provider, così come le situazioni in cui il cloud provider risulta tenuto a dare accesso ai dati alle autorità competenti.

Occorre, insomma, tenere presente che il contratto cloud presenta aspetti di rilevante complessità che richiedono una pianificazione preventiva tanto più attenta quanto più i dati esternalizzati (aziendali o personali) siano rilevanti poiché, in caso di criticità, un contratto poco chiaro rende difficili le tutele da approntare a posteriori.

Solo per quanto attiene al contratto di cloud SaaS, infatti, si riscontrano almeno tre differenti orientamenti[48] che lo riconducono, rispettivamente, al contratto di appalto di servizi, a quello di somministrazione di servizi o al contratto di outsourcing. Diversamente, per IaaS e PaaS, tra gli orientamenti prevalenti è degno di nota quello che li riconduce alla disciplina del contratto di locazione (con conseguente responsabilità del provider per il buon funzionamento dell'hardware e della collocazione dello stesso in locali adeguati, unitamente agli altri obblighi di predisposizione e programmazione del servizio stesso per le finalità di interesse dell'utente e di prestazione del servizio di assistenza): detta impostazione ha il beneficio di mantenere i mezzi per la prestazione del servizio (hardware e software di base) in capo al provider, lasciando invece interamente in capo all'utente ogni responsabilità circa i contenuti memorizzati tramite il servizio[49].

Tuttavia, i contratti cloud non possono mai essere contratti di locazione puri, bensì risultano sempre essere un ibrido tra locazione e appalto di servizi. Ciò diviene evidente nel momento in cui si considerano le clausole di esclusione di responsabilità tradizionalmente apposte ai contratti cloud, che in un tradizionale contratto di locazione sarebbero virtualmente nulle alla luce della ordinaria disciplina sui vizi della cosa locata ed a quella sulle limitazioni convenzionali della responsabilità del locatore[50].

Altra dottrina preferisce invece ricondurre la specifica disciplina dei servizi cloud IaaS - sempre nella forma di contratti misti all'appalto di servizi - al tradizionale contratto di deposito, ponendo a carico del provider gli obblighi tipici di un depositario[51]: il contratto cloud sarebbe così un ibrido tra la fattispecie regolare del deposito (per cui un depositante affida al depositario un "bene" da custodire senza servirsene a scopi personali e restituire alla fine del deposito) e quella c.d. "irregolare" (e cioè un depositante deposita una certa quantità di beni, del quale il depositante si può servire, essendo però obbligato a restituire, a fine deposito, la stessa quantità e tipologia di beni depositati, es. generi alimentari, energia o, in questo caso, "dati").

Essenzialmente, a prescindere dalle ricostruzioni e dalle fattispecie richiamate, in un contratto cloud ben strutturato si può individuare, quale elemento "tipico", la relazione per la quale la titolarità ed il pieno esercizio dei diritti sui dati spettano all'effettivo utente, mentre in capo al cloud provider si vanno a configurare una serie di obblighi, più o meno ampi a seconda della tipologia di cloud e di infrastruttura, correlati alla conservazione dei dati in questione. In particolare, i contratti devono definire una serie di regole che stabiliscono gli standard che il cloud provider applicherà per la conservazione e la sicurezza dei dati, nonché i livelli di servizio e gli obblighi per la gestione degli eventi emergenziali e contrattuali (es. cosa fare dei dati a fine contratto). Parimenti, il contratto dovrà stabilire le responsabilità per danneggiamenti ed inaccessibilità dei dati stessi, ad esempio in caso di eventi di forza maggiore.

Apposite previsioni contrattuali saranno inoltre dedicate al comportamento del cloud provider di fronte a richieste provenienti da autorità "competenti" ed in base alla legge "applicabile". È auspicabile che, tanto maggiore sarà la rilevanza dei dati memorizzati/elaborati nell'infrastruttura cloud, tanto più tali previsioni siano dettagliate sino a rimandare a veri e propri documenti procedurali che descrivano le policy applicate a

48 La pluralità di orientamenti deriva anche dai differenti contenuti possibili del contratto di cloud SaaS: l'elaborazione dei dati demandata al software in cloud può infatti avere differenti finalità e differente rilevanza contrattuale e con ciò mutare la tipologia contrattuale applicabile e la responsabilità del cloud provider. Un conto è l'elaborazione mensile degli stipendi o la tenuta della contabilità aziendale, altro è l'utilizzo in cloud di un videogame online.

49 Ai sensi dell'art. 1575 c.c., il locatore ha i tre fondamentali obblighi di "*1) consegnare la cosa locata in buono stato di manutenzione; 2) mantenere la cosa in stato da servire all'uso convenuto; 3) garantire al conduttore, durante la locazione, il pacifico godimento della cosa*". A detti obblighi vanno poi ad aggiungersi quelli di cui ai successivi artt. 1576-1577 circa il mantenimento della cosa locata e le riparazioni della stessa, che attribuiscono al locatore le attività di straordinaria amministrazione, lasciando al conduttore quelle ordinarie.

50 Artt. 1578-1581 c.c., a mente dei quali il locatore è responsabile per i vizi della cosa locata (esistenti o sopravvenuti) e deve risarcire il conduttore, qualora non provi di aver ignorato tali vizi senza colpa, al momento della consegna.

51 In primo luogo, l'obbligo di ricevere i beni (i dati) e quello di custodirli con la diligenza del buon padre di famiglia, secondo le previsioni di cui agli artt. 1766 e ss. c.c.

fronte delle richieste ricevute dal cloud provider, con esemplificazioni delle stesse[52]. Infatti, come si vedrà nel prosieguo, si possono verificare casi in cui, in virtù dei servizi di elaborazione dei dati forniti, il cloud provider può trovarsi a gestire dati nella veste di vero e proprio titolare, avendone il pieno possesso.

Le tipologie civilistiche più rilevanti: somministrazione ed appalto di servizi

La dottrina giuridica, a valle delle analisi cui si è accennato, ritiene oggi che il tipo di contratto che meglio rappresenta le obbligazioni che caratterizzano il contratto di cloud sia il c.d. "contratto di somministrazione di servizi" conosciuto nella gran parte degli ordinamenti europei di *civil law* come "*service provisioning*".

L'articolo 1559 del Codice civile definisce "somministrazione" il contratto con il quale una parte si obbliga, verso corrispettivo di un prezzo, a eseguire, a favore dell'altra, prestazioni periodiche o continuative di cose. Nel caso del cloud, l'obbligazione riguarda ovviamente la prestazione di servizi.

Si tratta di un contratto diverso dall'appalto perché i servizi sono standard e non sono realizzati su commissione, non devono essere "collaudati" per essere forniti e la fornitura avviene secondo precise scansioni temporali, a fronte delle quali matura il diritto al pagamento periodico. Il servizio viene così reso per un periodo di tempo indeterminato o comunque esteso nel tempo, mentre l'appalto viene usato normalmente per un'esigenza contingente e non prevede il pagamento continuativo.

Si avrà così un contratto disciplinato dalle norme del Codice civile sui contratti di somministrazione, mentre si potranno applicare alla fattispecie le norme sul contratto di appalto di servizi solo in via subordinata e nella misura in cui non siano confliggenti con le norme sulla somministrazione.

La differenza "genetica" tra appalto di servizi e somministrazione di servizi con riguardo al cloud, che consente di capire da subito quale sia la tipologia contrattuale cui il contratto fa riferimento, si può individuare avendo riguardo a quanto dispone l'art. 1560 c.c.: tale norma consente infatti al fornitore che provvede alla somministrazione di stipulare il contratto senza che sia esattamente determinata l'esatta entità della fornitura che sarà richiesta dal cliente nel periodo contrattuale, essendo possibile determinare soltanto il massimo e il minimo poiché, per il resto, si "*intende pattuita quella corrispondente al normale fabbisogno della parte che vi ha diritto*"; cosa invece problematica nel contratto di appalto, dove è necessaria una specifica di progettazione della fornitura che l'appaltante fornisce all'appaltatore.

Nel contratto di somministrazione, inoltre, il pagamento del prezzo è determinato, secondo l'art. 1561 c.c., avuto riguardo al tempo della scadenza delle singole prestazioni e al luogo in cui queste devono essere eseguite. Dunque, il prezzo previsto per ogni scadenza non è ripetibile in caso di recesso, poiché la prestazione è completa ed in caso di controversia sull'andamento del contratto il cliente non potrà richiedere le mensilità precedenti alla prima contestazione e già pagate.

Inoltre, al contratto qualificato come somministrazione è stato ritenuto non applicabile il divieto di subappalto di cui all'art. 1656 c.c., ma questo sul presupposto che le prestazioni somministrate (nel nostro caso in cloud) non siano oggetto di progettazione *ad hoc* (es. realizzate per le esigenze di uno specifico cliente) ma riconducibili ai servizi standard del cloud provider. Ciò comporta che un cloud provider potrebbe lecitamente avvalersi - salvi solo gli obblighi derivanti dal GDPR in tema di nomina a responsabili del trattamento e relative informative - di altri soggetti come subappaltatori di componenti del servizio somministrato e, come si diceva, tali soggetti potrebbero operare in territori diversi e, addirittura, sulla base di una diversa legge applicabile.

Scelta della tipologia contrattuale e conseguenze su titolarità e raggiungibilità dei dati

La configurazione contrattuale sopra-descritta ci porta a delineare un quadro giuridico in cui il dato viene affidato al cloud provider, ma senza che questi ne acquisisca alcuna titolarità; salvo che venga richiesto al provider un servizio di elaborazione del dato che ne comporta la gestione "in chiaro" e che richiede la cono-

52 Interessante in questo senso il "rapporto sulla trasparenza" di Google disponibile all'URL https://transparencyreport.google.com/?hl=it e che ha ad oggetto "Condivisione di dati che rivelano come le norme e gli interventi del governo e delle società influiscano su privacy e sicurezza dei dati nonché sull'accesso agli stessi": nell'ambito di tale rapporto, all'URL https://transparencyreport.google.com/user-data/overview?hl=it si rinviene una apposita sezione che elenca i dati sulle richieste globali di informazioni degli utenti ricevute da Google. In particolare, per quanto riguarda l'Italia, leggiamo che nel periodo luglio 2019-dicembre 2019, a fronte di 1486 richieste relative a 2099 account, Google ne ha soddisfatte, in tutto o in parte, circa il 50%.

scenza del dato da parte dell'operatore.

Il cloud provider, infatti, non "acquista" la proprietà del dato ma fornisce un servizio a supporto dell'integrità e sicurezza del dato stesso e, nel solo caso del SaaS, esegue un servizio di elaborazione del dato che, tuttavia, rimane sempre di titolarità del cliente. Si tratta di una fattispecie paragonabile a quella del parcheggio presso un garage: il garagista può accendere e spostare l'auto limitatamente a quanto necessario per parcheggiarla, ma non ne acquista la proprietà, né può effettuare alcun intervento su di essa. Non ne ha cioè il pieno possesso e la possibilità di utilizzo dell'auto è funzionale solo alla custodia, per cui se lo stesso "facesse un giro" con il mezzo in custodia commetterebbe il reato di appropriazione indebita.

Come già accennato, una parte della dottrina ravvisa nell'affidamento dei dati al cloud provider similitudini ed elementi compatibili con l'affidamento in custodia e con lo stesso contratto di "deposito", sicché si potrebbe rinvenire nel contratto di cloud così configurato un misto di obblighi della somministrazione combinati con quelli del deposito (piuttosto che con quelli dell'appalto di servizi). Utilizzando questo schema[53] normativo per ancorare tale fattispecie a consolidate norme del Codice civile e relativa giurisprudenza, risultano chiari gli obblighi del cloud provider che, ottenuti i dati dal cliente, può solo usarli secondo le modalità specificate dal cliente stesso e, non appena richiesto, li deve restituire (es. consentendo la lettura e il download del file) se non addirittura eliminare (in caso di restituzione definitiva). Secondo questa ricostruzione il cloud provider non ha quindi una disponibilità del dato per fini propri.

Se però i dati fossero affidati contestualmente a un contratto che richiede al cloud provider di elaborarli per fornire un servizio (es. usarli per operare arricchimento e annotazione di dati a fini di machine learning di un algoritmo di intelligenza artificiale), la situazione sarebbe diversa perché il cloud provider dovrebbe disporre dei dati in modo completo, tanto da esserne titolare, nella misura in cui ciò sia necessario per fornire quel particolare servizio. In questi casi può essere utile separare i vari contratti di cui si compone l'offerta cloud sottoscritta e distinguere i vari titoli di acquisizione ed elaborazione dei dati da parte del cloud provider.

Tali elementi sono di particolare importanza ai fini del presente Studio, in quanto consentono di stabilire a chi spetti- anche in corso di contratto e anche mentre i dati sono sui server del cloud provider - l'effettiva titolarità, disponibilità e agibilità del dato. In effetti il dato, in presenza di un contratto cloud correttamente strutturato, è localizzato dove si trova il titolare del medesimo e, se il cloud provider non ne la titolarità (come sopra definita), non può trovarsi contemporaneamente presso il cloud provider.

Pertanto, un eventuale provvedimento che riguardi i dati memorizzati presso il cloud provider (che non ha la titolarità del dato) ma non diretto al titolare dei dati sarebbe potenzialmente illegittimo: il cloud provider non avrebbe possibilità di consegnare a terzi un dato di cui non ha disponibilità, così come un ufficiale giudiziario non può pignorare un bene oggetto di leasing nel momento in cui gli viene fatto presente che il proprietario non è il titolare dell'impresa ma la società finanziaria.

Tuttavia, nei contratti cloud di tipo PaaS/SaaS quanto sinora detto deve essere contemperato con il fatto che l'oggetto del contratto non rientra nelle tipologie di cloud direttamente riconducibili alla custodia del dato: il dato viene infatti per forza di cose fornito al cloud provider per ottenerne l'elaborazione e la trasformazione in un dato "diverso" realizzate tramite la piattaforma e/o il software presenti sui sistemi del cloud provider. Alle tipologie contrattuali suddette - le quali sono anche applicabili a prescindere dal loro espresso richiamo ed in base alla analisi ed interpretazione ex post del contratto - si associano così diversi gradi di obblighi e responsabilità per la custodia e gestione del dato e, in questi casi, come già suggerito sopra, il rimedio consiste nel convenire con il cloud provider le procedure che lo stesso dovrà seguire a fronte di richieste di accesso e regolare, in base a tali informazioni, le tipologie di dati che potranno essere esternalizzati.

Al contrario, sulle basi delle affermazioni che precedono è possibile affermare che nel caso dello IaaS il cloud provider, in presenza di una adeguata configurazione contrattuale che incorpori gli elementi sopra suggeriti, normalmente non ha il possesso dei dati che tratta: in questi casi all'elemento contrattuale si accompagna anche l'elemento tecnico (dirimente) per cui i dati sono criptati con chiave inaccessibile al cloud provider per

53 Il modo migliore sarebbe di dichiarare espressamente applicabili (in un contratto soggetto alla Legge italiana) sia la disciplina di cui agli artt. 1560 e seguenti c.c. e, per ogni altro aspetto, la disciplina dell'art. 1766 c.c. e seguenti.

sancire una barriera tra il dato (del cliente) ed il servizio (del cloud provider)[54] ad evidenza di tale mancanza di possesso e disponibilità, così come i beni depositati in una cassetta di sicurezza non sono accessibili per la banca che ospita la cassetta medesima.

