RIVISTA ITALIANA DI INFORMATICA E DIRITTO
PERIODICO INTERNAZIONALE DEL CNR-IGSG

ISSN 2704-7318
Fascicolo 1-2021
DOI: 10.32091/RIID0023

Modelli tecnici e disciplina giuridica del c.d. cloud computing

Vanni Boncinelli

Il mercato dei servizi di *cloud computing* ha registrato negli ultimi anni uno tasso di crescita esponenziale, che la recente emergenza sanitaria mondiale finirà per rafforzare ulteriormente. Il successo di questo complesso e variegato "ecosistema" di tecnologie e servizi risiede in una combinazione "sinergica" di fattori, nonché dalla diffusione sempre più capillare di *smartphone* e *tablet*, che ha portato a nuove modalità di utilizzo dei servizi informatici. Le piattaforme *cloud* svolgono oggi una funzione "abilitante" rispetto a una varietà praticamente infinita di servizi, i quali non potrebbero esistere (o quasi) senza le risorse computazionali, applicative e di *storage* messe a disposizione da fornitori di *cloud computing*. Dal punto di vista giuridico, tuttavia, il *cloud computing* lascia sul tappeto enormi interrogativi ancora in gran parte irrisolti. Come proteggere i diritti degli interessati quando i loro dati possono essere spostati, spacchettati, ricomposti e replicati in qualsiasi nodo della rete globale con un semplice click? Come regolare un caleidoscopio di servizi così diversi tra loro e ripartire obblighi e responsabilità tra i vari soggetti che compongono la "filiera" *cloud*? Per molti versi, l'approccio seguito da Stati Uniti e Unione europea non potrebbe essere più diverso, ma entrambi scontano la pretesa di voler regolare in modo unilaterale un fenomeno – il *cloud computing* e, più in generale, Internet – nel quale "The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world".

Cloud computing – Cloud Act – e-Evidence Regulation

1. Introduzione

Nel giro di poco più di dieci anni, il *cloud computing* ha conosciuto uno sviluppo esponenziale che non accenna a rallentare[1]. Il successo di questo complesso e variegato "ecosistema" di tecnologie e servizi risiede in una combinazione sinergica di fattori tecnologici (la sovrabbondanza di risorse non utilizzate, lo sviluppo della virtualizzazione, ecc.), nonché dalla diffusione sempre più capillare di *smartphone* e *tablet*, che ha imposto nuovi modelli di fruizione dei servizi informatici. Le piattaforme *cloud* svolgono oggi una funzione "abilitante" rispetto a una varietà praticamente infinita di servizi, resi possibili dalle risorse computazionali, applicative e di *storage* messe a disposizione dagli operatori di *cloud computing*.

Questo sviluppo travolgente si è tuttavia accompagnato a crescenti difficoltà nel trovare un punto di equilibrio tra esigenze diverse e spesso contrapposte, che vanno dalle preoccupazioni per la privacy e la si-

V. Boncinelli è dottore di ricerca in "Teoria del diritto e della politica" presso l'Università degli Studi di Macerata (2005) e svolge la propria attività di consulente informatico specializzato in soluzioni *cloud* e architetture distribuite. Questo saggio fa parte della Sezione monografica *Ubi data, ibi imperium: il diritto pubblico alla prova della localizzazione dei dati* a cura di Simone Calzolaio.

curezza informatica, alla lotta all'evasione fiscale, dal perseguimento dei reati allo spionaggio industriale. Molto spesso si è finito per concentrarsi su un unico aspetto, trascurando le concrete modalità di funzionamento del *cloud computing* e, più in generale, della rete Internet. Si è così assistito alla proliferazione di obblighi più o meno generalizzati di localizzazione dei dati (*data residency*). Queste misure di localizzazione, per quanto possano assumere le forme più variegate e rispondere ai fini più disparati, sono accomunate dal fatto di porre intenzionalmente ostacoli al flusso di dati attraverso i confini nazionali, ad esempio imponendo di conservare i dati all'interno di server ubicati nel territorio dello Stato, ovvero subordinando il trasferimento dei dati al previo consenso dell'interessato. Il numero di Paesi che hanno introdotto obblighi di questo tipo è in continuo aumento[2]. Uno degli ultimi esempi di questo tipo è rappresentato dall'art. 6, co. 5, del D.L. 30 aprile 2020, n. 28, che nel dettare le linee guida per lo sviluppo della nota piattaforma per la prevenzione e il tracciamento dei casi di Covid-19 ("Immuni"), ha previsto che debba essere "realizzata con infrastrutture localizzate sul territorio nazionale"[3].

Quali che siano le motivazioni dietro all'introduzione di tali misure, è indubbio che stiamo assistendo a un'inversione di tendenza nell'atteggiamento nei confronti dei flussi di dati: se in passato la preoccupazione principale di molti Paesi era quella di mantenere alcune informazioni "al di fuori" dei confini nazionali (si pensi ai sistemi di censura e alla protezione della proprietà intellettuale), oggi gli sforzi maggiori sembrano esser rivolti nel senso opposto, ovvero quello di tenere le informazioni relative ai propri cittadini all'"interno"[4].

Contemporaneamente, però, si assiste anche al fenomeno inverso: quando si tratta di garantire l'interesse pubblico all'accertamento dei reati e all'acquisizione delle prove digitali che si trovano conservate al di fuori del territorio nazionale, anziché guardare al luogo di conservazione dei dati (che costringerebbe le autorità nazionali ad avviare le complesse procedure previste dai trattati di mutua assistenza giudiziaria) si preferisce agire sui soggetti, *in primis* i fornitori di servizi *cloud*, che su tali dati esercitano una qualche forma di controllo, affinché producano le informazioni richieste. In questa direzione si muovono, solo per fare alcuni esempi, tanto il contestatissimo *Cloud Act* del 2018, quanto la proposta di regolamento della Commissione europea relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (c.d. Regolamento *e-Evidence*), entrambi trattati nelle pagine che seguono.

Si crea così un perverso circolo vizioso, nel quale il proliferare degli obblighi di localizzazione viene assunto come giustificazione delle norme che mirano a "estendere" la giurisdizione degli Stati nazionali al di fuori del loro territorio, con ciò alimentando timori e diffidenze che si traducono nell'adozione di nuovi e più penetranti obblighi di localizzazione. Il problema è che, come accade ogniqualvolta si tenti di regolare in modo settoriale e locale un fenomeno di portata globale, si rischia non solo di non raggiungere il risultato sperato ma, anzi, di moltiplicare e amplificare gli effetti negativi sui diritti dei singoli, sulla sicurezza informatica e la privacy, la libertà di concorrenza e gli investimenti[5].

Scopo di questo contributo non è quello di fornire un'esaustiva ricognizione dei tanti, tantissimi punti critici che si accompagnano ai recenti tentativi di regolazione del fenomeno, né tantomeno di proporre soluzioni generali buone per tutte le stagioni. L'obiettivo, assai più limitato e circoscritto, è quello di evidenziare come, al di là delle definizioni astratte, quando si parla di *cloud computing* si fa in realtà riferimento a un complesso e variegato "ecosistema" di servizi, applicazioni, metodologie e pratiche che presentano tante differenze e peculiarità quanto sono i caratteri in comune. Il problema, ovviamente, non è solo di natura "tassonomica", poiché alla base di qualsiasi tentativo di regolazione del *cloud*, come del resto dell'intera Internet, vi dovrebbe essere la consapevolezza che gli interessi in gioco sono inevitabilmente confliggenti. Ragione in più per evitare tanto un approccio di tipo *one size fits all*, quanto la sua eccessiva "parcellizzazione" in tante legislazioni nazionali e di settore.

2. Un *cloud*, mille *cloud*. Genesi, evoluzione e caratteristiche del *cloud computing*

La storia del *cloud* è disseminata di piccole e grandi innovazioni, la più importante delle quali è stata certamente la nascita e l'inarrestabile diffusione di Internet, che oggi conta 4.5 miliardi di utilizzatori attivi, pari al 59% della popolazione mondiale[6]. Nel ricostruire la genesi del *cloud computing* si è soliti partire dalla tecnologia del *mainframe computing* sviluppata a partire dalla fine degli anni '50 del secolo scorso[7]. Questi costosissimi e ingombranti elaboratori venivano utilizzati per processare dati ed effettuare calcoli che oggi potrebbero essere svolti senza fatica anche dal più economico *smartphone* disponibile sul mercato. Se confrontati con gli standard odierni, questi sistemi erano estremamente difficili

da usare, privi com'erano di un'interfaccia umana, o persino di una tastiera, e programmati mediante schede perforate o nastri magnetici.

Considerato che un'università o un'azienda normalmente potevano permettersi al massimo uno o due *mainframe*, era necessario ottimizzare al massimo l'utilizzo delle risorse computazionali. L'idea alla base della condivisione delle risorse nasceva da una semplice constatazione: l'inserimento di un programma all'interno dell'elaboratore richiedeva un tempo considerevole, durante il quale le capacità computazionali rimanevano in larga parte inutilizzate. Al contrario, un ampio gruppo di utenti che lavoravano contemporaneamente avrebbe permesso di utilizzare le pause di un utente intento a inserire dati per destinare il tempo di elaborazione a vantaggio degli altri. Di qui l'elaborazione di metodi di *time-sharing* in grado di consentire a più utenti di condividere le risorse del *mainframe*, utilizzando dei terminali privi di una propria capacità di elaborazione (e per questo definiti anche *dumb terminal* o, con un'espressione tornata recentemente alla ribalta proprio in connessione con lo sviluppo del *cloud computing*, *thin client*).

Un'altra importante innovazione fu rappresentata dalla "virtualizzazione". A cavallo degli anni '60 e '70 furono rilasciati i primi sistemi operativi in grado di supportare la possibilità di condividere un insieme di risorse hardware (dischi rigidi, processori, ecc.) tra più sistemi operativi "virtuali" che "convivono" sullo stesso computer fisico. Questi sistemi operativi virtuali sono completamente isolati gli uni dagli altri, e possono utilizzare soltanto le risorse di tipo "logico" (capacità computazionale, di *storage*, di connettività, ecc.) messe a disposizione dal sistema di virtualizzazione, e da questo dinamicamente allocate tra le varie macchine virtuali a seconda delle esigenze (*pooling*).

Sebbene i concetti fondamentali del *cloud computing* risalgano dunque agli albori dell'informatica, l'uso del termine *cloud* per indicare un nuovo modo di accedere al software, potenza di calcolo e capacità di archiviazione dei dati attraverso il web è invece relativamente recente. Contrariamente a quanto si potrebbe pensare, l'espressione *cloud computing* non è nata nell'ambiente *hi-tech*, ma è stata coniata durante una (si presume fumosa) riunione dei responsabili del *marketing* tenutasi nel 1996 negli uffici di Houston della Compaq Computer. L'espressione non indicava tanto un insieme specifico di tecnologie, quanto piuttosto un diverso modello di consumo dei servizi informatici tramite Internet[8].

Le origini del termine spiegano forse il perché il concetto di *cloud*, con i suoi contorni indefiniti ed evanescenti, abbia sin da subito creato difficoltà, equivoci e incomprensioni (che continuano a tutt'oggi) non solo tra gli addetti ai lavori, ma anche per i governi che a più riprese sono intervenuti nel tentativo di regolare il fenomeno, i quali si sono trovati nella necessità di definire cosa rientri nel concetto di *cloud computing* e cosa no. Non a caso, una delle prime pubblicazioni dedicata al *cloud computing* da parte del *National Institute for Standards and Technology* (NIST), a cui si deve peraltro la più citata definizione di *cloud*, si apre con l'affermazione per cui «Cloud computing can and does mean different things to different people»[9]. In altre parole, non esiste un solo *cloud*. Come vedremo nelle prossime pagine, una parte consistente dei problemi che nascono sul piano della regolazione del fenomeno possono essere affrontati solo se si tengono in debito conto le peculiarità dei diversi modelli di *cloud*.

Dunque, di *cloud computing* esistono svariate definizioni, che pongono l'accento ora su alcuni caratteri, ora su altri[10]. Tuttavia, un aspetto generale su cui le varie formulazioni convergono è l'idea per cui il *cloud* abbia rappresentato un completo mutamento di paradigma rispetto alle forme tradizionali di utilizzo dei servizi informatici[11].

Volendo partire da una definizione comunemente accettata, possiamo prendere a prestito quella offerta proprio dal NIST: «Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction»[12].

