UNA STRATEGIA CLOUD PER UN'ITALIA PIÙ COMPETITIVA E SICURA



icom
istituto per la competitività

CURATORI

Stefano da Empoli

Lorenzo Principali

AUTORI

Silvia Compagnucci

Giusy Massaro

Thomas Osborn

Lorenzo Principali

Domenico Salerno

SI RINGRAZIANO

Laura Gagliarducci e Giulia Palocci

per le attente letture e l'impaginazione

SOMMARIO

INTRODUZIONE 3

1. LE CARATTERISTICHE DEL CLOUD 17

1.1 COS'È IL CLOUD COMPUTING 18

1.2 I SERVIZI CLOUD 20

1.3 I FALSI MITI SUL CLOUD 23

1.3.1 Falso mito #1: Il cloud non è sicuro 23

1.3.2 Falso mito #2: I dati presenti sul cloud possono essere visualizzati da chiunque 27

1.3.3 Falso mito #3: Hosting e Cloud computing sono la stessa cosa 28

1.3.4 Falso mito #4: una volta scelto un fornitore di servizi cloud è impossibile cambiare 29

1.3.5 Falso mito #5: Il passaggio al cloud è un processo lungo e oneroso 30

2. IL DIBATTITO INTERNAZIONALE SULLA SOVRANITÀ DIGITALE E SULLE INFRASTRUTTURE DEI DATI 33

2.1 LA SOVRANITÀ DIGITALE IN EUROPA 34

2.1.1 Il dibattito europeo tra autonomia strategica e sovranità tecnologica 34

2.1.2 La sovranità dei dati e il cloud computing 37

2.1.3 Le priorità digitali dell'attuale Commissione e delle altre istituzioni UE 40

2.2 LA EUROPEAN DATA STRATEGY 42

2.3 PROGETTI DI CLOUD A LIVELLO EUROPEO 46

2.3.1 Casi nazionali 46

2.3.2 Il progetto Gaia-X 52

2.3.3 La partecipazione dell'Italia e possibili scenari di Regional Hub 55

2.4 LA GESTIONE DEI DATI TRA EUROPA E USA 57

2.4.1 Dal caso Microsoft vs. USA al Cloud Act. Le potenziali frizioni con la normativa europea 57

2.4.2 Dalla sentenza Schrems II alle raccomandazioni dell'EDPB 63

3. SICUREZZA, CLOUD E DIGITALE IN ITALIA. COME ACCELERARE LA TRASFORMAZIONE DIGITALE E PROMUOVERE LA COMPETITIVITÀ NAZIONALE 69

3.1 IL QUADRO NORMATIVO NAZIONALE SULLA SICUREZZA CIBERNETICA 70

3.1.1 Dal recepimento della direttiva NIS all'istituzione del Perimetro Nazionale di Sicurezza Cibernetica 70

3.1.2 L'iter di attuazione della disciplina sul perimetro di sicurezza: l'adozione del primo DPCM e la proposta di DPR su CVCN e CV 76

3.1.3 Il DL Semplificazioni 82

3.2 L'IMPATTO DELLA DIGITAL TRANSFORMATION E DEL CLOUD SULLE

IMPRESE E SULLE PUBBLICHE AMMINISTRAZIONI 84
3.2.1 L'analisi sulle imprese 84
3.2.2 L'analisi sulla PA 88

3.3 LE CONSEGUENZE DELLA SOVRANITÀ DIGITALE SU COMPETITIVITÀ E TASSI DI INNOVAZIONE 91

3.4 IL CASO DEL CLOUD NAZIONALE 94
3.4.1 Il rischio di riduzione degli effetti benefici: economie di scala e tasso innovativo 94
3.4.2 La potenziale limitazione nell'offerta di servizi cloud avanzati 96
3.4.3 Il potenziale impatto di un eventuale cloud nazionale sulla cybersecurity 99
3.4.4 Maggiori difficoltà di certificazione e compliance normativa 104
3.4.5 Possibile riduzione dell'adozione del cloud da parte di PA e imprese 107
3.4.6 Il Cloud di Stato nel PNRR 110

4. CONCLUSIONI E SPUNTI DI POLICY 113

4.1 IMPATTO ECONOMICO E APERTURA DEL MERCATO 114

4.2 SICUREZZA, PROTEZIONE DELL'UTENTE E RESILIENZA 118

4.3 UNO SCHEMA OPERATIVO PER IL DIBATTITO 122

APPENDICE A - IL MODELLO DI STIMA DELL'IMPATTO DEL CLOUD SULLE IMPRESE ITALIANE 125

METODOLOGIA E DESCRIZIONE DELLE VARIABILI 126

I RISULTATI 126

APPENDICE B - METODO DI STIMA DELL'AUMENTO DI FATTURATO DELLE IMPRESE 129

APPENDICE C - IL QUADRO NORMATIVO EUROPEO E LE INIZIATIVE ADOTTATE DOPO LA PRONUNCIA DELLA SENTENZA SCHREMS II 131

DAL GDPR ALLE PROPOSTE DEL 2019 SUGLI ORDINI EUROPEI DI PRODUZIONE E DI CONSERVAZIONE DI PROVE ELETTRONICHE IN MATERIA PENALE 132

LE INIZIATIVE ADOTTATE DOPO LA SENTENZA SCHREMS II 138

INTRODUZIONE

L'avvento della pandemia e il mutato scenario internazionale, se da un lato hanno riportato al centro del dibattito l'importanza della trasformazione digitale, dall'altro hanno rafforzato il timore di cedere "sovranità" per via di un'eccessiva dipendenza dell'Europa da altre aree del mondo anche a livello tecnologico.

In questo contesto, il **cloud computing** ha assunto una particolare valenza strategica sia per il vasto utilizzo di servizi cloud da parte di imprese, PA e cittadini europei, sia perché questa tecnologia costituisce una piattaforma abilitante essenziale per la trasformazione digitale.

Il dibattito politico-tecnologico sul tema è stato complicato – e a tratti sensibilmente distorto – dalla natura di questa tecnologia (complessa, in continua evoluzione e per lo più sconosciuta al vasto pubblico) e dalle sue caratteristiche tecniche, che implicano l'ottimizzazione della gestione dei dati, il loro trasferimento e l'archiviazione in base alle risorse di rete e alla collocazione dei diversi data center, ma anche alla cifratura degli stessi, al punto che gli stessi provider non dispongono delle chiavi di accesso ai dati ospitati sulle proprie infrastrutture.

A ciò si aggiunge il cambio di paradigma IT, con il passaggio da un sistema in cui ogni individuo o organizzazione dispone di propri hardware e software a un nuovo contesto più fluido in cui gli utenti possono fruire dei servizi e predisporre l'intera infrastruttura IT direttamente sui propri terminali, mentre la capacità di calcolo, di immagazzinamento dati (e, nel caso dei servizi SaaS, anche la stessa installazione e fornitura delle applicazioni) sono tutte operazioni effettuate dal provider di servizi. A tal proposito, si è osservato come i contributi al dibattito nostrano in materia di passaggio al paradigma del cloud computing siano relativamente pochi, spesso focalizzati su posizioni ideologiche e di principio che non evidenziano la reale e variegata natura delle questioni da analizzare.

Il presente rapporto nasce quindi dalla volontà di fornire un contributo oggettivo e indipendente al dibattito sul tema in Italia, analizzando in profondità gli aspetti tecnici, legali e operativi, e soprattutto quelli legati all'innovazione e allo sviluppo del mercato, delineando una serie di possibili proposte di policy funzionali alla definizione di un "approccio Paese" al tema del cloud.

A tale scopo, lo studio parte dall'analisi degli aspetti tecnologici di questo nuovo paradigma, cercando di presentarli in forma divulgativa e facendo chiarezza su una serie di falsi miti che, pur basandosi su convinzioni

errate, hanno preso corpo nel dibattito italiano.

In secondo luogo, l'analisi si focalizza sul tema della sovranità digitale e delle infrastrutture dei dati in Europa, passando in rassegna le strategie, le priorità e i progetti in atto a livello europeo (su tutti Gaia-X, il cloud federato promosso da Germania e Francia, alle quali si è associata l'Italia), e vengono mostrate le principali esperienze europee in materia, ponendo l'accento sul caso britannico e sull'importanza di avviare una strategia di classificazione dei dati anche nel nostro Paese.

In terzo luogo è stato approfondita la relazione atlantica tra Europa e Usa in termini di scambio dei dati, sia a livello economico che normativo, anche al fine di fare chiarezza sul Cloud Act e sulle possibili implicazioni per gli utenti europei.

Infine, si è proceduto ad analizzare il contesto italiano sia a livello normativo, con particolare riferimento ai temi del cloud, della trasformazione digitale e della sicurezza cibernetica, sia a livello di impatto della digital transformation e dello stesso cloud computing sulle imprese e sulle Pubbliche Amministrazioni. A tal proposito, sono state analizzate le potenziali conseguenze della sovranità digitale in termini di restrizione delle dinamiche di mercato sia rispetto alla competitività del sistema, ai tassi di innovazione, agli effetti benefici derivanti dall'adozione del cloud, sia in relazione all'effettiva velocità di adozione di questa tecnologia da parte di PA e imprese.

L'intento è quindi fornire una panoramica a 360° sul settore, delineando la situazione attuale ed i possibili scenari e proponendo un set di raccomandazioni volte a ottimizzare il rapporto tra la regolamentazione dei vari ambiti connessi al passaggio verso il nuovo paradigma del cloud computing e a massimizzare l'impatto positivo verso il sistema-Paese nel suo complesso. Ciò allo scopo di fornire una base di supporto alle scelte di policy che guideranno il Governo Draghi nell'accelerare la transizione digitale nel nostro Paese, anche attraverso le riforme e i progetti da condurre nell'ambito della Recovery and Resilience Facility.

EXECUTIVE SUMMARY

Negli ultimi mesi stiamo assistendo ad un dibattito crescente sulla sovranità tecnologica che spesso ha generato interpretazioni fuorvianti. Infatti, se da un lato è importante per l'Italia e per l'Europa riguadagnare posizioni nel digitale, dall'altro posizioni sovraniste di estrema chiusura non sembrano motivate e coerenti con l'idea di creare una leadership digitale che a livello di Paese possa fare tesoro delle migliori competenze e risorse disponibili. Elementi centrali di questo dibattito sono stati i dati e il cloud.

Un ruolo fondamentale nel processo di digitalizzazione è svolto dall'utilizzo e dall'elaborazione dei dati, motore imprescindibile dello sviluppo nel nuovo contesto economico-sociale e allo stesso tempo elemento chiave che necessita di particolare tutela in termini di sicurezza.

In questo contesto, il **cloud computing** ha assunto una particolare valenza strategica sia per il vasto utilizzo da parte di imprese e PA e cittadini europei di servizi cloud, sia perché questa tecnologia costituisce una piattaforma abilitante essenziale per la trasformazione digitale.

Il cambio di paradigma economico e culturale che questo comporta – e che comprende il passaggio ad un modello in cui hardware, software e la stessa gestione e immagazzinamento dati vengono forniti da provider esterni – ha generato un dibattito politico-tecnologico che, complicato dalla complessa natura di questa tecnologia, è spesso scivolato verso derive ideologiche.

In considerazione di tale complessità e della strategicità di tale tecnologia in qualità di primario fattore abilitante della digital transformation del Paese, il presente rapporto punta a fornire un contributo oggettivo e indipendente al dibattito sul tema.

Partendo da un'analisi delle caratteristiche tecnologiche del cloud computing, lo studio prova a chiarirne i principali **aspetti tecnici, normativi e operazionali**, anche rispetto ai tanti falsi miti che lo circondano. Particolare attenzione è data agli effetti del cloud computing in termini di innovazione ed efficienza, nonché alle opportunità economiche e sociali che queste nuove tecnologie possono offrire a cittadini, PA e imprese in termini di ottimizzazione della gestione dei dati e accesso a servizi avanzati.

Ampio spazio è dedicato anche al dibattito geo-politico in materia di **sovranità digitale**, ai rapporti tra UE e Usa in termini di scambio dei dati e alle infrastrutture dei dati in Europa. Nel fornire un confronto tra le strategie

adottate in diversi stati UE, insieme ad una panoramica dei progetti in atto a livello europeo, su tutti Gaia-X, il rapporto dedica particolare attenzione alle implicazioni delle tecnologie cloud in termini di cybersecurity e di controllo dei dati da parte degli utenti. A ciò si aggiunge un focus sulle **relazioni Europa-Usa** relative alla regolamentazione dello scambio dei dati.

È inoltre presente un'analisi specifica del **contesto italiano**, sia per quanto concerne l'ambito normativo, sia a livello di impatto del cloud e della trasformazione digitale su imprese e pubbliche amministrazioni. A tal proposito, il rapporto si focalizza sulle potenziali conseguenze dell'estremizzazione del concetto di sovranità digitale in termini di restrizione delle dinamiche competitive rispetto al tasso di innovazione, ai benefici derivanti per l'Italia dall'adozione delle tecnologie cloud e all'effettiva velocità di adozione da parte di imprese e PA, e fornisce una serie di riflessioni e spunti finalizzati a fornire un set di raccomandazioni utili per l'azione del Governo, anche nel contesto del PNRR di prossima presentazione alle istituzioni europee.

Cloud computing, un cambio di paradigma per la transizione digitale

Il passaggio al cloud computing implica un vero e proprio salto di paradigma nel mondo IT. Combinato insieme ad altre tecnologie che si stanno diffondendo negli ultimi anni, il cloud costituisce la principale piattaforma abilitante per tutte le tecnologie avanzate (Intelligenza Artificiale, Big Data, Internet of Things) che fanno capo al processo di trasformazione digitale che sta interessando il mondo delle imprese, dei cittadini-consumatori e delle stesse istituzioni. Questa rivoluzione porterà notevoli benefici economici e sociali. Secondo le stime di I-Com, basate su un modello econometrico, **l'adozione di soluzioni cloud da parte delle imprese italiane potrebbe comportare un aumento di fatturato complessivo fino a 620 miliardi di euro**, di cui oltre la metà a beneficio delle PMI. La condivisione e l'apertura nei confronti di questa rivoluzione tecnologica e apporteranno notevoli benefici economici e sociali. Si tratta tuttavia di trasformazioni che occorre conoscere approfonditamente in modo da poterle padroneggiare e incanalare nella giusta direzione.

Il cloud computing implica il passaggio da un sistema in cui ogni individuo o organizzazione dispone di propri hardware e software ad un nuovo contesto più fluido in cui gli utenti possono fruire dei servizi e predisporre l'intera infrastruttura IT direttamente sui propri terminali, mentre la capacità di calcolo, di immagazzinamento dati (e, nel caso dei servizi SaaS, anche la stessa installazione e

fornitura delle applicazioni) sono tutte operazioni effettuate dal provider di servizi.

Per tali ragioni, la capacità di calcolo, storage, etc. sono fornite (e pagate) a richiesta, a seconda delle effettive necessità e del reale utilizzo.

A livello tecnico si distingue tra **IaaS (*Infrastructure as a service*)**, in cui il provider fornisce prevalentemente risorse hardware (server, capacità di rete, archivio e backup); **SaaS (*Software as a Service*)**, ovvero la fornitura di applicazioni chiavi in mano, inclusi servizi avanzati per gestire Big data, Machine learning, Intelligenza Artificiale e IoT; **PaaS (*Platform as a Service*)**, dedicato agli sviluppatori, che consiste nella fornitura di una intera piattaforma software.

A livello di fornitura è possibile distinguere tra **private cloud**, **public cloud** e **hybrid cloud**. Il private cloud identifica un servizio disegnato per una sola impresa o organizzazione, utilizzando sistemi spesso all'interno del proprio datacenter. Il public cloud prevede invece l'accesso di molteplici clienti alle stesse macchine virtualizzate e l'utilizzo dello stesso sistema di server all'interno di una rete condivisa ma in cui un utente non può accedere a dati e applicazioni degli altri. L'hybrid cloud indica un utilizzo combinato e flessibile di risorse di cloud pubblici e privati a vantaggio dell'organizzazione che lo utilizza e che ha bisogno di distribuire in modo interoperabile i carichi e i dati in ambienti diversi.