Va da sé che non sempre è possibile ottenere un contratto cloud soggetto al diritto italiano (o di altro Stato europeo con la medesima matrice di civil law), e neppure tale contratto può sempre essere negoziato per ottenere il tipo di struttura contrattuale più conforme ai propri interessi. Pertanto, occorre valutare anche scenari avulsi alle esperienze locali, quali quelli di un contratto cloud atipico e regolato da un diritto estero di matrice diversa: diritto USA, diritto cinese, diritto coreano, ecc... In questi casi la valutazione del contratto deve essere effettuata analizzandone le obbligazioni e ricostruendo cosa il cloud provider garantisce rispetto ai dati che il cliente affida alla sua gestione.

Occorre inoltre esaminare se il cloud provider consenta o meno al cliente di decidere quale sia la collocazione geografica dei server che elaboreranno i dati in cloud, poiché tale collocazione geografica, determinata in contratto, assume specifica rilevanza - come si rileverà al capitolo 4 - per l'operatività di specifiche previsioni che consentono ad alcune autorità giurisdizionali e governative di ordinare al cloud provider la produzione dei dati del cliente.

Il particolare regime dei dati elaborati in servizi cloud SaaS

Come già evidenziato, nel contratto cloud SaaS la prestazione del cloud provider assume una connotazione particolare. Infatti, esso non si limita a fornire uno spazio in cui il cliente può memorizzare dati. Il cloud provider prende in consegna dei dati che elabora tramite strumenti software propri su proprie piattaforme, restituendo al cliente, in forma di servizio, il risultato dell'elaborazione.

Non può dirsi che la prestazione del cloud provider sia limitata alla fornitura da remoto di software perché tale software non entra mai nella disponibilità del cliente: il cloud provider fornisce licenze di "accesso" ad un software installato su proprie infrastrutture.

I dati risultanti da elaborazioni compiute dal cloud provider a partire dai dati trasmessi dal cliente in ragione del servizio SaaS (es. anche soltanto restituire un file in formato pdf a fronte dell'input di semplice testo o restituire una foto ritoccata a fronte dell'input dell'originale) sono così da considerare come dati generati dal cloud provider, e quindi rientranti nella sua sfera di titolarità, almeno fino al momento della "consegna" al cliente. Anche dopo tale consegna, tuttavia, il contratto potrebbe disporre che il cloud provider conservi alcuni diritti su tali dati (es. diritti di proprietà intellettuale sulla forma in cui sono stati elaborati, es. la forma grafica di una presentazione).

È inoltre possibile, secondo alcune teorizzazioni, che ai sistemi in cloud e di big data si applichino le norme a tutela delle banche dati (il c.d. diritto *sui generis* previsto in UE dalla Direttiva 96/9/CE) per cui, nel momento in cui il cliente del cloud provider "alimenta" il sistema cloud con dati, essi vengono inseriti in una struttura che - quale frutto degli investimenti del cloud provider - è di titolarità del cloud provider. Di conseguenza l'estrazione (cioè il successivo recupero del dato utilizzando il database) diventa un diritto che il cloud provider "concede" al proprio cliente sulla base dell'accordo contrattuale, ferma restando la titolarità del dato grezzo in capo al cliente.

Altrimenti detto, a fronte di una maggiore complessità dei servizi cloud che vengono resi, specie in regime di SaaS, e in assenza di una chiara previsione contrattuale per cui il cloud provider non conserva alcuna titolarità del dato gestito, è altamente possibile che un'autorità esterna identifichi il cloud provider, e non il cliente, come colui avente titolarità o possesso dei dati, o di parte di essi, nei momenti del servizio appena successivi alla loro elaborazione in chiaro nei sistemi cloud.

Alla luce di quanto sopra, a fronte di norme di legge che prevedano l'accessibilità/raggiungibilità dei dati nella disponibilità del cloud provider, un contratto non sufficientemente preciso al riguardo creerebbe delle incertezze e delle criticità che potrebbero aprire il varco a richieste di accesso dei dati formulate da autorità estere

54 A prescindere dalla "forza" e inviolabilità del criptaggio. Il fatto che siano criptati costituisce una barriera logica, come una porta chiusa a chiave ma che si potrebbe sfondare con una lieve spallata: il fatto di dover "sfondare" a porta costringe il cloud provider ad una azione illegale e ciò rende illegittimo qualsiasi ottenimento del dato.

a cloud provider soggetti alla propria giurisdizione, come meglio si dirà nel Capitolo 4.

Vi è però da dire che, a livello contrattuale, l'enforcement di tali norme estere potrebbe trovare una difficoltà maggiore in contratti in cui la legge applicabile e la giurisdizione decise convenzionalmente dalle parti contraenti fossero mantenute comunque all'interno dell'Unione Europea poiché tali parti, anche ove si trovassero a dover controbattere richieste di accesso di governi esteri, dovrebbero comunque discuterne avanti ad un giudice europeo e sulla base di una normativa di uno Stato UE.

3.3. I dati non conformi agli accordi contrattuali

L'analisi svolta fino ad ora ha mirato a definire lo status giuridico dei dati, individuandone il titolare ed il contesto contrattuale ideale, al fine di valutare le condizioni di base per la raggiungibilità giuridica.

Occorre però considerare anche l'ipotesi in cui i dati siano detenuti dal cloud provider in un contesto differente, e cioè di non conformità a norme di legge o contrattuali.

Si tratta di comprendere se la presenza (in linea di principio indesiderata) di dati non conformi alle pattuizioni contrattuali o in violazione di legge sui sistemi del cloud provider muti il "titolo" giuridico di detenzione dei dati suddetti, imponendo al cloud provider di trattarli diversamente dai dati detenuti legittimamente in base la contratto o alla Legge.

A tal fine assumono specifica rilevanza i divieti contrattuali posti dall'operatore a carico del cliente per effetto delle c.d. Acceptable Use Policy (AUP), vale a dire l'allegato contrattuale in cui vengono regolati gli usi consentiti della infrastruttura hardware e software offerta dal fornitore cloud.

Infatti, se il cliente violasse l'AUP (che spesso al cliente non è nota, essendo un documento contrattuale sottoscritto a monte dal referente contrattuale) i dati in violazione non sarebbero "conformi" al contratto e come tali non potrebbero essere gestiti dal cloud provider, dovendo in teoria essere "restituiti" al cliente.[55]

Si pone pertanto la questione seguente: si potrebbe considerare "raggiungibile" da eventuali provvedimenti di autorità pubbliche un dato non conforme alla AUP e, dunque (potenzialmente) non soggetto alla sua custodia? Ad esempio, potrebbe trattarsi di un caso di file contenenti dati sanitari o di contenuti in violazione del diritto d'autore laddove la AUP prevedesse il divieto di memorizzazione di tale tipo di dati nell'infrastruttura cloud.

In linea di principio, ragionando con i principi che regolano la responsabilità del hosting provider contenuti nella Direttiva 2000/31/CE relativa al commercio elettronico, applicabili anche al cloud, sino a che il dato non conforme non fosse validamente segnalato al cloud provider (e/o restituito ed eliminato), il cloud provider non ne avrebbe una "consapevolezza" giuridica e dovrebbe gestirlo in buona fede alla stregua di ogni altro dato. Pertanto, la disciplina della raggiungibilità di questo dato non sarebbe così diversa, almeno fino a che il dato non venisse "segnalato". A quel punto il dato non conforme sarebbe, per così dire, un oggetto anomalo, non più coperto dalle previsioni contrattuali e affidato al cloud provider solo *de facto*: sarebbe il cloud provider ad averne comunque il possesso nella fase in cui esso non sia ancora restituito o distrutto e si ritiene che, in conseguenza, questo esponga il dato alla raggiungibilità in una misura maggiore ai dati invece conformi al contratto.

Anche una disciplina contrattuale che consentisse al cloud provider di effettuare verifiche preventive o a campione, ad esempio in ragione della tutela del copyright, dovrebbe essere attentamente parametrata: il dato non conforme non dovrebbe essere incamerato per non creare un corpus anomalo nella gestione dei dati cloud, potenzialmente aggredibile da provvedimenti di sorta e difficilmente eliminabile senza il coinvol-

55 Un caso recente e che ha destato molto clamore è quello Amazon-AWS/Parler, in cui il cloud provider americano ha interrotto il servizio IaaS di Parler, piattaforma social preferita della destra americana sostenitrice di Trump, di fatto spegnendola. Secondo Amazon-AWS, Parler avrebbe violato le AUP a causa dei contenuti falsi o pericolosi diffusi dagli utenti, rendendo così necessario il provvedimento. Parler ha preannunciato un'azione legale contro Amazon-AWS (si veda: https://www.bbc.com/news/technology-55615214) ritenendo di non aver violato le AUP.

gimento dell'utente[56]. Tali verifiche potrebbero essere contrattualmente convenienti per il cloud provider per evitare che le autorità possano ipotizzare una co-responsabilità del provider stesso, a fronte di caricamenti massivi di contenuti illegali[57].
La AUP e il contratto vengono a costituire il primo riferimento per i rapporti tra utente e cloud provider, specialmente nelle situazioni in cui il cloud provider riceva da una autorità competente l'ordine di inibire il servizio a un certo cliente o riguardo certi dati. Infatti, pur essendo l'ordine emanato dall'autorità competente, il provider eseguendolo si rende in tal modo potenzialmente inadempiente verso il proprio cliente, salvo che il contratto non preveda esclusioni di responsabilità riguardo a una situazione di questo tipo o vi sia una chiara situazione di inadempimento del cliente - ad esempio perché, come negli esempi portati poc'anzi, ha trasferito al cloud provider tipologie di dati non consentiti dalla AUP. In situazioni di incertezza il cloud provider potrebbe essere costretto a conservare dati sequestrati dall'autorità in attesa di provvedimenti al riguardo, senza potersene definitivamente liberare, a tutela di eventuali diritti del proprio cliente.

Occorre infine segnalare che l'analisi della materia individua provvedimenti di natura normativa o para-normativa che stabiliscono una raggiungibilità "a prescindere" dall'assetto contrattuale.
Tali sono, ad esempio, i provvedimenti che regolano la disponibilità dei dati in cloud dei soggetti investigati durante le attività di ispezione delle autorità indipendenti. Tali provvedimenti stabiliscono una equivalenza tra raggiungibilità del dato in cloud ed accessibilità del medesimo nel tentativo di fornire copertura giuridica ad operazioni di copia/sequestro effettuate nel corso di procedimenti investigativi di autorità indipendenti (ad es. antitrust) di qualsiasi dato che sia accessibile in cloud all'investigato, omettendo di verificare se vi sia o meno titolarità contrattuale del dato o proprietà intellettuale dello stesso in capo all'uno o all'altro, e senza dover rinunciare all'apprensione laddove il dato sia stato esternalizzato.
Si descrive così una raggiungibilità per così dire "funzionale" che consente all'autorità procedente di acquisire il dato in maniera ampia, giustificata dal fine di utilizzo limitato al procedimento in corso e dal regime del proprio segreto istruttorio (fatto salvo l'eventuale futuro diritto di accesso in forma omissata dei terzi controinteressati). Si tratta di una fattispecie di accesso a cui ha fatto spesso ricorso, tra gli altri, la DG Concorrenza della Commissione Europea (sin dal 2013[58]). Tuttavia, questa larghezza procedimentale ha trovato negli ultimi anni una vivace opposizione basata sull'art. 19 comma 2 della Convenzione di Budapest del 2001[59] in materia di contrasto alla criminalità informatica (laddove i poteri delle autorità antitrust sono equiparati alla magistratura penale in sede di ispezione). Tale norma prevede che "*Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire che, qualora le proprie autorità perquisiscano o accedano in modo simile a specifici sistemi informatici o parte di essi, in conformità al paragrafo 1.a, e abbiano ragione di ritenere che i dati ricercati si trovino presso un altro sistema informatico o parte di esso nel proprio territorio, e a tali dati sia possibile legalmente l'accesso dal sistema iniziale, le stesse autorità possano estendere rapidamente la perquisizione o l'accesso all'altro sistema*".
Di conseguenza l'apprensione dei dati su server estero, sulla base della possibilità di accesso, per quanto previsto dalla Convenzione di Budapest, in ipotesi di criminalità informatica o equiparate appare possibile solo ove vi siano specifici accordi tra i due Stati (come quelli previsti dal CLOUD Act USA di cui si dirà al successivo capitolo 4).

---

56 Nel caso instaurato dal Department of Justice USA contro il sito cyberlocker Megaupload, in cui veniva contestato l'uso primario del servizio per la condivisione di contenuti in violazione del copyright, il servizio fu spento ed i server posti sotto sequestro. Ciò nonostante, fu assai complesso dirimere la questione relativa se (e come) si potessero eliminare i dati, il cui costo di conservazione era stimato a USD 9000 al giorno. Si riconosceva infatti un teorico interesse degli utenti a recuperarli anche se le condizioni d'uso del servizio avvisavano gli utenti che la memorizzazione comportava il rischio della perdita completa dei dati in qualsiasi momento. I dati furono infine posti sotto la tutela della EFF (Electronic Frontiers Foundation) quale organismo neutrale incaricato della gestione delle residue richieste degli utenti, da effettuarsi entro un termine massimo.
57 Tale responsabilità è stata ipotizzata nel citato caso USA del cyberlocker Megaupload sulla base del fatto che il servizio cloud in questione era stato progettato e commercializzato per un *primary use* in violazione della Legge. Il caso però non arrivò mai alla discussione nel merito essendo intervenuti provvedimenti di cessazione del servizio e provvedimenti in sede penale prima della stessa. In UE la nuova Direttiva copyright 2019/790 esclude i "servizi cloud da impresa a impresa" ed i "servizi cloud che consentono agli utenti di caricare contenuti per uso personale" dalla particolare responsabilità per i contenuti caricati dagli utenti che la stessa delinea: essa ascrive il nuovo regime di responsabilità ai soggetti definiti «prestatore di servizi di condivisione di contenuti online» e cioé quelli il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro.
58 Cfr. Commission Explanatory Note https://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf
59 Cfr. https://rm.coe.int/16802f423d

CAPITOLO 4
L'INTERVENTO DELLE AUTORITÀ PUBBLICHE SULLA RAGGIUNGIBILITÀ DEL DATO

Come evidenziato nei capitoli precedenti, la configurazione giuridica del cloud, di cui alla normativa applicabile territorialmente e in virtù del contratto prescelto, incide sensibilmente sulla raggiungibilità dei dati ai fini dell'estrapolazione delle informazioni. Ciò comporta importanti ripercussioni sull'accessibilità dei dati e sul *modus operandi* da seguire da parte delle autorità procedenti (ad esempio, le autorità giudiziarie alla ricerca di prove digitali o di materiale illecito) con finalità, alternativamente, acquisitive o dirette alla rimozione dei dati presenti sui server diffusamente locati. La normativa contrattuale sarà infatti, in ogni caso rilevante, anche se di diversa nazione dal luogo di stabilimento, in caso di richiesta di accesso da parte dell'autorità competente per territorio.