Proviamo a specificare meglio la definizione sopra riportata, evidenziando alcune caratteristiche essenziali. Per prima cosa, il *cloud* introduce (o consiste di) una serie di livelli di "astrazione" che permettono di utilizzare determinate risorse senza doversi preoccupare della loro gestione, configurazione, manutenzione, messa in sicurezza, ecc. Sebbene la ripartizione delle responsabilità tra fornitore del servizio e utilizzatore vari in base al "modello di servizio" (su cui torneremo più avanti), l'elemento comune è che le risorse utilizzate dall'utente hanno, come si è accennato parlando di virtualizzazione, un carattere prettamente logico, anziché "fisico".

Tali risorse sono messe in comune per servire molteplici utenti mediante un modello condiviso (c.d. *multi-tenant*), assegnate e riassegnate dinamicamente in base alla domanda (*resource pooling*). Possono essere accedute, create, gestite o dismesse direttamente dall'utente, con poca o nessuna interazione con il fornitore e tramite meccanismi stan-

dard, accessibili via Internet da piattaforme eterogenee (*broad network access*), e utilizzate in piena autonomia, secondo le proprie necessità (*on-demand self-service*). Le risorse possono essere inoltre acquisite e rilasciate in modo elastico, in alcuni casi anche automaticamente, per scalare[13] rapidamente le capacità del sistema in relazione alla domanda (*rapid elasticity*). Infine, i sistemi *cloud* monitorano e ottimizzano costantemente l'uso delle risorse (*measured service*), facendo leva sulla capacità di misurazione ad un livello di astrazione appropriato per il tipo di servizio (ad esempio memoria, elaborazione, larghezza di banda e utenti attivi) e, in genere, con costi legati all'utilizzo delle risorse[14].

3. I principali modelli di servizio

Sulla base della definizione sopra riportata, il NIST individua tre specifici "modelli di servizio", distinti in base al tipo di risorsa messa a disposizione e al ruolo riservato all'utente che acquista il servizio: si parla così di *Infrastructure-as-a-Service* (IaaS), *Platform-as-a-Service* (PaaS), e *Software-as-a-Service* (SaaS).

In un servizio di tipo IaaS, il fornitore del servizio *cloud* mette a disposizione i componenti necessari a realizzare una propria infrastruttura informatica virtuale. Rispetto a una tradizionale infrastruttura locale, costituita da server, dischi rigidi e sistemi di rete che devono essere acquistati o noleggiati, gestiti per tutto il loro ciclo di vita e sostituiti in caso di problemi, un'infrastruttura *cloud* si basa sul carattere puramente "virtuale" delle risorse. Questo significa, tra le altre cose, che gli utenti non devono preoccuparsi dell'installazione, della configurazione e della manutenzione dell'hardware e dei sistemi infrastrutturali, che è a totale carico del fornitore *cloud*. Gli utenti rimangono invece responsabili della configurazione dei sistemi che vengono eseguiti sull'infrastruttura virtuale (come i sistemi operativi e le applicazioni che ci girano sopra). I più diffusi servizi IaaS sono rappresentati da macchine virtuali, servizi di *storage* dei dati e servizi di rete virtuali (*virtual networking*).

In un servizio di tipo PaaS, invece, la piattaforma mette a disposizione dell'utente l'ambiente di esecuzione di un'applicazione (quale ad esempio un sito web), a mantenerlo in esecuzione anche in caso di problemi nei livelli sottostanti dell'infrastruttura (grazie a sofisticati meccanismi di *fault-tolerance* e di replica geografica dei dati), garantendo inoltre alti livelli di performance e di scalabilità del servizio. In un servizio PaaS, il fruitore non si deve preoccupare dell'infrastruttura, della connettività, della configurazione del sistema operativo o di altri aspetti legati all'ambiente di esecuzione. Tutti questi dettagli sono a carico del fornitore *cloud* e all'utente resta la sola responsabilità di gestire l'applicazione[15].

Infine, le soluzioni SaaS liberano gli utenti sia dalla gestione del sistema operativo, che dalla supervisione dell'applicazione: tutto ricade nelle mani del fornitore del servizio. Tutto quello che l'utente deve fare è usare l'applicazione messa a disposizione dal fornitore senza doversi preoccupare di altro. Tipicamente, i servizi SaaS sono usufruiti tramite un *web browser*, e tanto i dati applicativi quanto il carico di lavoro sono trasferiti sull'infrastruttura dell'operatore *cloud*, il che rende possibile sfruttare un'ampia gamma di funzionalità direttamente dallo schermo del proprio *smartphone* o da qualunque altro dispositivo connesso a Internet. A essere interessati da questa trasformazione non sono soltanto gli utenti finali, ma anche le aziende e le pubbliche amministrazioni. Gran parte del lavoro che prima veniva svolto sfruttando applicazioni e servizi installati in locale (sui server aziendali o direttamente sulle postazioni lavorative), si avvale oggi del web per numerose funzioni (dall'archiviazione dei dati alle analisi di *business intelligence*, dai filtri *antispam* alla lotta al *malware*).

Con il tempo, accanto a questi tre modelli tradizionali se ne sono aggiunti di nuovi. Nel tentativo di dare specifico risalto alle peculiarità dei nuovi servizi lanciati a un ritmo quasi giornaliero, e forse anche per venderli meglio, sono stati elaborati un gran numero di acronimi (es. *Database-as-a-Service*, *Storage-as-a-Service*, *Disaster Recovery-as-a-Service*, *Workplace-as-a-Service*, *Desktop-as-a-service*, ecc.)[16]. Di recente, vista l'impossibilità di arginarne la proliferazione, è stata proposta anche un'ulteriore tipologia, definita "XaaS" (o *X-as-a-Service*), dove la "X" sta a indicare non tanto uno specifico modello di servizio, quanto piuttosto una sorta di categoria residuale entro cui ricondurre tutti quei servizi *cloud* che non si lasciano facilmente incasellare in una delle tre categorie tradizionali, vuoi perché se ne differenziano sotto aspetti rilevanti, vuoi perché presentano elementi di tutte e tre le classificazioni precedenti.

Questo tipo di classificazione ha ovviamente un valore puramente esemplificativo e non ha alcuna pretesa di esaustività delle differenze e delle particolarità dei numerosi servizi *cloud* oggi disponibili sul mercato. Quando, poco più di dieci anni fa, questa classificazione si è affermata tra gli addetti ai lavori, i servizi offerti erano relativamente pochi (macchine virtuali, servizi di rete, applicazioni web, ecc.). In quel contesto, la distinzione tra IaaS, PaaS e SaaS era sufficiente a descrivere, se non tutti, la gran par-

te dei servizi offerti. Negli ultimi anni si è assistito al proliferare di decine e decine di nuovi servizi, sempre più sofisticati ed evoluti. Oggi si contano centinaia di servizi *cloud* diversi, che sono andati ad arricchire l'offerta accanto a quelli più "tradizionali": servizi di intelligenza artificiale e *machine learning*, analisi dei dati, *Internet of Things* (IoT), *blockchain* e cripto-valute, *streaming* di contenuti multimediali, realtà aumentata (*augmented reality*), sicurezza informatica, servizi per dispositivi mobili, ecc.

Anche con tutti questi limiti, tuttavia, la distinzione tra IaaS, PaaS e SaaS ha una sua rilevanza. Come abbiamo visto, nel caso di servizi IaaS e PaaS l'utente ha un controllo molto più accentuato sui dati, potendo innanzitutto scegliere dove tali dati devono essere conservati, partizionati o replicati. Nel caso di servizi SaaS, invece, l'utente non ha in genere alcun controllo su dove i dati sono conservati o sulle misure di sicurezza applicate. Tra queste ultime, una menzione particolare va alla cifratura dei dati conservati o in transito sull'infrastruttura. Nei servizi SaaS, la scelta di cifrare o meno i dati di cui è "titolare" l'utente del servizio (ad esempio le fatture dei clienti, le e-mail, i messaggi scambiati in software, i dati di produzione, ecc.) ricade sul fornitore del servizio software, che decide anche le modalità di gestione delle relative chiavi. Nei servizi di tipo IaaS e PaaS, la gestione di questi aspetti è lasciata per lo più all'utente, e dipende in buona sostanza dal livello di sicurezza che quest'ultimo mira a implementare[17]. Queste differenze nel grado di libertà lasciato all'utilizzatore del servizio discendono dal fatto che, mentre questi ultimi due modelli sono rivolti principalmente a organizzazioni, pubbliche o private, dotate delle necessarie competenze tecnologiche e professionali, i servizi SaaS, nella misura in cui sollevano l'utente da qualunque responsabilità in merito alla loro gestione, possono essere utilizzati da chiunque, sia esso un utente finale o un'organizzazione (si potrebbe dire, sotto questo profilo, che sono servizi "chiavi in mano").

In altri termini, i servizi infrastrutturali (così come la maggior parte di quelli PaaS, in cui la "piattaforma" può essere vista come una sorta di "ponte" tra l'infrastruttura e il servizio applicativo finale), oltre a rappresentare un modello alternativo alla gestione in proprio di risorse informatiche (con tutti i benefici che ne derivano in termini di risparmio e flessibilità), possono essere visti anche come una "borsa degli attrezzi" a cui attingere per "confezionare" servizi applicativi ad alto valore aggiunto (come ad esempio sistemi per la gestione e la fidelizzazione dei clienti, per la pianificazione delle risorse aziendali, ovvero per facilitare lo *smart-working* e la collaborazione da remoto, ecc.) destinati ad essere rivenduti a clienti finali (altre organizzazioni o persone fisiche).

Questo rilievo mette in luce un aspetto spesso sottovalutato quando si tratta di elaborare le regole da applicare al *cloud computing*. Sempre più spesso, infatti, la realizzazione di una soluzione *cloud* comporta la combinazione di molteplici servizi, di natura anche assai diversa e con l'intervento di fornitori terzi. Tale complessità è in genere "trasparente"[18] dal punto di vista dell'utente finale, il quale si limita a utilizzare il servizio senza rendersi conto della sottostante complessità. Ad esempio, se dalla prospettiva di un utente, il servizio di archiviazione *cloud* di Dropbox può apparire come un classico SaaS, dietro le quinte il servizio ha utilizzato per molti anni l'infrastruttura messa a disposizione da un altro fornitore (in questo caso Amazon AWS)[19]. Dropbox era dunque al tempo stesso un utilizzatore di servizi di tipo IaaS (forniti da Amazon) e, dal punto di vista dei suoi utenti, un fornitore di servizi di tipo SaaS.

La struttura naturalmente aperta e "partecipativa" del *cloud* pone non pochi interrogativi quando si tratta, ad esempio, di definire formalmente i ruoli dei vari soggetti coinvolti nel trattamento di dati personali. Come vedremo meglio nelle prossime pagine, tutte queste differenze giocano un ruolo importante anche sul piano degli effetti della regolazione. Lo stesso vale, seppur sotto altri profili, per i diversi modelli di distribuzione dei servizi *cloud* oggi presenti sul mercato, che si distinguono principalmente in base ai loro destinatari.

4. I modelli di distribuzione del *cloud computing*

Accanto ai tre modelli di servizio, il NIST individua infatti anche quattro modelli di distribuzione, distinguendo tra *cloud* pubblici, privati, "comunitari" (*community cloud*) e ibridi.

In un *cloud* pubblico, la modalità di distribuzione di gran lunga più comune e diffusa, l'infrastruttura è predisposta per essere utilizzata dalla generalità degli utenti. Le risorse sono di proprietà del fornitore e vengono distribuite tramite Internet a chiunque ne faccia richiesta (esempi di *cloud* pubblici sono Amazon Web Services, Microsoft Azure e Google Cloud). Nel *cloud* pubblico le risorse hardware sono condivise dai vari utenti (o *tenant*) e allocate secondo logiche che ne massimizzano l'efficienza.