In relazione al cloud ed ai servizi ad esso connessi, persistono tuttora una serie di opinioni spesso non corroborate da fatti, che ne hanno modificato la percezione e rallentato la diffusione su larga scala. Uno di questi **"falsi miti"** è collegato all'effettiva **sicurezza delle informazioni** che vi si immagazzinano. Nella percezione di molti sembra affermarsi l'idea che, una volta usciti dai propri server o data center, si verifichi la perdita del controllo sui propri dati, che divengono un più facile bersaglio dei criminali informatici. È importante ricordare che i principali cloud provider sono consapevoli delle minacce informatiche che si stanno diffondendo con la stessa rapidità dell'evoluzione della tecnologia e, per questo motivo, investono sulla sicurezza ingenti risorse economiche, facendone un proprio punto di forza. Infatti, i dati che vengono affidati ai cloud provider sono protetti da livelli di sicurezza che difficilmente gli stessi proprietari sarebbero in grado di garantire, come dimostrato dalla conformità al quadro regolatorio che consente ai primi di essere conformi ai più elevati standard di sicurezza fisica e delle informazioni. Inoltre il livello raggiunto da questi operatori è allineato a **framework di cybersecurity, leggi e certificazioni internazionali** che sono puntualmente verificati formalmente da

auditor indipendenti. A ciò si collega il tema della **crittografia** e dell'accesso ai dati custoditi sul cloud. Al contrario di quanto comunemente ritenuto, i dati migrati sul cloud sono sottoposti a un processo di cifratura che permette di accedervi esclusivamente a chi è in possesso delle chiavi di decrittazione. Le aziende e gli enti pubblici che scelgono di avere come partner un cloud provider possono decidere di gestire autonomamente le chiavi, rimanendo quindi l'unico soggetto abilitato ad accedere ai propri dati localizzati sui server remoti.

Un altro dei falsi miti che riguardano il cloud computing è relativo al fatto che quest'ultimo generi necessariamente un effetto lock-in nei confronti dei cloud provider. Al contrario, l'utilizzo di un **approccio multi-cloud** (ovvero l'utilizzo contemporaneo di più fornitori cloud), pur potendo rappresentare un maggior costo per l'utente (per operatività e necessaria formazione del personale), è un'alternativa che consente di sfruttare gli standard di interoperabilità che caratterizzano queste soluzioni per distribuire dati e applicazioni su ambienti diversi, senza affidare l'intera struttura digitale della propria organizzazione ad un unico soggetto.

Il contesto europeo ed internazionale

Già con il suo arrivo alla guida della Commissione Europea, la Presidente Ursula von der Leyen aveva ulteriormente enfatizzato il proprio impegno nei campi dell'economia digitale, facendo dell'accesso a una rete sicura ed economicamente vantaggiosa una delle priorità del proprio mandato. L'attenzione della Commissione si è incentrata in particolare su una serie di settori strategici quali l'intelligenza artificiale, l'e-commerce, la sicurezza cibernetica e la gestione di dati in cloud computing.
Grande attenzione è stata posta al tema della **sovranità sui dati** intesa come l'accesso, il controllo, l'elaborazione e l'utilizzo dei dati. Il mercato dei dati, particolarmente strategico sia per la **sicurezza nazionale** dei singoli Stati, sia per le opportunità di **crescita economica** da esso generato, è in continua espansione e si prevede possa raggiungere un valore complessivo della domanda aggregata di oltre 100 miliardi di dollari entro il 2025.

Il tema della sovranità dei dati ha assunto massima rilevanza, nel dibattitto europeo e internazionale, all'indomani dell'adozione del CLOUD Act (2018) che, pur introducendo un obbligo di ostensione ampio e pervasivo in capo ai fornitori di "*servizi di comunicazione elettronica o servizi di calcolo a distanza*", tra cui i cloud provider, che siano sottoposti alla giurisdizione degli Stati Uniti (che include anche le società aventi sede legale in Paesi diversi dagli USA ma con società partecipate operative negli Stati Uniti), indipendentemente dal fatto che tali

comunicazioni, registrazioni o altre informazioni si trovino all'interno o all'esterno degli Stati Uniti, ha apprestato un set di limitazioni e garanzie procedimentali che consentono un equo contemperamento tra l'esigenza di assicurare adeguate forme di tutela e la necessità di garantire efficacia di azione alle autorità che necessitino di accedere a determinati dati per perseguire reati di particolare gravità.

La delicatezza della relazione USA-UE in tema di dati è diventata ancora più centrale in conseguenza dell'adozione della sentenza Schrems II che, dichiarando l'invalidità della decisione di esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, ha determinato un grave vuoto regolamentare da colmare[1]. In questa fase, comunque, le *standard contract clause* (SCC), unitamente ad altre misure di supporto, rappresentano un meccanismo efficace per gestire la transizione.

A livello italiano, il dibattito sulla sovranità dei dati ha spesso trascurato quanto accaduto in altri importanti Paesi europei, dando l'impressione di voler assumere a tratti toni ideologici, tendenzialmente mirati ad assumere una posizione di chiusura e di protezione territoriale.

La **Francia**, nel 2009, aveva avviato il percorso verso la creazione di un "**cloud sovrano**", *Andromède*, nato con lo scopo di fornire un cloud nazionale per il settore pubblico e le imprese. Questo avrebbe dovuto essere realizzato attraverso un partenariato pubblico-privato che avesse lo Stato in qualità di azionista di maggioranza e che coinvolgesse gli operatori privati del mercato. Tuttavia, il progetto iniziale è stato abbandonato, portando all'uscita dei soggetti

[1] Nella logica di fornire certezze e colmare questo vuoto regolamentare, a quattro mesi dalla pronuncia di tale sentenza, il 29 ottobre scorso lo European Data Protection Supervisor (EDPS) - il Garante europeo della protezione dei dati ha pubblicato *la Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling,* volta a delineare un piano strategico per assicurare che i trasferimenti internazionali in corso e futuri siano effettuati in conformità a quanto previsto dalla Carta europea dei diritti fondamentali e dal Cap. V del regolamento n. 1725/2018, mentre il Comitato europeo per la protezione dei dati (EDPB), il 10 novembre scorso ha pubblicato le "*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*" e le "*Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*". Si tratta di interventi che se da un lato hanno l'indubbio merito di cercare di fare chiarezza sullo stato dell'arte mediante un'attenta opera di mappatura delle varie tipologie di trasferimenti diretti a soggetti privati in particolare negli USA, promuovere un approccio ragionevolmente fondato sull'analisi del rischio (precision regulation) ed offrire supporto agli esportatori di dati nel complesso compito di valutare i paesi terzi ed individuare, se necessario, adeguate misure supplementari, pongono numerosi interrogativi e lasciano aperte numerose questioni.

pubblici e all'interruzione dei servizi inizialmente previsti.

Iniziative maggiormente inclusive si sono rivelate più efficaci. Nel **Regno Unito**, nel 2012, è stato avviato il Programma "***G-Cloud***" finalizzato a diffondere l'utilizzo del cloud nel settore pubblico e ad agevolare **l'acquisto dei servizi attraverso accordi con i cloud provider privati, nel frattempo aprendo l'accesso al mercato PA per le startup capaci di realizzare applicazioni per il pubblico**. Rispetto al caso francese, le maggiori interazioni e collaborazioni con gli operatori privati, **anche extra-europei,** hanno favorito la realizzazione di una serie di accordi quadro con i provider, grazie ai quali le PA possono selezionare i servizi richiesti e concludere accordi di fornitura, oltre alla creazione di uno store online di servizi cloud e ad una strategia per il consolidamento dei data center. In aggiunta, nel 2013 il governo ha adattato la propria struttura organizzativa e di sicurezza alle nuove tecnologie e alla gestione di dati sensibili attraverso sistemi di cloud con una riforma della propria **Data Classification Strategy**. Costruita in modo da facilitare la digitalizzazione dei processi, quest'ultima prevede tre livelli di sicurezza che indicano il grado di sensibilità dei contenuti trattati dal Governo, dai dipartimenti e le agenzie del governo centrale e dalle forze armate. Ad ogni livello è associato un livello di sicurezza e di controlli adeguati, al fine di **contenere e contrastare rischi informatici**. È interessante notare come le informazioni classificate come *"**secret**"* e "***top secret***" non superino complessivamente il **5%** delle informazioni gestite dagli enti pubblici del Regno Unito.

Sempre nell'ottica di allargare e rendere maggiormente inclusivo il perimetro della regolamentazione e del mercato dei dati, di recente la Commissione Europea ha promosso il progetto di ispirazione franco-tedesca **"Gaia-X"**, che implica la creazione di un data framework in cui stabilire regole comuni ai paesi UE e standard tecnologici da applicare per tutte le soluzioni Cloud presenti sul mercato siano esse pubbliche o private. Il progetto punta a trovare un equilibrio tra la **protezione dei dati** di enti, cittadini e imprese, anche attraverso strumenti normativi come il GDPR, e lo sviluppo di strumenti innovativi capaci di incrementare efficienza, tecnologia, e benessere per la cittadinanza all'interno di **un ecosistema digitale aperto e trasparente**.

I vantaggi derivanti da un approccio sovranazionale consentirebbero di sfruttare al meglio le opportunità economiche derivanti dal mercato dei dati, con la creazione di un ecosistema più ampio basato su regole uniformi e sul rispetto delle normative comunitarie, evitando gli effetti negativi della frammentazione in sistemi cloud nazionali. Per tali ragioni l'**Italia** ha dimostrato grande fiducia nel progetto, con un numero di aziende partecipanti secondo

solo a quello di Germania e Francia, e con l'adesione di operatori delle telecomunicazioni e delle principali infrastrutture nazionali e l'intenzione di dotarsi di un **Regional Hub** sul suolo nazionale.

Sicurezza, sovranità e crescita economica in Italia

All'interno di questo quadro generale, l'Italia sta giocando la propria partita, sino ad ora impostata in particolare sulla **sicurezza**. Si tratta di una prova straordinariamente importante da cui dipende, in buona misura, lo sviluppo e l'innovazione digitale nel nostro Paese e che si dipana attraverso un percorso molto complesso e articolato che vede innestare, accanto alla normativa sul ***golden power***, il **perimetro di sicurezza nazionale cibernetica.**

Quest'ultimo, in particolare, è stato istituito dal decreto legge n. 105/2019 (convertito con la legge n. 133/2019) che ha individuato una serie piuttosto corposa di DPCM e regolamenti attuativi indispensabili per comporre l'articolato mosaico normativo indispensabile a garantirne la concreta applicabilità di cui soltanto il primo (**DPCM n. 131 del 30 luglio 2020**) – con cui sono state definite le modalità e i criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica e sono stati individuati i criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica – è stato oggetto di pubblicazione sulla G.U. il 21 ottobre scorso, in ritardo rispetto alla tabella di marcia indicata dal decreto istitutivo del perimetro.

È ancora *in itinere*, invece, la procedura di adozione dello schema di regolamento indispensabile ai fini dell'operatività del **CVCN** e che definisce le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati, i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione delineata, le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

Si tratta di un ritardo attuativo grave che, sebbene trovi parziale giustificazione nella necessità, per tutte le istituzioni nazionali, di gestire la pandemia ancora in atto, impone un'accelerazione ormai improcrastinabile in considerazione della necessità, all'interno di un contesto europeo auspicabilmente armonizzato, di creare un ecosistema normativo quanto più possibile certo e chiaro in grado di orientare, rafforzare ed attrarre investimenti ed innovazione e favorire la ripresa economica del sistema paese.

Queste considerazioni assumono un valore ancora superiore in un contesto come quello italiano, dove il settore ICT, che incide sul PIL solo per il 3,3%, **sconta un significativo svantaggio rispetto alle economie più avanzate**. Tale dinamica è importante anche alla luce delle scelte da intraprendere per indirizzare le policy che guideranno gli investimenti in digitalizzazione compresi nel PNRR.

Se puntare a colmare rapidamente il gap potrebbe significare non progettare adeguatamente il futuro, allo stesso tempo la previsione di investimenti che guardano troppo al lungo termine rischierebbe di indebolire il Paese nel breve periodo. Rispetto alla destinazione di parte delle risorse alla promozione del **cloud computing**, la strategia di puntare direttamente alla creazione di un **cloud di Stato**, come avvenuto anni fa in Francia, potrebbe rischiare di non colmare il gap tanto nel breve quanto nel lungo periodo, ancor di più se si restringesse il campo dei fornitori per nazionalità.

Infatti, se la crisi pandemica ha messo a dura prova la resilienza di tutti i Paesi europei, **le esigenze che la gestione del sistema IT governativo è chiamato ad affrontare sono molteplici e varie**. In questo contesto, il cambio verso il paradigma del cloud necessita dell'identificazione delle giuste soluzioni in grado soddisfare il bisogno di sicurezza e efficienza e, al contempo, di garantire sistemi IT sufficientemente performanti, innovativi e flessibili. In particolare, l'opportunità di utilizzare al meglio gli effetti di scala, insieme all'esigenza di evitare costi di duplicazione e garantire interoperabilità, fanno emergere forti incertezze sull'ipotesi di infrastrutture cloud nazionali implementate con risorse limitate all'ambito domestico. La frammentazione derivante da queste, infatti, rischierebbe di limitare l'efficienza dei processi e di far venire meno la spinta propulsiva della transizione digitale e gli innumerevoli vantaggi delle tecnologie cloud in termini di efficienza, accessibilità e sicurezza.

Inoltre, si osserva come l'implementazione di un cloud nazionale che limitasse l'accesso alle risorse dei provider di mercato, in particolare quelli tecnologicamente più avanzati,

rischierebbe di ridurre sensibilmente la varietà, la qualità e l'adattabilità di servizi finali offerti, così come il numero di applicazioni disponibili. In questo scenario, il ventaglio di scelta per consumatori, imprese ed enti pubblici risulterebbe fortemente ridotto, in particolare per quanto concerne tutte quelle applicazioni che sono state già sviluppate, utilizzate, e migliorate a livello internazionale, col rischio di rallentare i processi produttivi e operativi all'interno dei quali tali applicazioni sono ormai integrate.

Una limitazione dell'accesso alle risorse dei principali provider di mercato rischierebbe di influenzare anche lo stesso **tasso di adozione** del cloud da parte di aziende e PA, per via della minore capacità che un ristretto numero di servizi avrebbe nel soddisfare le esigenze di enti e aziende, oltre che, paradossalmente, di avere delle ripercussioni anche sul **livello di sicurezza** complessivo di enti pubblici e aziende. Questo è particolarmente rilevante per il nostro Paese, in quanto presenta profili di rischio più alti sia rispetto alla media europea, con il primato per numero di computer compromessi con software malevoli (12,47%) e un costo medio delle violazioni che si è attestato nel 2020 sui 101 mila dollari per le PMI e su 1,09 milioni per le grandi imprese.

Inoltre, poiché aziende e PA avevano già iniziato o effettuato la propria migrazione al cloud, ai pericoli citati si aggiungerebbe il **rischio** di **vanificare parte dei miglioramenti** importanti di cui sia le **imprese** che le **Pubbliche Amministrazioni** hanno già beneficiato grazie all'**adozione del cloud**, costringendole ad un'ulteriore migrazione verso servizi necessariamente meno sviluppati, testati e pronti all'uso. Infatti, considerando la mole di investimenti in R&S, la varietà e la qualità raggiunta dai maggiori provider internazionali, che offrono servizi già utilizzati, testati e migliorati da molteplici enti e aziende a livello globale, difficilmente potrebbe essere raggiunta internamente con un approccio ispirato puramente a criteri geografici.

Di conseguenza, è ragionevole ritenere che una **limitazione della concorrenza** e dell'accesso a risorse e servizi di operatori privati, nazionali, europei ed extra-europei rischi fortemente di determinare un deterioramento sia in termini di qualitativi che di diffusione dei nuovi servizi più avanzati. In questo senso, appare opportuno valutare una rosa di alternative, tra cui la possibile adozione di **forme di cloud ibride e aperte all'utilizzo di soluzioni provenienti dal mercato**, che siano soggette a qualche forma di qualificazione nazionale (come già avviene con AgID), attraverso le quali si consentirebbe di non limitare il maggiore tasso innovativo derivante da un mercato aperto, e di garantire al contempo i più elevati standard di

qualità, varietà, sicurezza e di efficienza. Questo risulterebbe particolarmente importante per l'Italia dove, con innovazione e digitalizzazione ancora in ritardo rispetto agli altri attori internazionali, è necessaria una progettazione strategica quantomai urgente ma nel contempo capace di affrontare le sfide di medio-lungo termine.

Gli spunti per una strategia cloud nazionale

Allo scopo di ottimizzare il rapporto tra la regolamentazione dei vari ambiti connessi al passaggio verso il nuovo paradigma del cloud computing e la massimizzazione dell'impatto positivo verso il sistema-Paese, si propongono una serie di riflessioni e spunti finalizzati a fornire un set di raccomandazioni utili per l'azione del Governo.

- ✓ **CONCORRENZA:** assicurare un'elevata competitività del mercato del cloud con la partecipazione di tutti i cloud service provider nazionali e internazionali, in modo da favorire maggiori investimenti, italiani ed esteri, in innovazione, infrastrutture e tecnologie sul territorio nazionale e innalzare il livello di sviluppo e di conoscenze interno; promuovere una **collaborazione basata su valori e principi comuni, senza discriminazioni geografiche**.

- ✓ **RETI E COMPETENZE**: completare la **rete di accesso** ad **alta velocità** distribuita su tutto il territorio nazionale e implementare appositi **programmi** per rafforzare le **competenze digitali** dei lavoratori pubblici e privati, degli studenti e dei cittadini.