Riguardo a questo aspetto, come evidenziato dall'analisi svolta fino ad ora, il fattore di maggiore rilevanza appare essere il luogo di stabilimento del cloud provider, la cui variazione comporta conseguenze ai fini della raggiungibilità delle informazioni da parte delle autorità governative e giudiziarie, delle forze dell'ordine e dei servizi di intelligence. Ulteriori variabili possono derivare dalle differenti configurazioni ed allocazioni dei data center che sono sovente fisicamente collocati in una serie di ubicazioni sottoposte a giurisdizioni differenti, pur lavorando in sincronia nel gestire i medesimi dati[60].

Un ulteriore aspetto che deve essere tenuto in dovuta considerazione è la variegata tipologia di contenuti che possono essere contenuti in cloud: tale strumento, data la sua versatilità, e la variegata tipologia di destinatari (ad esempio privati, professionisti, imprese, pubbliche amministrazioni ed istituzioni) si presta ad immagazzinare diverse tipologie di informazioni (dati personali anche particolari, documenti riservati, coperti da segreto, soggetti al segreto professionale, privilegiati, creazioni scientifiche, industriali e artistiche ecc.) per le quali è necessario un alto grado di sicurezza nella conservazione ed un'elevata protezione per prevenire gli accessi non autorizzati.

Quanto sopra induce a ritenere che l'intervento dell'autorità giudiziaria e delle forze dell'ordine debba essere perimetrato chirurgicamente, operando opportuni distinguo procedurali, in base alla tipologia di informazione ricercata e dia luogo a valutazioni in diritto piuttosto complesse e che possono essere anche molto diverse a seconda di come si compongono le variabili del caso specifico.

Tale complesso background tecnologico e giuridico scardina alcuni dei principali presupposti su cui gli ordinamenti hanno lavorato per secoli ed ha pertanto imposto una ridefinizione del panorama procedurale esistente, nonché di riconsiderare le metodologie e gli istituti tradizionali in tema di identificazione, raccolta/acquisizione, conservazione e analisi delle potenziali fonti di prova a livello nazionale ed internazionale.

Si procederà in questa sede anzitutto alla disamina degli approcci regolatori presenti nel panorama statunitense ed europeo. Gli USA hanno infatti adottato di recente un nuovo paradigma normativo per l'accesso alle prove elettroniche, volto altresì a modificare i rapporti con i paesi terzi per la ricerca di dette prove e rappresentano attualmente il paese dove hanno sede il maggior numero di provider che offrono servizi cloud.

4.1. La disciplina USA

La disciplina USA è particolarmente rilevante per l'oggetto del presente Studio poiché i più grandi cloud provider a livello mondiale, e che detengono importanti quote di mercato in Europea ed in Italia, sono appunto americani o, comunque, usano infrastrutture basate negli Stati Uniti.

La disciplina statunitense, normalmente costituita dal Stored Communications Act (SCA), è stata recente-

60 Come evidenziato *supra* (§ 1.3) le informazioni, già di per sé consistenti di bit che possono essere disaggregati con la tecnica dello *striping*, possono essere distribuite su vari server ubicati in differenti giurisdizioni, anche contemporaneamente.

mente novellata con il Clarifying Lawful Overseas Use of Data Act (c.d. "CLOUD Act") entrato in vigore il 23 marzo 2018. Tale nuova normativa è stata adottata anche per risolvere uno dei primi ed importanti contenziosi nel settore, il caso Microsoft.

Il caso Microsoft

Il caso riguardava l'efficacia di un warrant - un ordine di esibizione - ex §2703 dello SCA - emanato prima della novella ad opera del CLOUD Act - per richiedere a Microsoft l'accesso ad una certa quantità di caselle e-mail che questa però gestiva sui propri server irlandesi. Ci si chiedeva, in buona sostanza, se Microsoft, in quanto hosting provider, una volta emesso il search warrant fosse obbligata a condividere comunicazioni (nel caso di specie le caselle e-mail ed altre informazioni correlate all'account di suoi clienti) sotto il suo possesso, custodia o controllo, anche se custoditi su server esteri. Infatti, Microsoft contestava l'efficacia del warrant nei confronti dei data center ubicati a Dublino, dove le informazioni venivano effettivamente registrate e, su questa base, chiedeva l'annullamento del provvedimento.

Sulle querelle era stato richiesto il certiorari (revisione) della Corte Suprema degli Stati Uniti, che tuttavia alla fine non si è pronunciata proprio per via dell'introduzione - nelle more degli accadimenti - del §103(a)(1) del CLOUD Act che, emendando lo SCA, ha reso irrilevante l'ubicazione estera dei dati ai fini della loro raggiungibilità: "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States".[61]

> *"La disciplina USA è particolarmente rilevante per l'oggetto del presente studio, perché i più grandi cloud provider mondiali, e che detengono importanti quote di mercato in Europea e in Italia, sono appunto americani o con infrastrutture basate negli Stati Uniti".*

Successivamente, in virtù della nuova legge, il governo americano ha richiesto ed ottenuto un nuovo warrant che ha sostituito il precedente, e, pertanto, la Corte Suprema ha rinviato alla Corte d'Appello per il Secondo Circuito con l'indicazione di annullare il respingimento della mozione di annullamento proposta da Microsoft, per poi ordinare al Tribunale distrettuale di chiudere il caso.

Non sono però state rinvenute fonti che documentano l'effettiva consegna dei dati da parte Microsoft e, come si vedrà, è ben possibile che siano tuttora in corso i passaggi esecutivi e normativi che rendano possibile eseguire un tale ordine - valido dal punto di vista del diritto USA - su server siti nella UE.

Il CLOUD Act

Il CLOUD Act ha avuto lo scopo di chiarire limiti ed aree grigie dello SCA di fronte al fenomeno della circolazione globale dei dati. Lo SCA infatti consentiva pacificamente ai giudici USA di emettere warrant aventi ad oggetto dati di soggetti USA, detenuti da provider USA e situati in territorio USA, ma presentava criticità di fronte a fattispecie più complesse e che, con l'evolversi della tecnologia, rendevano estremamente semplice eluderne l'applicazione trasferendo i dati in altre nazioni. In particolare il CLOUD Act ha inteso superare soprattutto i seguenti problemi:

1. i *warrant*, aventi ad oggetto la produzione di customer records (informazioni sui clienti) in possesso dei provider soggetti alla giurisdizione USA ed emessi in forza dello SCA, trovavano limitazioni quando

61 "*Un [service provider] deve ottemperare agli obblighi di questo capitolo al fine di preservare, eseguire il backup o divulgare il contenuto di una comunicazione via cavo o elettronica e qualsiasi record o altra informazione relativa a un cliente o abbonato* ***in possesso, custodia o controllo di tale fornitore****, indipendentemente dal fatto che tali comunicazioni, registrazioni o altre informazioni si trovino entro o al di fuori degli Stati Uniti*" (trad. dell'Autore)

avevano ad oggetto dati di un soggetto straniero collocati al di fuori del territorio USA;

2. i provider (e clienti) soggetti a tali ordini non avevano chiarezza su quale fosse lo strumento giuridico per richiedere la revoca (*quash*) del *warrant*, laddove volessero sostenere di fronte alla Corte USA che la stessa era illegittima in base al diritto dello Stato dove i dati erano materialmente collocati e del diritto nazionale del titolare (sia perché i dati erano ospitati da altro Stato, sia perché il diritto contrattuale applicabile non era quello USA);

La riforma del CLOUD Act verte così su tre punti fondamentali:

(I) viene emendato lo SCA e così viene introdotto il principio secondo cui una società, soggetta alla giurisdizione statunitense, nei termini che si diranno, può essere soggetta a richieste di produzione (*warrant* emessi da un giudice indipendente) di dati "**posseduti, gestiti o controllati**" dalla stessa, indipendentemente dal luogo di archiviazione di questi e anche se tali dati sono di titolarità di un soggetto straniero;

(II) viene chiarita la possibilità di opporre un *warrant* emanato sulla base del CLOUD Act richiedendo al Giudice che lo ha emanato di effettuare una *comity analysis*, cioè una particolare analisi giuridica in cui il giudice deve prima mettere a confronto la legittimità del *warrant* con eventuali disposizioni confliggenti del diritto nazionale applicabile al luogo in cui sono custoditi i dati e all'entità titolare[62] ma poi, una volta considerati tutti gli elementi, può decidere autonomamente ed effettuare una sorta di mediazione tra il diritto USA e le disposizioni che ha analizzato o motivare il fatto che egli se ne discosta, non essendo egli vincolato al rispetto di disposizioni estere; in caso vengano stipulati gli agreement, descritti al punto seguente, tra USA ed altri Stati viene però meno la possibilità di richiedere il rimedio appena descritto;

(III) la possibilità per gli USA di automatizzare le procedure internazionali in questione stipulando i c.d. "CLOUD Act Agreement", vale a dire una tipologia di accordi che introducono dei meccanismi bilaterali ed automatici di accesso ai dati in cloud tra USA ed altri stati (in base ai motivi consentiti nei rispettivi ordinamenti), così eliminando la possibilità per il cloud provider e il cliente/titolare dei dati di opporsi all'ordine sulla base della discussione della legittimità internazionale di ogni singolo *warrant*.

Per una migliore comprensione del CLOUD Act appare utile tenere conto del white paper dell'aprile 2019 adottato dall'US Department of Justice "*Promoting Public Safety, Privacy, and Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*". Il documento chiarisce quali provider sono ricompresi nell'ambito applicativo dell'Act, specificando che le disposizioni concernenti la conservazione e la divulgazione dei dati da parte dei provider sono applicabili unicamente ai provider di "*electronic communication services*" e di "*remote computer services*". Tali servizi sono definiti dall'Electronic Communications Privacy Act che al 18 US Code §?2510(15) definisce i servizi elettronici di comunicazione come qualsiasi servizio che fornisce agli utenti la possibilità di inviare o ricevere comunicazioni elettroniche, mentre il §?2711(2) descrive i servizi di elaborazione da remoto come la fornitura al pubblico di servizi di elaborazione e archiviazione mediante un sistema di comunicazione elettronica. Pertanto, ricadono nell'ambito applicativo potenziale del CLOUD Act i fornitori di caselle di posta, le compagnie telefoniche, le piattaforme social ed i servizi di cloud storage.

In conclusione, affinché il CLOUD Act sia nel concreto applicabile alle categorie di soggetti enumerate devono così sussistere le seguenti condizioni:

- i dati richiesti devono essere sotto il possesso, gestione o controllo del provider;
- i provider devono essere soggetti alla giurisdizione statunitense, sulla base di una valutazione che tutt'ora

62 Per *comity analysis* il diritto USA intende – in estrema sintesi e semplificando molto il tema -un procedimento in cui il Giudice considera "a titolo di cortesia" il diritto di uno Stato estero. La decisione finale rimane però del Giudice USA che non è giuridicamente vincolato dalle disposizioni estere.

non è scevra da criticità.[63]

Il CLOUD Act non ha modificato le caratteristiche intrinseche del *warrant* rispetto alla disciplina precedente e, in particolare, rimane fermo il fatto che richiesta di accesso debba provenire dagli USA ed avere per oggetto dati situati negli USA e sotto il controllo di una entità USA. La riforma, da questo punto di vista, si è limitata a chiarire il contenuto del *warrant*, lasciando impregiudicati i requisiti previsti dalla legge per il suo rilascio ma, come si è detto, ne estende l'applicazione territoriale e soggettiva.

Il *warrant* emesso ai sensi del CLOUD Act deve così, come nel precedente regime, essere accompagnato da una dichiarazione giurata - pena la commissione del reato di spergiuro - che dimostri la "probabile causa" che induce a ritenere che il luogo soggetto a perquisizione conterrà elementi di cui è necessario il sequestro.

La richiesta deve essere arricchita da ulteriori elementi, quali il reato contestato, le informazioni soggette a *disclosure* e le prove per il sequestro. Il provvedimento è sottoposto al vaglio di un giudice indipendente.

Rileva altresì il tema della definizione dell'oggetto del *warrant*, che per la definizione dello studio in oggetto riveste particolare importanza. Anche da questo punto di vista, la fattispecie di *warrant* prevista dallo SCA non ha subito modifiche o ampliamenti nel suo raggio d'azione, pertanto:

- la raccolta dei dati deve essere circoscritta dal provvedimento;
- I dati accessibili per mezzo del provider in virtù del *warrant* sono quelli in possesso o nel controllo del provider stesso.

Di conseguenza, qualora dei dati siano sotto il controllo esclusivo del cliente e senza nessun accesso da parte del cloud provider (es. criptati con chiave non disponibile al cloud provider), è discutibile che possano essere soggetti al *warrant*.

Il ruolo del cloud provider secondo il CLOUD Act

Il citato white paper sottolinea la coerenza definitoria del CLOUD Act con il paragrafo 173 della relazione esplicativa della Convenzione di Budapest sulla criminalità informatica (che persegue il fine di una politica comune contro il cybercrime) a mente della quale "*il termine 'possesso o controllo' si riferisce al possesso fisico dei dati interessati nel territorio della Parte ordinante ed alle situazioni in cui i dati che devono essere prodotti si trovino al di fuori del possesso fisico della persona, ma questa può in ogni caso controllare liberamente la produzione dei dati nel territorio della Parte ordinante (ad esempio, soggetti ai privilegi applicabili, una persona a cui è stato servito un ordine di produzione per le informazioni memorizzate nel proprio account tramite un servizio di archiviazione online remoto, deve produrre tali informazioni). Allo stesso modo, la semplice capacità tecnica di accedere ai dati da remoto (ad esempio, la capacità di un utente di accedere tramite un collegamento a dati che tuttavia non rientrano nel suo legittimo controllo), non costituisce 'controllo' ai sensi della presente disposizione...*".

La tematica del controllo e del possesso dei dati è di primaria importanza[64], se si considerano le possibili implicazioni dovuta a fattori quali le finalità per le quali il dato è detenuto dal provider.