In un *cloud* privato, invece, l'infrastruttura tecnologica è predisposta per essere utilizzata in via esclusiva da una singola organizzazione. In questo caso, a consumare le risorse condivise sono in genere le diverse unità che compongono l'organizzazione

(dipartimenti, direzioni, uffici, ecc.). Tanto l'ubicazione fisica quanto la proprietà dell'infrastruttura è irrilevante: può essere gestita direttamente dall'organizzazione o affidata, in tutto o in parte, a fornitori terzi, così come può comprendere un solo *data center* situato all'interno dei locali dell'organizzazione, ovvero più *data center* distribuiti in località diverse. Quello che conta è che nell'infrastruttura, anche se gestita da un terzo, tutte le risorse sono dedicate a uno specifico cliente. Molto spesso le organizzazioni di una certa dimensione optano per un *cloud* privato (magari riconvertendo l'infrastruttura tradizionale già esistente) per motivi legati alla sicurezza dei dati (dal momento che questi rimangono all'interno del perimetro dell'organizzazione), ovvero per soddisfare particolari requisiti di localizzazione previsti da normative di settore, o ancora per il tipo particolare di applicazioni utilizzate dall'azienda.

Il *cloud* comunitario, nonostante il nome, è assimilabile *in toto* a quello privato, con la sola differenza che in questo caso l'infrastruttura è messa a esclusiva disposizione di più organizzazioni che hanno obiettivi o necessità (es. di sicurezza, normativi, ecc.) condivise. Come un qualsiasi *cloud* privato, può essere gestito da una o più organizzazioni della comunità o affidato, in tutto o in parte, a un fornitore terzo (che può consistere, ad esempio, in un raggruppamento temporaneo di imprese).

Nel *cloud* ibrido, infine, *cloud* pubblici e privati sono integrati per svolgere funzioni distinte all'interno della stessa organizzazione. Negli ultimi anni questa forma di *cloud* ha conosciuto una notevole diffusione, acquisendo sempre maggiori quote di mercato rispetto agli altri modelli di distribuzione[20], grazie ai vantaggi che presenta per le organizzazioni, che possono sia usufruire delle risorse illimitate (e poco costose) messe a disposizione dal *cloud* pubblico, sia soddisfare particolari esigenze di sicurezza o di *compliance* normativa garantite dal *cloud* privato.

Ciascun modello di distribuzione porta con sé vantaggi e svantaggi. In generale, tanto i *cloud* pubblici che quelli privati sono caratterizzati da un'alta efficienza grazie alla virtualizzazione e alla condivisione delle risorse, consentendo così un migliore bilanciamento del carico di lavoro; da un'elevata disponibilità, che minimizza i tempi di inattività e migliora la continuità aziendale; nonché da una scalabilità elastica (che nel caso di *cloud* privati incontra tuttavia un limite nelle risorse fisiche non infinite a disposizione di un'organizzazione, mentre in quello pubblico sono virtualmente illimitate).

Alcuni vantaggi, invece, sono specifici del *cloud* pubblico, quali bassi costi iniziali (mentre in quello privato sono particolarmente elevati); elevate economie di scala in termini di potere di acquisto delle apparecchiature che di efficienza nella gestione; semplicità di gestione, in quanto l'infrastruttura è gestita, configurata e mantenuta dal fornitore (mentre in quello privato sono richieste competenze tecniche specifiche, oltre che capacità organizzative e disponibilità economiche al di fuori della portata di molte organizzazioni).

Di contro, il *cloud* privato consente, come si è detto, di avere un maggiore controllo in tema di sicurezza e conformità normativa, nonché di garantire una maggiore qualità del servizio, poiché l'infrastruttura può essere configurata e ottimizzata per venire incontro alle specifiche esigenze di un'organizzazione[21].

Sulla base di questa classificazione, un'eventuale infrastruttura *cloud* gestita da o per conto di soggetti che svolgono compiti e funzioni di natura pubblica si configurerebbe comunque come *cloud* privato (o comunitario, qualora condiviso da più soggetti), indipendentemente dal fatto che a fornire (e a gestire) l'infrastruttura sia o meno un soggetto pubblico. L'unico elemento rilevante, in questo schema, è infatti il carattere esclusivo delle risorse *cloud* usufruibili, e non la "natura" del soggetto (o dei soggetti) che, a seconda dei casi, forniscono o utilizzano detti servizi[22].

5. Una classificazione alternativa di *cloud computing*: *Data Shard*, *Data Localization*, *Data Trust*

Le tradizionali classificazioni dei servizi *cloud* sin qui sommariamente illustrate dovrebbero aver già lasciato intuire la complessità dei modelli che stanno dietro l'erogazione di servizi apparentemente semplici, se considerati dal punto di vista dell'utente finale. A queste classificazioni, però, se ne affianca un'altra che riveste un'importanza assolutamente centrale quando si affrontano le tematiche relative alla localizzazione dei dati, perché basata sulla diversa modalità di gestione dell'infrastruttura, o meglio dei dati che su tale infrastruttura circolano: *Data Shard*, *Data Localization* e *Data Trust*[23].

Nel modello definito *Data Shard*, l'informazione è divisa, o meglio "partizionata", in molteplici "frammenti" (*shard*) dispersi in vari nodi della rete. Tramite il partizionamento, un archivio di grandi dimensioni viene suddiviso in "componenti" più piccoli, più efficienti e "maneggevoli" rispetto all'originale[24]. Alle strategie di partizionamento si ricorre in genere per migliorare le performance delle operazioni che coinvolgono grandi volumi di dati, ovvero per "avvicina-

re" i dati agli utenti sulla base della loro ubicazione geografica, in modo da ridurre i tempi di latenza e migliorare le prestazioni complessive[25]. Le ragioni che stanno dietro questo tipo di strategie sono dunque di natura eminentemente tecnica: «The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world»[26].

Nel modello denominato *Data Localization*, il fornitore dei servizi *cloud* conserva i dati all'interno di un certo ambito geografico che, a seconda dei casi, può avere estensioni assai diverse, e che solo occasionalmente coincide con i confini di uno Stato. Nell'individuazione dei diversi ambiti geografici in cui suddividere l'infrastruttura concorrono molteplici ragioni, di natura economica, tecnica e, non ultima, legale, come l'esistenza di obblighi positivi di localizzazione dei dati (es. Francia e Germania).

Solitamente, l'infrastruttura globale dei grandi operatori di servizi *cloud* comprende più aree geografiche o regioni più o meno estese (ad esempio Europa centrale, Stati Uniti occidentali, ecc.). Ciascuna di queste aree è, a livello infrastrutturale, completamente autonoma e indipendente dalle altre, così da garantire la massima stabilità e tolleranza ai guasti. Ogni area o regione è a sua volta suddivisa in più zone di disponibilità. Queste zone, che comprendono uno o più *data center* muniti di impianti indipendenti per l'energia, il raffreddamento e la rete, sono fisicamente isolate le une dalle altre, ma connesse tramite collegamenti dedicati a bassa latenza. Mediante la suddivisione di un'area in zone più circoscritte si cerca di garantire la costante disponibilità dei servizi all'interno di quell'area, mediante la replica delle risorse in diverse zone geografiche, di modo che queste siano sempre accessibili anche quando, ad esempio a seguito di una calamità naturale, si verificano dei problemi in uno o più *data center*[27].

Il modello di *Data Trust* è senz'altro quello più interessante ai fini della nostra discussione, se non altro perché non nasce per soddisfare esigenze tecniche, quanto piuttosto come tentativo, da parte dei fornitori di servizi *cloud* (in questo caso Microsoft), di trovare una via d'uscita da una situazione sempre più insostenibile. Come vedremo meglio nelle prossime pagine, infatti, l'approvazione del *Cloud Act* da parte del Congresso USA e la conseguente pretesa di poter accedere ai dati degli utenti custoditi dai fornitori *cloud* americani indipendentemente dal luogo in cui sono conservati, ha gettato ulteriore benzina sui timori di indesiderate interferenze da parte degli Stati Uniti sui dati dei cittadini di altri Paesi[28]. Di fronte al moltiplicarsi degli obblighi di localizzazione dei dati, spaventati dalla possibilità di perdere rilevanti quote di mercato a favore di concorrenti più piccoli, ma fuori dalla portata del governo americano, alcune aziende d'oltreoceano hanno finito per elaborare un approccio assolutamente originale, che combina elementi legali, organizzativi e tecnici per separare nettamente la gestione dell'infrastruttura dall'accesso ai dati che su tale infrastruttura insistono.

Nel modello di *Data Trust*, elaborato a partire da concetti e istituti giuridici di origine anglosassone, il fornitore di servizi *cloud* si avvale infatti di un soggetto esterno, detto *data trustee*, per la gestione di tutto ciò che esula dalla stretta manutenzione operativa dell'infrastruttura. L'elemento giuridico essenziale è dato dal ricorso alla figura negoziale del *trust*[29], mediante il quale il fornitore si spoglia completamente della facoltà giuridica di accedere ai dati che transitano sull'infrastruttura per affidarli a una terza parte (nel caso in questione, una sussidiaria della tedesca Deutsche Telekom). Qualsiasi attività operativa svolta dal fornitore dell'infrastruttura che potrebbe potenzialmente consentire l'accesso ai dati dei clienti (come ad esempio la gestione degli incidenti, l'aggiornamento del software, ecc.) è soggetta a controlli tecnici che richiedono l'approvazione e la supervisione esplicite del fiduciario dei dati. L'accesso ai sistemi è inoltre consentito solo nell'ambito di un servizio specifico, per uno scopo definito, e solo per il tempo strettamente necessario allo svolgimento delle attività tecniche, che sono strettamente registrate e monitorate.

Sul piano tecnico, la separazione dei profili relativi alla gestione dell'infrastruttura da quelli dell'accesso ai dati viene garantita, oltre che dalla segregazione fisica e logica di reti e sistemi, principalmente da meccanismi di cifratura dei dati, le cui chiavi sono conservate in via esclusiva dal fiduciario. Tutte le richieste di accesso ai dati, dunque, devono essere indirizzate al *trustee* (l'unico in possesso delle chiavi di cifratura), il quale sarà tenuto a valutarle esclusivamente sulla base del diritto nazionale. Proprio l'elaborazione del principio di separazione tra la gestione dell'infrastruttura e l'accesso ai dati che su di essa insistono rappresenta uno degli elementi maggiormente innovativi e, possibilmente, più dirompenti dell'attuale panorama dei servizi di *cloud computing*.

È opportuno precisare, prima di continuare oltre, che questi diversi modelli non si escludono necessariamente l'un l'altro, ma – entro certi limiti – possono combinarsi variamente all'interno di una stessa soluzione. Il modello di *Data Trust* tedesco, ad esempio, prevede che i dati siano conservati all'interno dei confini nazionali (*Data Localization*), anche se – dal punto di vista teorico – questo non sembra essere

un requisito necessario per raggiungere le finalità che tale modello persegue (prima fra tutte quella di evitare l'insorgere di conflitti di giurisdizione), poiché le modalità tecniche, organizzative e legali adottate sono di per sé sufficienti a escludere qualunque accesso esterno ai dati stessi (anche qualora, in ipotesi, fossero localizzati in *data center* collocati in altri Paesi europei). Né l'eventuale presenza di obblighi di localizzazione esclude, di per sé, il ricorso alle tecniche di partizionamento dei dati (*Data Shard*), anche se queste avranno una portata assai più limitata, potendo riguardare unicamente *data center* collocati entro i confini nazionali (con ciò sacrificando in misura significativa l'efficacia complessiva del sistema).

Nei prossimi paragrafi ci soffermeremo su alcuni dei passaggi salienti che hanno caratterizzato l'accidentato percorso seguito dalla giurisprudenza e dal legislatore USA in tema di accesso ai dati custoditi su *cloud* da parte delle pubbliche autorità. In questo breve *excursus* non si può non partire dalla celebre decisione della corte d'appello nel caso *Microsoft Ireland*, che, dando prevalenza all'ubicazione geografica dei dati, ha riconosciuto il diritto del fornitore a non ottemperare all'ordine delle autorità federali di comunicare il contenuto di e-mail conservate nel territorio irlandese. Vedremo anche come tale decisione, al netto delle questioni ermeneutiche di diritto interno, sia stata di fatto resa possibile dal particolare modello di servizio utilizzato dall'operatore *cloud* (di tipo *Data Localization*). Vedremo anche come siano state sempre le effettive modalità di gestione del servizio *cloud* a rendere impossibile l'applicazione dello stesso principio in un caso apparentemente identico (*Google Pennsylvania*), perché espressione di un diverso modello di *cloud* (*Data Shard*). Infine, accenneremo agli aspetti salienti del *Cloud Act*, approvato dal Congresso USA proprio per disinnescare le potenziali conseguenze della decisione del caso *Microsoft Ireland*, ma che ha finito per ottenere il risultato opposto rispetto a quello perseguito, a dimostrazione di come la complessità e la varietà dei modelli *cloud* siano state, ancora una volta, sostanzialmente ignorate.