- ✓ **ECOSISTEMA APERTO E INTEGRATO:** incoraggiare **l'interoperabilità dei servizi cloud** e la **portabilità di dati e applicazioni**, l'utilizzo di standard aperti, favorendo la partecipazione, l'integrazione e la flessibilità, in modo da aumentare il livello di innovazione del Paese e la condivisione di tecnologie e best practice capaci di migliorare il livello complessivo di innovatività del sistema; garantire il **pieno controllo sui dati** attraverso modalità di governo degli stessi allineate agli standard europei e di mercato e la diffusione di **Codici di Condotta** – come ad esempio quello di CISPE (Cloud Infrastructure Services Providers in Europe) – che aiutino soggetti pubblici e privati ad assicurarsi che il fornitore della loro infrastruttura cloud utilizzi standard appropriati per la protezione dei dati che siano conformi al Regolamento generale sulla protezione dei dati

(GDPR); **armonizzazioni** di settore per i principali data space e business ecosystem, nel solco tracciato dal **progetto Gaia-X** e con altri **sistemi giuridici** e di regolazione (anche alla luce delle Raccomandazioni del Comitato europeo della protezione dei dati in seguito alla sentenza Schrems II).

- ✓ **SICUREZZA DEI DATI**: effettuare una **classificazione di dati e asset strategici** per valutare quali sono quelli che necessitano di un particolare livello di protezione, con criteri che garantiscano il migliore trade-off tra sicurezza e competitività del mercato; garantire una gestione trasparente e responsabile dei dati, facendo riferimento a quanto previsto dalle principali organizzazioni europee ed internazionali.

- ✓ **INCENTIVI ALLA MIGRAZIONE VERSO IL CLOUD:** proseguire e rafforzare i programmi nazionali (in particolare il **Piano Transizione 4.0**) e gli incentivi per la **trasformazione digitale** delle **PMI** tramite il **cloud** computing; accelerare il **percorso *cloud-first***, previsto dal Piano Triennale per l'ICT pubblico sin dal 2018, secondo un **modello di cloud ibrido**, con l'obiettivo di migrare le migliaia di data center oggi dispersi e inefficienti che non riescono a garantire standard di sicurezza adeguati; promuovere l'utilizzo di fondi con cui valorizzare le esperienze e le capacità presenti nella Pubblica Amministrazione **evitando la centralizzazione su unico operatore privato di mercato per la gestione in partnership dei PSN** (i **Poli Strategici Nazionali**) ma rafforzando l'infrastruttura pubblica esistente al fine di utilizzarla per le applicazioni non migrabili al cloud di mercato; **favorire l'accompagnamento** alle nuove tecnologie e la **modernizzazione** delle **applicazioni** attraverso forme di incentivi che **premino** l'adozione di percorsi sinergici di migrazione e la scelta di operatori che facciano della **sostenibilità** un impegno concreto.

- ✓ **UN APPROCCIO DI POLICY CONDIVISO PER UNA STRATEGIA CLOUD DI LIVELLO PAESE INTEGRATA E SINERGICA**: all'interno del documento si propone un possibile **quadro di riferimento per lo sviluppo di policy** capace di indirizzare le criticità emerse dal dibattito e favorire lo sviluppo del mercato lungo **due dimensioni fondamentali: 1. Integrazione e armonizzazione; 2. Innovazione e competitività.** Al

riguardo, la creazione di un tavolo permanente di confronto tra operatori e Governo può favorire consapevolezza e convergenza sulle priorità da indirizzare. Ciò in una logica di regolamentazione che prenda in considerazione la via migliore all'innovazione, nell'ottica della protezione dei diritti dei cittadini e della responsabilità degli operatori.

1. LE CARATTERISTICHE DEL CLOUD

1.1 COS'È IL CLOUD COMPUTING

Il cloud computing è stato definito dal NIST come "*un ambiente di esecuzione elastico che consente l'accesso via rete e su richiesta ad un insieme condiviso di risorse di calcolo configurabili (ad esempio rete, server, dispositivi di memorizzazione, applicazioni e servizi) sotto forma di servizi a vari livelli di granularità. Tali servizi possono essere rapidamente richiesti, forniti e rilasciati con minimo sforzo gestionale da parte dell'utente e minima interazione con il fornitore.*" In generale, il cloud computing può essere assimilato a un insieme di modelli di servizio che consente ai singoli, alle imprese e alle organizzazioni di utilizzare in modo flessibile sia le proprie risorse ICT, intese come infrastrutture e applicazioni, sia quelle messe a disposizione, tramite la crescente accessibilità e diffusione e capacità delle reti, da un fornitore di servizi specializzato, generalmente definito "cloud provider".

Il National Institute of Standards and Technology identifica per il cloud computing 5 caratteristiche principali (Fig.1.1): self-service a richiesta; accesso a banda larga; condivisione delle risorse; rapida elasticità; e monitoraggio dei servizi utilizzati.

Il **self-service a richiesta** (on-demand self-service) indica la possibilità per un cliente di richiedere la fornitura di risorse computazionali, memorizzazione o altri tipi risorse a seconda delle proprie necessità, senza bisogno di richiedere un intervento umano da parte del fornitore del servizio.

Questa caratteristica dà la possibilità all'utente di utilizzare servizi a richiesta nel momento e secondo i quantitativi necessari, che vengono fatturati in base all'effettivo sfruttamento, consentendo quindi risparmi in termini di investimenti in infrastrutture interne. L'**accesso a banda larga** (Broad network access) indica la possibilità di beneficiare delle risorse sopraindicate tramite device semplici o complessi (dagli smartphone ai portatili, fino a computer dotati di maggiori capacità di calcolo) purché dotati di connettività adeguata all'uso specifico richiesto. La **condivisione delle risorse** (Resource pooling) implica che le risorse di calcolo del fornitore vengono raggruppate per servire molteplici clienti secondo un modello multi-tenant[2], che

[2] Il modello multi-tenant si riferisce ad architetture virtuali in cui una singola istanza del software è condivisa tra più utilizzatori, detti tenant. L'architettura è sviluppata per essere in grado di mantenere una separazione virtuale tra i dati e le configurazioni dei vari tenant, che quindi non possono accedere ai dati di altri utenti. Per ognuno è inoltre possibile applicare personalizzazioni a livello di interfaccia, ma il codice alla base del software rimane comune.

prevede l'assegnazione dinamica delle risorse fisiche e virtuali a seconda della richiesta dei singoli clienti. La **rapida elasticità** (Rapid elasticity) identifica la possibilità di fornire e assegnare le risorse, anche automaticamente, per scalare rapidamente sia verso l'alto che verso il basso (ovvero aumentare o diminuire l'intensità delle risorse offerte) in modo commisurato alla richiesta del cliente.

Per quest'ultimo le risorse disponibili appaiono pressoché illimitate e possono essere fornite senza limiti in termini di tempo e quantità. Questa caratteristica è particolarmente importante perché consente di abbattere i costi fissi per le infrastrutture ICT e di commisurare la spesa all'effettiva necessità. Per tali ragioni, l'utilizzo del cloud computing comporta particolari benefici per le startup e le imprese di dimensioni contenute, che in questo modo possono accedere a capacità e servizi del livello più avanzato senza doversi sobbarcare gli ingenti costi che la realizzazione di tali complesse infrastrutture e servizi comporterebbero.

Si identifica infatti con il **monitoraggio** (measured service) dei servizi utilizzati la caratteristica propria del cloud di controllare e ottimizzare automaticamente il consumo di risorse. Ciò avviene attraverso un'appropriata capacità di misurazione del loro utilizzo a seconda delle diverse tipologie di servizio (storage, processamento dati, capacità di

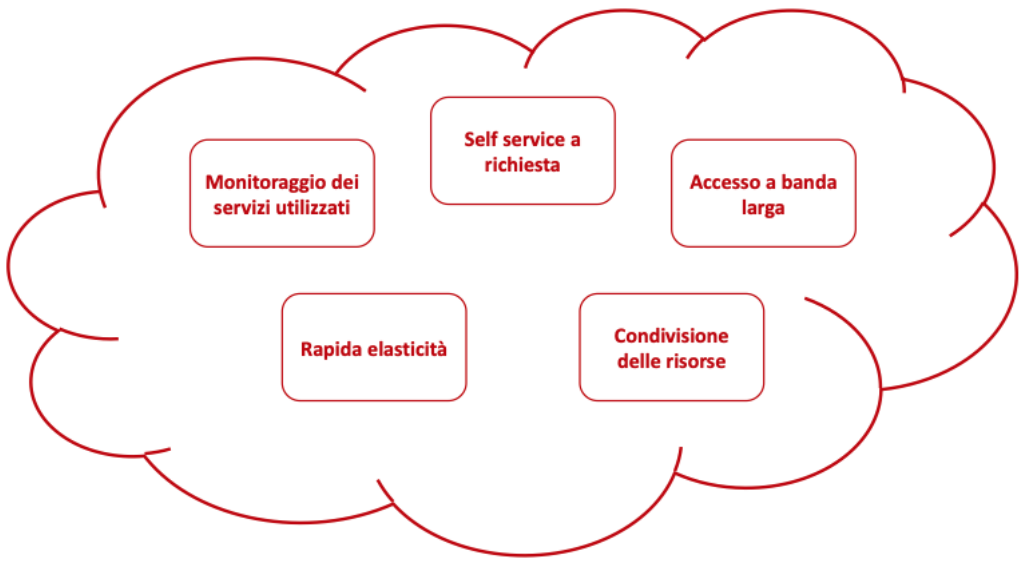


FIGURA 1.1 Le caratteristiche del cloud

Fonte: I-Com

banda e servizi avanzati offerti direttamente sui terminali degli utenti).

Queste caratteristiche configurano il cloud computing come la principale piattaforma abilitante della digital transformation, che consente alle imprese e alle organizzazioni di estendere la capacità di elaborare, archiviare o accedere potenzialmente a qualunque mole di dati, e di usufruire di qualunque tipologia di servizi, anche estremamente avanzati, direttamente sui propri terminali. In particolare, l'adozione di piattaforme di cloud computing abilita le imprese e gli enti della Pubblica Amministrazione ad accedere a servizi di Big Data Analysis, Intelligenza Artificiale, Machine Learning, Blockchain e Internet of Things.

1.2 I SERVIZI CLOUD

I servizi cloud si differenziano a seconda del tipo di servizio offerto e del livello di coinvolgimento del provider, che varia dalla fornitura di risorse fino alla messa a disposizioni di applicazioni pronte da utilizzare. In generale, i servizi cloud sono tipicamente raggruppati in 3 categorie principali (Fig.1.2): l'*Infrastructure as a service* (**IaaS**), il *Software as a Service* (**SaaS**) e il *Platform as a Service* (**PaaS**).

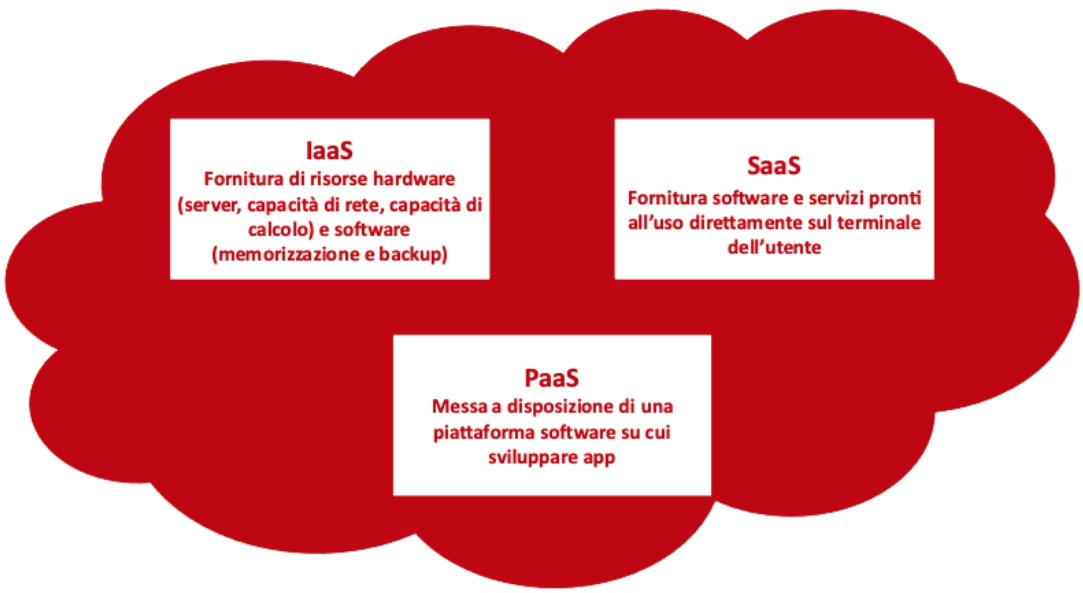


FIGURA 1.2 I servizi offerti dal cloud

Fonte: I-Com

Lo **IaaS** consiste nella messa a disposizione dell'utente (ovvero dell'impresa o dell'organizzazione che ne beneficia), oltre che di risorse virtuali in remoto, anche di risorse hardware, quali server, capacità di rete, sistemi di memoria, archivio e backup. Su queste infrastrutture l'utente può installare i software di cui ha bisogno (come applicazioni o sistemi operativi). La particolare caratteristica dello IaaS consiste nella sua scalabilità, che consente nel mettere a disposizione dell'utente le risorse richieste (capacità di calcolo, di rete o di memoria) al momento e nella misura in cui in cui una piattaforma ne ha bisogno. In genere i vendor forniscono anche le adeguate protezioni (cybersecurity) per i dati immagazzinati nei loro data center e per l'accesso ai servizi offerti. Grazie alla scalabilità, lo IaaS consente di usufruire delle risorse necessarie ad elaborare i dati per l'analisi dei Big data e l'utilizzo di tecnologie che fanno capo all'Intelligenza Artificiale e all'Internet of Things che altrimenti sarebbero troppo dispendiosi per aziende di medie dimensioni, così come per le organizzazioni e le pubbliche amministrazioni, in particolare locali.

Il **SaaS**, che generalmente viene identificato nell'utilizzo da parte dell'utente di software installati su un server remoto (cioè fuori dal proprio computer fisico o dalla LAN locale), consiste di fatto nella fornitura della più ampia gamma di servizi, che vanno dalla disponibilità di programmi CRM (Customer Relationship Management), ERP (Enterprise Resource Planning), e applicazioni di finanza e controllo fino a servizi capaci di gestire Big data, Machine learning, Intelligenza Artificiale e IoT. Questi vengono "impacchettati" in applicazioni che possono essere affittate in diverse configurazioni e ne consentono l'utilizzo su molteplici tipologie di device. Nello specifico, il cloud provider installa l'applicazione nei propri data center e fornisce agli utenti un'interfaccia per utilizzarla.

Il **PaaS** indentifica altresì il processo in cui, anziché uno o più programmi singoli, viene eseguita in remoto una intera piattaforma software, in genere costituita da programmi, librerie software ed altri prodotti per i quali il cloud provider fornisce anche una interfaccia di programmazione (API) che permette all'utente di scrivere applicazioni che interagiscono con il servizio. Talvolta viene fornito anche un ambiente di sviluppo e di testing delle stesse applicazioni.

Per quanto concerne i modelli di dispiegamento, si distingue tra public cloud (da non confondere con il cloud di Stato), private cloud e hybrid cloud (Fig.1.3). Il **private cloud**, detto anche internal cloud o corporate cloud, identifica un servizio cloud di immagazzinamento e gestione dei dati disegnato per una sola impresa o

organizzazione, che comprende diversi utenti (ad esempio diverse business unit). Può essere posseduto, gestito e operato dalla stessa organizzazione o azienda, da fornitori terzi o da entrambi, e può esistere sia on- che off-premise (ovvero all'interno o all'esterno dei locali dell'azienda che lo utilizza). Le Raccomandazioni sull'utilizzo del cloud di DigitPA (ora AgID) indicano come il cloud privato venga prevalentemente installato da un utente nel proprio data center per suo utilizzo esclusivo. Alternativamente, aziende o soggetti pubblici possono installare il proprio cloud privato nel data center di un fornitore terzo, disponendo di macchine dedicate e del relativo controllo di configurazione, seppure queste non risiedano nel loro dominio. A differenza dei public cloud, il private cloud utilizza quindi un perimetro specifico per delineare specifiche risorse (ad esempio i server) che vengono usate da una singola impresa.

Nel **cloud pubblico** (o "cloud di mercato", per evitare di confonderlo con il cloud di Stato o fornito/utilizzato da enti della PA) invece, è consentito l'accesso di molteplici clienti alle stesse macchine virtualizzate e viene utilizzato lo stesso sistema di server all'interno di una rete pubblica. Infrastruttura e servizi sono messi a disposizione da parte di un provider (un'azienda o un'organizzazione governativa o accademica o da una combinazione di queste tipologie) ad un pubblico più ampio.
Laddove il modello di cloud privato prevede per definizione la restrizione dell'accesso ad utenti esterni al provider, il public cloud condivide le risorse per offrire un livello unificato (e ottimizzato) di servizio. In particolare, gli utenti del public cloud possono accedere solo alle proprie informazioni, mentre l'accesso a quelle degli altri utenti viene impedito. I vantaggi per gli utenti di cloud pubblici consistono nel poter usufruire dei servizi nel momento e nella scala di performance richiesti, riducendo quindi l'impatto degli investimenti e la gestione dei picchi di carico, mentre dipendono dal fornitore le policy relative all'allocazione geografica di elaboratori e dati, nonché alla protezione di questi ultimi.