Differenze evidenti sono rinvenibili in base al diverso titolo per cui i dati sono nella disponibilità del provider. Come già evidenziato al §3.2., occorre infatti operare un distinguo sulla base del servizio fornito dal provider:

63 Da questo punto di vista non vi sono state modifiche delle previsioni dello SCA, che vengono confermate e, pertanto, si possono considerare come "soggette alla giurisdizione USA" a questo fine le società statunitensi, le società con sede negli USA e le società di proprietà di persone degli Stati Uniti; tuttavia, ben possono essere considerate assoggettate a giurisdizione USA anche quelle società non rientranti nelle categorie appena elencate, ma che hanno comunque contatti rilevanti con gli US (ad esempio le società che in tale nazione conducono un'attività significativa) tali da far ritenere all'organo giurisdizionale possibile l'estensione della giurisdizione. In questi termini, i criteri per definire i soggetti ricompresi o che potranno essere ricompresi non hanno criteri nitidi, ma sono rimessi ad una valutazione caso per caso da parte del giudice; margini discrezionali si rinvengono altresì nel vaglio dei rapporti intercorrenti tra una società e la sua controllata in termini di controllo dei dati posseduti o controllati dalla seconda da parte della prima. È bene sottolineare come in questi casi la struttura ed il rapporto tra le due società non infici la valutazione, che dovrà essere in ogni caso effettuata dall'organo giurisdizionale. All'esito di tale valutazione, verrà stabilito se è possibile o meno emettere il *warrant*.
64 Si veda *supra*, § 2.1.

se il dato viene trattato ai fini della modifica, dell'elaborazione o dell'implementazione, è ben possibile ipotizzare il controllo ed il possesso del dato in capo all'operatore; se, invece, le informazioni raccolte sul cloud sono immagazzinate ai soli fini di storage, si presume che esse sono al di fuori del possesso e della sfera del controllo del provider. Nell'ultimo caso il cloud provider non potrebbe avere accesso ai contenuti, disponibili unicamente per l'accesso da parte dell'utente.

Peraltro, ad alimentare la convinzione che detti dati siano al di fuori della disponibilità del provider, vi è il fatto che sovente - o meglio, quasi sempre - in questi casi si ricorre a tecniche di criptaggio, volte ad assicurare l'accesso univoco del cliente, che, in alcuni casi, oltre ad assicurare l'accesso all'informazione, permettono la prodromica ricomposizione dei frammenti della stessa, che sono distribuiti su differenti data center. Sul punto è bene chiarire che neppure il warrant SCA post-CLOUD Act può spingersi sino a richiedere al provider la laboriosa, quanto improbabile, decrittazione dei file, anzi il white paper esclude espressamente tale possibilità.

In conclusione, il dato criptato non può essere né accessibile né raggiunto dal provider ed è pertanto al di fuori del suo possesso o controllo, rendendo inapplicabile la disposizione del CLOUD Act.

Quanto poi alla tipologia di dati estrapolabili, questi, se raggiungibili, possono potenzialmente includere il contenuto delle comunicazioni, i metadati ad essi associati, le informazioni sull'abbonato e i dati archiviati per conto dell'utente.

L'accesso a dati appartenenti a cittadini non statunitensi ed i CLOUD Agreement

Un'ultima questione, che poi apre al secondo tema affrontato dal CLOUD Act, riguarda l'accesso a dati appartenenti a cittadini/residenti non statunitensi (tra i quali, per l'appunto, i cittadini/residenti italiani ed europei). Occorre ricordare che i provvedimenti basati sul CLOUD Act considerano la cittadinanza o la residenza del cliente come elemento determinante, mentre il luogo di ubicazione dei dati rileva in misura minore.

> *"Con il CLOUD Act qualsiasi società soggetta alla giurisdizione statunitense può essere assoggettata a richieste di produzione di dati posseduti, gestiti o controllati dalla stessa, indipendentemente dal luogo di archiviazione di questi e anche se tali dati sono di titolarità di un soggetto straniero."*

Come abbiamo appena dimostrato, le società soggette alla giurisdizione USA dovrebbero adeguarsi pacificamente ad un *warrant* avente ad oggetto dati di cittadini/residenti non statunitensi qualora esista un CLOUD Agreement con lo Stato ove sono ubicati i dati. Viceversa, in assenza di tale accordo e qualora il warrant si ponesse in contrasto con la legge del paese di destinazione, l'efficacia del provvedimento potrebbe essere messa in discussione sino a restringere le sue pretese per conformarsi all'ordinamento di destinazione (e ciò con lo strumento della richiesta di *quash* attraverso la *comity analysis*).

Inoltre, qualora i dati fossero oggetto di storage in molteplici Stati ed in assenza di pertinenti CLOUD Agreement, l'esecuzione di un *warrant* potrebbe essere opposta dal cloud provider e dal titolare con molteplici *comity analysis*, rendendola alquanto difficoltosa, anche in virtù del fatto che le molteplici parti di dati soggette alla giurisdizione di differenti Stati potrebbero essere soggette a decisioni diverse.

In alternativa, qualora non si volessero utilizzare gli strumenti previsti dal CLOUD Act, le autorità procedenti dovrebbero esperire procedure più tradizionali quali la negoziazione in buona fede o la riproposizione della richiesta sulla base di un Mutual Legal Assistance Treaty (MLAT); si tratta tuttavia di strumenti complessi che per tale motivo tendono ad essere visti come assolutamente secondari.

I CLOUD Agreement e i MLAT

Si comprende, quindi, come la possibilità di concludere degli Agreement sulla base del CLOUD Act rappresenti il secondo elemento portante della riforma.

La stipula di tali accordi è subordinata al riconoscimento, da parte degli USA[65], che l'ordinamento giuridico dello Stato contraente offra uno standard di protezione in materia di privacy e libertà civili almeno equivalente a quello degli Stati Uniti.

Alla data in cui si scrive non risulta che Stati membri UE che abbiano concluso dei CLOUD Act Agreement con gli USA.

L'unico accordo di questo tipo ad oggi è stato firmato dal Regno Unito nell'ottobre 2019[66] ed ha subito sollevato interrogazioni all'Europarlamento circa la sua legittimità[67]. A seguito della Brexit, è inoltre probabile la necessità di una sua revisione in quanto esso fa riferimento a meccanismi previsti dalle Convenzioni tra UE e Stati Uniti sul trasferimento di dati relativi alla prevenzione dei reati[68]. Nel complesso l'Agreement disegna un meccanismo di salvaguardie reciproche nel caso i trasferimenti richiesti (comunque solo di dati relativi a indagini penali) siano contrari a quelli che vengono definiti "interessi essenziali" degli Stati contraenti.

È comunque fuor di dubbio che uno Stato non potrebbe ratificare un tale Agreement in violazione delle proprie stesse disposizioni (nel caso degli Stati membri della UE, ad esempio, il GDPR).

Il CLOUD Act contempla anche i MLAT come ulteriore meccanismo idoneo a coprire gli ambiti che non fossero coperti dagli Agreement. La peculiarità di tali accordi, stipulati per ordinarie vie diplomatiche nella forma di trattati internazionali, risiede nel fatto che questi non consentono, in linea di principio, di riconoscere - come invece avviene nei CLOUD Agreement - l'efficacia automatica di ordini dell'altro Stato contraente ma solamente la possibilità di inoltrare alle Autorità competenti dello Stato una richiesta da convalidarsi ma che potrebbe anche essere rifiutata.

Nonostante sia necessario che le leggi dei paesi con cui vengono sottoscritti gli Agreement siano a livello con gli standard degli Stati Uniti, valutazione che come detto verrà effettuata ex ante, il procedimento per l'emanazione del provvedimento, corrispondente al US *warrant*, deve così, nel caso del MLAT seguire l'*iter* previsto dalla legge nazionale dell'altro paese per poter arrivare al provvedimento finale e richiedere, ed ottenere, le informazioni direttamente dal provider.

I MLAT possono dunque aversi per quanto riguarda la materia delle misure a contrasto di reati gravi, in caso di procedimenti penali, al fine della prevenzione, individuazione, indagine o perseguimento degli stessi.

Le critiche al CLOUD Act

L'approvazione del CLOUD Act ha riscosso severe critiche in Europa come a livello mondiale.

Tali critiche riguardano, per lo più, la eccessiva semplificazione delle procedure e la riduzione delle garanzie poste a presidio dei diritti fondamentali che si viene a determinare quando viene stipulato il CLOUD Agreement, considerate peggiorative rispetto al regime in precedenza assicurato dalla sola previsione dei MLAT, valida comunque anche prima del CLOUD Act.

L'effetto è infatti quello di ridurre l'efficacia di disposizioni di Stati terzi predisposti a tutela della protezione dei dati personali e abolire, nei fatti, la possibilità di opporsi richiedendo la *comity analysis* e, con essa, la considerazione delle ragioni di diritto dello Stato terzo potenzialmente ostative al trasferimento[69].

L'analisi della normativa evidenzia inoltre la mancanza di una procedura che preveda una qualsivoglia comunicazione o notifica ufficiale allo Stato in cui i dati sono archiviati o allo Stato di appartenenza della persona interessata dell'avvio di procedure di richiesta dati, anche ad accesso concluso o quando, comunque, le indagini non verrebbero compromesse, ha indotto, ad esempio, alcuni grandi provider cloud a introdurre una

65 Si tratta di una certificazione, da essere effettuata preventivamente, ad opera del US Attorney General del Congresso.
66 Cfr. Agreement of 3 October 2019 between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, disponibile online su https://cli.re/jJ7Z3D
67 Cfr. https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html
68 Cfr. Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses done at Amsterdam; 2 June 2016, disponibile su https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN
69 Cfr. Schwarz-Peifer, Data Localization, Under the CLOUD Act and the GDPR, Computer Law Review International, 2019/1

policy[70] di notifica al cliente delle richieste ricevute ai sensi del CLOUD Act.

Preoccupazione è stata inoltre espressa dal Parlamento europeo[71] circa l'ambito del trattamento dei dati personali, con particolare riferimento all'art. 48 del GDPR che subordina il riconoscimento di decisioni o sentenze di autorità straniere che dispongono il trasferimento o la comunicazione di dati personali, al loro fondamento su di un MLAT Agreement in vigore tra il paese richiedente e l'Unione europea (o un suo Stato membro) e non su un CLOUD Act Agreement. Sotto tale luce, il CLOUD Act non sembra offrire il conforto necessario affinché il provvedimento giurisdizionale possa essere considerato in linea con il GDPR. Infatti, in difetto di un accordo MLAT o di altra base legale ai sensi del GDPR, il provider non potrebbero divulgare e trasferire legalmente i dati personali richiesti dagli USA. Per altro, a detto trasferimento non sarebbe neppure sembrato applicabile il Privacy Shield - recentemente invalidato dalla sentenza della CGUE Schrems II - in quanto lo stesso si applicava al trasferimento transatlantico dei dati personali per finalità commerciali.

L'EDPB e l'European Data Protection Supervisor (EDPS), intervenuti sulla questione, hanno concordato sulla necessità quantomeno di riconoscere e rendere esecutivo l'US CLOUD Act sulla base di un accordo internazionale che contenga garanzie procedurali e sostanziali per allineare i livelli di protezione del trasferimento dei dati secondo standard europei[72]. In tal modo, la base giuridica del trattamento sarebbe riconducibile all'obbligo di legge, riconosciuto dall'art. 6, par. 1, lett. c) del GDPR.

Le discrasie in breve riportate appaiono come la sintomatologia di una grave tensione tra il CLOUD Act ed taluni diritti fondamentali riconosciuti in ambito europeo, tra cui in particolare il diritto alla privacy, che viene individuato dal diritto primario dell'Unione e, segnatamente, dalla Carta europea dei diritti fondamentali dell'Unione europea (artt. 7 e 8), di cui il GDPR rappresenta precipitato normativo, nonché dalla Convenzione Europea dei Diritti dell'Uomo (art. 8) come declinato dalla giurisprudenza della CGUE e della Corte EDU.

Anche il Council of Bars and Law Societies of Europe (CCBE) ha manifestato[73] la sua preoccupazione in ordine alle informazioni estrapolabili dalle comunicazioni intercorrenti tra avvocati e clienti. La riservatezza è elemento essenziale dell'etica professionale ed è generalmente riconosciuta come corollario del diritto alla difesa. Il sequestro indiscriminato e non procedimentalizzato di materiale privilegiato o coperto dal segreto professionale lede gravemente i diritti delle persone sottoposte alla disclosure di informazioni, a maggior ragione se il difensore non viene messo al corrente dell'avvenuto sequestro. Pertanto, anche sotto tale profilo il CLOUD Act si pone come potenzialmente lesivo dei diritti delle persone ad un giusto processo. Ed invero, la stessa la mancata previsione dell'inammissibilità delle prove raccolte con tali modalità fa protendere per l'incompatibilità della disposizione con i principi poc'anzi richiamati.

> *"Deve essere verificata la compatibilità degli ordini emanati in base al CLOUD Act con le previsioni del GDPR".*

La rilevanza transnazionale della disposizione induce ad una riflessione sulle possibili implicazioni in termini di comity internazionale, che il CLOUD Act sembra risolvere in via autoritativa e secondo logiche volte espansione della giurisdizione, non sempre propriamente compatibili con i sistemi giuridici con cui si relaziona.

Gli sviluppi in tema di cooperazione giudiziaria

Le preoccupazioni che sono state espresse in ambito europeo, da più parti, sono in parte riflesse nella raccomandazione di decisione del Consiglio[74] che ha autorizzato l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la coope-

70 Cfr. White Paper Google su Data residency, operational transparency,and privacy for European customers on Google Cloud, disponibile all'URL: https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf?hl=cs
71 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, nn. 27 e 28 available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN
72 Si veda la risposta congiunta EDPB/EDPS del 12 luglio 2019, accessibile al seguente link: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_de nella quale l'EPDB ha concluso che: "service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the US on such requests.".
73 Si veda il position paper del 28 febbraio 2019 accessibile al seguente link: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf
74 Atto del 5 febbraio 2019, accessibile al seguente link:
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0070

razione giudiziaria in materia penale.

Un precedente accordo, concernente la cooperazione transatlantica in materia di giustizia penale e la lotta contro la criminalità organizzata ed il terrorismo, era stato firmato nel giugno 2003 ed è entrato in vigore nel febbraio 2010. Detto accordo è stato poi riesaminato nell'aprile 2016.

Dal canto suo, l'Unione europea vorrebbe affrontare la questione dell'accesso transfrontaliero a dati e metadati nella prospettiva della protezione dei diritti e dei valori europei, integrando nel nuovo Agreement sia l'accordo UE-USA sulla protezione dei dati e sulla privacy del febbraio 2017 che il Judicial Redress Act statunitense, estendendo ai cittadini europei le garanzie del US Privacy Act del 2016.

In particolare, secondo il Consiglio, "*L'accordo dovrà rispettare i diritti fondamentali, le libertà e i principi generali del diritto dell'UE, come sanciti dai trattati dell'Unione europea e dalla Carta dei diritti fondamentali, i diritti procedurali tra cui il diritto a un ricorso effettivo e a un giudice imparziale, la presunzione di innocenza e i diritti della difesa, i principi della legalità e della proporzionalità dei reati e delle pene e qualsiasi obbligo che incombe alle autorità giudiziarie o di contrasto a tal fine. Per quanto riguarda le necessarie garanzie in materia di protezione dei dati per i dati personali trasferiti dall'Unione europea agli Stati Uniti, le disposizioni applicabili dell'accordo UE-USA in materia di protezione dei dati e della vita privata saranno integrate da garanzie aggiuntive per tener conto del livello di sensibilità delle categorie di dati interessate e delle esigenze specifiche del trasferimento di prove elettroniche direttamente dai prestatori di servizi*."