6. L'approccio al *cloud* al di là dell'oceano: i casi *Microsoft Ireland* e *Google Pennsylvania*

Il *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* è stato adottato dal Congresso USA nel marzo del 2018 come risposta alla decisione della corte d'appello nel caso *United States v. Microsoft Corp.*[30]. In quell'occasione, Microsoft si era opposta a un ordine (*warrant*) emesso dalle autorità federali americane sulla base delle disposizioni dello *Stored Communication Act* (SCA) del 1986, di produrre, tra le altre cose, il contenuto di e-mail riconducibili a un determinato *account* di posta elettronica[31].

Microsoft, che pure aveva fornito alle autorità i dati custoditi sui server in territorio americano, si era rifiutata di dare accesso ai contenuti delle e-mail perché conservate nei suoi *data center* di Dublino, dunque al di fuori del territorio statunitense, con ciò suggerendo l'idea della prevalenza dell'ubicazione "fisica" dei dati nella determinazione della giurisdizione. Nell'accogliere il ricorso di Microsoft e ribaltare la decisione di primo grado, il giudice d'appello muove infatti dal rilievo secondo cui Microsoft archivia i dati associati al contenuto della posta elettronica dei propri utenti su oltre cento *data center* sparsi per il mondo. Quando viene creato un *account*, l'utente seleziona automaticamente un "codice Paese" e Microsoft archivia il contenuto delle e-mail associate a quell'*account* (nonché tutta una serie di contenuti ulteriori, quali documenti, calendari, ecc.) nel *data center* più vicino al Paese identificato dall'utente[32]. L'ubicazione fisica dei dati è, per la corte, l'elemento oggettivo da cui partire per decidere dell'applicabilità extra-territoriale delle disposizioni dello SCA: «Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States»[33].

Quando, nel 1986, il Congresso approvò lo SCA come parte del più ampio *Electronic Communications Privacy Act*, l'obiettivo era quello di proteggere la privacy degli utenti nel contesto dei nuovi mezzi tecnologici che richiedono l'interazione di un utente con un fornitore di servizi, anche perché "trent'anni fa, i confini internazionali non venivano attraversati così regolarmente come lo sono oggi", grazie a reti e infrastrutture hardware sparse in tutto il mondo per soddisfare le richieste degli utenti. Né esplicitamente, né implicitamente, lo SCA prende in considerazione l'applicazione delle sue disposizioni al di fuori del territorio americano. E questa – conclude la corte – è esattamente la vera questione del giudizio: «It is important to recognize, however, that the dispute here is not about privacy, but rather about the international reach of American law. (...) It will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders. But there are significant practical and

policy limitations on the desirability of doing so. We live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate interests. The attempt to apply U.S. law to conduct occurring abroad can cause tensions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our border»[34].

La decisione ha sorpreso molti commentatori perché, nell'offrire una lettura molto più restrittiva delle norme dello SCA (e in particolare dell'istituto del *warrant*), ha messo in discussione il tradizionale test in base al quale l'elemento critico nel determinare se l'ordine di produrre la documentazione richiesta sia o meno eseguibile è dato dal fatto che il destinatario abbia o meno "il controllo, la custodia o il possesso" della stessa, indipendentemente dal luogo in cui tali informazioni sono conservate al momento della richiesta[35]. Il timore che la decisione del caso *Microsoft Ireland* potesse porre, ove confermata dalla Corte Suprema davanti alla quale la questione era stata sollevata, un ostacolo alle indagini aventi ad oggetto dati collocati al di fuori del territorio statunitense ha spinto il Congresso ad approvare rapidamente il *Cloud Act*.

Il carattere "eccezionale" del caso *Microsoft Ireland* è stato spesso ricondotto alla diversa lettura offerta dalla corte d'appello circa l'estensione dello SCA al di fuori del territorio americano. A riprova di tale carattere viene solitamente citato il caso *Google Pennsylvania*, di poco successivo al primo, nel quale il giudice ribalta il principio espresso nel caso Microsoft e impone al fornitore *cloud* di ottemperare all'ordine emesso dalle autorità federali[36]. Solo pochi commentatori hanno invece evidenziato come l'opposto risultato raggiunto nei due casi dipenda in larga parte dal diverso modello di *cloud* al centro della contesa[37].

Nel caso *Google Pennsylvania*[38], infatti, a essere coinvolti erano una serie di servizi i cui dati sono suddivisi in componenti che la sottostante infrastruttura provvede a smistare tra vari nodi della sua rete globale, spostandoli automaticamente da un nodo all'altro sulla base di logiche di natura prettamente tecniche, legate alla complessiva efficienza e affidabilità del sistema. Si trattava insomma di un caso di *Data Shard*, secondo la classificazione esposta nella prima parte del contributo.

Il caso riguardava due *search warrant* emessi per dati associati ad altrettanti *account* di utenti di Google. Quest'ultimo, da parte sua, aveva parzialmente ottemperato alla richiesta fornendo informazioni archiviate in *data center* situati negli Stati Uniti. Al tempo stesso, basandosi sul precedente Microsoft, si era rifiutata di fornire i dati che, in base a logiche interne di partizionamento, si trovavano su server collocati all'estero. Uno dei passaggi fondamentali seguiti dalla corte nell'arrivare alla conclusione positiva circa l'obbligo di Google di fornire per intero le informazioni richieste muove proprio dalla questione relativa a come i dati siano stati partizionati e dove si trovino i vari *shard*[39]: «Even if the interference with a foreign state's sovereignty is implicated, the fluid nature of Google's cloud technology makes it uncertain which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process. (...) Google's architecture not only divides user data among data centers located in different countries, but also partitions user data into shards. Furthermore, the data automatically moves data from one location on Google's network to another as frequently as needed, to optimize for performance, reliability, and other efficiencies. Because of the structure of this system, Google cannot say with any certainty which foreign country's sovereignty would be implicated when Google accesses the content of communications in order to produce it in response to legal process»[40].

Secondo la Corte, piuttosto che a mere *possibilities and legal abstractions*, occorre guardare alla realtà dei fatti. In questo caso, la realtà era che Google avrebbe potuto accedere a tutte le informazioni direttamente dalla sede centrale in territorio americano, a nulla rilevando l'ubicazione fisica dei dati, che in questo caso è così frammentaria da considerarsi evanescente. Il ricorso al criterio del "possesso, custodia o controllo" è dunque una strada resa necessaria dalla natura stessa del servizio *cloud*. L'opposto orientamento mostrato dalla corte d'appello nel caso Microsoft nasce dalla diversa configurazione del servizio *cloud* al centro della contesa, nel quale tutti i dati rilevanti erano conservati "in via esclusiva e in modo stabile" nel suo *data center* irlandese. Nel caso *Google*, invece, il giudice muove dalla constatazione secondo cui non sussiste alcuna prova circa l'esatta ubicazione dei server su cui sono ospitate le informazioni richieste dalle autorità federali.

«Electronically transferring data from a server in a foreign country to Google's data center in California does not amount to a "seizure" because there is no meaningful interference with the account holder's possessory interest in the user data. Indeed, (...) Google regularly transfers user data from one data center to another without the customer's knowledge. Such transfers do not interfere with the customer's

access or possessory interest in the user data. Even if the transfer interferes with the account owner's control over his information, this interference is de minimis and temporary».

Il fatto che l'operatore *cloud* ricorra a tecniche di partizionamento per massimizzare l'efficienza dell'infrastruttura, in modo del tutto invisibile e trasparente per l'utente finale (che anzi non ha alcuna idea circa l'ubicazione dei propri dati, né tantomeno delle sottostanti logiche di partizionamento) implicherebbe, secondo la corte, che non si possa parlare di interferenza con il possesso dei dati da parte dell'utente. Se, per effetto di queste logiche interne, i dati si trovano partizionati in *data center* collocati all'estero, questo rappresenta un elemento del tutto accidentale, perché in fondo neppure il fornitore saprebbe indicare con precisione dove e in quali server sono presenti questi frammenti[41]. L'unico elemento rilevante è, per la Corte, la possibilità di accedere ai dati, nella loro forma "ricomposta", dalla sede centrale del fornitore, situata in territorio USA e come tale soggetta all'osservanza delle norme federali.

Nel confermare l'obbligo di Google di adempiere a quanto richiesto dalle autorità USA, il giudice esclude però che questo comporti un'applicazione extraterritoriale alle disposizioni dello SCA. L'argomento principale sembra essere dunque di natura prettamente contingente, relativo al particolare modello di servizio *cloud* al centro della questione: «No one knows which country to ask, and even if specific servers could be identified, the data may no longer be there by the time its location has been identified»[42].

Mettendo a confronto il caso *Microsoft Ireland* con il caso *Google Pennsylvania*, è facile notare come le due decisioni abbiano ad oggetto modelli di servizio e di gestione del *cloud* assai diversi[43]. La prevalenza al criterio dell'ubicazione fisica dei dati nel primo, così come la prevalenza del criterio del controllo sui dati, nel secondo, dipendono in ultima analisi dal tipo di servizio al centro della discussione. Nel caso Microsoft, l'applicazione del criterio del luogo di residenza dei dati è resa possibile dal particolare modello di gestione dell'infrastruttura, in cui l'informazione si trova stabilmente ubicata all'interno di confini definiti (*Data Localization*). Questa caratteristica tecnica del servizio, frutto di scelte più o meno arbitrarie dell'operatore *cloud*, rappresenta l'elemento che abilita, sul piano pratico, la discussione sull'eventuale efficacia extraterritoriale delle norme che ne prevedono la confisca o il sequestro, alla pari di qualunque altro oggetto fisico.

Anche nel caso Google sono i caratteri contingenti del servizio a indirizzare e condizionare l'inquadramento legale del caso. Qui, le modalità tecniche scelte dal fornitore per ottimizzare la complessiva infrastruttura (*Data Shard*) rendono virtualmente impossibile ricorrere al criterio della ubicazione dei dati, sia dal punto di vista concettuale che da quello pratico. Questi vengono infatti spostati e riallocati continuamente da un nodo della rete ad un altro sulla base di logiche interne, largamente automatizzate, che rendono difficilmente percorribili i tradizionali canali della cooperazione giudiziaria internazionale. La vera questione, secondo il giudice, non è tanto l'applicabilità extraterritoriale delle disposizioni dello SCA, quanto piuttosto il rischio, concretissimo, di rendere eccessivamente difficoltoso, o addirittura impossibile, l'accesso alle informazioni da parte delle forze di polizia e dell'autorità giudiziaria: il timore del c.d. *going dark*.

7. Alcune osservazioni sul *Cloud Act*

Se è vero che esistono sostanziali differenze tra Stati Uniti e Unione europea in merito agli standard di protezione dei dati personali, che il *Cloud Act* ha peraltro contribuito ad acuire, è anche vero che quest'ultimo si proponeva, almeno nelle intenzioni, di facilitare la cooperazione internazionale attraverso lo strumento degli *executive agreement* e, al tempo stesso, offrire alle aziende destinatarie delle richieste di accesso un meccanismo giuridicamente azionabile per contestarne la legittimità. Alla base della soluzione prescelta dal legislatore USA vi erano infatti alcune condivisibili preoccupazioni. In primo luogo, l'aumento esponenziale delle richieste di accesso ai dati da parte di Paesi terzi, dovuto proprio all'esplosione dei servizi di *cloud computing* (i cui principali operatori sono, per l'appunto, domiciliati negli USA)[44].

L'aumentato carico di lavoro per l'ufficio dell'US Department of Justice (DOJ) ha comportato un repentino allungamento dei tempi necessari per completare i complessi adempimenti procedurali previsti dai vari trattati di mutua assistenza legale (MLAT), con il conseguente rischio di vanificare importanti indagini giudiziarie[45]: «The number of MLAT requests has increased dramatically in recent years, in light of the massive volume of electronic communications that occur daily over the Internet and the enormous amount of electronic data held by companies located throughout the world. While the MLAT process remains a critical evidence-gathering mechanism, the system has faced significant challenges keeping up with the increasing demands for electronic evidence in criminal investigations worldwide. Moreover, because many [Cloud Service Provider] move data among data storage centers in various countries, and

split up data into different pieces stored in different locations, it can be difficult both for governments and for the CSPs themselves to know where relevant data is located at any point in time for purposes of sending and fulfilling MLAT requests. The international community thus faces a critical question of how to provide governments efficient and effective access to evidence needed to protect public safety while preserving respect for sovereignty and privacy.»[46]

Due sono gli elementi essenziali del *Cloud Act*[47]. Il primo riguarda l'esplicito riconoscimento dell'applicabilità delle disposizioni dello SCA anche alle informazioni digitali conservate da fornitori di servizi *cloud* al di fuori del territorio USA. Ciò che conta è che il fornitore sia soggetto alla giurisdizione nazionale e abbia il possesso, la custodia o il controllo sui dati di cui si richiede la trasmissione: «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.»