Nel modello di **cloud ibrido** l'infrastruttura consiste in un qualche tipo di combinazione degli altri due modelli di dispiegamento che, se da un lato rimangono entità distinte, dall'altro sono legate da comuni tecnologie, proprietarie o standardizzate, che consentono la portabilità di dati e applicazioni. L'hybrid cloud indica quindi un utilizzo combinato di risorse di cloud pubblici e privati a vantaggio di un utente (inteso come entità), consentendo ad esempio ad aziende dotate di cloud privati di appoggiarsi anche a cloud pubblici nell'eventualità di picchi particolarmente intensi di lavoro (come



FIGURA 1.3 Tipologie di Cloud

Fonte: I-Com

nel caso di cloud privati all'interno di data center che offrono anche servizi di cloud pubblico).

1.3 I FALSI MITI SUL CLOUD

In relazione al cloud ed ai servizi connessi ad esso, nel corso degli ultimi anni si sono diffuse presso l'opinione pubblica e parte degli stakeholder una serie di opinioni spesso distorte e di veri e propri pregiudizi, catalogabili come "falsi miti", che ne hanno modificato la percezione e rallentato la diffusione su larga scala. Nei seguenti sottoparagrafi vengono approfonditi tali aspetti nel tentativo di chiarire come questi miti siano in realtà privi di fondamento nell'ecosistema cloud.

1.3.1 Falso mito #1: Il cloud non è sicuro

Uno dei principali falsi miti che riguardano il cloud è collegato all'effettiva sicurezza delle informazioni che si immagazzinano su di esso. Nella visione collettiva che si riscontra nel dibattito pubblico sembra affermarsi l'idea che, **una volta usciti dai propri server o data center, vi sia una perdita di controllo sui propri dati**, che divengono un più facile bersaglio dei criminali informatici. Nella realtà, si osserva come la sicurezza informatica sia direttamente proporzionale agli investimenti che vengono effettuati per garantirla. Di conseguenza, gli **operatori che**

investono il maggior numero di risorse in questo comparto sono in genere anche quelli capaci di garantire i livelli di sicurezza più alti, grazie a sistemi e tecnologie di ultimissima generazione. A maggior ragione, sistemi che ospitano più soggetti in concorrenza tra la loro hanno accesso alle migliori risorse disponibili, e possono dunque garantire un livello di sicurezza complessivamente più alto rispetto ai sistemi chiusi. Secondo uno studio pubblicato da Markets and Markets Research nel luglio del 2020, gli investimenti globali sulla sicurezza informatica del cloud hanno raggiunto i 34,5 miliardi di dollari nel 2020 e dovrebbero arrivare a 68,5 miliardi di dollari entro il 2025. I principali fattori che guidano la crescita degli investimenti includono la necessità di anticipare e fronteggiare il numero crescente di sofisticati attacchi informatici alle organizzazioni pubbliche e private e l'introduzione da parte degli Stati di normative sempre più stringenti in tema di sicurezza informatica. Gli **hyperscaler,** i cloud service provider che operano a livello mondiale, facendo della sicurezza un proprio punto di forza, **investono su di essa ingenti risorse economiche.** Per questo motivo, deve essere ben chiaro che **i dati che vengono affidati a questi soggetti sono protetti da livelli di sicurezza che difficilmente altri soggetti (es. piccoli operatori o singoli operatori nazionali) sarebbero in grado di garantire. Inoltre il livello di sicurezza ICT raggiunto da questi operatori è allineato a framework di cybersecurity, leggi e certificazioni internazionali che sono puntualmente verificati formalmente da auditor indipendenti.** Ciò ancor più vero per i dati conservati in server proprietari o piccoli data center da parte degli enti della PA locale.

Per quanto concerne gli aspetti strettamente tecnici che riguardano la sicurezza delle piattaforme di cloud computing, questi si basano su una complessa interazione di tecnologie, controlli, processi. **Cyber Threat Intelligence** e **Continous Monitoring**, **Intrusion Detection Systems (IDS)** e **Intrusion Prevention Systems (IPS)**, **Resilienza della piattaforma** costituiscono poi la spina dorsale della sicurezza nel cloud.

Gli strumenti *di Threat Intelligence* rappresentano la capacità di intelligence sviluppata in ambito cybersecurity. Includono la raccolta e l'analisi di informazioni al fine di caratterizzare possibili minacce informatiche dal punto di vista tecnico, di risorse, di motivazioni e di intenti, spesso in relazione a contesti operativi specifici. Gli IDS sono strumenti atti ad eseguire un monitoraggio continuo della sicurezza, allo scopo di identificare in anticipo tutti gli attacchi alle reti informatiche e ai computer.
Gli IPS sono invece dei componenti software attivi che registrano e tentano di segnalare e bloccare gli attacchi alle reti informatiche.

Questi rappresentano un'estensione degli strumenti di IDS, poiché posizionati inline e abilitati a prevenire e bloccare le intrusioni identificate. Nello specifico, gli IPS possono mandare un allarme, eliminare pacchetti malevoli, resettare le connessioni e/o bloccare il traffico da un indirizzo IP attaccante, correggere gli errori CRC (Cyclic redundancy check), deframmentare pacchetti, evitare problemi di sequenza TCP e ripulire i livelli di trasporto e la rete da opzioni indesiderate. La **resilienza della piattaforma** consiste nella capacità della infrastruttura cloud di ripristinarsi quando sollecitata dal carico di lavoro (più richieste di servizio), da attacchi (accidentali a causa di un bug o intenzionali) e guasti di qualsiasi componente nei componenti del carico di lavoro.

Altro aspetto fondamentale che permette ai cloud provider di mantenere le proprie reti sicure sono i **test di vulnerabilità e di penetrazione**. Questi prevedono un'analisi attiva e passiva dei sistemi al fine di individuare eventuali punti deboli, difetti tecnici e vulnerabilità. I test sono utili a far emergere problematiche derivanti da difetti di progettazione, implementazione e gestione del sistema. Tali vulnerabilità, se identificate da malintenzionati, potrebbero essere sfruttate per aggirare i sistemi di sicurezza del sistema.

Un ultimo aspetto, spesso trascurato, è quello della **sicurezza fisica dei luoghi** in cui i dati vengono custoditi. I data center gestiti dai cloud service provider di scala globale sono posizionati in luoghi (generalmente segreti) protetti da stringenti misure di sicurezza più simili a caveau delle banche piuttosto che ad una classica sede aziendale. I data center degli hyperscaler sono realizzati in modo tale da essere completamente fault-tolerant e prevedere ridondanza per ogni componente. Nella fase di scelta dei luoghi dove collocare i data center, i cloud provider eseguono inoltre valutazioni preliminari di natura ambientale e geografica. Le location vengono selezionate in modo da limitare il rischio di danni di natura ambientale, come alluvioni, condizioni climatiche estreme e attività sismiche. In caso di imprevedibili e disastrosi avventi avversi, al fine di salvaguardare la continuità delle operazioni, i cloud provider mettono a disposizione dei propri partner servizi di Disaster Recovery, ovvero misure tecnologiche che permettono, in caso di imprevisto, di ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi. Di fronte ad una grave emergenza che mina il funzionamento dei sistemi aziendali, le procedure di Disaster Recovery permettono di ripristinare il software di sistema ed i file che sono stati classificati e documentati come critici. La tecnologia offerta dai cloud service provider offre inoltre la possibilità di realizzare soluzioni di continuità che

permettono un'erogazione continua dei servizi IT ridondando i dati in un sito secondario, consentendo di conseguenza di ripristinare le attività anche nel caso in cui i sistemi primari siano colpiti in maniera irreparabile.

Case study: Comune di Codogno

Il Comune di Codogno è responsabile dei servizi pubblici a Codogno, una cittadina di circa 16.000 abitanti in Lombardia, nel Nord Italia, purtroppo finita sotto i riflettori in quanto è stato il primo comune italiano a registrare casi confermati di COVID-19 e successivamente ad essere colpito da un grande numero di contagiati.

Mentre l'Italia entrava in lockdown, il governo nazionale ha scelto di utilizzare i servizi offerti da un provider cloud per garantire che comuni come Codogno potessero continuare a operare anche se i dipendenti comunali dovevano rimanere a casa per la propria sicurezza.

Il call center in cloud è stato identificato come la soluzione ideale alla sfida che i comuni dovevano affrontare. Il servizio è stato attivato nel giro di una settimana e ha permesso ai dipendenti comunali di rispondere alle chiamate da casa e reindirizzare gli utenti all'ufficio di competenza.

Il servizio ha, infatti, offerto al personale del Comune di Codogno la comodità di rispondere alle chiamate tramite smartphone o laptop, utilizzando una tastiera softphone basata sul web. I dipendenti pubblici sono stati in grado di reindirizzare le chiamate non solo ad altri uffici municipali, ma anche a enti governativi, come il Dipartimento della Protezione Civile, a livello regionale e nazionale. Inoltre, attraverso il servizio, il personale del Comune di Codogno ha potuto evadere le richieste di buoni spesa e di supporto tramite i servizi sociali.

Essendo la soluzione completamente configurabile via web, i dipendenti del Comune di Codogno hanno potuto modificare i messaggi di chiamata persa sui propri telefoni e il Comune ha potuto adattare i

processi di chiamata ogni qualvolta fossero necessarie modifiche durante la fase di emergenza COVID-19.

Il personale del Comune di Codogno ha gestito in media 7.187 minuti di chiamate in entrata e 6.445 minuti di chiamate in uscita al mese, rispondendo alle domande dei residenti pur rimanendo al sicuro nella propria abitazione.

Fonte: https://www.aboutamazon.it/innovazioni/confermando-il-nostro-impegno-in-italia-apertura-della-regione-aws-europe-milano

1.3.2 Falso mito #2: I dati presenti sul cloud possono essere visualizzati da chiunque

Il tema della sicurezza si collega direttamente a quello della crittografia e dell'accesso ai dati custoditi sul cloud. Un falso mito particolarmente diffuso è infatti quello che riguarda la possibilità da parte dei cloud provider di avere liberamente accesso ai dati dei propri clienti. Al contrario, è importante osservare che **i dati migrati sul cloud sono sottoposti ad un processo di cifratura che permette di accedervi esclusivamente a chi è in possesso delle chiavi di decriptazione. Le aziende e gli enti pubblici** che scelgono di avere come partner un hyperscaler cloud provider **possono quindi decidere di gestire autonomamente le chiavi**, rimanendo quindi l'unico soggetto abilitato ad accedere ai propri dati localizzati sui server remoti. Inoltre, i cloud provider mettono a disposizione dei propri utenti sistemi di Identity and Access Management (IAM) che consentono di **controllare chi ha effettivamente l'accesso ai dati e alle applicazioni**. Gli IAM offerti dai cloud provider combinano l'autenticazione multi-fattore con strumenti di gestione delle policy di accesso che consentono agli amministratori di modificare il ruolo degli utenti, tenere traccia delle loro attività, creare report su tali attività e applicare le policy di accesso su base continuativa.

Nell'ambiente cloud i servizi di IAM sono spesso definiti come *Identity-as-a-Service* (IDaaS) e utilizzano serie di metodiche di autenticazione utente. Tra queste, le principali sono: l'autenticazione a più fattori (MFA) che prevede l'uso di più fattori di autenticazione per verificare l'identità di un utente; il *single sign-on* (SSO) che consente ad un utente di effettuare un'unica autenticazione valida per accedere nonché un luogo centralizzato gestire tutte le applicazioni SaaS a cui ogni utente ha accesso; l'identity provider (IdP) che archivia e gestisce le identità degli utenti tramite la combinazioni di username, password e altri fattori.

Nel complesso, quindi, la crittografia incrementa la sicurezza dei dati e la loro riservatezza, evitando il rischio che i dati possano essere compromessi sia in caso di attacco informatico, sia in caso di tentativo di accesso, fisico o virtuale.

1.3.3 Falso mito #3: Hosting e Cloud computing sono la stessa cosa

Un altro tema su cui si genera spesso confusione è relativo alla differenza tra hosting e cloud computing. Questi due servizi vengono spesso confusi, nonostante tra i due esistano delle fondamentali differenze.

L'**hosting**, in particolare, è un servizio offerto da **un service provider che ospita e fa funzionare i server fisici su cui si appoggiano i sistemi aziendali o degli enti pubblici** (ad esempio i siti web e le applicazioni). I server messi a disposizione dai service provider possono essere dedicati, ovvero di esclusiva pertinenza dell'azienda o dell'ente, o condivisi con altri utenti, ma in entrambi i casi il soggetto che acquista il servizio ha diritto ad una quantità precisa di banda e spazio di archiviazione. Le aziende ed enti possono inoltre decidere se optare per un servizio di **colocation**, che consiste nel posizionare un server di proprietà presso il data center di un service provider.

Il cloud computing, oltre ai servizi di hosting, offre anche risorse (sia hardware che software) on demand e personalizzabili che si possono utilizzare al consumo a seconda delle necessità puntuali dell'utente. **I servizi offerti in cloud sono infatti scalabili sia in aumento che in diminuzione, permettendo agli utilizzatori di poter affrontare anche un picco momentaneo di traffico senza la necessità di dover sottoscrivere servizi aggiuntivi.**

Il cloud computing inoltre, a differenza dell'hosting, è ***un'infrastruttura as a service***, ovvero permette di utilizzare risorse hardware e software senza necessita di acquistarle o svilupparle. Un'altra fondamentale differenza tra cloud e hosting consiste nel fatto che i servizi e le applicazioni offerte dai cloud provider seguono un processo di continua innovazione, crescendo e adattandosi alle esigenze del cliente. Questo è uno dei motivi per cui gli utenti (aziende ed enti pubblici) che si affidano ad un hyperscaler vengono definiti "partner".

Aziende ed enti che utilizzando servizi cloud, in particolare se forniti da operatori di grandi dimensioni, non si limitano a svolgere un ruolo passivo ma divengono coprotagonisti nello sviluppo e nella crescita dell'ecosistema di servizi di cui entra a far parte.

1.3.4 Falso mito #4: una volta scelto un fornitore di servizi cloud è impossibile cambiare

Un altro dei falsi miti che riguardano il cloud computing è relativo al fatto che quest'ultimo generi necessariamente un **effetto lock-in** dei soggetti fruitori nei confronti dei cloud provider. Infatti, sebbene il rischio di rimanere vincolati al proprio fornitore di servizi sia comune a molte soluzioni digitali e sia possibile anche nel caso del cloud computing, ciò non significa che i soggetti che scelgono di utilizzare servizi cloud non possano adottare soluzioni per evitare di rimanere vincolati al proprio fornitore. Uno degli approcci utilizzabili è quello di utilizzare più di un fornitore di servizi cloud.

L'approccio multicloud, pur rappresentando un maggior costo per l'utente, può offrire all'utente la possibilità di non affidare l'intera struttura digitale della propria organizzazione ad un unico soggetto, diminuendo il peso di una singola piattaforma sulle scelte aziendali.

Utilizzando un sistema **multicloud** è possibile utilizzare più ambienti di cloud pubblico o privato, ovvero una combinazione dei due. Nella pratica un utente che decide di utilizzare un approccio di questo tipo può scegliere di affidare la propria infrastruttura IT o porzioni di essa a cloud provider diversi. La possibilità di utilizzare un approccio multicloud si lega ad un altro aspetto da non trascurare, ovvero quello relativo all'utilizzo di **architetture open standard interoperabili che permettono una transizione semplice tra diverse piattaforme cloud.** Uno standard aperto (esempi celebri ne sono i linguaggi XML, SQL e HTML) ha tra le sue principali caratteristiche la possibilità di essere liberamente adottato, implementato e aggiornato. Il paradigma dell'open standard si riferisce infatti ad un formato o protocollo che, oltre ad essere soggetto ad una completa valutazione pubblica, è privo di licenze (in ogni sua componente) e disponibile per chiunque. **Gli standard aperti** sono inoltre, nella maggior parte dei casi, gestiti da una fondazione composta da tutte le parti interessate al progetto. Questo fa sì che si possano **creare e far rispettare regole comuni riguardo aggiornamenti o modifiche** che gli utenti possono apportare. **In questo modo è possibile garantire che lo standard mantenga qualità ed interoperabilità.**

Utilizzare uno standard aperto, o addirittura open source[3], all'interno di un settore come quello del cloud computing, permette quindi

3 Un formato o protocollo open source è creato per essere liberamente disponibile, ovvero ne sono consentite la ridistribuzione e la modifica parte di chiunque. Nella maggior parte dei casi le licenze open source impongono che qualsiasi aggiornamento da parte degli utilizzatori diventi gratuito e aperto alla comunità.

di prevenire eventuali affetti lock-in. Inoltre, l'interoperabilità delle piattaforme cloud fa sì che, nell'ottica di offrire al partner i migliori servizi presenti sul mercato, i provider continuino a creare nuovi servizi e ad aggiornare quelli esistenti al fine di offrire la migliore esperienza di utilizzo possibile.