Le negoziazioni formali tra UE e US sono iniziate nel settembre 2019 e, tuttavia, non si sono ancora concluse.

4.2. La disciplina europea

Lo scenario europeo appare in movimento. Nel tempo sono state poste in essere riforme periodiche concernenti nuovi meccanismi di cooperazione, con l'intento di adeguare l'attività investigativa al processo di digitalizzazione di società e sistema economico, accelerare le procedure di reperimento delle prove elettroniche transfrontaliere nonché ricondurre a sistema le procedure nazionali frammentate.

Bisogna ricordare in primis la Direttiva 2014/41/UE del Parlamento europeo e del Consiglio del 3 aprile 2014 relativa all'ordine europeo di indagine penale (OEI), che rappresenta una versione europea della rogatoria internazionale. Quest'ultima consiste nell'incarico che un'autorità giudiziaria assegna ad una seconda, ubicata in diversa giurisdizione, di eseguire un atto processuale legato a necessità afferenti ad un procedimento o un processo penale, in itinere innanzi all'incaricante. Il contenuto della rogatoria può ovviamente essere l'attività di acquisizione probatoria, nell'ambito della quale rientrano le richieste di accesso ai dati contenuti in un server.

Si ricordi, per completezza, che la materia dell'assistenza giudiziaria è regolata innanzitutto dalla Convenzione europea d'assistenza giudiziaria penale, firmata a Strasburgo in data 20 aprile 1959 e, nel contesto europeo, dalla Nuova convenzione di assistenza giudiziaria in materia penale tra i quindici Stati membri dell'Unione europea firmata il 29 maggio 2000.

Con stretto riferimento alla cooperazione contro la criminalità informatica, deve poi essere menzionata la Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001 (c.d. Convenzione di Budapest), riguardante, *inter alia*, le procedure coordinate da seguire per l'ottenimento delle prove elettroniche. La convenzione di Budapest, ratificata da un numero cospicuo di Stati membri, prevede istruttorie più rapide, data la natura delle prove e la loro rapidità circolazione.

Tuttavia, gli strumenti giuridici attuali sembrano tuttora armi spuntate per contrastare la diffusa parcellizzazione di informazioni che caratterizza il modello strutturale della tecnologia adoperata dai cloud. Ed in effetti, se da un lato vi è un problema di tempestività e durata delle richieste avanzate presso autorità straniere, dall'altro queste potrebbero non essere risolutive, se si considera che i dati, o meglio i relativi bit, potrebbero essere distribuiti in ubicazioni diverse e sottoposte a diverse giurisdizioni. Inoltre, anche in questo caso riemerge il dilemma se i dati ricercati possano essere considerati nel possesso e nel controllo del provider, qualora quest'ultimo non abbia la possibilità di superare il sistema di crittografia

per ricomporre il dato e poterlo visualizzare.

Recentemente si sta vagliando l'opportunità di introdurre anche in Europa nuove misure che prescindano dal luogo di conservazione dei dati, indirizzando la richiesta direttamente al cloud provider. L'esigenza scaturisce dal sempre crescente numero di indagini che richiedono l'approvvigionamento di prove contenute su server esteri, anche se con riferimento a reati commessi interamente sul territorio procedente.

Al riguardo deve rilevarsi che è stata messa in cantiere dall'aprile 2018 una proposta di Regolamento per gli ordini europei di produzione e di conservazione di prove elettroniche[75] che opererà in ambito penale. Lo strumento dovrebbe affiancare il già menzionato OEI per semplificare la raccolta di prove detenute in altra giurisdizione. In particolare, secondo la proposta, il provvedimento per reperire le prove elettroniche (c.d. "e-evidence") sarebbe reciprocamente riconosciuta - tramite convalida - tra gli Stati membri, coinvolgendo l'autorità estera solo in caso di necessaria esecuzione forzata.

Tuttavia, deve rilevarsi che nonostante la semplificazione procedurale, che sembra riprendere il modello statunitense, il Regolamento è comunque una fonte di diritto derivato e, pertanto, deve conformarsi al sostrato giuridico primario, che delinea i diritti fondamentali dell'UE.

La proposta di regolamento affronta anche la tematica degli obblighi di reciprocità con Stati terzi, ma dovrà necessariamente confrontarsi con l'evoluzione dei negoziati - che si sono instaurati successivamente alla presentazione della proposta da parte della Commissione - intercorrenti tra UE e US per l'elaborazione dell'Agreement.

È inoltre da considerare con attenzione il già citato Regolamento (UE) 2018/1807 per il libero flusso dei dati non personali che si propone di eliminare le barriere che attualmente impediscono la libera circolazione transfrontaliera all'interno della UE dei dati non personali, vale a dire i dati che non riguardano persone fisiche identificate o identificabili ma, al contempo, sembra prefigurare una disciplina UE della raggiungibilità giuridica di questa tipologia di dati.

Le nuove disposizioni contenute nel Regolamento 2018/1807 integrano quelle che prevedono la libera circolazione e la portabilità dei dati personali all'interno della UE contenute nel GDPR, ed assieme a queste ultime, nell'intenzione del legislatore europeo, vorrebbero contribuire alla creazione di quello "spazio comune europeo dei dati" auspicato più volte dalla stessa Commissione europea[76], come uno dei presupposti per lo sviluppo del mercato unico digitale e dell'economia dei dati all'interno dell'Unione. Il Regolamento 2018/1807 in questione individua principalmente due categorie di ostacoli alla libera circolazione dei dati non personali: essi sono le pratiche di vendor lock-in nel settore privato e gli obblighi di "localizzazione" dei dati[77] posti in essere dalle autorità dei singoli Stati membri. Questi ultimi sono quelli rilevanti ai fini del tema della raggiungibilità. Essi possono essere individuati nelle legislazioni degli Stati membri che impongono (a) obblighi di localizzazione dei dati a fini di trattamento in un determinato territorio, o (b) requisiti specifici che rendono più difficile trattare dati al di fuori di un determinato territorio.

La Commissione ha quindi individuato numerose restrizioni relative ai luoghi di archiviazione o di elaborazione dei dati, che interessano la mobilità dei dati, in diversi settori, ad esempio:

- le autorità di vigilanza che raccomandano ai fornitori di servizi finanziari di archiviare i dati a livello locale;
- le norme in materia di segreto professionale (come ad esempio nel caso del settore sanitario) che prevedono l'archiviazione o l'elaborazione dei dati a livello locale;
- le norme generali che impongono l'archiviazione locale delle informazioni generate dal settore pubblico,

75 Proposta del 17 aprile 2018 accessibile al seguente link: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

76 Cfr. Comunicazione della Commissione europea del 2 luglio 2014 "Verso una florida economia basata sui dati", nonché le Comunicazioni del 25 aprile 2018 e del 15 maggio 2018;

77 L'art. 3, n. 5), definisce obbligo di localizzazione dei dati "*qualsiasi obbligo, divieto, condizione, limite o altro requisito, previsto dalle disposizioni legislative, regolamentari o amministrative di uno Stato membro o risultante dalle prassi amministrative generali e coerenti in uno Stato membro e negli organismi di diritto pubblico, anche nell'ambito degli appalti pubblici, fatta salva la direttiva 2014/24/UE, che impone di effettuare il trattamento di dati nel territorio di un determinato Stato membro o che ostacola il trattamento di dati in un altro Stato membro*".

indipendentemente dalla sensibilità delle stesse;

- le norme che impongono di utilizzare dispositivi tecnologici che siano omologati o certificati in un determinato stato membro (cfr. considerando (4) del Regolamento).

A fronte di obblighi di localizzazione dei dati, come quelli appena descritti, il Regolamento 2018/1807 dispone l'illegittimità di norme nazionali che impongano obblighi di localizzazione, se non per ragioni di pubblica sicurezza e nei limiti del principio di proporzionalità e, soprattutto, prevede che debba essere garantito alle "autorità competenti"[78] l'accesso ai dati archiviati o elaborati in un altro Stato membro (cfr. art. 5).

Esso si applica alle attività di trattamento di dati elettronici diversi dai dati personali nell'Unione, che sono fornite come servizio ad utenti (persona fisiche o giuridiche, comprese pubbliche autorità e organismi di diritto pubblico) residenti o stabiliti nell'Unione, indipendentemente dal fatto che il fornitore del servizio sia o meno stabilito nell'Unione; o effettuate da una persona fisica o giuridica residente o stabilita nell'Unione.

Nel caso di un insieme di dati composto sia da dati personali sia da dati non personali, il Regolamento 2018/1807 si applica solo alla parte dell'insieme che contiene i dati non personali, mentre nel caso in cui i dati personali e non personali in un determinato insieme fossero indissolubilmente legati, il Regolamento 2018/1807 lascia impregiudicata l'applicazione del GDPR.

Il considerando (9) del Regolamento 2018/1807 precisa che l'espansione dell'Internet of Things, l'intelligenza artificiale e l'apprendimento automatico sono fonti importanti di dati non personali, come nel caso del loro utilizzo in processi automatizzati di produzione industriale.

Lo stesso considerando (9) fornisce alcuni esempi specifici di dati non personali: gli insiemi di dati aggregati e anonimizzati usati per l'analisi dei metadati, i dati sull'agricoltura di precisione che possono monitorare e ottimizzare l'uso di acqua e pesticidi ed i dati sulle esigenze di manutenzione di impianti industriali.

Il considerando (9) precisa inoltre che, qualora i progressi tecnologici consentissero di trasformare dati anonimizzati in dati personali, essi sarebbero considerati come dati personali, con la conseguente applicazione del GDPR.

Infine, l'art. 2, paragrafo 3, del Regolamento 2018/1807 precisa che lo stesso non si applica alle attività che non rientrano nell'ambito di applicazione del diritto dell'Unione. Su questo punto, il considerando (12) ci ricorda che, ai sensi dell'art. 4 del Trattato sull'Unione europea, la sicurezza nazionale è di esclusiva competenza di ciascuno Stato membro.

4.3. La disciplina nazionale

Passando al contesto domestico, è bene ricordare l'art. 234-bis c.p.p. secondo cui: "*È sempre consentita l'acquisizione di documenti e dati informatici conservati all'estero, anche diversi da quelli disponibili al pubblico, previo consenso, in quest'ultimo caso, del legittimo titolare*". La norma reinterpreta l'art. 32 della Convenzione di Budapest ed opera senza necessario mezzo della rogatoria o dell'OEI. Non appaiono limitazioni in ordine ai reati per i quali l'articolo risulta applicabile.

L'ambito applicativo interseca la tematica oggetto del presente Studio con riferimento ai dati informatici conservati all'estero e non accessibili al pubblico, proprio in quanto organizzati secondo il modello del cloud. Con riferimento a tale ultima osservazione deve però specificarsi che qualora i contenuti siano relativi a comunicazioni private archiviate (per il flusso di informazioni dovrebbe applicarsi l'intercettazione ex art. 266-bis c.p.p.) o comunque che riguardino metadati, tornerebbe necessario per l'acquisizione un provvedimento dell'autorità giudiziaria e la richiesta a mezzo di rogatoria internazionale, o OEI, rendendo la disposizione mero incisiva di quanto non sia in apparenza.

78 Definite dal Regolamento come "un'autorità di uno Stato membro o qualsiasi altro ente autorizzato, in virtù del diritto nazionale, a esercitare una funzione pubblica o a esercitare i pubblici poteri, che ha la facoltà di ottenere accesso ai dati trattati da una persona fisica o giuridica ai fini dell'esercizio delle sue funzioni ufficiali, come previsto dal diritto dell'Unione o nazionale". Come si vede la definizione lascia aperta la porta al fatto che l'Autorità possa essere anche un ente estero, purché "autorizzato".

Ad avvalorare le perplessità sulla funzionalità semplificativa della disposizione in esame è l'ambiguo riferimento al "consenso del legittimo titolare", concetto evanescente e che di certo non può essere ricondotto certo senza riserve alcune al cloud provider, a meno che non venga definito tale all'interno del contratto con l'utente. D'altro canto, il parallelismo con il concetto di titolare come individuato nel GDPR risulterebbe inconferente e limitato ai soli dati personali. Altrettanto problematico sarebbe considerare tale il soggetto sottoposto alle indagini (o imputato), dovendo essere prestato da questo un paradossale consenso.

E comunque la disposizione in esame risulta poco incisiva rispetto alle moderne tecnologie di storage che, come detto più volte, tendono ad un'ubicazione parcellizzata e diffusa dei dati, rendendo difficile identificare il paese estero a cui indirizzare la richiesta, giacché la stessa dovrebbe essere rivolta ad una pluralità di destinatari - tra l'altro difficilmente identificabili - che nella maggior parte dei casi non sono situati nel medesimo paese della sede del provider.

CAPITOLO 5
CONCLUSIONI

5.1 Il quadro complessivo

Lo Studio ha evidenziato come la scelta del cloud provider debba essere oggetto di una valutazione specifica qualora i dati affidati al cloud siano strategici, o comunque rilevanti, per l'impresa o l'ente titolare.

La criticità dei dati non riguarda solamente la natura di dati personali dei medesimi, ma qualsiasi valenza industriale o valore pubblico che i dati medesimi possono rivestire. Da un punto di vista imprenditoriale i dati non personali, in particolare aziendali, possono essere più delicati da affidare in cloud rispetto a dati personali in virtù del loro valore economico e della recente disciplina UE che sembra aprire a nuovi meccanismi di accessibilità transfrontaliera dei medesimi, non possibili invece per i dati personali. Il discorso riguarda soprattutto il mercato B2B e corporate ma, in un'ottica di ampio respiro, potrebbe essere esteso anche al mercato consumer e SoHo. In effetti, qualsiasi utente privato dovrebbe essere ben consapevole circa la sorte e lo status dei propri dati una volta che questi vengono immessi in un sistema cloud, soprattutto perché in tale relazione il cloud provider detiene uno strapotere contrattuale.

L'affidamento in cloud porta con sé innegabili ed amplissimi vantaggi nella gestione dei dati, che difficilmente una infrastruttura locale potrebbe assicurare in alternativa. Si tratta di vantaggi non sono soltanto di tipo economico, ma anche e soprattutto in termini di sicurezza, scalabilità delle infrastrutture e possibilità di condivisione ed elaborazione dei dati. Ma il cambiamento di paradigma, dal locale al cloud, porta con sé ulteriori problematiche e, in particolare, il potenziale rischio di perdita di controllo sui propri dati, non solo in termini tecnologici, ma anche giuridici.

Nel contesto attuale, proprio per la prospettiva di tali enormi vantaggi ma in assenza di ponderata valutazione dei rischi collaterali ed a fronte di strumenti giuridici di contrasto ancora acerbi, vi è il rischio che la decisione di esternalizzare i dati in cloud possa essere presa senza le dovute valutazioni ed attenzioni dal punto di vista contrattuale e normativo e ciò, in particolare, per quanto riguarda il tema della "raggiungibilità" che è stato l'oggetto di analisi del presente Studio.