Per quanto, come si è accennato, tale previsione non abbia rappresentato di per sé una novità – in quanto il principio era già applicato da tempo dalla giurisprudenza prevalente, oltre che riconosciuto a livello internazionale dalla Convenzione del Consiglio d'Europa sulla criminalità informatica del 2001[48] – la sua formalizzazione in un atto legislativo ha avuto se non altro il merito di aver reso esplicito l'atteggiamento del governo federale nei confronti degli operatori *cloud* domiciliati negli Stati Uniti, prevedendo al contempo alcune garanzie procedurali e sostanziali a tutela dei diritti dei cittadini e residenti USA, oltre che un meccanismo per contestare le richieste delle autorità federali (su cui subito *infra*).

Il secondo elemento è dato dalla previsione di un meccanismo basato su *executive agreement*, e dalla connessa definizione di *qualifying foreign government*. In particolare, il *Cloud Act* consente al governo USA di stipulare "accordi esecutivi" (*executive agreements*) bilaterali con Paesi terzi[49]. Questi accordi consentono ai Paesi firmatari di presentare, nell'ambito di indagini aventi ad oggetto *serious crimes*[50], richieste semplificate di accesso ai dati direttamente ai fornitori di servizi domiciliati negli Stati Uniti, secondo un meccanismo che andrebbe a completare, anziché a sostituire, le procedure attualmente previste dai trattati di assistenza giudiziaria esistenti.

Il *Cloud Act* introduce anche un meccanismo per consentire ai fornitori di servizi *cloud* di contestare (*quash*) le richieste delle autorità federali, qualora ricorrano due condizioni: il disvelamento delle informazioni può comportare per il fornitore il rischio concreto di violare un obbligo previsto dalla legislazione di un *qualifying foreign government*, e l'utilizzatore del servizio *cloud* non è un cittadino statunitense, né risiede negli Stati Uniti. Prima di accogliere la richiesta dell'operatore *cloud*, tuttavia, il giudice è chiamato a soppesare con attenzione tutti gli interessi in gioco nel caso specifico, alla luce di una serie di parametri indicati dallo stesso *Cloud Act* (la cosiddetta *comity analysis*)[51]. Nel prevedere una corsia preferenziale per i Paesi terzi che abbiano sottoscritto un *executive agreement* con gli Stati Uniti, il *Cloud Act* pone anche un importante limite a tutela dei cittadini e residenti USA. Per accedere ai dati di questi ultimi, infatti, il *Cloud Act* richiede il necessario ricorso ai tradizionali meccanismi previsti dagli accordi di mutua assistenza legale, ove esistenti.

Particolarmente interessante è la previsione del *Cloud Act* che esclude espressamente che gli *executive agreement* possano richiedere agli operatori *cloud* di decifrare i dati conservati sulla propria infrastruttura[52]. Questa previsione, che si pone in netta antitesi rispetto al timore del *going dark* che pure era alla base della stessa adozione del *Cloud Act*, è al tempo stesso un atto necessario per non danneggiare gli interessi economici degli operatori USA, e una vistosissima falla nell'intero meccanismo predisposto dal governo statunitense[53]. Non è un caso che, nelle pagine dedicate a illustrare l'impatto della nuova legislazione sulle loro politiche interne di protezione dei dati, i grandi operatori *cloud* d'oltreoceano – oltre a mettere ben in evidenza il loro costante impegno nell'opporsi alle richieste delle autorità ogni volta che ne ricorrano le condizioni – promuovano attivamente la cifratura quale strumento indispensabile per impedire l'accesso ai dati dei loro clienti da parte di "qualunque" soggetto terzo[54]. Del resto, la stessa elaborazione del modello di *Data Trust* illustrato nella prima parte di questo contributo è resa possibile, dal punto di vista tecnico, dall'applicazione generalizzata di algoritmi di cifratura sicuri.

Volendo tentare un primo bilancio degli effetti del *Cloud Act* sulla regolazione del fenomeno del *cloud computing*, gli aspetti negativi sembrano superiori ai benefici che il legislatore USA si proponeva di conseguire[55].

In primo luogo, nell'adottare un approccio unilaterale al fenomeno del *cloud computing* per garantire l'accesso alle informazioni da parte del governo USA, il *Cloud Act* ha finito per rafforzare le spinte ver-

so la localizzazione dei dati da parte di molti Stati, proprio quando uno dei fini perseguiti era dichiaratamente quello di evitare l'esacerbarsi dei conflitti legali, e della conseguente proliferazione di obblighi di localizzazione negli altri Paesi[56]. Anche gli operatori, dal canto loro, hanno in più occasioni mostrato di preferire un approccio "pragmatico" quando tratta di opporsi alle richieste delle pubbliche autorità nei Paesi nei quali offrono i loro servizi: in alcuni casi, hanno fatto leva sul principio di localizzazione per limitare l'accesso da parte delle autorità ai soli dati conservati sui *data center* del Paese richiedente. In altri casi, hanno mostrato di preferire il ricorso al criterio del controllo sui dati per opporsi a richieste provenienti da Paesi diversi dagli USA, nel quale erano domiciliati.

Inoltre, se è certamente vero che le procedure previste dagli accordi di mutua assistenza legale si sono dimostrate – proprio a causa della crescente diffusione di Internet, in generale, e dei servizi *cloud* in particolare – sempre più onerose in termini di tempo e risorse, è altrettanto vero che queste procedure erano state progettate segnatamente per offrire adeguate garanzie a tutela dei diritti e delle libertà fondamentali degli individui contro indebite intromissioni da parte dei pubblici poteri: «The rigorous procedures in the MLAT system are important safeguards for privacy and due process. When providing an alternative way, one would expect that the new regime would provide at least equivalent safeguards to those provided by the MLAT system. The CLOUD Act, however, removes some of the layers of protections provided by the MLAT system such as the rigorous reviews by [Department Of Justice], Attorney General, and courts without providing equivalent safeguards. Hence, bypassing the MLAT system could be faster for law enforcement, but it diminishes privacy standards. This is especially true for individuals in countries where there is no adequate privacy protection»[57].

In terzo luogo, nella sua pretesa di disciplinare con un unico tratto di penna un fenomeno così complesso e articolato, il *Cloud Act* omette completamente di regolare i rapporti tra i vari fornitori che compongono la "filiera" *cloud*. Come abbiamo evidenziato nella prima parte, una larghissima parte dei servizi *cloud* offerti sul mercato sono resi possibili dalla combinazione, verticale e orizzontale, di numerosi elementi infrastrutturali e applicativi messi a disposizione da una pluralità di operatori, ciascuno dei quali può avere un grado variabile di "possesso, custodia o controllo" sui dati[58]. In uno scenario di questo tipo, come scegliere il soggetto a cui inoltrare la richiesta di fornire i dati richiesti? Occorre privilegiare il livello infrastrutturale (dove i dati sono "fisicamente" conservati) o quello applicativo (tramite il quale sono generalmente acceduti)? Come vedremo nelle prossime pagine, il problema della definizione dei ruoli dei vari soggetti coinvolti nella fornitura di un servizio *cloud* all'utente finale non sono esclusive del *Cloud Act*, ma affliggono in maniera simile anche la normativa comunitaria.

8. L'accesso ai dati conservati sul *cloud*: la proposta di Regolamento *e-Evidence*

Nonostante tutti i suoi limiti, il *Cloud Act* ha contribuito a sollevare il velo su una questione di centrale importanza, ovvero il superamento del criterio dell'ubicazione fisica dei dati nel determinare la giurisdizione applicabile, in favore di un diverso principio, quello cioè del controllo sui dati. Al tempo stesso, ha mostrato tutti i limiti di un approccio unilaterale al fenomeno, che ha consentito agli operatori di sfruttare la babele di legislazioni nazionali (oltre che elementi di natura tecnica) per vanificare la pretesa di mantenere una qualche forma di controllo per finalità di interesse pubblico. Il problema rimane di estrema attualità anche nell'ambito dell'Unione europea, ed è alla base della recente proposta di Regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[59].

Rispetto al *Cloud Act*, la proposta di regolamento mostra grande attenzione al problema delle garanzie, procedurali e sostanziali, a tutela dei diritti e delle libertà degli interessati, ma – allo stesso tempo e in modo analogo al *Cloud Act* – prende atto della portata dirompente dei modelli di distribuzione e gestione dei servizi e delle infrastrutture di *cloud computing* per dedurne l'inapplicabilità del criterio dell'ubicazione dei dati come base per affermare (o negare) la giurisdizione di uno Stato: «In molti casi i dati non sono più conservati nel dispositivo dell'utente ma sono messi a disposizione su un'infrastruttura *cloud* che consente in linea di massima l'accesso da qualsiasi luogo. I prestatori di servizi non hanno bisogno di essere stabiliti o avere server in ogni giurisdizione ma ricorrono piuttosto a un'amministrazione centralizzata e a sistemi decentrati per conservare i dati e fornire i servizi. In tal modo ottimizzano il bilanciamento del carico e riducono i tempi di risposta alle richieste di dati degli utenti. (...). Le imprese possono così fornire i contenuti dal server più vicino all'utente o in grado di inoltrare la comunicazione attraverso una rete meno congestionata»[60].

Per questo motivo, il Regolamento abbandona esplicitamente «il criterio di collegamento rappresentato dall'ubicazione dei dati, *poiché generalmente la conservazione dei dati non comporta alcun controllo da parte dello Stato nel cui territorio i dati sono conservati. Nella maggior parte dei casi il luogo di conservazione è determinato dal prestatore di servizi sulla base di considerazioni commerciali.*»[61].

Il Regolamento si applica ai servizi *cloud* e agli altri servizi di *hosting* che forniscono «una vasta gamma di risorse informatiche, quali reti, server o altre infrastrutture, mezzi di conservazione, app e servizi che permettono di conservare dati a diversi scopi»[62]. L'elemento decisivo per determinare se un servizio rientri o meno nell'ambito di applicazione del Regolamento è dato dalla conservazione dei dati, che deve rappresentare un momento essenziale del contratto di servizio: «I servizi per i quali la conservazione di dati *non è una componente propria* non sono contemplati dalla proposta. Sebbene la maggior parte dei servizi forniti dai prestatori comprenda qualche tipo di conservazione dei dati, specialmente quando sono forniti online a distanza, è possibile distinguere servizi per i quali la conservazione dei dati *non è una caratteristica principale bensì un elemento puramente accessorio*, quali servizi giuridici, architettonici, ingegneristici e contabili *forniti* online a distanza».

È facile immaginare come il criterio del carattere "non accessorio" della custodia dei dati sarà uno dei punti dolenti della normativa in sede di applicazione: oggigiorno, la conservazione dei dati per conto del titolare, anche nell'ambito dell'erogazione di servizi di natura professionale (si pensi ad esempio ai tantissimi servizi *cloud* utilizzati da aziende e privati per la contabilità, la gestione del personale, incluse le buste paga, la sicurezza sul lavoro, ecc.) rappresenta un elemento così comune dall'essere dato quasi per scontato. Al tempo stesso, si potrebbe anche obiettare che, nella fornitura di servizi IaaS e PaaS, la conservazione dei dati non rappresenta l'elemento principale, poiché lo scopo è quello di mettere a disposizione dell'utente una serie di risorse di natura logica, che questi è libero di utilizzare come meglio crede.