Case study 2: Epiphany

Fondata a Milano, Italia nel 2017, Epiphany sviluppa soluzioni tecnologiche per i settori bancario e finanziario. Il suo prodotto di punta, la piattaforma aperta Epiphany ONE, fornisce la struttura per una serie di microservizi e applicazioni che modernizzano i sistemi bancari tradizionali in piattaforme bancarie digitali. Le soluzioni includono il pacchetto di conformità Epiphany PSD2, l'applicazione Account Aggregation per la raccolta dei dati, InstaCredit per l'offerta di linee di credito e l'elaborazione dei pagamenti mobili InstaPay.

Quando Epiphany ha concepito la sua rivoluzionaria piattaforma di open banking, aveva bisogno di un ambiente cloud ricco e robusto per crearla e distribuirla. La startup ha scelto il servizio Kubernetes e utilizza servizi cloud aggiuntivi, ottenendo l'agilità e la disponibilità necessarie per far crescere il proprio business e indirizzare le esigenze dei propri clienti bancari. Sono stati così raggiunti tre risultati principali dall'adozione di servizi in Cloud: riduzione dei costi iniziali grazie ad un deployment automatizzato e ad un continuo monitoraggio delle applicazioni containerizzate, fornitura di microservizi innovativi per guidare la trasformazione digitale, supporto alla crescita e massima soddisfazione del cliente, attraverso una rete di datacenter distribuiti in tutto il mondo.

Epiphany ONE fornisce alle organizzazioni un ambiente per testare e distribuire prodotti bancari digitali altamente personalizzati ed esporli come microservizi per l'utilizzo da parte dei clienti. La piattaforma fornisce anche la struttura per una serie di soluzioni verticali, inclusa l'applicazione di conformità Epiphany PSD2 dell'azienda. In quanto pacchetto di conformità pronto per l'uso, l'applicazione è progettata per eliminare l'onere della conformità PSD2 entro due settimane.

Fonte: https://www.ibm.com/case-studies/epiphany-cloud

1.3.5 Falso mito #5: Il passaggio al cloud è un processo lungo e oneroso

Un altro dei falsi miti più comuni riguarda le presunte difficoltà, o presunte tali, riguardo **alla migrazione dell'infrastruttura IT aziendale (o parte di essa) sul cloud**. I cambiamenti tecnologici necessitano sempre di una trasformazione dei processi e un periodo di adattamento e questo è

ovviamente vero anche per quanto riguarda il passaggio al cloud computing. Quello che non trova conferme nella realtà è che il trasferimento possa essere eccessivamente oneroso o portare a un peggioramento dei processi aziendali.

Uno dei timori più comuni è che le applicazioni utilizzate sul cloud possano soffrire di una maggiore **latenza** rispetto a quelle basate su un data center interno. Questo, quando accade, è spesso il risultato di un **errato utilizzo del sistema cloud**, ovvero del tentativo del reparto IT aziendale di eseguire il backhaul dei dati attraverso i data center interni. Il backhauling (l'instradamento del traffico attraverso le reti interne) crea una maggiore latenza, aumenta la complessità del processo e di conseguenza peggiora l'esperienza dell'utente. Questa scelta è spesso dettata dalla volontà di aumentare la sicurezza della rete, protetta già dai sistemi perimetrali offerti dal cloud provider, ma finisce per peggiorarne le prestazioni. Se le aziende smettessero di eseguire il backhaul dei propri dati potrebbero sperimentare, grazie alla scalabilità del cloud, addirittura una minore latenza del cloud rispetto a quella delle reti interne.

Un altro mito non veritiero è che sia necessario **migrare l'intero data center sul cloud** perché il cambio di tecnologia porti dei benefici. Questo passaggio però, oltre a dover essere graduale, non è necessario per sperimentare un aumento dell'efficienza dei processi. Il modo più semplice per le aziende di iniziare il graduale passaggio al cloud computing e goderne appieno i benefici è quello di spostare sulla nuvola tutte le componenti legate ad una singola operation aziendale. **Lo spostamento dell'infrastruttura IT sottostante a un'unica funzione aziendale è un passaggio molto meno complesso rispetto alla migrazione di un intero data center,** quindi comporterà **minori costi ma permetterà all'azienda di sperimentare l'intera gamma di potenziali vantaggi del cloud (**ad esempio un **time-to-market più rapido**, una **maggiore flessibilità** e una **maggiore affidabilità).**

L'ultimo dei falsi miti riguardanti la migrazione al cloud riguarda eventuali problematiche di **compatibilità con le applicazioni aziendali.** Un'erronea convinzione è infatti quella che le uniche due possibilità per migrare le proprie applicazioni sul cloud siano il *lift and shift*, ovvero la virtualizzazione senza apportare modifiche, e la rifattorizzazione completa. Un'applicazione non nata per funzionare sul cloud potrebbe però sperimentare una latenza più elevata o altri problemi di prestazioni. D'altra parte, un refactoring completo dell'applicazione e l'ottimizzazione della sua architettura al cloud aumentano notevolmente il tempo ed i costi della migrazione. **Esistono però tecniche specifiche, come la containerizzazione, che sono di più rapida attuazione e meno**

costose rispetto alla rifattorizzazione[4] completa e consentono comunque alle aziende di ottenere i vantaggi aziendali di una maggiore agilità, un time-to-market più rapido e una maggiore resilienza. La containerizzazione implica l'incapsulamento, o il packaging, del codice software e di tutte le sue dipendenze in modo che possa essere eseguito in modo uniforme e coerente su qualsiasi infrastruttura. Nel metodo classico, quando il codice viene trasferito in una nuova posizione, ad esempio quando uno sviluppatore trasferisce il codice da un computer desktop a una macchina virtuale (VM), possono verificarsi bug o errori. La containerizzazione elimina questo problema raggruppando il codice dell'applicazione insieme ai relativi file di configurazione, librerie e dipendenze necessarie per l'esecuzione. Questo singolo pacchetto viene estratto dal sistema operativo diventando quindi autonomo e portatile, ovvero in grado di funzionare su qualsiasi piattaforma o cloud.

Case study 3: ENEL

ENEL è la principale utility europea nonché uno dei principali operatori integrati di elettricità e gas. Il gruppo opera in 35 Paesi situati in 5 continenti e conta circa 69.000 impiegati e 73 milioni di clienti. Nel 2014, la società, per affrontare le nuove sfide tecnologiche, ha deciso di effettuare un cambiamento radicale spostando la maggior parte delle proprie attività digitali sul cloud pubblico. L'operazione, articolata su un timing di 9 mesi, prevedeva la chiusura nel minor tempo possibile di tutti i contratti di outsourcing e la conseguente migrazione di circa 10.000 server (40 al giorno) sul cloud. La strategia usata da ENEL è stata quella di replicare le applicazioni in-house nel cloud senza riprogettarle e di utilizzare la capacità on-premise per quelle che non potevano essere migrate istantaneamente. A novembre 2018, l'80% dell'infrastruttura aziendale è stato spostato sul cloud con l'obiettivo di raggiungere il 100% entro la fine dell'anno. A seguito della migrazione, ENEL ha raggiunto un risparmio del 60% sui costi di storage e del 20% sui costi computazionali.



Fonte: https://aws.amazon.com/it/solutions/case-studies/enel/

[4] La rifattorizzazione (o *code refactoring*) è un'operazione che prevede la modifica della struttura interna del codice di un software senza modificarne il comportamento esterno

2. IL DIBATTITO INTERNAZIONALE SULLA SOVRANITÀ DIGITALE E SULLE INFRASTRUTTURE DEI DATI

2.1 LA SOVRANITÀ DIGITALE IN EUROPA

2.1.1 Il dibattito europeo tra autonomia strategica e sovranità tecnologica

La pandemia da Covid-19, e le sue implicazioni più ampie che hanno causato conseguenze in quasi tutti i settori dell'economia, hanno evidenziato l'importanza della trasformazione digitale dell'Europa nel garantire il benessere sociale ed economico dei cittadini europei. Questo mutato scenario internazionale ha nuovamente sollevato l'attenzione delle istituzioni europee e degli Stati membri sui temi della "**sovranità tecnologica**". Anche se già con il cambio al vertice della Commissione Europea, guidata da Ursula von der Leyen, anche sulla base di importanti prese di posizione dei principali leader europei, aveva acquisito un'evidente centralità nel dibattito il concetto di **autonomia strategica dell'Unione**, rispetto in particolare alle superpotenze economiche quali Stati Uniti e Cina e ai loro colossi tecnologici.

Riconoscendo i propri gap sia in termini di investimenti economici che di capacità e conoscenze[5], la Commissione ha evidenziato come ad oggi le pubbliche amministrazioni e le aziende UE facciano in gran parte affidamento su servizi e infrastrutture extra-europee, impattando sulla possibilità dell'Unione di sviluppare infrastrutture digitali autonome ed esponendo i cittadini al trattamento e utilizzo dei propri dati da parte di Paesi stranieri in cui non vi sono garanzie di controllo e sicurezza. La Commissione riporta infatti la preoccupazione per gli investimenti nel settore delle infrastrutture digitali, che risultano essere ancora troppo esigui e, soprattutto, frammentati, causando una adozione insufficiente delle nuove tecnologie sia nel settore privato che in quello pubblico. Vi sono pertanto **esigenze di investimenti aggiuntivi nella trasformazione digitale che, secondo le stime della Commissione, ammontano a un totale di 125 miliardi di euro all'anno**.

Per quanto concerne il dibattito in corso, si osserva come, sebbene il concetto di sovranità tecnologica e digitale sia diventato uno dei principali temi di dibattito in materia di policy del digitale, non c'è una definizione chiara di cosa significhi effettivamente in termini di normative e scelte strategiche, e altresì non vi è specificazione se i concetti di sovranità digitale e sovranità tecnologica siano necessariamente concetti interscambiabili e dal medesimo significato.

[5] Esposti nel documento "*Identifying Europe's recovery needs*" pubblicato il 27 maggio 2020 dalla Commissione UE.

La Cancelleria Federale tedesca, ad esempio, riporta che "*la sovranità digitale descrive la capacità di indirizzare i processi di trasformazione digitale in modo autodeterminato per quanto riguarda l'hardware, il software, i servizi e le competenze. **Essere digitalmente sovrani non significa ricorrere a misure protezionistiche o fare tutto da soli. Essere digitalmente sovrani significa, nel quadro del diritto applicabile, prendere decisioni sovrane sui settori in cui l'indipendenza è desiderata o necessaria***". Secondo questa visione, i lavori della Commissione si basano sull'idea largamente diffusa che il successo economico dell'Unione e degli Stati membri non possa provenire da scelte che intendono rendere l'Europa indipendente dagli sviluppi tecnologici all'estero, ma piuttosto da politiche mirate al **rendere l'UE competitiva e pronta al dialogo con le potenze economiche mondiali attraverso i propri strumenti, le proprie competenze, ma anche con collaborazioni internazionali**. L'attenzione e il lavoro della Commissione si è infatti incentrato su settori strategici, come l'intelligenza artificiale e l'e-commerce, e sui settori ad alto rischio, come la sicurezza cibernetica e la gestione di dati sensibili attraverso strutture di cloud computing.

Il dibattito europeo si focalizza fortemente anche sul concetto di "**autonomia**", promosso pubblicamente da Jean-Claude Juncker, Presidente della Commissione Europea 2014-2019, che già nel 2018 sottolineava **l'importanza di maggiori investimenti in innovazione e tecnologie per garantire alla UE una maggiore competitività internazionale.** In questo senso, anche l'attuale Commissione riconosce nel concetto di autonomia europea l'esigenza di poter autodeterminare il proprio futuro nei settori in questione attraverso scelte politiche ed economiche stabilite dai processi decisionali portati avanti nelle istituzioni dell'Unione. L'attenzione, in particolare, è volta ad evitare che questi possano invece essere determinati da influenze politiche ed economiche provenienti dai concorrenti globali e, al contempo, si intende invertire la tendenza che vede l'Europa e gli Stati membri costretti a dover ricorrere a tecnologie e conoscenze estere per mancanza di investimenti e competenze all'interno della UE.

Di conseguenza, la ricerca dell'autonomia strategica in questi campi implica per l'Unione la ricerca di nuovi equilibri economici, normativi e culturali, mirati a migliorare la sovranità tecnologica e, al contempo, a promuovere **la crescita economica, lo sviluppo e l'apertura nei campi dell'innovazione e del digitale nell'ottica del mercato unico e di un nuovo framework legislativo che garantisca un mercato equo, sicuro e normato.** Il rafforzamento della competitività della UE nei

confronti degli attori dominanti nel mercato digitale, in particolare Stati Uniti e Cina, punta inoltre a consolidare la posizione dell'Unione sullo scenario internazionale, favorendo una maggiore integrazione dei mercati e degli strumenti legislativi quantomeno con i partner dell'area OECD e dell'alleanza transatlantica.

Contestualizzando il discorso in termini di mercato, si osserva come il comparto mondiale delle nuove tecnologie digitali dovrebbe raggiungere i 2,2 trilioni di euro entro il 2025, mostrando come l'Europa abbia forti interessi nel partecipare rafforzando la propria posizione e allo stesso tempo la propria collaborazione con gli altri principali attori internazionali. Questo è particolarmente vero per gli accordi con gli **Stati Uniti** che, oltre ad essere leader nel settore tecnologico, **formano con l'UE il partenariato economico più forte del mondo**. Gli Stati Uniti e l'UE sono infatti il primo partner commerciale e il primo investitore nell'economia reale l'uno rispetto all'altro. Inoltre, le aziende statunitensi sono attori chiave dell'economia europea, creando milioni di posti di lavoro, e viceversa. **Questo è particolarmente vero nell'economia digitale, dove gli Stati Uniti e l'UE rappresentano i rispettivi principali importatori di tecnologie abilitati e servizi digitali**. Nello specifico, gli Stati Uniti hanno esportato **$213 miliardi** di servizi nei settori della tecnologia, dell'informazione e della comunicazione (ICT), nell'UE nel 2018 e, a loro volta, hanno importato beni e servizi digitali per un valore complessivo di $120 miliardi. Per quel che riguarda nello specifico i servizi **ICT**, **le società statunitensi hanno fornito**

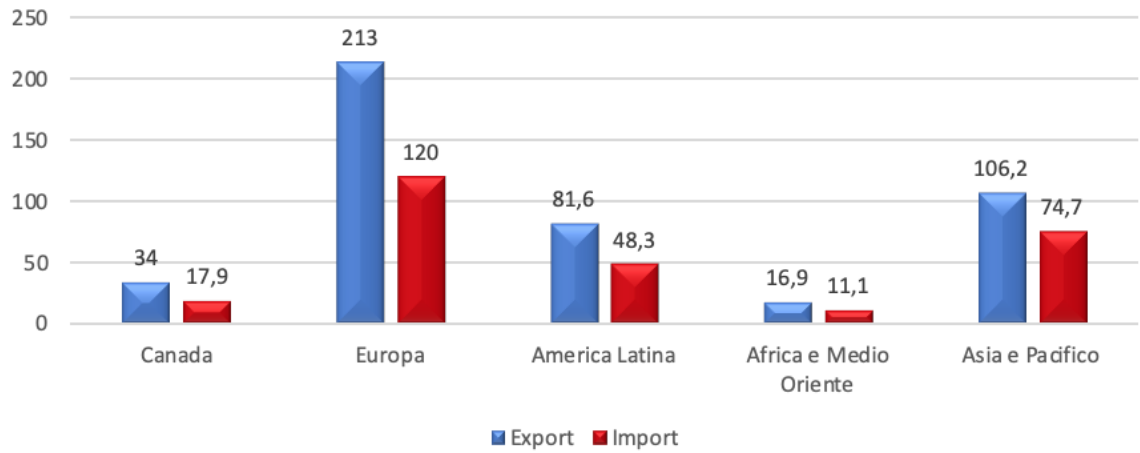


FIGURA 2.1 Mercato dei servizi digitali, USA (2018, miliardi $)

Fonte: Camera di Commercio USA

$175 miliardi attraverso aziende affiliate situate in Europa, mentre hanno fornito solo $3 miliardi di beni in Cina e $21 miliardi in America Latina. Non sorprende che, sul totale degli investimenti americani all'estero nel settore dell'informazione, il 73% di essi fosse indirizzato in Europa (2018).