Il quadro normativo che si va delineando a livello internazionale - e del quale il CLOUD Act americano costituisce una delle propaggini più avanzate - prevede un regime per cui le autorità pubbliche che abbiano giurisdizione sul cloud provider al quale i dati vengono affidati abbiano, in certe condizioni, la possibilità di "raggiungere" tali dati anche se essi sono rientrano nella titolarità di un soggetto che non ricade nella propria giurisdizione e persino (e qui cade la novità principale del CLOUD Act) quando essi non siano fisicamente ospitati in server soggetti alla giurisdizione dello Stato che ha emanato l'ordine. Questa possibilità, che non è limitata all'ordinamento USA ma sta trovando progressiva diffusione nei vari ordinamenti mondiali, compresa l'Unione Europea, deve però essere inquadrata nella corretta prospettiva.

Occorre infatti considerare che non esiste, se non in ordinamenti che non siano rispettosi dei Diritti Umani, possibilità di accesso indiscriminato delle Autorità pubbliche e governative ai dati esternalizzati in cloud. L'accesso delle autorità pubbliche ai dati detenuti dai cloud provider resta regolato dalle ordinarie procedure giuridiche nazionali oppure internazionali, quest'ultimo caso qualora tali dati riguardino soggetti - privati o d'impresa - cittadini di altri ordinamenti: ad esempio, i cittadini UE sono tutelati dal GDPR per quanto riguarda i dati personali mentre l'uso dei dati in procedimenti penali, come si è detto, è regolato dalla Convenzione di Budapest. Gli Stati si sono già da tempo dotati di strumenti per accedere ai dati dei propri cittadini ed imprese gestiti in cloud dai propri provider nazionali nelle circostanze che il diritto considera lecite (sicurezza nazionale, prevenzione reati, indagini su reati, antiterrorismo, ecc.).

Dunque, affidare i dati in cloud a livello nazionale non comporta di per sé escluderli dalla "raggiungibilità" delle proprie autorità pubbliche nelle circostanze in cui tali dati sarebbero stati comunque "raggiungibili" ove fossero rimasti presso il titolare o, addirittura, di autorità estere autorizzate dallo Stato di residenza, in circostanze in cui il diritto nazionale non offra specifiche ragioni di protezione (es. dati non personali e non protetti quali proprietà intellettuale o altrimenti e specificamente contrattualizzati come indisponibili al cloud provider).

5.2 Ipotesi di criticità circa la raggiungibilità dei dati, e relative raccomandazioni

Vi sono però aspetti critici della "raggiungibilità" che riguardano quelle circostanze in cui uno Stato estero, che non sarebbe stato in grado di "raggiungere" i dati ove fossero rimasti nella gestione locale del titolare o presso un cloud nazionale, in certe circostanze quali quelle che sono state descritte al Capitolo 4, potrebbe per il solo motivo dell'affidamento in cloud ad un provider soggetto alla propria giurisdizione o alla giurisdizione di uno Stato con cui lo Stato abbia stipulato accordi internazionali, essere in grado di "raggiungere" i dati di un soggetto anche se localizzati al di fuori del proprio territorio. Si tratta di uno scenario che può sensibilmente influire sulle scelte commerciali delle imprese e dei committenti pubblici, creando delle serie barriere alla diffusione dei servizi cloud a livello globale.

In tali casi, la soluzione individuata nel presente Studio consiste nel negoziare, attraverso una accurata analisi e negoziato (ove possibile) del contratto e, in particolare, degli allegati tecnici quali il DPA, lo SLA e gli allegati sulla sicurezza, una serie di cautele e, segnatamente:

- uno storage dei dati distribuito, in maniera fissa o variabile, tra molteplici giurisdizioni, preferibilmente in Stati Membri UE per assicurare che i dati siano gestiti con le tutele previste dal GDPR e che tali tutele siano applicate per via di legge statuale, e non per obbligo convenzionale del provider;
- il criptaggio dei dati presso il cloud provider, con chiave del cliente e non disponibile al cloud provider (salvo laddove sia indispensabile che il cloud provider abbia accesso ai dati), in modo da assicurare che, anche dove vi sia un ordine di esibizione dei dati, tale ordine non possa che avere ad oggetto dati criptati;
- l'applicazione ai contratti cloud, ove non vi siano specifiche esigenze, di legge contrattuale e giurisdizione per controversie di Stati UE, in modo da assicurare che eventuali contese su ordini di esibizione abbiano luogo sulla base del diritto UE e avanti a Corti UE;
- un'adeguata informativa precontrattuale, anche tramite la AUP, circa situazioni, servizi e tipologie di dati che il cloud provider considera accessibili alle proprie Autorità pubbliche ed in base a quali tipi di ordini (su cui anche infra);
- l'ottenimento dai cloud provider di specifiche garanzie circa l'informazione e la possibilità di intervento in caso vi siano richieste di accesso da parte di autorità pubbliche ai dati in cloud;
- l'ottenimento dal cloud provider di informazioni preventive alla stipula del contratto su come lo stesso si sia comportato a fronte di richieste di accesso ai dati in cloud da parte di autorità pubbliche in servizi analoghi a quelli proposti e di report periodici sul punto;
- l'ottenimento di garanzie circa gli eventuali subappaltatori, i quali dovranno utilizzare i medesimi territori, essere della medesima nazionalità (o, comunque, di nazionalità autorizzate dal Cliente) ed offrire le medesime garanzie contrattuali;
- la previsione contrattuale su come gestire il rientro dei dati qualora, a seguito di mutamenti legislativi, le garanzie contrattuali di cui sopra non possano più essere rispettate dal cloud provider, oppure quando quest'ultimo non può più mantenere i dati per ordine dell'autorità straniera o per decisione dello stesso provider.[79]

> *"Con il CLOUD Act USA le Autorità pubbliche con giurisdizione sul cloud provider a cui i dati vengono affidati, in certe condizioni possono "raggiungere" tali dati anche se il titolare non ricade nella propria giurisdizione e anche – questa la novità principale del CLOUD Act – se i dati non sono fisicamente ospitati in server soggetti alla giurisdizione dello Stato che ha emanato l'ordine".*

Solo nei prossimi anni si saprà se il quadro internazionale è capace di creare una rete di accordi fra Stati, ed in particolare tra grandi macro-aree economiche, che renderanno automatica l'operazione di apprensione dei

79 Si veda ad esempio il caso Parler / AWS Amazon, già citato.

dati a livello internazionale sulla base di principi comuni ed armonizzati. Le recenti vicende in tema di data flow, ed in particolare l'annullamento del Privacy Shields, hanno da un lato creato forte incertezza nel settore, dall'altro responsabilizzato maggiormente le imprese ed i governi che hanno compreso la necessità di dover creare una governance globale dei dati.

Attualmente anche previsioni come il CLOUD Act USA, pur "teoricamente" efficienti, scontano notevoli complessità applicative date dalla necessità di arrivare alla esecuzione dei *warrant* di esibizione dei dati verificandone la legittimità caso per caso.

È possibile contrastare la stipula di tali accordi automatici con un'opera tesa a chiarire in maniera puntuale, a beneficio dei giudici chiamati ad interpretare le situazioni e dei cloud provider/entità chiamate a valutare l'eventuale opposizione, quali siano le situazioni di illegittimità delle richieste, in maniera da formare una base di casi che, ad oggi, manca e che, a sua volta, darà certamente spunti per migliorare quanto previsto negli accordi contrattuali.

In questo gli stessi cloud provider possono lavorare concretamente in termini di informativa pre-contrattuale, specificando non solamente quali siano le AUP ma anche le situazioni, servizi e tipologie di dati che essi considerano accessibili alle proprie Autorità pubbliche ed in base a quali tipi di ordini, evitando invece clausole generali che prevedano l'obbedienza a "qualsiasi ordine" emanato "in base alla legge applicabile", poiché il tema della raggiungibilità o meno dei dati da parte di entità esterne, in una società sempre più fondata sui dati, non può che essere una questione da chiarire con estrema precisione e trasparenza.

Un rimedio potrebbe ritrovarsi nello studio di un "contratto tipo" di cloud e di un codice di condotta - anche internazionale - che potrebbe essere adottabile come best practice da qualsiasi cloud provider voglia presentarsi al cliente offrendo le più ampie garanzie di protezione transfrontaliera del dato e contenente impegni verificati da terze parti in questo senso. Anche a fronte di un tale meccanismo si è visto però che alcune "raggiungibilità" di imperio possono essere ineludibili se i dati vengono elaborati in territori soggetti a normative che prevedono la soggezione dei cloud provider ivi operanti ed in possesso dei dati a procedure d'imperio di messa a disposizione dei dati verso autorità - giudiziarie o governative - richiedenti senza adeguate possibilità di opporsi per il titolare dei dati.

Peraltro, come si è evidenziato nel documento, il dettaglio contrattuale - che potrebbe arrivare a divenire un "codice di condotta" - diventa quanto mai essenziale e strumento di garanzia sia per l'utente che per il provider in determinati casi - oggi più che mai di attualità - per regolamentare procedure di inibizione, restituzione e cancellazione dei dati che l'utente affida al cloud provider e ciò sia a fronte di ordini dell'Autorità competente, sia a fronte di iniziative in autotutela del cloud provider.

PROFILI DEGLI AUTORI

EUGENIO PROSPERETTI

Eugenio Prosperetti è avvocato e docente universitario presso l'Università LUISS "Guido Carli" di Roma. Si dedica da oltre 20 anni ai temi giuridici dellle nuove tecnologie, assistendo imprese nazionali e multi-nazionali sui questioni regolamentari, contrattuali e giudiziali riguardanti servizi, contratti e compliance nei mercati dell'information technology.

Studi

- 2005: dottore di ricerca in diritto commerciale con tesi avente ad oggetto "La regola del rapporto tra creatore e utilizzatore di software" (Facoltà di Economia, Università di Roma "Tor Vergata")
- 1998: laurea in giurisprudenza con 110/110 presso l'Università di Roma "Tor Vergata"

Attività professionale

Iscritto all'Ordine degli Avvocati di Roma, con abilitazione alla professione di Avvocato, giurisdizioni superiori.
Dopo alcuni anni di esperienza in studi internazionali a partire dal 1998 (Baker & McKenzie - associate e Portolano Colella Cavallo Prosperetti - socio), assume la guida nel 2005 del proprio studio legale in Roma dove assiste clienti italiani ed esteri, ivi incluse pubbliche amministrazioni, in materia che comprendono regolamentazione dell'information technology, piattaforme cloud complesse, privacy e gestione dati, comunicazioni elettroniche, sistemi di pagamento digitale, gestione dati e servizi nei sistemi di intelligenza artificiale, sistemi blockchain, antitrust nelle piattaforme digitali, compliance antitrust, piattaforme e-government, commercio elettronico, procedimenti per pratiche commerciali scorrette, appalti pubblici. Assiste inoltre la clientela nel relativo contenzioso amministrativo e civile e verso autorità indipendenti.

Attività istituzionale:

Da maggio 2017 a giugno 2019: incarico di 25 mesi quale consulente giuridico Agid - progetto FICEP (First Italian Crossborder Eidas Proxy) per l'interoperabilità transfrontaliera delle identità elettroniche.

- 2017: componente della Task Force Agid per l'Intelligenza Artificiale
- 2016: componente dei tavoli di lavoro che hanno studiato e redatto la riforma del Codice dell'Amministrazione Digitale (in attuazione art. 1 L. 124/2015 - riforma P.A.) presso Ministero della Funzione Pubblica e chiamato a partecipare quale tecnico di supporto alle riunioni del Comitato di Indirizzo Agid sui medesimi temi, ha ricevuto il ringraziamento del Ministro Madia per l'opera prestata.
- 2014-2015: componente del Tavolo Permanente per l'Innovazione e l'Agenda Digitale Italiana presso la Presidenza del Consiglio dei Ministri istituito ex art. 47, L. 5/2012, nominato con DPCM
- 2013-2014: ha partecipato quale invitato ai gruppi di lavoro presso la Presidenza del Consiglio dei Ministri che hanno studiato e poi redatto la normativa sullo SPID - Sistema Pubblico dell'Identità Digitale (convocato quale tecnico a tutte le riunioni, ha ricevuto ringraziamento dell'allora commissario Francesco Caio per la partecipazione e il contributo)
- 2010: Componente del gruppo di lavoro incaricato di uno dei Work Packages dello studio ISBUL - Infrastrutture a Banda Larga e Ultra Larga promosso da AGCOM (formalmente riportato tra gli Autori dello Studio)

- 2007: È stato componente, nominato con apposito DM, della Segreteria Tecnica del Ministro delle Comunicazioni, On. Paolo Gentiloni occupandosi in quella sede dell'attuazione in Italia di normativa delle comunicazioni elettroniche e normativa attuativa di Trattati Internazionali in materia di sicurezza informatica e di copyright digitale e componente della commissione che ha redatto bando e disciplinare wi-max/BWA italiano; ha ricevuto encomio del Ministro Paolo Gentiloni per il lavoro svolto
- 2007: E' stato componente del Comitato per la Tutela della Proprietà Intellettuale presso la Presidenza del Consiglio dei Ministri

Attività accademica principale:

- dal 2021, professore a contratto di "Algorithm and Data Management Law" presso la Facoltà di Giurisprudenza dell'Università LUISS "Guido Carli" di Roma;
- dal 2015 al 2020 professore a contratto di Legal Aspects of Information Technology (informatica giuridica progredita in lingua inglese) presso la Facoltà di Giurisprudenza dell'Università "LUISS Guido Carli" di Roma;
- dal 2017: idoneo quale professore di seconda fascia di diritto commerciale (IUS/04 - SSD 12/B1);
- è autore di numerose pubblicazioni in riviste scientifiche e volumi collettanei; tra i temi trattati: contratti software, contratto cloud, regime giuridico dei big data, sull'opera digitale, sul digital rights managment e del saggio monografico "La circolazione dell'opera digitale tra regole e mercato" (Giappichelli, 2012)

INNOCENZO MARIA GENNA

Innocenzo Genna è un giurista specializzato in politiche e regolamentazioni europee per il digitale, la concorrenza e le liberalizzazioni. Con oltre 25 anni di esperienza nel settore, attualmente svolge la propria attività professionale a Bruxelles, dove ricopre incarichi associativi ed assiste operatori italiani e stranieri.