Ciò detto, la proposta di regolamento prevede due nuovi strumenti per la produzione e la conservazione dei dati che si rendono necessari nell'ambito di indagini o procedimenti penali: rispettivamente, gli ordini europei di produzione e gli ordini europei di conservazione. Entrambi gli ordini possono essere utilizzati per chiedere di produrre o conservare dati di cui il fornitore del servizio, situato in un'altra giurisdizione rispetto a quella dove gli ordini sono emessi, abbia la disponibilità. Tali ordini possono essere notificati direttamente al prestatore del servizio, e "sono eseguiti allo stesso modo degli ordini nazionali comparabili nella giurisdizione in cui il prestatore di servizi riceve l'ordine". Perché tali ordini siano validi, sono tuttavia necessarie alcune condizioni. In primo luogo, devono essere emessi o convalidati da un'autorità giudiziaria di uno Stato membro, previa valutazione della proporzionalità e necessità nel singolo caso, nell'ambito di un procedimento penale[63]. In secondo luogo, i dati di cui si richiede la conservazione o la produzione devono essere "necessari come prova in indagini o procedimenti penali". Devono cioè riferirsi a specifici autori, noti o sconosciuti, di un reato che è già stato commesso. In particolare, l'ordine europeo di conservazione consente di chiedere la conservazione solo di dati che sono già nella disponibilità del fornitore al momento della ricezione dell'ordine, e non di accedere a dati in una fase successiva alla ricezione dell'ordine stesso. In terzo luogo, gli ordini di produzione e conservazione possono essere emessi "solo se una misura dello stesso tipo è disponibile per lo stesso reato in una situazione nazionale comparabile nello Stato di emissione".

Il tema è, ancora una volta, troppo complesso e articolato per essere approfondito in questa sede nei suoi vari profili. Dalla particolare prospettiva di questo contributo, però, si deve segnalare come non sia sfuggita alla più attenta dottrina come, nella proposta di Regolamento, il tema della cifratura dei dati rappresenti (ancora una volta) il punto dolente in grado di vanificare l'intero edificio normativo messo in piedi dalla Commissione[64]. Nel Considerando n. 19 si legge infatti che i dati devono essere forniti dal prestatore di servizi "a prescindere dal fatto che siano criptati o meno". Mentre il *Cloud Act* esonera espressamente il fornitore del servizio dal comunicare alle autorità le chiavi di cifratura, nel caso del Regolamento la questione è assai più incerta, e dipende in ultima analisi da chi abbia il controllo sulle chiavi stesse. Se, come accade nella gran parte dei casi, le chiavi sono detenute dal fornitore del servizio, manca nel testo un'esplicita previsione che obblighi il rappresentante del *service provider* a produrre obbligatoriamente le chiavi di cifratura assieme ai dati cifrati, o quantomeno a produrre il testo decifrato mediante le chiavi in suo possesso. Si tratta di una lacuna tutt'altro che secondaria, anche considerato che molto spesso le chiavi sono detenute da soggetti stabiliti in Paesi terzi che, pur facendo capo al *service provider*, non coincidono con la società che rappresenta il *provider* nel territorio dell'Unione[65].

Nel caso in cui, invece, il fornitore utilizzi un sistema di cifratura c.d. *end-to-end*, la cifratura e la decifratura dei messaggi avviene interamente sui dispositivi degli utenti finali, con la conseguente im-

possibilità per i fornitori di accedere al contenuto dei messaggi perché, semplicemente, non dispongono delle relative chiavi. In questa ipotesi, l'acquisizione dei dati attraverso l'ordine europeo di produzione si rivelerebbe del tutto inutile. È stato quindi osservato che, qualora l'Unione europea «non trovi il modo di obbligare tutti i prestatori di servizi a consegnare i dati in chiaro per finalità di giustizia, indipendentemente dal sistema di criptazione utilizzato, i progressi investigativi nell'acquisizione transnazionale della prova elettronica non potranno che essere esigui e la sensazione potrebbe essere alla fine che la montagna avrà partorito un topolino»[66]. Tuttavia, se si considerano le caratteristiche "intrinseche" del *cloud computing* che abbiamo sin qui sommariamente evidenziato, è lecito dubitare che esista realmente una strada praticabile per raggiungere il risultato voluto. Del resto, il silenzio del Regolamento sul punto, che dedica alla cifratura solo uno scarso passaggio nel Considerando n. 19, dovrebbe essere emblematico proprio di tale difficoltà.

9. Riflessioni conclusive

Alla fine di questa lunga carrellata, peraltro non esaustiva, dei problemi che la regolazione del fenomeno *cloud* ha incontrato e incontra tutt'ora a livello nazionale e internazionale, si possono tentare alcune riflessioni.

Come abbiamo evidenziato più volte nel corso di questo contributo, molte delle difficoltà che si incontrano quando ci si appresta a regolare il fenomeno del *cloud computing* discendono dall'estrema eterogeneità dei servizi genericamente ricondotti sotto l'ombrello del *cloud*. Se è vero che questi servizi presentano alcuni tratti comuni (il carattere logico delle risorse utilizzate, la loro assegnazione in base alla domanda, la possibilità per l'utente di gestire tali risorse in autonomia tramite piattaforme eterogenee, ecc.), questi elementi non sempre offrono un "appiglio" sufficiente dal punto di vista della regolazione. Anche dal punto di vista dei modelli di servizio (IaaS, PaaS e SaaS, per limitarci alla classificazione tradizionale) e dei modelli di distribuzione (*cloud* pubblico, privato, comunitario e ibrido), le differenze sono tante e tali da rendere estremamente difficile ricostruire un quadro unitario. Se a tutto ciò si aggiungono anche le variazioni nei modelli di gestione dell'infrastruttura, e dei dati che su tali infrastrutture transitano o sono conservati (cha abbiamo riassunto, senza peraltro alcuna pretesa di completezza, nella tripartizione *Data Shard*, *Data Localization*, *Data Trust*), il quadro che ne emerge assomiglia più a un complicato mosaico, in cui soluzioni tecniche, organizzative e, non ultime, legali, si combinano in modi sempre diversi a seconda del contesto e delle esigenze.

Proprio perché il contesto è così complesso e – per certi versi – confuso, è necessario trovare alcuni punti fermi da cui partire per regolare un fenomeno che non può e non deve essere lasciato interamente alle scelte degli operatori *cloud*, poiché riguarda aspetti fondamentali della nascente "società dei dati".

Innanzitutto, occorre partire da un rilievo di natura concettuale. Secondo una concezione più tradizionale, i dati non sarebbero poi così diversi dagli altri beni intangibili, come il denaro, e che il *cloud* in fondo sia poco più del metallo e dei bulloni che ne compongono l'hardware: «Despite the technological wizardry of modern life, the 'cloud' is actually a network of storage drives bolted to a particular territory, and there is substantial case law suggesting that courts think of data as a physical object. Moreover, even if the cloud were a free-floating ether, data can be thought of as an intangible asset, like money or debt, which flows across borders; courts have been adjudicating such jurisdictional disputes for centuries.»[67]

Ovviamente, non c'è alcuna *wizardry* nelle modalità di funzionamento del *cloud* e, più in generale, di Internet. Tuttavia, se è vero che alla fine qualunque tecnologia può essere ridotta a una massa di server, dischi, cavi e altri apparecchi fisici, è anche vero che le "pratiche" che tali oggetti abilitano (si pensi, oggi, alle possibilità offerte dalle *blockchain*, dall'*Internet of Things* e agli sviluppi dell'intelligenza artificiale, solo per fare degli esempi) impongono di adottare un atteggiamento non riduzionista, e non unilaterale, in grado di guardare ai fenomeni nella loro complessità. Lo stesso vale, a maggior ragione, per i dati che su queste infrastrutture transitano. Discutere se, dal punto di vista dell'applicazione di istituti e norme giuridiche, questi presentino analogie con il denaro o con altri beni intangibili rischia di tradursi, almeno ad avviso di chi scrive, in un mero esercizio di stile. Se non altro, perché sono proprio i beni intangibili come la moneta o il debito ad andare incontro a vere e proprie "mutazioni genetiche" a seguito dell'erompere di nuove tecnologie "abilitanti" (si pensi al crescente peso acquisito dalle criptovalute come Bitcoin), e non viceversa.

Ciò è particolarmente vero quando si discute degli obblighi di localizzazione dei dati all'interno dei confini nazionali. Che la loro previsione possa essere sufficiente, "di per sé", a soddisfare le spesso contrastanti esigenze pubbliche legate alla disponibilità dei dati (inclusa la possibilità di sottoporre a sequestro i server su cui i dati sono conservati) non tiene in debito conto né la natura composita e al tempo stes-

so fluida di Internet, né delle possibilità tecnologiche che possono rendere vana qualsiasi pretesa di accesso ai dati per l'esercizio di pubblici poteri, né – e questo è forse la lezione più importante impartita dal *Cloud Act* – delle possibili "reazioni" a catena che tali previsioni possono innescare da parte dei vari soggetti coinvolti, sia pubblici che privati (lo dimostra in modo esemplare il modello di *Data Trust* elaborato da Microsoft come risposta al *Cloud Act*).

Entrambi gli obiettivi perseguiti dal *Cloud Act*, ovvero ridurre il proliferare di obblighi di localizzazione a livello internazionale mediante la conclusione di accordi bilaterali, e assicurare alle autorità federali la possibilità di poter continuare ad accedere ai dati necessari all'esercizio delle funzioni pubbliche, possono dirsi falliti. Al tempo stesso, però, proprio il *Cloud Act* ha mostrato i limiti del criterio basato sul possesso, custodia o controllo dei dati, mediante il quale si cerca di agire sui fornitori di servizi *cloud* affinché siano questi ad attivarsi per rendere disponibili i dati dei propri utenti conservati – o, il più delle volte, sparsi – sulla loro infrastruttura globale, a prescindere dalla loro ubicazione geografica. A non funzionare, in questo caso, è stato soprattutto l'approccio unilaterale al fenomeno (oltre che una generale sottovalutazione della complessità della filiera *cloud*), che ha consentito ai grandi operatori di fare quello che di solito tendono a fare in casi simili: sfruttare la frammentazione delle legislazioni nazionali a loro vantaggio, in questo caso specifico per "spogliarsi", nella forma e nella sostanza, di qualunque controllo sui dati.

Molto meglio allora partire dalla particolare combinazione di elementi giuridici, organizzativi e tecnici alla base del modello di "Data Trust" per affrontare seriamente il problema della "sovranità dei dati". Indipendentemente dalle questioni circa la riproducibilità e la scalabilità dell'esperimento tedesco, l'introduzione del principio di separazione della "gestione dell'infrastruttura" rispetto alle questioni legate all'accesso ai dati potrebbe rivelarsi, con gli opportuni adattamenti, una delle chiavi di lettura di un futuro assetto europeo della regolamentazione sul *cloud*. Questa distinzione, del resto, la si ritrova anche all'interno del progetto di *cloud* franco-tedesco, oggetto di analisi all'interno di questo stesso volume. Come è stato osservato, infatti, nella documentazione di GAIA-X "vengono utilizzati sia il termine *data sovereignty* che *digital sovereignty*. Mentre la sovranità digitale viene definita come il potere di decidere «about how digital processes, infrastructures and the movement of data are structured, built and managed», la *data sovereignty* viene presentata come un particolare aspetto della sovranità digitale, consistente nel pieno controllo del *data owner* rispetto alla collocazione e all'uso dei dati. La sovranità sui dati sarebbe dunque il primo passo per assicurare una sovranità digitale piena"[68].

Note

[1]Nel 2020 il mercato mondiale dei servizi *cloud* ha raggiunto i 371.4 miliardi di dollari. Anche per effetto della recente pandemia di COVID-19, si stima che nel 2025 il mercato ammonterà a 832 miliardi di dollari, con un tasso di crescita annuo del 17.5% (fonte: *Research and Markets*).

[2]Per una sistematica revisione delle misure di localizzazione adottate a livello mondiale si vedano A. Chander, U.P. Le, *Data Nationalism*, in "Emory Law Journal", 2015, n. 3, p. 677-739; Organisation for Economic Co-operation and Development, *Trade and cross-border data flows*, TAD/TC/WP(2018)19/FINAL.

[3]Sulle vicende legate alla piattaforma "Immuni" si veda V. Pagnanelli, *Immuni: spunti per una riflessione privacy-oriented*, in "Questione Giustizia", maggio 2020.

[4]A. Chander, U.P. Le, *op. cit.*, p. 679.

[5]Per una disamina degli effetti negativi delle misure di localizzazione sulla sicurezza e la concorrenza si vedano, fra i tanti, J. Selby, *Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?*, in "International Journal of Law and Information Technology", 2017, n. 3, p. 213-232; H. Brehmer, *Data Localization: the unintended consequences of privacy litigation*, in "American University Law Review", 2018, n. 3, p. 927-969; R. Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and other Online Activities*, National Telecommunications and Information Administration, 2016; J. Lenhart, *Security for the 21st Century Economy: Borders Hold Less Meaning – and That's a Good Thing*, Information Technology Industry Council, 2017.