Anche alla luce di questi dati, la Commissione europea riconosce che gran parte del potenziale di crescita dell'Europa risiede nei mercati digitali e nella possibilità di competervi ad armi pari. In relazione al rafforzamento della propria posizione nello scacchiere globale, l'UE ha pertanto messo in atto diversi strumenti per ridurre il divario in termini di investimenti con gli altri attori internazionali. Ad esempio, **Horizon Europe**, il programma quadro UE per la Ricerca & Innovazione per il periodo 2021-2027, prevede l'investimento di 95,5 miliardi di euro di finanziamenti pubblici, consentendo tra l'altro investimenti sulle tecnologie digitali strategiche come la nanoelettronica, fotonica, robotica, 5G, calcolo ad alte prestazioni, big data, cloud computing, e AI. Ai fondi per la ricerca si aggiungono i 7,5 miliardi di euro del programma **Digital Europe**, che finanzieranno nello stesso arco di tempo le tecnologie digitali (in particolare HPC, AI e cybersecurity). Un ulteriore, decisivo, rafforzamento delle infrastrutture digitali in Europa sarà consentito anche con le risorse del **NextGenerationEU**, il fondo per la ripresa costituito da 750 miliardi per il quale la Commissione europea ha previsto che almeno il 20% degli investimenti vadano a finanziare la transizione digitale.

2.1.2 La sovranità dei dati e il cloud computing

In questo contesto, sempre maggior rilievo è stato assunto dal controllo e dall'utilizzo dei dati personali, mettendo la fornitura dei servizi di cloud computing e la sovranità dei dati ai primi posti tra i temi del dibattito sulla sovranità digitale.

Nello specifico, per **sovranità dei dati** si intende generalmente **l'autonomia di un fornitore di dati**, sia esso un individuo o un'entità, nel **prendere decisioni indipendenti su chi accede, elabora o usa i dati propri (o dei propri clienti), avendo la capacità e i mezzi per muoversi nel digital data market in maniera autodeterminata e ben informata.**[6]

Il mercato dei dati è particolarmente strategico per due ordini di ragioni: da un lato per la tutela delle informazioni riservate a

[6] Definizione tratta dal documento "*German EU Council Presidency digital sovereignty*" redatto da Erste Lesung per la Cancelleria Tedesca https://erstelesung.de/wp-content/uploads/2020/10/20-10-14_Germany_EU_Digital-Sovereignty.pdf

livello di **sicurezza nazionale** dei singoli Stati, e per la tutela delle infrastrutture critiche; dall'altro, perché tale mercato apre **nuove opportunità di crescita economica**, sia per le grandi imprese, sia per le PMI, consentendo lo sviluppo di applicazioni di IA che possono incrementare produttività ed efficienza in numerosi ambiti della società, dalla gestione ottimizzata di reti e infrastrutture, e quindi alla lotta contro il cambiamento climatico, alla manifattura, alla finanza, fino al settore sanitario.

Negli ultimi mesi, a seguito dell'emergenza da Covid-19, gli Stati membri hanno assistito a un aumento consistente di cyber-attacchi da parte di molteplici fonti. Questi hanno provato a sfruttare le lacune causate dall'improvvisa e brusca accelerazione digitale causata dalla pandemia, nonché dalla mancanza di preparazione digitale di milioni di persone che sono state improvvisamente costrette ad effettuare attività quotidiane in modalità telematica, finendo per esporsi a minacce e violazioni di privacy. La sicurezza della tecnologia si sta infatti affermando come un argomento critico e centrale per uno sviluppo in sicurezza della rivoluzione digitale e dell'economia dei dati. La Commissione Europea riporta quindi la necessità di rafforzare le sinergie tra i fornitori di rete e le istituzioni di regolamentazione, in modo da tutelare tanto gli utenti quanto gli Stati membri e la sicurezza nazionale di questi.

Per quanto concerne il **mercato dei servizi dati**, si osserva come questo sia continua espansione, con previsioni per un valore complessivo della domanda aggregata di oltre 100 miliardi di dollari entro il 2025, mentre diversi indicatori evidenziano come l'UE sia in ritardo nella corsa globale per le nuove

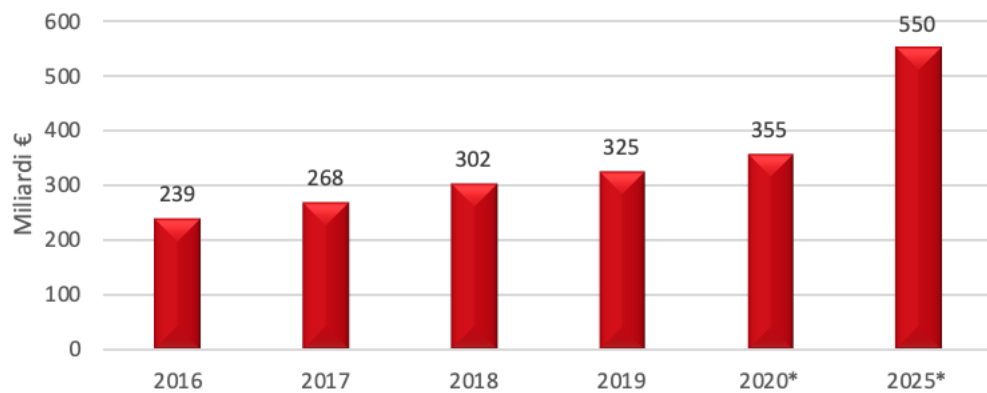


FIGURA 2.2 Valore complessivo della data economy (EU-27)

*Stima
Fonte: IDC European Data Market Monitoring Tool, 2020

tecnologie, le infrastrutture legate ai servizi digitali e l'intelligenza artificiale. Secondo le stime Digital Economy Compass (2019), nel 2020 lo storage di dati in infrastrutture cloud dovrebbe superare lo storage dei dispositivi fisici, diventando la soluzione principale di stoccaggio dei dati in tutto il mondo. Ad oggi i dati del IDC European Data Market Monitoring Tool (2020), che misura l'impatto delle attività portate avanti nel mercato europeo sull'intero sistema economico, riportano un valore complessivo[7] della data economy che supera la soglia dei € 350 miliardi per i paesi EU-27 (2020), segnando una crescita del 9,2% rispetto all'anno precedente. Si prevede un tasso di crescita del mercato in ulteriore espansione nei prossimi anni, con una scenario baseline della UE che prevede il raggiungimento di un valore complessivo di €550 miliardi per i paesi EU-27 nel 2025.

Nel tentativo di tutelare le proprie informazioni strategiche e contemporaneamente sfruttare al meglio le opportunità derivanti dall'economia dei dati, diversi Stati Membri hanno iniziato a sviluppare strategie indipendenti di autonomia digitale, con l'obiettivo di contrastare l'attuale tendenza per la quale imprese e amministrazioni pubbliche europee utilizzano da servizi cloud forniti da operatori extra-europei, in particolare statunitensi o cinesi. Tuttavia, tali tentativi di creazione di infrastrutture cloud nazionali non sempre hanno raggiunto gli obiettivi prefissati (come mostrato dal caso francese, cfr. paragrafo 2.3.1.1).

Un approccio diverso è stato ideato in Germania, e recentemente portato dalla Commissione europea all'attenzione degli Stati membri: il Progetto cloud **"Gaia-X", un'infrastruttura di dati federata e trasversale nella UE che consentirebbe all'Unione di garantire determinati standard di privacy e sicurezza e, al contempo, di sfruttare al meglio le opportunità economiche derivanti dal mercato dei dati.** Come descritto con un maggiore grado di approfondimento nel paragrafo ed esso dedicato, l'obiettivo del progetto non è di creare un cloud europeo alternativo ai colossi statunitensi e asiatici, bensì di garantire la nascita di una piattaforma basata su sistemi di interoperabilità e standard di sicurezza in modo da promuovere un ecosistema digitale aperto e trasparente, in cui dati e servizi possono essere resi disponibili, raccolti e condivisi in un ambiente di fiducia. Al fine di promuovere parità di condizioni per tutti coloro che accettano questi principi comuni, e per evitare di scontrarsi con questioni geopolitiche riguardanti barriere di mercato e

[7] Il valore complessivo della data economy include anche tutte le attività parallele e i processi intermedi.

protezionismo, l'adesione all'Ecosistema Gaia-X è consentita anche ad aziende extra-europee che decidono di accettare e sottoscrivere gli standard e i valori dell'UE.

2.1.3 Le priorità digitali dell'attuale Commissione e delle altre istituzioni UE

Il Covid-19 ha evidenziato con ulteriore chiarezza l'impatto che beni e servizi digitali hanno nella vita di tutti i cittadini, dimostrando l'importanza di investimenti che possano aiutare la UE ad affrontare una transizione digitale verso un'economia digitale prospera, sicura e sostenibile. Come descritto precedentemente, l'attuale Commissione ha fatto dell'azione nei campi del digitale e dell'innovazione una propria priorità, affrontando il tema tanto da un punto di vista economico, quanto dai punti di vista culturali e normativi. La Commissione intende infatti favorire un ecosistema in cui aziende e cittadini siano protagonisti attivi del mercato digitale, usufruendo dei beni, dei servizi, e delle opportunità da esso derivanti in modo sicuro e protetto, con la necessità di trovare un equilibrio, all'interno di una cornice etica e valoriale, tra la protezione dei cittadini in merito alla privacy e al trattamento dei dati e lo sviluppo di strumenti innovativi capaci di incrementare efficienza, tecnologia, e benessere per la cittadinanza. Parallelamente, si sta lavorando infatti a politiche che possano generare la formazione e consapevolezza tra i cittadini dell'Unione in modo da rafforzare e uniformare le competenze lavorative e regolamentari, e per innescare fiducia nei consumatori affinché si sentano sicuri, informati e protetti.

Il 2020 è stato inoltre caratterizzato dal già citato impegno dell'UE sul fronte dell'economia dei dati. L'attuale Commissione è particolarmente intenta ad affrontare i temi legati alla proprietà di dati sensibili e alla gestione di questi all'interno dell'Ue in modo da sopperire all'esposizione a possibili violazioni di privacy derivanti dall'uso da parte di cloud provider extra-europei.

Oltre all'impegno verso la realizzazione del cloud federale europeo nella cornice del progetto Gaia X, è stata firmata una dichiarazione congiunta che promuove la nascita di un *EU Cloud Rulebook* per favorire un quadro normativo che uniformi specificità tecniche e requisiti di sicurezza. L'Alleanza europea per i Dati Industriali e il Cloud, nata a dicembre 2020 e composta da rappresentanti degli Stati membri, fornitori di cloud computing e utenti industriali del cloud, dovrebbe guidare l'implementazione del cloud pan-europeo con un budget fino a dieci miliardi di euro.

Dal punto di vista normativo, il lavoro della Commissione segue i principi del GDPR, il regolamento approvato nel 2016 che fornisce un quadro molto rigoroso per la privacy e la

protezione dei dati. Ad esso si sono poi aggiunti due ulteriori importanti interventi legislativi quali il regolamento sulla libera circolazione di dati non personali (Reg. 2018/1807) e la direttiva Open Data (Dir. 2019/1024).

Per garantire un approccio omogeneo e coerente, la Commissione von der Leyen ha già stabilito una serie di azioni rilevanti sul tema, in particolare la Strategia Europea per i dati, che rappresenta uno dei progetti più importanti e significativi dei prossimi anni. L'agenda di lavoro di quest'ultima, di cui una prima importante tappa è stata la proposta di Data Governance Act del novembre 2020, è stato delineato con la pubblicazione nel febbraio 2020 della comunicazione *"A European strategy for data"*, accompagnata dalla comunicazione *"Shaping Europe's digital future"* e dal libro bianco *"Artificial Intelligence: a European Approach to excellence and trust"*. Infine, per rafforzare il mercato unico dei servizi digitali e promuovere l'innovazione e la competitività dell'ambiente online europeo, il 15 dicembre 2020 sono stati pubblicati il Digital Services Act (n. 361/2020) e il Digital Markets Act (DMA).

Un'altra priorità delle istituzioni UE riguarda la **sicurezza informatica**. Come per i servizi cloud, anche l'affidamento alle infrastrutture di 5G extra-europee, ed in particolare asiatiche, è stato identificato come un elemento critico di debolezza per l'Unione. La mancanza di un cyberspazio europeo unificato e normato espone infatti a possibili rischi tanto i cittadini quanto le istituzioni nazionali degli Stati membri che fanno uso di queste reti per attività sensibili e riservate. Già con la c.d. "direttiva NIS" (Network Information Society) del 2016 erano state poste delle prime basi per la cooperazione europea sul tema e su possibili misure da imporre su compagnie e aziende per evitare attacchi cibernetici nei settori chiave come l'energia, la sicurezza nazionale, il mercato finanziario e il sistema di trasporti. La direttiva obbligava infatti gli Stati membri ad adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, stabilendo obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali. La direttiva NIS, all'art. 23, prevede un riesame periodico da parte della Commissione circa il funzionamento della stessa e fissa al 9 maggio 2021 la formulazione della prima relazione a Parlamento europeo e Consiglio. A tal fine, nel corso del 2020 la Commissione ha lanciato una consultazione pubblica propedeutica alla proposta di c.d. "direttiva NIS2", pubblicata a metà dicembre. Il quadro che è emerso fotografa ancora una forte disuguaglianza ed inefficienza degli strumenti di sicurezza informatica di cui si sono dotati gli Stati membri in relazione a quanto disposto dalla Direttiva e, conseguentemente, la necessità

di ridurre la frammentazione normativa per favorire la creazione di condizioni di parità indispensabili per l'ulteriore sviluppo del mercato unico.

Sempre in materia di cybersecurity, alla direttiva è seguito lo European Cybersecurity Act (2018) che ha dato vita al primo sistema europeo di certificazioni da parte dell'ENISA per i prodotti ICT sui possibili rischi derivanti da attacchi cibernetici. Con la raccomandazione n. 2019/534, la Commissione ha poi individuato una roadmap chiara e stringente secondo cui gli Stati membri devono valutare i rischi, aggiornare i requisiti di sicurezza e i metodi di gestione dei rischi applicati alle reti 5G e aggiornare i pertinenti obblighi imposti alle imprese che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico.

Il 29 gennaio 2020 è stata infine pubblicato dalla Commissione e dal gruppo di cooperazione NIS il pacchetto di strumenti dell'UE (Toolbox sul 5G) comprendente misure di attenuazione dei rischi e proposte di misure strategiche e tecniche. Il documento, in particolare, fa il punto su alcuni dei settori rispetto ai quali il 5G opererà quale fattore abilitante una serie di importanti applicazioni e, nello specifico, e-health, reti energetiche intelligenti, fabbriche del futuro, media ed intrattenimento e mobilità. L'obiettivo dichiarato dal documento è identificare un possibile insieme comune di misure in grado di mitigare i principali rischi per la sicurezza informatica delle reti 5G e fornire una guida per la selezione delle misure da adottare al fine di creare un solido quadro di misure che garantisca un adeguato livello di sicurezza informatica delle reti 5G in tutta l'UE ed un approccio coordinato tra gli Stati membri.

2.2 LA EUROPEAN DATA STRATEGY

Negli ultimi anni, la governance dell'Unione Europea ha dimostrato grande consapevolezza sugli sviluppi e le opportunità derivanti dalle attività economiche che dipendono fortemente dall'uso, dall'elaborazione, e dalla condivisione di dati e informazioni. L'impatto di tali attività è destinato ad incrementare ulteriormente nei prossimi anni, con un conseguenze sempre maggiore nell'economia degli Stati membri e nei livelli occupazionali.

Per rafforzare la presenza europea in una società globalizzata basata sulla condivisione e l'elaborazione di dati in sicurezza, la Commissione Europea nel febbraio 2020 ha pubblicato la comunicazione ***"A European strategy for data"***, delineando il piano per far diventare l'Unione leader nella data economy. La strategia si fonda sui tre principali atti legislativi che attualmente costituiscono il

quadro normativo in materia di trattamento di dati: il GDPR, ovvero il regolamento generale sulla protezione dei dati (Reg. 2016/679), il regolamento sulla libera circolazione di dati non personali (Reg. 2018/1807) e la direttiva *Open Data* (Dir. 2019/1024).

La comunicazione presenta le policy e gli investimenti necessari per fare della UE la data economy più attraente, sicura e dinamica del mondo, sfruttando le potenzialità dei dati per migliorare ed efficientare i processi decisionali e la vita di cittadini e imprese.[8] La strategia si sviluppa su quattro pilastri all'interno dei quali sono delineati alcuni interventi chiave.

Il **primo** pilastro riguarda la **creazione di un quadro di governance intersettoriale sui temi dell'accesso e dell'utilizzo dei dati**, e come interventi prevede: a) un nuovo impianto normativo per uniformare i parametri di accesso e utilizzo dei dati e per regolare la governance dei data spaces comuni, b) l'adozione di una norma sui data set di alto valore in conformità con la Direttiva Open Data, in modo da renderli accessibili gratuitamente in tutta l'Unione e standardizzati secondo le caratteristiche delle *Application Programming Interfaces* (APIs); c) l'adozione del *Data Act*; d) la revisione degli interventi di policy previsti nell'ambito del Digital Service Act.

Il **secondo** pilastro della Strategia riguarda **nuovi investimenti in digital enablers**, ovvero i fattori abilitanti che consentano un'accelerazione nei processi di trasformazione digitale e un rafforzamento delle capacità delle infrastrutture europee in termini di **data hosting, di elaborazione e di interoperabilità.** Gli interventi chiave in questo ambito sono: a) investimenti in progetti High Impact sui **data space europei**; b) la sottoscrizione da parte degli stati membri di un Memorandum d'Intesa per la nascita di una **Federazione Cloud europea**; c) il lancio di un **mercato di servizi cloud europeo** che integri anche tutti i servizi già esistenti; d) la creazione di un **Cloud Rulebook**.