Studi

Innocenzo Genna è laureato in giurisprudenza, ho conseguito due master in diritto europeo ed un diploma francese in diritto comparato:

- è stato studente Erasmus dal 1989 al 1990 a Brema (Germania),e nello stesso periodo ha frequentato privatamente alcuni corsi a Berlino Ovest presso la Freie Universität;
- si è laureato in giurisprudenza nel 1991 a Macerata con il massimo dei voti (110 e lode), con una tesi in diritto internazionale vertente sullo status giuridico di Berlino fino alla riunificazione tedesca;
- nel 1992 ha conseguito il Master in diritto europeo (LLM) presso il Collegio d'Europa a Bruges, con una tesi su "Droit communautaire et privatisations";
- nell'agosto 1993 ha conseguito il Diplôme supérieur en droit comparé rilasciato dalla Facoltà Internazionale di diritto comparato dell'Università di Strasburgo, completando una serie di corsi iniziati nel 1991 presso varie sedi accademiche, vale a dire Treviri, Strasburgo, Trapani e Firenze;
- nel settembre 1993 ha conseguito il Magister Iuris (LLM) presso la facoltà di giurisprudenza dell'Università di Treviri (Germania).

Esperienza professionale da avvocato

Ha conseguito l'abilitazione professionale forense nel 1995, ma le sue esperienze professionali nell'ambito legale sono iniziate già nel 1992. Si è occupato sia di diritto europeo che di diritto nazionale e comparato, con

particolare focus su digitale, privacy, antitrust, commerciale e societario:

- nel 1992 é stato praticante presso lo Studio legale Tizzano & Pappalardo a Bruxelles;
- dal marzo al settembre 1993 è stato praticante presso la Corte di Giustizia delle Comunità Europee a Lussemburgo;
- dall'ottobre 1993 fino al maggio 1997 ha svolto la professione forense presso lo Studio legale Bernini a Bologna;
- dal giugno 1997 fino al marzo 2002 ha svolto la professione forense presso lo Studio legale Ughi e Nunziante di Roma, dove è diventato socio nel 2000;
- nell'aprile 2002 è divenuto dirigente e capo dell'ufficio legale presso il Gruppo Tiscali a Cagliari e Milano, dove ha iniziato ad occuparsi anche di relazioni istituzionali europee, fino al 2006;
- dal 2004 al 2006 è stato membro del Comitato ministeriale Internet e Minori.

Esperienza professionale come giurista e nel public affairs europeo

- Dalla metà del 2006 Innocenzo Genna si è trasferito a Bruxelles dove ha iniziato ad occuparsi in maniera specialistica del diritto europeo del digitale, assistendo imprese italiane ed europee e rivestendo vari ruoli associativi):
  - nel 2007 è stato nominato presidente di ECTA (l'associazione europea degli operatori telecom new entrants), incarico che ha mantenuto fino al 2009;
  - dal 2010 ha fondato e dirige Genna Cabinet Sprl, una società di consulenza strategica e public affairs europeo nel settore del digitale e delle liberalizzazioni;
  - è Vicepresidente di Euroispa, l'associazione europea degli Internet Service Providers, nel cui board siede dal 2007;
  - dal 2016 è VicePresidente di MVNOEurope, l'associazione europea degli MVNO;
  - ha ricoperto l'incarico di Board member della EIF (European Internet Forum) in varie fasi, dal 2004 al 2006, e successivamente dal 2014 fino al 2021;
  - dal 2018 è membro del Communications Committee di IBA (International Bar Association) dove ricopre il ruolo di EU Liaison Officer.

Pubblicazioni e varie

- Innocenzo Genna cura il blog professionale dedicato al digitale europeo RadioBruxellesLibera (https://radiobruxelleslibera.com).
- È autore di varie pubblicazioni su numerosi temi legati al digitale. Inoltre, scrive di innovazione e digitale per La Stampa, il Foglio, Wired, Il Post, l'Huffington Post ed Agenda Digitale.
- È cofondatore di Digit@talians, il network dei professionisti italiani del digitale. In tale veste ha organizzato e gestito, dal 2014 ad oggi, numerosi eventi dedicati all'Italia ed al digitale.
- È cofondatore e presidente dell'associazione Allez les Marche! - Marchigiani a Bruxelles

Hanno collaborato:

GIULIO PASCALI

Laureato in Giurisprudenza presso l'Università "LUISS Guido Carli" in Roma, ha conseguito presso la stessa Università il Diploma di Perfezionamento in Diritto e Gestione della Proprietà Intellettuale, della Concorrenza e delle Comunicazioni. Avvocato dal 2012, svolge la propria attività professionale presso lo Studio Prosperetti in Roma, occupandosi di Privacy, Contratti Cloud e Appalti di servizi cloud, Servizi di comunicazione elettronica evoluti e telemarketing, Diritto d'Autore, Fintech e Start-Up Innovative.

Collabora con le cattedre di "Informatica Giuridica", "Legal Aspects of Information Technology" e "Algorithm and Data Management Law" presso il Dipartimento di Giurisprudenza della LUISS Guido Carli e le cattedre di "Informatica Giuridica" e "Diritto dell'Amministrazione Digitale" presso l'UniTelma Sapienza.

DAVIDE TUZZOLINO

Avvocato, collabora con lo Studio Prosperetti dal 2020 dove si occupa prevalentemente di data privacy, contratti cloud e contenzioso in materia di information technology. Ha maturato particolare esperienza in materia di trattamento dei dati personali, cloud e proprietà intellettuale digitale anche nell'ambito delle ricerche svolte nell'ambito accademico e sta attivamente lavorando ad alcune pubblicazioni di prossima uscita in questi ambiti.

Davide è al secondo anno del dottorato di ricerca presso l'Università Europea di Roma ed è assistente alla cattedra di Diritto Privato presso la stessa Università.

È inoltre assistente alla cattedra di Informatica Giuridica presso l'Università LUISS Guido Carli di Roma.

È fellow dell'Italian Academy of the Internet Code (IAIC).

Si è laureato presso l'Università degli Studi di Roma "La Sapienza", ha conseguito il diploma di specializzazione per le professioni legali presso l'Università Europea di Roma ed il master di secondo

livello in Diritto Privato Europeo presso l'Università degli Studi di Roma "La Sapienza".

RACCOLTA NOTE

1 Tra i dati più recenti, si veda Synergy Research Group, Primo trimestre 2020, http://www.globenewswire.com/NewsRoom/AttachmentNg/5d1edd1e-dc3c-4847-9fc0-23-a5e0eb20d5/en

2 Definizione di cui a https://cloud.italia.it .

3 Una gestione dei dati in cloud può offrire la possibilità di ospitare i dati in infrastrutture con livelli di sicurezza altrimenti inaccessibili a piccole e medie imprese imprese/studi professionali, e gestita da personale specializzato.

4 National Institute of Standards and Technology, US Department of Commerce; The Nist Definition of Cloud computing, Special Publication 800-145, settembre 2011. Disponibile al seguente link https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

5 Il "balzo in avanti" accaduto in Italia dovuto al Covid è ben rappresentato dalle statistiche Eurostat, Cloud computing - statistics on the use by enterprises, 19 gennaio 2021.

6 Dati Eurostat: Use of cloud computing services in enterprises, 2020.

7 Edizione 2019-2020 dell'Osservatorio Cloud Transformation dell'ottobre 2020; si veda il comunicato stampa accessibile al seguente link: https://www.osservatori.net/it/ricerche/comunicati-stampa/cloud-italia-mercato-2020

8 Intervento del Ministro Paola Pisano, al Summit Gaia-X online, 19 ottobre 2020, disponibile al seguente link qui: https://innovazione.gov.it/assets/docs/2020-11-19-intervento-ministra-pisano-a-gaia-x-summit.pdf

9 Adottato con DPCM del 17 luglio 2020 e disponibile al seguente link: https://www.agid.gov.it/sites/default/files/repository_files/piano_triennale_per_l_informatica_nella_pa_2020_2022.pdf

10 Versione adottata nel 2016, e seguito delle osservazioni della Commissione Europea, e disponibile al seguente link: https://www.agid.gov.it/sites/default/files/repository_files/documentazione/strategia_crescita_digitale_ver_def_21062016.pdf

11 I 3 elementi della strategia sono disponibili al seguente link: https://cloud.italia.it

12 Si vedano le Circolari AgID n. 2 e n.3 del 9 aprile 2018. Si veda anche: https://cloud.italia.it/marketplace/

13 Il Marketplace indica anche le modalità? di acquisizione con cui uno specifico servizio potrà? essere acquisito da una amministrazione rimandando allo strumento di procurement disponibile (il portale www.acquistinretepa.it) per procedere con l'acquisizione.

14 Cfr. https://www.consip.it/attivita/gara-spc-cloud-disponibile-la-documentazione e siti tematici dei contratti quadro aggiudicati: lotto1: https://www.cloudspc.it/ lotto 2: https://www.spc-lotto2-sicurezza.it/ lotto 3: www.spclotto3.it lotto 4: www.spclotto4.it

15 Al di là dei menzionati compiti contrattuali verso la PA, il principale scopo di questi reseller locali è quello di fornire forza commerciale sul territorio ed assicurare l'integrazione dei servizi (sia cloud che altri). Tuttavia, può essere scarsa la possibilità per tali reseller, se di piccole dimensioni, di influire su policy, tecnologia e governance dei

servizi cloud (ad esempio per quanto riguarda le policy di sicurezza, la distribuzione territoriale dei dati, la configurazione dei servizi), elementi che rimangono prevalentemente nelle mani dell'operatore globale. Si tratta di un aspetto da valutare caso per caso. Si nota peraltro, nel contesto nazionale, ad indicare la crescente importanza di realtà nazionali in grado di interloquire con i grandi operatori cloud (in questo caso Google), la recentissima costituzione della nuova società Noovle Spa dedicata alle attività di cloud enabling in cui è confluita la rete data center del gruppo Telecom. Italia.

16 Cfr. http://www.politicheeuropee.gov.it/it/comunicazione/approfondimenti/pnrr-approfondimento/

17 Definizione tratta da http://www.dei.unipd.it/~dinunzio/fdi-2014-2015/04_dati_informazioni.pdf

18 Regolamento (UE) 2014/910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, art. 3 comma 35.

19 Cfr. capitolo 2 dello Studio.

20 Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019, articoli 1 e 2.

21 Articolo 2 (1) della "Proposal for a Regulation of the European Parliament and of the Council on European data (Data Governance Act) {SEC(2020) 405 final}: "data' means any digital representation of acts, facts or information and any compilation of such acts, facts or information, including in the form of sound, visual or audiovisual recording;".

22 Articolo 4(1) del GDPR in relazione alla definizione di dato personale: "«dato personale»: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)".

23 Regolamento (UE) 2018/1807 del Parlamento europeo e del Consiglio del 14 novembre 2018 relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea

24 Interessante la norma italiana prevista dall'art. 64 comma 2-quinquies del CAD (Codice dell'Amministrazione Digitale approvato con D.Lgs. 82/2005 successivamente modificato e integrato) che prevede l'esenzione di responsabilità derivanti dall'obbligo generale di sorveglianza per le attività sui propri siti laddove si preveda l'accesso con il sistema di identità digitale SPID. Ciò perché gli utenti sono in questo caso identificati con certezza e dunque le attività compiute su siti in hosting sono ascrivibili con certezza a utenti identificati e non ricadono in nessun caso sul hosting provider.

25 Art. 3 GDPR

26 Così, infatti, dispone l'art. 832 del Codice civile, in una definizione rimasta sostanzialmente immutata dalla sua codificazione.

27 A mente dell'art. 810 del Codice civile, infatti, "sono beni le cose che possono formare oggetto di diritti".

28 Caso emblematico, con riferimento alle informazioni, è ad esempio rappresentato dalla tutela giuridica attribuita dall'ordinamento alle c.d. "Banche Dati", definite dall'art. 2, n.9 della L. 633/1941 come "raccolte di opere, dati o altri elementi indipendenti sistematicamente o metodicamente disposti ed individualmente accessibili mediante mezzi elettronici o in altro modo", e reputate degne di tutela da abusi di terzi in ragione del loro valore economico.

29 Ex art. 1140 del Codice civile, "il possesso è il potere sulla cosa che si manifesta in un'attività corrispondente all'esercizio della proprietà o di altro diritto reale. Si può possedere direttamente o per mezzo di altra persona, che ha la detenzione della cosa". Come è agevole notare, la definizione può forse giovare a ricostruzioni sul "possesso" di un bit da parte dei vari soggetti coinvolti, ma non aiuta del tutto a definire se chi possiede tali bit possa o debba esserne responsabile a monte.

30 Il "controllo" è infatti oggetto di molteplici definizioni normative, tutte però a tema squisitamente societario.

31 Senza voler qui scendere troppo nel dettaglio delle ricostruzioni giuridiche, l'etimologia stessa della parola spinge a considerare il "titolo" di un diritto, dunque l'atto o fatto giuridicamente rilevante, al ricorrere del quale un soggetto acquista il diritto medesimo (es.: per regola generale, ai sensi dell'art. 2 del Codice civile, una persona acquista la capacità di agire - e dunque di compiere con coscienza negozi giuridicamente rilevanti - non appena compiuti 18 anni).

32 Il D.lgs. 115/2008 e s.m.i., preposto alla definizione delle reti elettriche e dei sistemi semplici di produzione e consumo dell'energia stessa, parla infatti a più riprese di "titolarità" delle unità di produzione e di consumo di energia elettrica in capo a più soggetti giuridici.

33 Prima fra tutte la disciplina di cui al D.lgs. 70/2003 e s.m.i., attuazione della Direttiva 2000/31/CE sull'e-commerce.

34 Tale status giuridico è suffragato dalle innumerevoli norme Italiane ed internazionali in materia di opere derivate, che tutelano il creatore delle stesse, senza dimenticare perciò - perlomeno a livello morale se non addirittura sostanziale - i diritti delle opere originali dalle quali le stesse derivano.

35 Emblematico, sul punto, il dettato dell'art. 1677 del Codice civile, a mente del quale "se l'appalto ha per oggetto prestazioni continuative o periodiche di servizi, si osservano, in quanto compatibili, le norme di questo capo [n.d.r.: cioè quelle dell'appalto] e quelle relative al contratto di somministrazione".

36 Mentre, ad esempio, il provider di sistemi cloud in modalità SaaS offre servizi applicativi software e dovrà presumibilmente garantirne il corretto funzionamento, un provider cloud in modalità IaaS avrà, invece, perlomeno il diverso obbligo di mettere a disposizione dei propri clienti le sole risorse hardware virtualizzate.

37 La nozione di Responsabile del trattamento dei dati personali, originariamente riferibile a soggetti ed entità che trattano dati personali su incarico del Titolare e che potevano o meno essere presenti anche all'interno dell'organizzazione stessa del Titolare, è stata modificata a seguito del Parere 1/2010 - WP 169 dell'Art. 29 Working Party sui concetti di "responsabile del trattamento" e "incaricato del trattamento" (https://www.garanteprivacy.it/documents/10160/10704/wp169+-+Parere+1+2010+sui+concetti+di+responsabile+del+trattamento+e+incari.pdf/64cd4700-f0d4-4c04-b834-9-c3da69a93ea?version=1.1), i cui concetti sono stati poi trasposti nel GDPR. Ad oggi, la nozione di Responsabile del Trattamento, definito all'art. 4, paragrafo 1, n.8) del GDPR come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento", disciplina espressamente - unitamente a quanto all'art. 28 GDPR - il ruolo di un soggetto esclusivamente esterno all'organizzazione del Titolare.