[6]Fonte: *Statista*. Dati riferiti ad aprile 2020.

[7]Sulla storia e l'evoluzione del *cloud computing* si vedano, tra i tanti, M.S. Gendron, *Business Intelligence and the Cloud*, John Wiley & Sons, 2014; V.V. Arutyunov, *Cloud Computing: Its History of Development, Modern State, and Future Considerations*, in "Scientific and Technical Information Processing", 2012, n. 3, p. 173-178.

[8]A. Regalado, *Who coined "Cloud computing"?*, in "MIT Technology Review", 31 ottobre 2011.

[9]NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, 9 December 2011, Special publication n. 800-144, p. IV. Definire il fenomeno in modo univoco è difficile per almeno due ragioni: «First, as there is no clear difference between the cloud and the Internet itself, any attempt to create a legal distinction among various online services will invariably lead to legal "overreach" with unintended consequences. Second, forcing such a distinction is likely to mislead the very consumers that the legislation is intended to protect because they might wrongly think that a particular rule, regulation, or practice will protect them so long as the services they are using are labeled as cloud services» (Cfr. P.S. Ryan, S. Falvey, R. Merchant, *When the Cloud Goes Local: The Global Problem with Data Localization*, in "Computer", 2013, n. 12, p. 55.

[10]I limiti propri di qualunque definizione sono del resto stati messi in evidenza dallo stesso NIST: «Much of what has been written about cloud computing is definitional, aimed at identifying important paradigms of deployment and use, and providing a general taxonomy for conceptualizing important

facets of service». Cfr. NIST, *Guidelines on Security and Privacy in Public Cloud Computing*, cit., p. 3).

[11] «Cloud computing can be considered a new computing paradigm insofar as it allows the utilization of a computing infrastructure at one or more levels of abstraction, as an on-demand service made available over the Internet or other computer network. Because of the implications for greater flexibility and availability at lower cost, cloud computing is a subject that has been receiving a good deal of attention», *ibidem*.

[12] NIST, *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, September 2011, Special publication n. 800-145.

[13] Per "scalabilità" si intende la capacità di un sistema di aumentare o diminuire le proprie prestazioni (e dunque il carico di lavoro che è in grado di svolgere nella stessa unità di tempo) in funzione della necessità e della disponibilità. La scalabilità si distingue in "orizzontale" e "verticale". La prima è la capacità di aumentare la capacità di lavoro sfruttando più componenti hardware o software in modo che funzionino come una singola unità logica (in pratica, il lavoro viene suddiviso tra più sistemi, ciascuno dei quali in grado di operare autonomamente). La scalabilità verticale, invece, aumenta la capacità aggiungendo più risorse a una stessa unità (ad esempio, aggiungendo nuova memoria o dischi più capienti, aumentando il numero di processori, ecc.). Mentre prima della diffusione del *cloud* la scalabilità poteva essere ottenuta solo comprando o noleggiando ulteriori componenti hardware e software, e dunque solo a seguito di un'attenta pianificazione e a fronte di notevoli investimenti, i servizi *cloud* possono essere scalati "elasticamente", ossia in base all'andamento (in tempo reale) del carico di lavoro. Il che significa anche che, una volta che il carico diminuisce, è possibile ridurre l'erogazione delle risorse in eccesso e, cosa assai rilevante, smettere di pagare per ciò che non si usa.

[14] Per chiarire meglio l'impatto dei modelli di *cloud computing*, si può immaginare il caso di un'azienda che decida di vendere i propri prodotti sul web. Prima dell'avvento dei servizi *cloud*, per realizzare e ospitare sulla propria infrastruttura un sito di *e-commerce* avrebbe dovuto preoccuparsi di tutta la "filiera" tecnologica: l'acquisto, l'installazione e la configurazione di server, *firewall*, *load balancer* e apparati di rete, nonché della predisposizione di adeguate misure di sicurezza fisica (sale adeguate, impianti di condizionamento, sistemi antincendio, ecc.) e logica (DMZ, sistemi di autenticazione, monitoraggio del traffico di rete, ecc.), la configurazione degli ambienti di produzione e di test, l'acquisto delle licenze software necessarie, e tantissimi altri aspetti. Nel decidere il tipo di hardware da acquistare (numero di processori, memoria, spazio disco, ecc.), l'azienda avrebbe dovuto stimare accuratamente non il carico di lavoro "medio", ma quello massimo ipotizzabile. Il carico di lavoro di un servizio web, infatti, non è mai costante: periodi di bassa e moderata attività (ad esempio durante le ore notturne) si alternano a picchi di lavoro più o meno intensi che possono mettere a dura prova le risorse disponibili (si pensi, per esempio, al periodo natalizio o ai sempre più frequenti saldi promossi online). Se queste risorse non sono sufficienti per far fronte alle richieste in un certo momento, una parte di queste richieste non potrà essere servita, causando disservizi e malumori agli utenti, o addirittura malfunzionamenti del sistema. Al tempo stesso, durante i periodi di inattività o di "scarico", tutte le risorse in eccesso, acquistate solo per poter far fronte ai momenti di picco, sono destinate a rimanere inutilizzate, nonostante siano state investite somme ingenti per acquistarle. È vero che un'azienda avrebbe potuto noleggiare tutto il necessario, anziché acquistarlo in proprio, ma anche in questo caso la "rigidità" del sistema rimarrebbe sostanzialmente inalterata e i costi largamente fissi. Grazie al *cloud*, invece, l'azienda può concentrarsi su ciò che le interessa davvero, ossia vendere i propri prodotti sul web, senza doversi preoccupare di acquistare (o noleggiare) e configurare le risorse necessarie. Queste possono essere create, aggiunte o ridimensionate in tempo reale, per seguire l'andamento del carico di lavoro e, una volta che non sono più necessarie, possono essere dismesse in tutta facilità, smettendo così di pagare per ciò che non viene utilizzato.

[15] Il confine tra IaaS e PaaS, relativamente netto in teoria, nella pratica è andato sempre più sfumando, sia perché i primi offrono oggi funzionalità di alto livello, come ad esempio macchine virtuali già preconfigurate per poter svolgere un numero sempre crescente di compiti; sia perché i servizi PaaS tendono a permettere all'utente che lo desideri un controllo più granulare sulle caratteristiche della sottostante infrastruttura virtuale.

[16] Per una "carrellata" sui diversi modelli di servizio si rinvia a A. Biasiotti, *Il nuovo regolamento europeo sulla protezione dei dati*, EPC Editore, 2018, p. 723 ss.

[17] Questa affermazione deve essere presa con le dovute cautele, poiché sempre più spesso anche i servizi infrastrutturali e/o di piattaforma prevedono (si potrebbe dire "per impostazione predefinita") forme di cifratura dei dati, in transito o "a riposo", che permettono di assicurare già in partenza un livello di sicurezza piuttosto elevato, salva la possibilità per l'utente di applicare misure ulteriori per soddisfare requisiti di sicurezza più stringenti.

[18] In informatica, l'aggettivo "trasparente" ha un significato diverso dal linguaggio comune, indicando un processo che si svolge senza che l'utente ne sia consapevole e senza che a quest'ultimo sia richiesto alcun tipo di intervento. Ad esempio, una modifica che attiene al modo con cui un software salva e organizza i dati è "trasparente" rispetto all'utente finale se, dal punto di vista di quest'ultimo, il software continua a operare come prima, senza che vi siano cambiamenti nell'interfaccia utente o nei flussi di lavoro, che rimangono quelli soliti ai quali l'utente è abituato.

[19] Nel 2017 Dropbox ha avviato la migrazione di gran parte dei suoi sistemi dall'infrastruttura di AWS sui propri *data center*.

[20] Fonte: *Mordor Intelligence*.

[21] V.V. Arutyunov, *op. cit.*

[22] In merito alla strategia italiana per l'adozione dei servizi *cloud* nell'ambito delle Pubbliche Amministrazioni si veda V. Pagnanelli, *Conservazione dei dati e sovranità digitale. Una rilettura della (big) data governance pubblica alla luce delle nuove sfide globali*, in questo fascicolo.

[23] P.M. Schwartz, *Legal Access to the Global Cloud*, in "Columbia Law Review", 2018, n. 6, p. 1681-1762.

[24] Esistono almeno tre diverse strategie di partizionamento dei dati. Nel partizionamento "orizzontale" (quello chiamato propriamente *sharding*), ogni partizione ha lo stesso schema di tutte le altre, ossia contiene le stesse tipologie di dati (ad esempio, gli ordini dei clienti). Nel partizionamento "verticale", invece, ogni partizione contiene un particolare sottoinsieme dei dati archiviati, suddivisi in base al loro modello di utilizzo. In questo modo, i dati utilizzati più spesso possono essere collocati in una partizione verticale, mentre quelli usati raramente possono essere collocati in un'altra partizione. Infine, nel partizionamento "funzionale", dati sono aggregati in base alla loro modalità di utilizzo: in un sistema di *e-commerce*, ad esempio, i dati delle fatture potrebbero essere archiviati in una partizione dedicata all'area amministrativa, e quelli relativi all'inventario dei prodotti in magazzino in un'altra partizione, pronti per essere utilizzati dalla logistica e dalle vendite.

[25] In un server, la quantità di spazio di archiviazione su disco è in genere limitata, ma è possibile sostituire i dischi esistenti con versioni più capienti o aggiungere altri dischi man mano

che i volumi di dati aumentano. Tuttavia, il sistema finirà prima o poi per raggiungere un limite oltre al quale non è più possibile aumentare la capacità di archiviazione, se non a costi proibitivi. Allo stesso modo, un singolo server che ospita tutti i dati potrebbe non essere in grado di fornire la potenza di calcolo necessaria per servire le interrogazioni (*query*) degli utenti, con conseguente aumento dei tempi di risposta e frequenti errori dovuti all'indisponibilità delle risorse. Anche in questo caso potrebbe essere possibile aggiungere ulteriore capacità computazionale e/o memoria, ma il sistema raggiungerà comunque un limite quando non sarà possibile aumentare ulteriormente le risorse di calcolo. Infine, c'è da considerare la larghezza di banda della rete. Anche in questo caso, infatti, un elevato numero di richieste aventi ad oggetto grandi quantità di dati possono generare un traffico di rete superiore alla capacità della rete usata per la connessione al server, con conseguente aumento dei tempi di risposta ed errori.

[26] P.M. Schwartz, *op. cit.*, p. 1965.

[27] Per maggiori informazioni sulla complessiva infrastruttura di Amazon Web Services, si veda "Regioni e zone di disponibilità". Anche l'infrastruttura *cloud* di Microsoft Azure prevede un'articolazione simile; per maggiori informazioni si veda "Azure geographies".

[28] Timori peraltro non infondati, se solo si pensa al caso "Snowden" e all'acuirsi delle tensioni tra l'Unione europea e gli Stati Uniti. Per un approfondimento delle vicende si rinvia a E.J. Snowden, *Errore di sistema*, Longanesi, 2019.

[29] Riconosciuto nel nostro ordinamento grazie alla l. 16 ottobre 1989, n. 364, con cui è stata ratificata la Convenzione dell'Aja sulla legge applicabile ai *trusts* e sul loro riconoscimento, adottata da L'Aja il 1° luglio 1985.

[30] *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. 2016), 14 July 2016.

[31] Oltre al contenuto delle e-mail riconducibili a un determinato *account* di posta elettronica, l'ordine includeva anche la produzione di ulteriori informazioni collegate a detto *account*, conservate sui server della sede americana. Queste informazioni sono sostanzialmente di tre tipi: «First, Microsoft stores some non-content e-mail information in a U.S.-located "data warehouse" that it operates "for testing and quality control purposes." Second, it may store some information about the user's online address book in a central "address book clearing house" that it maintains in the United States. Third, it may store some basic account information, including the user's name and country, in a U.S.-sited database». *Ivi*, p. 9.

[32] Tale scelta dipendeva peraltro da esigenze di natura tecnica (*in primis* diminuire il tempo di latenza portando i dati più vicino al luogo di accesso), non quello di soddisfare particolari esigenze di localizzazione.

[33] *Microsoft Corp. v. United States*, cit., p. 20.

[34] *Ivi*, p. 7.

[35] D. Callaway, L. Determan, *The New US Cloud Act. History, Rules, and Effects*, in "The Computer & Internet Lawyer", 2018, n. 8.