Il **terzo** pilastro della Strategia riguarda il rafforzamento delle competenze e gli investimenti in formazione e competenze per

[8] Per il raggiungimento di questi obiettivi, la Commissione sottolinea la necessità di superare diverse criticità: **a)** maggiore accessibilità di dati, ad oggi ancora insufficiente e limitante per processi efficienti di condivisione di dati a livelli di *business-to-business* (B2B), di *Government-to-business* (G2B) e di *business-to-Government* (B2G); **b)** squilibri nel potere di mercato per la fornitura di servizi digitali; **c)** interoperabilità e qualità dei dati; **d)** governance dei dati; **e)** infrastrutture e tecnologie dei dati; **f)** rafforzamento delle competenze e della conoscenza dei propri diritti da parte dei cittadini; **g)** skills e competenze; **h)** cybersecurity.

cittadini e PMI, in modo da dare ai cittadini maggiore controllo sull'accesso e l'utilizzo di dati[9].

Infine, il **quarto** pilastro concerne la **nascita di data space**, ovvero gli "spazi" comuni europei di dati, per i settori strategici e di pubblico interesse. Tra i settori economici in cui la Commissione intende investire, tramite la creazione di queste infrastrutture, sono presenti la filiera manufatturiera, il Green Deal, la mobilità, la salute, la finanza, l'energia, l'agricoltura e la PA. L'obiettivo è creare un framework comune che consenta di quantificare i flussi di dati in questi campi, stimandone il valore economico.

Per rafforzare il mercato unico dei servizi digitali e promuovere l'innovazione e la competitività dell'ambiente online europeo, il 15 dicembre 2020 è stata pubblicata la proposta di regolamento della Commissione per l'adozione del DSA, il **Digital Services Act (n. 361/2020)**[10]. Si tratta di un intervento dalla rilevanza straordinaria con il quale la Commissione, come già evidenziato, intende offrire una risposta normativa agli enormi cambiamenti nell'economia e nella società, cui si accompagnano non solo grandi opportunità ma anche nuovi rischi e criticità.[11]

La scelta di favorire la massima armonizzazione con la normativa esistente, e quindi un'applicabilità più rapida, ha guidato la decisione di includere le disposizioni della direttiva e-commerce che rimarranno in vigore all'interno di un regolamento che non lascia discrezionalità agli Stati membri, essendo un atto immediatamente applicabile che non richiede alcun tipo di attività di recepimento nei singoli ordinamenti nazionali.

Nello specifico, la proposta, articolata in cinque capitoli, introduce un quadro orizzontale per tutte le categorie di contenuti, prodotti, servizi e attività sui servizi di intermediazione nel quale però viene delineato un regime di responsabilità diversificato in base ai servizi offerti ed alla dimensione del fornitore (es. alcuni obblighi sono limitati solo a piattaforme online molto grandi, che per la loro portata hanno acquisito un ruolo centrale e sistemico). La stessa proposta pone a carico degli Stati

[9] Possibilmente incluso del Data Act del 2021.

[10] Previsto nel secondo pilastro della comunicazione ufficiale *"Shaping Europe's digital future"*.

[11] A tale cambio di paradigma la Commissione ha risposto con l'adozione di un atto che va a modificare - pur mantenendone saldi i principi chiave - la direttiva e-commerce adottata nel 2000 al fine di garantire le migliori condizioni per la fornitura di servizi digitali innovativi nel mercato interno, contribuire alla sicurezza online e alla protezione di diritti fondamentali (in particolare la libertà di espressione ed informazione), e stabilire un modello di governance solido e duraturo per la supervisione dei fornitori di servizi di intermediazione.

membri specifici obblighi di verifica della compliance di tali soggetti operanti nei rispettivi territori rispetto alle previsioni contenute nel regolamento proposto anche istituendo nuovi soggetti (Coordinatori per i Servizi Digitali) e definisce meccanismi di enforcement e cooperazione tra gli Stati.

Insieme al Digital Services Act, la proposta di **Digital Markets Act** (DMA) è uno degli elementi centrali della strategia digitale europea. Anch'esso pubblicato lo scorso 15 dicembre, è frutto di un'ampia consultazione pubblica lanciata il 2 giugno e conclusa l'8 settembre nell'ambito della quale è emersa una diffusa consapevolezza circa l'esistenza di problematiche strutturali non risolvibili con l'attuale quadro normativo e la necessità di intervenire con dei correttivi tutte le volte in cui nel mercato si trovi a operare un gatekeeper. Per quanto attiene la posizione espressa dalle piattaforme, sono emerse opinioni contrastanti hanno visto da un lato la maggior parte delle grandi piattaforme interrogarsi circa l'effettiva necessità di introdurre nuovi strumenti e, dall'altro, molte piattaforme di piccole e medie dimensioni, in particolare quelle che si interfacciano con piattaforme di dimensioni maggiori, che hanno espresso il loro sostegno per l'iniziativa evidenziando, in molti casi, l'importanza di introdurre adempimenti di tipo procedurale piuttosto che comportamentale.

La proposta di regolamento sui mercati digitali, partendo dalla constatazione dell'importanza sempre crescente dei servizi digitali per lo svolgimento delle quotidiane attività e del loro straordinario contributo in termini di incremento delle opportunità di scelta per i consumatori, e della presenza nel mercato di un esiguo numero di grandi piattaforme con una quota di mercato estremamente significativa, stabilisce una serie di criteri oggettivi strettamente definiti per qualificare le grandi piattaforme online come gatekeeper. Applicando un approccio ex ante, vengono quindi introdotti una serie di obblighi e divieti in capo a tali soggetti.

La normativa proposta è rivolta, dunque, unicamente a quelle piattaforme che, forti del ruolo di gateway o gatekeeper tra utenti business e utenti finali, e godendo di una posizione consolidata nel mercato, si trovano nella possibilità di fare usi impropri dei dati degli utenti. La Commissione punta quindi a contrastare il rischio di potenziali rafforzamenti delle barriere all'ingresso in un mercato già di per sé ristretto, e di comportamenti scorretti nei confronti degli utenti commerciali e degli utenti finali.

Al pari del DSA, la Commissione ha proposto lo strumento del regolamento nella logica di assicurare la massima armonizzazione nel mercato interno. L'ambito applicativo di tale regolamento è concentrato sui "*core platform*

services", intendendo con tale espressione servizi di intermediazione online, motori di ricerca online, social network, piattaforme di condivisione di video, servizi di comunicazione interpersonale indipendente dal numero, sistemi operativi, servizi di cloud computing e servizi pubblicitari, comprese eventuali reti pubblicitarie, scambi di pubblicità e qualsiasi altro servizio di intermediazione pubblicitaria.

2.3 PROGETTI DI CLOUD A LIVELLO EUROPEO

2.3.1 Casi nazionali

2.3.1.1 Esperienze di cloud di Stato in Francia

Nel 2009, la Francia è stata una delle prime nazioni dell'Unione Europea ad avviare il percorso verso la creazione di un "cloud sovrano" operante attraverso datacenter ubicati sul suolo nazionale. Il primo progetto concreto è stato ***Andromède***, originariamente previsto per il 2011 e nato con lo scopo di fornire un cloud nazionale per il settore pubblico e le imprese, evitando che soggetti esterni potessero accedere ai dati strategici della pubblica amministrazione francese e di società francesi ed europee. In particolare, l'intento consisteva nel "*progettare, costruire e gestire l'infrastruttura di una 'centrale digitale', con vocazione europea, a servizio delle società francesi e della competitività economica*", gestito attraverso un partenariato pubblico-privato che avesse lo Stato in qualità di azionista di maggioranza, e parallelamente coinvolgesse i principali operatori tlc e Ict francesi, cui dovevano essere affidate le responsabilità relative alla sicurezza, all'affidabilità e alla gestione dei dati e dei sistemi. A tal fine, il cloud "sovrano" avrebbe dovuto essere realizzato in partnership tra le autorità nazionali e gli operatori Orange (ovvero l'ex-incumbent France Télécom), Thales e Dassault Systèmes, cui dovevano essere affidate anche responsabilità di gestione. Tuttavia, a seguito di un disaccordo tra due degli operatori, il progetto iniziale è stato abbandonato nel 2012.

Il progetto di "cloud sovrano" è stato quindi rimodulato per favorire la nascita di due nuovi soggetti: **Cloudwatt**, gestito da Orange e Thales; e **Numergy**, capeggiato da SFR e Bull, operatore che ha preso il posto di Dassault Systèmes. Le due società sono state sviluppate con strutture finanziarie simili: un grande operatore privato come socio di maggioranza (Orange con il 44,4% di Cloudwatt e SFR con il 47% di Numergy), finanziamenti statali di €75 milioni ciascuna tramite la Cassa dei Depositi (Caisse des Dépôts) per il 33% del capitale, ed un'azienda specializzata in sicurezza in qualità di socio

minoritario (Thales 22,2% per Cloudwatt e Bull per il 20% a Numergy).

A seguito di iniziali difficoltà finanziarie, le due aziende hanno subìto nuove modifiche nell'assetto azionario. Nel 2015 Orange ha rilevato le quote di Thales e Caisse des Dépôts diventando socio unico al 100% e trasformando Cloudwatt in un servizio cloud IaaS (*Infrastructure as a Service*). Pur continuando a far leva sullo slogan di Cloud Sovrano e contando su due data center ubicati sul suolo nazionale, **i servizi offerti da Cloudwat4t sono ora rivolti sia alla pubblica amministrazione che alle aziende private, con tariffe "*pay per use*" analoghe ad altri servizi cloud del settore privato**. Dopo due anni di attività il progetto aveva generato solo sei milioni di euro di ricavi, suscitando critiche e portando all'incertezza finanziaria. La situazione si è aggravata fino ad arrivare all'interruzione di tutti i servizi il 1° febbraio 2020, accompagnata dalla **cancellazione di tutti i dati dei clienti**.

Nel 2016, anche Numergy ha visto l'uscita dei soggetti pubblici, con l'acquisto della totalità delle quote di Caisse des Dépôts e Atos da parte di SFR, diventando a tutti gli effetti un offerta cloud IaaS gestita quindi da un singolo operatore privato (anch'essa rivolta a imprese ed enti pubblici).

A livello nazionale, nel 2012 è invece stato lanciato il progetto RIE (*Réseau interministériel de l'état*) per le PA, con lo scopo di razionalizzare le varie reti in un'unica infrastruttura capace di collegare amministrazioni centrali e locali. Secondo il *rapport d'activité* RIE 2017, il perimetro della rete di trasporto è arrivato a collegare più di 11.500 siti e 18 entità ministeriali, che rappresentano oltre 450.000 utilizzatori (0,67% della popolazione nazionale).

Una terza iniziativa consisteva nel lancio di una piattaforma di e-Government all'interno del portale Service-Public.fr (2013) finalizzata all'offerta di servizi ai cittadini (relativi a tassazione, identità, procedure lavorative, ecc.) e alla fornitura di servizi cloud interministeriali in modalità IaaS, PaaS (e SaaS tra ministeri). Il portale è stato poi inserito nel più ampio progetto "*Service Public 2016*", ideato per offrire agli utenti un unico punto di accesso per informazioni, orientamento e servizi online. Parallelamente, nel 2014 è stata sviluppata la piattaforma di Cloud interministeriale, incaricata di fornire IaaS e PaaS per ministeri e amministrazione centrale utilizzando architetture ibride, utilizzando Cloud privato operato da terzi per i dati sensibili e Cloud pubblico per sviluppi web e open data.

Con uno scenario che ancora fatica a riprendersi dal fallimento del progetto Andromède di Cloud nazionale sovrano, la posizione che il Governo nazionale vuole intraprendere sul tema appare ancora in

divenire. Bruno Le Mairre, Ministro dell'economia e delle finanze, sembra insistere su una forma di cloud a carattere nazionale ma con tratti differenti, in modo da non ricadere negli errori commessi in precedenza. L'obiettivo sembra essere la conclusione di un accordo strategico tra lo Stato francese e le due società francesi, OVH e Oodrive, in veste di ISP, per la creazione di un nuovo ecosistema cloud nazionale. **Il Ministro ha però sottolineato che i provider verranno selezionati non solo in base alla nazionalità, ma soprattutto in base alla capacità di garantire integrità dei dati e autonomia strategica.**[12] L'operazione, inoltre, si svilupperà sull'asse franco-tedesco, prefigurando una collaborazione prima bilaterale e poi europea sul progetto, in un'ottica che segue gli sviluppi del cloud federale, Gaia-X (cfr. paragrafo 2.3.2).

2.3.1.2 G-Cloud initiative e Data Classification strategy nel Regno Unito

In termini di iniziative adottate dagli Stati europei in materia di cloud computing, un altro caso interessante è quello del Regno Unito. Già nel 2012 era stato avviato il Programma "**G-Cloud**", iniziativa finalizzata a diffondere l'utilizzo del cloud nel settore pubblico e ad agevolare l'acquisto dei servizi attraverso accordi con i cloud provider e la messa a disposizione degli stessi tramite piattaforme aperte e pubbliche.

A livello organizzativo, il progetto è basato su diversi pilastri. Il primo riguarda una serie di accordi quadro con i provider, grazie ai quali le PA possono selezionare i servizi richiesti e concludere accordi di fornitura senza dover completare l'intero iter relativo all'assegnazione di appalti tramite bando pubblico. Rispetto all'iniziativa francese si osserva come **alcuni tra i principali fornitori extra-europei**, in particolare Amazon Web Services (AWS) e Google, **fossero stati inizialmente esclusi** dal governo britannico nel 2012, **per poi essere reintegrati** (rispettivamente nel 2013[13] e nel 2020[14]). Questi accordi sono finalizzati all'inquadramento e alla classificazione della fornitura di servizi cloud (in particolare, cloud hosting, cloud software e cloud support) alle PA da parte di operatori privati. Il programma viene aggiornato ogni 9-12 mesi e l'ultima

[12] A tal proposito, si evidenzia come OVH abbia iniziato a stringere in autonomia partnership strategiche con operatori hyperscaler internazionali basata su open source, trasparenza, interoperabilità e reversibilità, al fine di introdurre una nuova offerta di Hosted Private Cloud gestita e operata sul suolo europeo dal proprio team.

Fonte:https://www.ovh.it/news/press/cpl1689.ovhcloud-e-google-cloud-annunciano-partnership-strategica-realizzare-congiuntamente-soluzione-cloud

[13] G-Cloud 4.

[14] Il 3 giugno 2020 lo UK Crown Commercial Service (CCS) ha firmato un Memorandum d'intesa con Google.

versione disponibile, il G-Cloud 11, si è conclusa il 18 dicembre 2020. Quest'ultima prevede una classificazione in tre lotti: 1. Cloud Hosting (Iaas e Paas), 2. Cloud software (Saas) e 3. Cloud Support.

Il secondo pilastro riguarda uno *store online* di servizi cloud. Inizialmente chiamato Cloud Store e rinominato ***Digital Market Place*** nel 2014, questa piattaforma consiste in una banca dati consultabile ed accessibile al pubblico di servizi offerti da G-Cloud. A fine 2019 gli accordi conclusi tramite lo store avevano superato **sei miliardi di sterline**, con un incasso di quasi tre miliardi nel solo biennio 2018/19.

La terza iniziativa riguarda il **consolidamento dei data center** ("Data Centre Consolidation"). Nel 2010 è stato condotto un censimento che ha identificato 220 data center pubblici facenti capo al Governo centrale e stimato centinaia di altre infrastrutture relative alla PA locale. Per tali ragioni, si è proceduto ad una razionalizzazione in termini di ottimizzazione, sicurezza e resilienza dei servizi, da completarsi entro il 2020. Insieme alla **riduzione dei costi**, stimata in circa £300 milioni all'anno, e all'incremento della sicurezza e dell'affidabilità delle strutture, è stato identificato anche un **risparmio in termini energetici** fino al 75%.

Infine, nel maggio 2013 il Governo ha approvato la ***"Cloud First Policy"***, uno dei punti cardine delle linee guida *Technology Code of Practices*. Secondo questo principio, le PA devono considerare le soluzioni cloud prioritariamente rispetto ad altre soluzioni disponibili. Le PA sono in ultima analisi libere di utilizzare altre opzioni, ma devono dimostrare che le alternative offrono livelli di sicurezza, flessibilità e/o rapporto qualità/prezzo migliori rispetto alle soluzioni cloud. Con *Cloud First*, il Governo ha sottolineato l'importanza di dare priorità a servizi di cloud pubblici piuttosto che a modelli ibridi o privato. Le PA sono incoraggiate a considerare in primo luogo modelli Saas, in particolare per le funzioni IT e di backup.