38 È opportuno sin d'ora precisare che, nonostante il GDPR faccia espressamente riferimento a specifiche tipologie di dati (delle quali si dirà a breve), esso fornisce una

disciplina di carattere generale appropriata all'utilizzo per una gamma ben più ampia di generici "dati".

39 Questo assetto, previsto dall'interazione tra gli artt. 24 e 28 del GDPR, è in realtà delineato dalle stesse definizioni dei due soggetti, nn.7) ed 8) dell'art. 3 GDPR, ed è codificato come "accountability" (responsabilizzazione); esso si traduce in un maggior carico di responsabilità a carico del Titolare, che determina mezzi e modalità di trattamento a proprio integrale rischio e responsabilità), ma che può poi riversare responsabilità specifiche a carico del Responsabile esterno cui affida i dati, e su cui può poi rivalersi a livello contrattuale, in caso di inottemperanza.

40 Ai sensi dell'art. 28, comma 3, del GDPR, "i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento." Tale specifico atto, i cui specifici contenuti sono ulteriormente disciplinati nel prosieguo del comma in questione, prende spesso le forme di un Data Processing Agreement, spesso in congiunzione alle clausole ed alle previsioni richieste per trattamenti extra-UE, in ossequio agli artt. 44-49 del GDPR in materia.

41 Il divieto in questione si ricava dall'art. 45 del GDPR.

42 Si veda art. 46, commi 2 e 3, GDPR.

43 La norma è posta specificamente a tutela del diritto degli interessati a che i loro dati personali non siano sottoposti a trattamenti particolarmente "invasivi" della loro sfera personale, in quanto suscettibili di incidere in maniera significativa sulla stessa.

44 Cfr. ad esempio https://www.corrierecomunicazioni.it/digital-economy/blackout-mondiale-per-google-services-tutto-risolto-in-poche-ore/ ; https://st.ilsole24ore.com/art/tecnologie/2011-04-29/incendio-server-arubait-tilt-121947.shtml?refresh_ce=1 ; https://www.bbc.com/news/technology-36460328 .

45 Si veda https://www.hostingtalk.it/cloud-computing-quando-il-provider-fallisce_-c0000067g/

46 Cfr. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

47 Si vedano ad esempio le Linee Guida EBA sull'outsourcing a cloud provider, vincolanti per l'industria finanziaria ed assicurativa: https://www.eba.europa.eu/regulation-and-policy/internal-governance/recommendations-on-outsourcing-to-cloud-service-providers

48 La pluralità di orientamenti deriva anche dai differenti contenuti possibili del contratto di cloud SaaS: l'elaborazione dei dati demandata al software in cloud può infatti avere differenti finalità e differente rilevanza contrattuale e con ciò mutare la tipologia contrattuale applicabile e la responsabilità del cloud provider. Un conto è l'elaborazione mensile degli stipendi o la tenuta della contabilità aziendale, altro è l'utilizzo in cloud di un videogame online.

49 Ai sensi dell'art. 1575 c.c., il locatore ha i tre fondamentali obblighi di "1) consegnare la cosa locata in buono stato di manutenzione; 2) mantenere la cosa in stato da servire all'uso convenuto; 3) garantire al conduttore, durante la locazione, il pacifico godimento della cosa". A detti obblighi vanno poi ad aggiungersi quelli di cui ai successivi artt.

1576-1577 circa il mantenimento della cosa locata e le riparazioni della stessa, che attribuiscono al locatore le attività di straordinaria amministrazione, lasciando al conduttore quelle ordinarie.

50 Artt. 1578-1581 c.c., a mente dei quali il locatore è responsabile per i vizi della cosa locata (esistenti o sopravvenuti) e deve risarcire il conduttore, qualora non provi di aver ignorato tali vizi senza colpa, al momento della consegna.

51 In primo luogo, l'obbligo di ricevere i beni (i dati) e quello di custodirli con la diligenza del buon padre di famiglia, secondo le previsioni di cui agli artt. 1766 e ss. c.c.

52 Interessante in questo senso il "rapporto sulla trasparenza" di Google disponibile all'URL https://transparencyreport.google.com/?hl=it e che ha ad oggetto "Condivisione di dati che rivelano come le norme e gli interventi del governo e delle società influiscano su privacy e sicurezza dei dati nonché sull'accesso agli stessi": nell'ambito di tale rapporto, all'URL https://transparencyreport.google.com/user-data/overview?hl=it si rinviene una apposita sezione che elenca i dati sulle richieste globali di informazioni degli utenti ricevute da Google. In particolare, per quanto riguarda l'Italia, leggiamo che nel periodo luglio 2019-dicembre 2019, a fronte di 1486 richieste relative a 2099 account, Google ne ha soddisfatte, in tutto o in parte, circa il 50%.

53 Il modo migliore sarebbe di dichiarare espressamente applicabili (in un contratto soggetto alla Legge italiana) sia la disciplina di cui agli artt. 1560 e seguenti c.c. e, per ogni altro aspetto, la disciplina dell'art. 1766 c.c. e seguenti.

54 A prescindere dalla "forza" e inviolabilità del criptaggio. Il fatto che siano criptati costituisce una barriera logica, come una porta chiusa a chiave ma che si potrebbe sfondare con una lieve spallata: il fatto di dover "sfondare" a porta costringe il cloud provider ad una azione illegale e ciò rende illegittimo qualsiasi ottenimento del dato.

55 Un caso recente e che ha destato molto clamore è quello Amazon-AWS/Parler, in cui il cloud provider americano ha interrotto il servizio IaaS di Parler, piattaforma social preferita della destra americana sostenitrice di Trump, di fatto spegnendola. Secondo Amazon-AWS, Parler avrebbe violato le AUP a causa dei contenuti falsi o pericolosi diffusi dagli utenti, rendendo così necessario il provvedimento. Parler ha preannunciato un'azione legale contro Amazon-AWS (si veda: https://www.bbc.com/news/technology-55615214) ritenendo di non aver violato le AUP.

56 Nel caso instaurato dal Department of Justice USA contro il sito cyberlocker Megaupload, in cui veniva contestato l'uso primario del servizio per la condivisione di contenuti in violazione del copyright, il servizio fu spento ed i server posti sotto sequestro. Ciò nonostante, fu assai complesso dirimere la questione relativa se (e come) si potessero eliminare i dati, il cui costo di conservazione era stimato a USD 9000 al giorno. Si riconosceva infatti un teorico interesse degli utenti a recuperarli anche se le condizioni d'uso del servizio avvisavano gli utenti che la memorizzazione comportava il rischio della perdita completa dei dati in qualsiasi momento. I dati furono infine posti sotto la tutela della EFF (Electronic Frontiers Foundation) quale organismo neutrale incaricato della gestione delle residue richieste degli utenti, da effettuarsi entro un termine massimo.

57 Tale responsabilità è stata ipotizzata nel citato caso USA del cyberlocker Megaupload sulla base del fatto che il servizio cloud in questione era stato progettato e commercializzato per un primary use in violazione della Legge. Il caso però non arrivò mai alla discussione nel merito essendo intervenuti provvedimenti di cessazione del servizio e provvedimenti in sede penale prima della stessa. In UE la nuova Direttiva copyright 2019/790 esclude i "servizi cloud da impresa a impresa" ed i "servizi cloud che consen-

tono agli utenti di caricare contenuti per uso personale" dalla particolare responsabilità per i contenuti caricati dagli utenti che la stessa delinea: essa ascrive il nuovo regime di responsabilità ai soggetti definiti «prestatore di servizi di condivisione di contenuti online» e cioé quelli il cui scopo principale o uno dei principali scopi è quello di memorizzare e dare accesso al pubblico a grandi quantità di opere protette dal diritto d'autore o altri materiali protetti caricati dai suoi utenti, che il servizio organizza e promuove a scopo di lucro.

58 Cfr. Commission Explanatory Note https://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf

59 Cfr. https://rm.coe.int/16802f423d

60 Come evidenziato supra (§ 1.3) le informazioni, già di per sé consistenti di bit che possono essere disaggregati con la tecnica dello striping, possono essere distribuite su vari server ubicati in differenti giurisdizioni, anche contemporaneamente.

61 "Un [service provider] deve ottemperare agli obblighi di questo capitolo al fine di preservare, eseguire il backup o divulgare il contenuto di una comunicazione via cavo o elettronica e qualsiasi record o altra informazione relativa a un cliente o abbonato in possesso, custodia o controllo di tale fornitore, indipendentemente dal fatto che tali comunicazioni, registrazioni o altre informazioni si trovino entro o al di fuori degli Stati Uniti" (trad. dell'Autore)

62 Per comity analysis il diritto USA intende - in estrema sintesi e semplificando molto il tema -un procedimento in cui il Giudice considera "a titolo di cortesia" il diritto di uno Stato estero. La decisione finale rimane però del Giudice USA che non è giuridicamente vincolato dalle disposizioni estere.

63 Da questo punto di vista non vi sono state modifiche delle previsioni dello SCA, che vengono confermate e, pertanto, si possono considerare come "soggette alla giurisdizione USA" a questo fine le società statunitensi, le società con sede negli USA e le società di proprietà di persone degli Stati Uniti; tuttavia, ben possono essere considerate assoggettate a giurisdizione USA anche quelle società non rientranti nelle categorie appena elencate, ma che hanno comunque contatti rilevanti con gli US (ad esempio le società che in tale nazione conducono un'attività significativa) tali da far ritenere all'organo giurisdizionale possibile l'estensione della giurisdizione. In questi termini, i criteri per definire i soggetti ricompresi o che potranno essere ricompresi non hanno criteri nitidi, ma sono rimessi ad una valutazione caso per caso da parte del giudice; margini discrezionali si rinvengono altresì nel vaglio dei rapporti intercorrenti tra una società e la sua controllata in termini di controllo dei dati posseduti o controllati dalla seconda da parte della prima. È bene sottolineare come in questi casi la struttura ed il rapporto tra le due società non infici la valutazione, che dovrà essere in ogni caso effettuata dall'organo giurisdizionale. All'esito di tale valutazione, verrà stabilito se è possibile o meno emettere il warrant.

64 Si veda supra, § 2.1.

65 Si tratta di una certificazione, da essere effettuata preventivamente, ad opera del US Attorney General del Congresso.

66 Cfr. Agreement of 3 October 2019 between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, disponibile online su https://cli.re/jJ7Z3D

67 Cfr. https://www.europarl.europa.eu/doceo/document/E-9-2019-003136_EN.html

68 Cfr. Agreement between the United States of America and the European Union on the Protection of Personal Information relating to the Prevention, Investigation, Detection and Prosecution of Criminal Offenses done at Amsterdam; 2 June 2016, disponibile su: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:22016A1210(01)&from=EN

69 Cfr. Schwarz-Peifer, Data Localization, Under the CLOUD Act and the GDPR, Computer Law Review International, 2019/1

70 Cfr. White Paper Google su Data residency, operational transparency,and privacy for European customers on Google Cloud, disponibile all'URL: https://services.google.com/fh/files/misc/googlecloud_european_commitments_whitepaper.pdf?hl=cs

71 European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield, nn. 27 e 28 available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2018-0315+0+DOC+PDF+V0//EN

72 Si veda la risposta congiunta EDPB/EDPS del 12 luglio 2019, accessibile al seguente link: https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_de nella quale l'EPDB ha concluso che: "service providers subject to EU law cannot legally base the disclosure and transfer of personal data to the US on such requests.".

73 Si veda il position paper del 28 febbraio 2019 accessibile al seguente link: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-Assessment-of-the-U-S-CLOUD-Act.pdf

74 Atto del 5 febbraio 2019, accessibile al seguente link:

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52019PC0070

75 Proposta del 17 aprile 2018 accessibile al seguente link: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en

76 Cfr. Comunicazione della Commissione europea del 2 luglio 2014 "Verso una florida economia basata sui dati", nonché le Comunicazioni del 25 aprile 2018 e del 15 maggio 2018;

77 L'art. 3, n. 5), definisce obbligo di localizzazione dei dati "qualsiasi obbligo, divieto, condizione, limite o altro requisito, previsto dalle disposizioni legislative, regolamentari o amministrative di uno Stato membro o risultante dalle prassi amministrative generali e coerenti in uno Stato membro e negli organismi di diritto pubblico, anche nell'ambito degli appalti pubblici, fatta salva la direttiva 2014/24/UE, che impone di effettuare il trattamento di dati nel territorio di un determinato Stato membro o che ostacola il trattamento di dati in un altro Stato membro".

78 Definite dal Regolamento come "un'autorità di uno Stato membro o qualsiasi altro ente autorizzato, in virtù del diritto nazionale, a esercitare una funzione pubblica o a esercitare i pubblici poteri, che ha la facoltà di ottenere accesso ai dati trattati da una persona fisica o giuridica ai fini dell'esercizio delle sue funzioni ufficiali, come previsto dal diritto dell'Unione o nazionale". Come si vede la definizione lascia aperta la porta al fatto che l'Autorità possa essere anche un ente estero, purché "autorizzato".

79 Si veda ad esempio il caso Parler / AWS Amazon, già citato.

Questo lavoro di ricerca è stato
promosso e sponsorizzato da:

DOMINION
HOSTING
HOLDING

DHH S.p.A.
(Borsa Milano AIM DHH.MI - http://dhh.international)

Data pubblicazione
Dicembre 2020

Questa ricerca è soggetta a licenza
Creative Commons

Una **Licenza CC (Creative Common)** può essere utilizzata quando un autore vuole concedere ad altri il diritto di usare o modificare un'opera che lui stesso (l'autore) ha creato. CC permette all'autore di scegliere le modalità di utilizzo (per esempio può permettere solo un uso non commerciale di una determinata opera) e protegge le persone che usano o diffondono un'opera di altri dalla preoccupazione di infrangere il diritto d'autore, purché siano rispettate le condizioni specificate dall'autore stesso nella licenza.

BY

Permette che altri copino, distribuiscano, mostrino ed eseguano copie dell'opera e dei lavori derivati da questa a patto che venga indicato l'autore dell'opera, con le modalità da questi specificate.

Ad esempio, potrebbe essere richiesto a chi cita un'opera di indicare oltre all'autore anche il link al sito web dell'opera o dell'autore.

ND

Permette che altri copino, distribuiscano, mostrino ed eseguano soltanto copie identiche (verbatim) dell'opera; non sono ammesse opere derivate o sue rielaborazioni.

SA

Permette che altri distribuiscano lavori derivati dall'opera solo con una licenza identica (non maggiormente restrittiva) o compatibile con quella concessa con l'opera originale.

LA RAGGIUNGIBILITÀ GIURIDICA DEI DATI

Il cloud: rischi e regole di condotta nell'affidare i dati alla nuvola informatica

Ricerca a cura di:
Innocenzo Genna
Eugenio Prosperetti

hanno collaborato:
Giulio Pascali
Davide Tuzzolino

sponsored by DOMINION HOSTING HOLDING

Data Pubblicazione
Dicembre 2020