[36] A riprova del carattere "eccezionale" del caso *Microsoft Ireland* si vedano anche i casi *Yahoo Winsconsin*, *Yahoo Florida* e *Google California*, tutti successivi al primo, nei quali viene riaffermato il principio per cui le disposizioni dello SCA trovano applicazione a prescindere dal luogo in cui sono ubicati i dati.

[37] P.M. Schwartz, *op. cit.*, p. 1685 ss.

[38] *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d 708 (2017).

[39] *Ivi*, p. 25-26.

[40] *Ibidem*.

[41] In argomento si vedano le considerazioni di D. Reisman, *Where Is Your Data, Really?: The Technical Case Against Data Localization*, LAWFARE, May 22, 2017.

[42] *Ibidem*.

[43] P.M. Schwartz, *op. cit.*, p. 1681-1762.

[44] Oggi circa l'85% delle indagini di polizia si basa su elementi di prova digitali, e in due terzi di questi casi vi è la necessità di richiedere tali elementi a fornitori di servizi *cloud* localizzati in altre giurisdizioni. Il numero di richieste verso i principali operatori è cresciuto dell'84% in soli cinque anni (2013-2018). Dati della Commissione europea.

[45] U.S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, White Paper, April 2019.

[46] *Ibidem*.

[47] Per approfondimenti sul *Clarifying Lawful Overseas Use of Data* (CLOUD) *Act* si vedano, tra i tanti, J. Galbraith, *Congress Enacts the Clarifying Lawful Overseas Use of Data (CLOUD) Act, Reshaping U.S. Law Governing Cross-Border Access to Data*, in "American Journal of International Law", 2018, n. 3, p. 487-493; D. Callaway, L. Determan, *op. cit.*

[48] Si veda in particolare l'art. 18 della Convenzione, in base al quale «Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control (...)».

[49] Perché possa essere concluso un *executive agreement* con un Paese terzo, il *Cloud Act* prevede che l'*Attorney General*, assieme al Segretario di Stato, verifichino e certifichino in forma scritta al Congresso USA che la legislazione del Paese terzo offra «robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement».

[50] Sino ad oggi, l'unico accordo sottoscritto dal governo USA è quello con la Gran Bretagna. Nel testo viene chiarito che, per *serious crime* si intende, ai sensi dell'art. 1, n. 14, dell'accordo, qualunque reato che preveda come massimo edittale almeno tre anni di reclusione («Serious Crime means an offense that is punishable by a maximum term of imprisonment of at least three years»). Cfr. l'*executive agreement*.

[51] Ai sensi dell'articolo 2713 dello SCA (come emendato dal *Cloud Act*) gli elementi che devono essere tenuti in considerazione dalla corte nel decidere sulla richiesta di *quash* sono i seguenti: «a) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure; b) the interests of the qualifying foreign government in preventing any prohibited disclosure; c) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider; d) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country; e) the nature and extent of the provider's ties to and presence in the United States; f) the importance to the investigation of the information required to be disclosed; g) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and h) if the legal process has been sought on behalf of a foreign authority pursuant to sec-

tion 3512, the investigative interests of the foreign authority making the request for assistance».

[52]18 U.S. Code § 2523 (b) (3): «the terms of the agreement shall not create any obligation that providers be capable of decrypting data or limitation that prevents providers from decrypting data».

[53]Falla da cui, come si vedrà più avanti, non è esente neppure la proposta di Regolamento europeo relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (c.d. Regolamento *e-Evidence*). Il tema della crittografia, in particolare quella c.d. *end-to-end* (nel quale solo gli utenti che stanno comunicando sono in grado di leggere i messaggi, ad esclusione di qualsiasi altro soggetto, incluso il fornitore del servizio) è tornata di recente sotto i riflettori a seguito della presentazione di due proposte di legge, al momento entrambe all'esame del Senato USA. La prima proposta, denominata *Lawful Access to Encrypted Data Act* (o *LEAD Act*), mira a obbligare i fornitori di dispositivi e di servizi internet a decifrare i dati e a metterli a disposizione delle autorità in forma intellegibile. In questo senso, la proposta «is an actual, overt, make-no-mistake, crystal-clear ban on providers from offering end-to-end encryption in online services, from offering encrypted devices that cannot be unlocked for law enforcement, and indeed from offering any encryption that does not build in a means of decrypting data for law enforcement» (R. Pfefferkorn, *There is now an even worse anti-encryption bill than EARN IT. That doesn't make the EARN IT bill ok*, in The Center for Internet and Society, Stanford Law School, 24 giugno 2020). La seconda proposta di legge, l'*Eliminating Abusive and Rampant Neglect of Interactive Technologies Act* (il c.d. *EARN IT Act*) pone una serie di ostacoli, per lo più indiretti, al ricorso alle tecniche di crittografia per proteggere i contenuti.

[54]Si consideri, a titolo di esempio, quanto riportato nella documentazione ufficiale di Amazon Web Services: «In the event we cannot resolve a dispute, we do not hesitate to go to court. Amazon has a history of formally challenging government requests for customer information that we believe are overbroad or otherwise inappropriate. We will continue to resist requests, including those that conflict with local law such as GDPR in the European Union, to do everything we can to protect customer data. We will also continue to notify customers before disclosing content, and we provide advanced encryption and key management services that customers can use to protect their content further. We have industry leading encryption services that give our customers a range of options to encrypt data in-transit and at rest, and to manage encryption/decryption keys – because encrypted content is rendered useless without the applicable decryption keys».

[55] Per una disamina approfondita del Cloud Act si vedano, tra i tanti, P.M. Schwartz, *op. cit.*, p. 1748 ss.; D. Callaway, L. Determan, *op. cit.*

[56]Si veda la lettera inviata da Peter J. Kadzik, *Assistant Attorney General* presso il Dipartimento di Giustizia USA, al presidente del Senato Joseph R. Biden (luglio 2016): «The current situation is unsustainable. Some countries have begun to take enforcement actions against U.S. companies, imposing fines or even arresting company employees. If foreign governments cannot access data, they need for legitimate law enforcement, including terrorism investigations, they may also enact laws requiring companies to store data in their territory. Such data localization requirements would only exacerbate conflicts of law, make Internet enabled communications services less efficient, threaten important commercial interests, undermine privacy protections by requiring data storage in jurisdictions with laws less protective than ours, and ultimately impede U.S.-government access to data for its investigations. And as the global market for Internet related services expands, the U.S. government will increasingly need effective and efficient access to electronic information stored or uniquely accessible abroad. Conflicts of law may increasingly pose an obstacle to such access».

[57]H.H. Abraha, *How compatible is the US 'CLOUD Act' with cloud computing? A brief analysis*, in "International Data Privacy Law", 2019, n. 3, p. 213. Proprio per ovviare alle evidenti inefficienze dell'attuale sistema basato sull'accordo di mutua assistenza legale del 2001 tra Stati Uniti e Unione europea, rafforzando al contempo gli standard di protezione dei diritti degli interessati, il Comitato europeo per la protezione dei dati personali ha sottolineato l'urgenza di ridisegnare l'intero processo per dar vita a una "nuova generazione" di accordi: «The Mutual Legal Assistance Treaty already in force between the EU and the US, as a legal instrument mainly aimed at facilitating judicial cooperation, contains only very limited provisions relevant from a data protection point of view. The EDPB and EDPS therefore wish to emphasize the urgent need for a new generation of MLATs to be implemented, allowing for a much faster and secure processing of requests in practice. In order to provide a much better level of data protection, such updated MLATs should contain relevant and strong data protection safeguards such as, for example, guarantees based on the principles of proportionality and data minimisation. In addition, the "dual criminality principle" providing safeguard against discrepancy between how a crime is defined under the foreign law and how the same crime is legally defined under EU law should be preserved» (EDPB, *LIBE Committee letters to the EDPS and to the EDPB regarding legal assessment of the impact of the US Cloud Act on the European legal framework for personal data protection*, 10 luglio 2019).

[58]H.H. Abraha, *op. cit.*, p. 208: «In the cloud computing environment, 'the delivery of cloud services often depends on complex, multi-layered arrangements between various providers.' This means that different providers can be involved in a particular cloud service offering with different degrees of control over the underlying technologies and stored data. This complicates the task of law enforcement agencies in identifying who is in 'possession, custody, or control' of personal data in view of serving a subsequent order. The consequence is that the CLOUD Act may target service providers (such as Infrastructure Service providers) who do not have effective 'possession, custody, or control' over the sought-after data. In this regard, one would argue that the CLOUD Act is not compatible with some business and technological realities of cloud computing».

[59]Commissione europea, *Proposta di Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale*, COM(2018) 225 final, 2018/0108.

[60]*Ibidem*. Si osserva inoltre che «Dato che internet non conosce frontiere, tali servizi possono essere prestati da qualsiasi luogo del mondo e non richiedono necessariamente un'infrastruttura fisica né la presenza di un'azienda o di personale negli Stati membri in cui sono offerti o nel mercato interno nel suo insieme. Non richiedono nemmeno un luogo specifico in cui conservare i dati: spesso il prestatore di servizi sceglie tale luogo in base a considerazioni legittime quali la sicurezza dei dati, le economie di scala e la rapidità di accesso. Di conseguenza, in un numero crescente di procedimenti penali riguardanti qualsiasi tipo di reato, le autorità degli Stati membri richiedono l'accesso ai dati che potrebbero servire da prove e che sono conservati al di fuori del loro paese e/o da prestatori di servizi situati in altri Stati membri o in paesi terzi».

[61]*Ibidem*, nostro il corsivo.

[62]Il Regolamento si applica anche «ai mercati digitali che consentono ai consumatori e/o alle imprese di concludere operazioni tramite contratti di vendita o di servizi online. Tali operazioni sono effettuate o sul sito web del mercato online o sul sito web di un professionista che utilizza i servizi informatici forniti dal mercato online. È pertanto questo mercato che generalmente detiene prove elettroniche che possono essere necessarie nel corso di procedimenti penali».

[63]Si intende dalla fase preprocessuale delle indagini preliminari fino alla chiusura del procedimento con sentenza o altra decisione. Il regolamento opera anche una distinzione tra (meta) dati relativi agli accessi e quelli relativi al contenuto dei dati stessi: «gli ordini per la produzione di dati relativi agli abbonati o agli accessi possono essere emessi per qualsiasi reato, mentre quelli per la produzione di dati relativi alle operazioni o al contenuto possono essere emessi solo per reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni o per specifici reati precisati nella proposta e se vi è un collegamento specifico con gli strumenti elettronici e i reati rientranti nel campo di applicazione della direttiva (UE) 2017/541 sulla lotta contro il terrorismo».

[64]Sul punto si rinvia all'approfondita analisi e alle acute osservazioni di R. Pezzuto, *Accesso transnazionale alla prova elettronica nel procedimento penale: la nuova iniziativa della Commissione europea al vaglio del Consiglio dell'Unione*, in "Diritto Penale Contemporaneo", 2019, n. 1, p. 71 ss., da cui sono tratte le considerazioni che seguono.

[65]Sul punto cfr. R. Pezzuto, *op. cit.*, in part. pp. 73-74.

[66]*Ibidem*, p. 74.

[67]A.K. Woods, *Against Data Exceptionalism*, in "Stanford Law Review", 2016, n. 4, p. 729.

[68]V. Pagnanelli, *op. cit.*

* * *

Cloud computing: technical models and legal frameworks

Abstract: The cloud computing market has experienced an exponential growth rate in recent years, which the recent global pandemic emergency will eventually strengthen further. The success of this complex and varied "ecosystem" of technologies and services lies in a synergistic combination of factors, as well as the increasingly widespread diffusion of smartphones and tablets, which has led to new ways of using IT services. Cloud platforms today perform an enabling function with respect to a practically infinite variety of services, which could not exist without the resources made available by cloud computing providers. From a legal point of view, however, cloud computing leaves enormous questions still largely unresolved. How to protect the rights of data subjects when their data can be moved, unpacked, recomposed and replicated in any node of the global network with a simple click? How to regulate such kaleidoscope of different services and how to share obligations and responsibilities among the various subjects that make up the cloud supply chain? In many respects, the approach followed by the United States and the European Union could not be more different, but both pretend to unilaterally regulate a phenomenon - cloud computing and, more generally speaking, the Internet - in which "The data are shared according to the logic of the system, and not according to venerable historical lines drawn on a map of the world".

Keywords: Cloud computing – Cloud Act – e-Evidence Regulation