Allo scopo di adattare la propria struttura organizzativa e di sicurezza alle nuove tecnologie e alla gestione di dati sensibili attraverso sistemi di cloud, dal 2013 il Governo britannico ha iniziato una riforma della propria **Data Classification Strategy**, ovvero il modo attraverso cui vengono classificate e protette le informazioni. Nel 2014, infatti, è stato superato il Government Protective Marking Scheme (GPMS), il sistema precedentemente in adozione, che prevedeva la suddivisione dei dati in *unclassified, protect, restricted, confidential, secret* e *top secret.* Poiché tale modello era stato progettato per i documenti cartacei, il

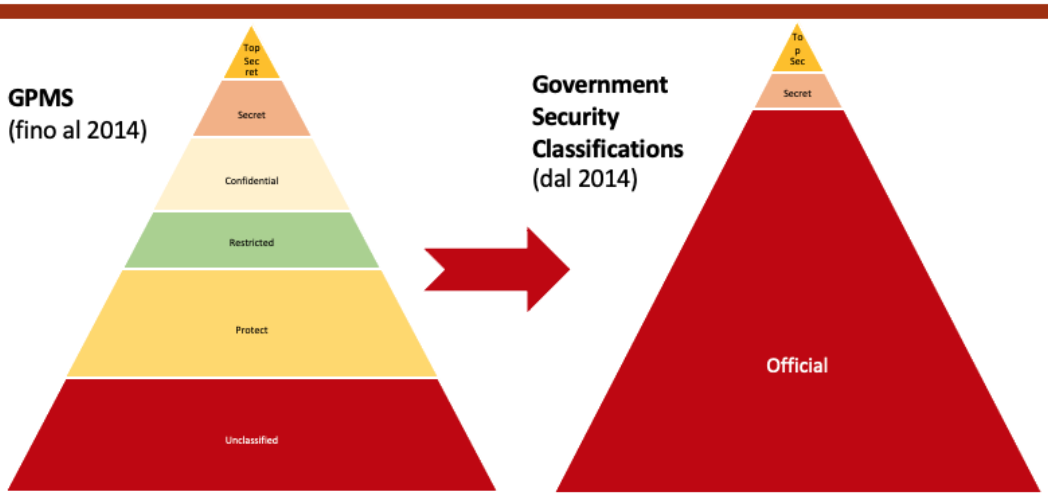


FIGURA 2.3 La classificazione dei dati sensibili nel Regno Unito

Fonte: Cabinet Office (UK)

Governo non lo considerava facilmente adattabile alla transizione digitale. Al posto del GPMS sono state create le **Government Security Classifications**, ovvero **tre livelli di sicurezza** che indicano il livello di sensibilità dei contenuti trattati dal Governo, dai dipartimenti e le agenzie del governo centrale e dalle forze armate. **Ad ogni livello è associato un livello di sicurezza e di controlli adeguati, al fine di contenere e contrastare rischi informatici**. Le tre classificazioni stabilite sono *Official*, *Secret* e *Top Secret*.

Il livello *"Official"* contiene la gran parte delle informazioni create ed elaborate dal settore pubblico, incluse le attività legate allo sviluppo delle politiche implementate dal Governo, le forniture di servizi, le consulenze legali, oltre a dati personali e amministrativi, contratti, statistiche e dossier. Sono dati a cui non vengono associati rischi di maggiore profilo, sebbene il Governo garantisca l'impegno affinché non vengano rubati, persi o diffusi dai media. Rientrano in *"Official"* anche le informazioni che rischiano di causare danni alle persone, alle organizzazioni, o al Governo. Queste vengono però contrassegnate come *"Official Sensitive"*, e richiedono misure di intervento aggiuntive.

In totale è stimato che la vasta **categoria *"Official"* racchiuda circa il 95% di tutte le informazioni gestite dal Governo**, mentre il restante 5% è suddiviso nelle classificazioni *"Secret"* e *"Top Secret"*.

Nello specifico, il **livello *"Secret"*,** racchiude informazioni governative considerate molto sensibili che potrebbero danneggiare relazioni internazionali e capacità militari, o che riguardano indagini particolarmente gravi

o collegate alla criminalità organizzata. Ad esse si aggiungono anche i contenuti che potrebbero minacciare direttamente la vita, la libertà o la sicurezza degli individui. Sono quindi informazioni che richiedono e giustificano **misure di protezione più stringenti contro attacchi cibernetici.**

Infine, il livello ***"Top Secret"*** è dedicato alle **informazioni che richiedono i massimi livelli di protezione e di sicurezza.** Queste includono tutti i dati del Governo direttamente collegati alla sicurezza nazionale del Regno Unito e dei suoi alleati, nonché tutte le informazioni che potrebbero causare ingenti perdite di vite umane, generare conflitti internazionali o provocare danni di lungo termine all'economia britannica. Queste richiedono livelli di protezione estremamente elevati, in modo da garantire difese stabili verso tutti i tipi di minacce.

Il caso del Regno Unito, che rappresenta il Paese maggiormente attivo in Europa nel campo della digitalizzazione e dell'economia dei dati in termini di investimenti, di valore, e di formazione, è di forte interesse per gli altri Stati membri dell'Unione. Con la Data Classification Strategy, infatti, è stato introdotto un sistema di classificazione che tiene conto sia della gestione digitale ed uniforme delle informazioni e dei dati della PA, sia dell'effettivo grado di informazioni sensibili all'interno di esse, identificando quelle meritevoli delle massime misure di protezione.

Case study 4: Il Cloud pubblico nel settore della difesa

Il cloud pubblico può trovare spazio anche in settori tradizionalmente chiusi e che gestiscono dati estremamente sensibili, ad esempio quello della Difesa. Una dimostrazione pratica di come questa tecnologia si adatti perfettamente ad un settore così delicato senza minarne la sicurezza, ma al contrario incrementandola, è quello del Regno Unito. Le forze armate UK hanno iniziato ad utilizzare il cloud pubblico per gestire i propri dati ufficiali (ad eccezione di quelli ritenuti di importanza e segretezza critica). Secondo quanto affermato da Rich Crowther, Head of the Defense Digital Service (DDS), l'utilizzo di un cloud pubblico sta permettendo alle forze armate di gestire i propri servizi digitali in maniera più efficiente e in maggiore sicurezza rispetto a quanto veniva fatto precedentemente on-premise. Uno dei motivi principali a sostegno di quest'affermazione deriva dalla velocità di aggiornamento delle patch di sicurezza. I cloud provider, in particolare quelli di grandi dimensioni, aggiornano infatti le patch di sicurezza con una brevissima cadenza temporale. Questo fa sì che i criminali informatici abbiano pochissimo tempo per

decodificare le informazioni di sicurezza e penetrare il sistema. Prima del passaggio al cloud pubblico potevano passare settimane (o addirittura mesi) prima che una patch venissero aggiornate. Il cambio di paradigma ha permesso che quest'operazione venisse svolta in pochi giorni.

Un'altra caratteristica che rende il cloud pubblico più sicuro è la possibilità di implementare controlli di sicurezza su larga scala in pochissimo tempo. Alcune operazioni di sicurezza, ad esempio riguardo il controllo degli accessi, che on-permise richiedevano giorni, grazie al cloud pubblico possono essere svolte in maniera quasi istantanea su tutto il sistema. L'utilizzo del cloud computing fornito dagli hyperscaler ha fatto si, inoltre, che potessero essere introdotte delle nuove funzionalità di sicurezza come il controllo degli accessi just in time, ovvero un sistema che consente l'accesso a determinati utenti solo quando (e per il tempo in cui) è necessario.

Fonte: https://www.gov.uk/

2.3.2 Il progetto Gaia-X

Come dimostra l'approvazione del GDPR e il lavoro sulla *European Data Strategy* nel corso del 2020, c'è una crescente attenzione tra i paesi dell'UE sull'importanza che i dati possono avere in termini di crescita economica, di efficienza, e di sicurezza degli Stati membri. In particolare, si evidenziano i **rischi che possono emergere da una eccessiva dipendenza da tecnologie straniere e i limiti che inevitabilmente caratterizzano i tentativi di realizzazione di strutture cloud nazionali.**

A fronte dei tentativi di diversi Stati membri nello sviluppare strategie di autonomia digitale a livello nazionale, la Commissione Europea ha recentemente proposto la nascita di un'iniziativa di cloud europeo all'interno del secondo pilastro della Strategia "*A European strategy for data*". Nello specifico la Commissione sta promuovendo la nascita del progetto cloud **"Gaia-X", un'infrastruttura di dati federata per consentire la gestione, l'accesso e il controllo di dati appartenenti a cittadini e imprese dell'Unione.**

Gaia-X è stata fortemente promossa dai governi di Francia e Germania e da alcune delle loro aziende nazionali leader nel settore dell'alta tecnologia e delle comunicazioni. Il progetto è infatti stato fondato da 22 aziende tra cui imprese fornitrici di servizi cloud, di infrastrutture, di telecomunicazioni, ma anche società di ricerca attive nei campi dell'innovazione, le quali, il 15 settembre 2020, si sono ufficialmente registrate come organizzazione no-profit ("GAIA-X AISBL", *association internationale sans but lucratif*).

La piattaforma opererà principalmente nelle aree che riguardano la creazione di meccanismi di trust per garantire l'identità delle fonti e dei destinatari, i diritti di accesso e di utilizzo, e una generale armonizzazione degli standard esistenti per l'interoperabilità e la portabilità tra infrastrutture, applicazioni, dati e termini di utilizzo. Inoltre, interverrà nella fornitura stessa di dati attraverso cataloghi federati e con la creazione di certificazioni e standard obbligatori a livello europeo per supportare gli operatori nell'offerta di servizi sicuri e interoperabili. Si osserva in particolare, come l'obiettivo consista nel **garantire interoperabilità e standard di sicurezza in modo da promuovere un ecosistema digitale aperto e trasparente**, in cui dati e servizi possono essere resi disponibili, raccolti e condivisi in un ambiente sicuro, **piuttosto che creare un cloud europeo alternativo ai colossi statunitensi e asiatici.**

Il progetto prevede infatti la creazione di una nuova **piattaforma paneuropea che metta in comune diversi fornitori di servizi cloud, anche extra-europei, nella misura in cui accettino il set di requisiti, standard e valori promossi a livello EU**. In tal modo, si punta a valorizzare il più ampio expertise dei provider di dimensioni globali che, grazie a maggiori investimenti ed esperienza, possono contare su una riconosciuta qualità dei servizi, velocità, usabilità e costi inferiori.

Allo stesso tempo, Gaia-X dovrebbe garantire agli user anche la **sovranità dei propri dati**. Infatti, ogni utente potrà stabilire in autonomia dove far conservare conservati i dati personali, chi potrà avere accesso ad essi, e chi potrà elaborarli e per quale scopo. Sulla base delle regole di standardizzazione e delle diverse opzioni di gestione e controllo, **i dati possono quindi successivamente essere scambiati ed elaborati tra le aziende, e infine monetizzati in reti di creazione di valore che sfruttano le sinergie e la maggiore efficienza determinata dal sistema aggregato e interoperabile.**

Nel complesso, il progetto ambisce a creare una piattaforma in cui i fornitori di soluzioni cloud (CSP), High Performance Computing (HPC) e specifici Cloud attivi nei sistemi di *edge computing* possano condividere e archiviare informazioni sotto standard di sicurezza europei al fine di consentire un ecosistema infrastrutturale user-friendly e sicuro. Lo sviluppo di questi servizi seguirà i principi della *security by design* e includerà anche il concetto di *privacy by design*, al fine di garantire i più elevati requisiti di sicurezza e protezione della privacy. Per consentire alle imprese più piccole e ai nuovi operatori del mercato di competere, i servizi seguiranno anche i due Codici di Condotta di autoregolamentazione sui temi di portabilità e cloud switching come '*Infrastructure as a*

service' e portabilità come '*Software as a service'*.

Il percorso di costruzione di Gaia-X prevede l'impegno su due binari. Il primo, ***"Workstream 1: User ecosystems and requirements"*, riguarda la definizione di procedure e regole**. Verranno definiti specifici requisiti settoriali e requisiti intersettoriali. A oggi il progetto include 8 settori rappresentati e organizzati in gruppi di lavoro: Industria 4.0/PMI, settore sanitario, settore pubblico, Finanza, Energia, Mobilità, Agricoltura e Smart-living. Questi hanno già presentato più di **40 user case**.

Il secondo, ***"Workstream 2: Technical implementation"*, riguarda la definizione di standard tecnologici e infrastrutturali in conformità con le normative europee**. Attraverso un'implementazione *domain-specific* che tiene conto del punto di vista degli utenti, si stanno attualmente sviluppando i requisiti tecnici della struttura e stabilendo le funzionalità tecniche di base dell'infrastruttura di dati. La scelta di un approccio bottom-up, unito ai contribuiti forniti dalle aziende aderenti al progetto, è riconducibile alla volontà di creare un sistema agile che sia adattabile agli sviluppi tecnologici e alle peculiarità dei vari quadri giuridici nazionali. Anche per questo Workstream sono stati avviati gruppi di lavoro tematici incentrati sui vari aspetti legali e innovativi riguardanti l'implementazione del servizio cloud.

È inoltre prevista **un'unità intermedia** tra i due pilastri, la ***Joint Requirements Experts Tribe,*** composta da esperti dei due Workstream. Questa si occupa di temi caratterizzati da una forte interdipendenza tra i due filoni di lavoro, e include interventi specifici sui requisiti tecnici generali e sugli aspetti normativi.

Oltre all'impegno verso la realizzazione del cloud federale europeo nella cornice del progetto Gaia X, è stata firmata una dichiarazione congiunta che promuove la nascita di un **EU Cloud Rulebook** per favorire un quadro normativo che uniformi specificità tecniche e requisiti di sicurezza. **L'Alleanza europea per i Dati Industriali e il Cloud**, nata a dicembre 2020 e composta da rappresentanti degli Stati membri, fornitori di cloud computing e utenti industriali del cloud, dovrebbe guidare l'implementazione del cloud pan-europeo con un budget fino a **dieci miliardi di euro**.

Come osservato, al fine di promuovere parità di condizioni per tutti coloro che accettano i princìpi comuni, e prevenire i possibili effetti negativi derivanti da protezionismo e innalzamento di barriere di mercato, l'adesione all'ecosistema Gaia-X è consentita anche ad aziende extra-europee che

decidono di accettare e sottoscrivere gli standard e i valori dell'UE.

Allo stesso tempo, per quanto riguarda la **partecipazione di multinazionali** o di gruppi aventi la sede principale fuori dall'Unione europea, l'adesione è consentita all'azienda capogruppo e non alle proprie filiali europee. Tuttavia, **qualora la capogruppo di un cloud provider multinazionale extra-UE non dovesse partecipare, l'accesso sarà consentito ad una sola delle sue filiali con sede nell'Unione** mentre tutte le eventuali altre, inclusa la capogruppo, saranno automaticamente escluse.

Inoltre, per quel che riguarda il **board di Gaia-X,** si rileva come **solo le società aderenti con sede in Europa possano candidare un proprio componente per il Consiglio di Amministrazione** della nuova infrastruttura paneuropea, mentre tale possibilità appare al momento preclusa agli altri potenziali partner internazionali. A tal proposito, si osserva preliminarmente come tale prassi potrebbe non essere la soluzione migliore per garantire l'apertura e la competitività del mercato europeo, in quanto le decisioni potrebbero essere soggette a «bias» e veicolare formule o pre-giudizi in grado di limitare l'accesso al mercato europeo di aziende con headquarter al di fuori del continente.

Resta inoltre da definire la libertà con cui i vari Paesi potranno **selezionare i fornitori specifici** all'interno della piattaforma Gaia-X. Nel caso venissero definite **regole più restrittive**, che prevedano il coinvolgimento esclusivo di operatori che rispondono prioritariamente alla giurisdizione nazionale o europea e che garantiscono esclusivamente la 'residenza fisica' dei dati sul territorio nazionale o europeo, si osserva come tale limitazione rischierebbe di impedire l'esportazione di dati nazionali in server oltre i confini Ue, limitando i benefici derivanti da un effettivo accesso ad un sistema europeo e internazionale interoperabile, e quindi più efficiente, sicuro e innovativo.

2.3.3 La partecipazione dell'Italia e possibili scenari di Regional Hub

I princìpi delineati nel progetto sono stati ribaditi nel Pan-European Gaia-X Summit del 18 e 19 novembre 2020, dove sono state ufficializzate anche le 159 società provenienti da 18 Paesi che hanno aderito al progetto e che si sono dunque aggiunte alle 22 aziende fondatrici. Queste includono realtà attive nella produzione e diffusione energetica, nelle Tlc, nelle comunicazioni, ma anche imprese dei settori delle infrastrutture, delle poste, e della difesa. Si punta a formare una cooperazione stabile tra governi, mondo delle imprese e le più elevate competenze scientifiche e tecnologiche, allo scopo di definire una roadmap e dei requisiti comuni per la realizzazione di un'infrastruttura cloud

che possa soddisfare i più alti standard di sicurezza, di sovranità digitale e di innovazione.

In totale la Germania conta 49 adesioni e la Francia 33, confermandosi come le maggiori forze trainanti del progetto. Anche l'**Italia** ha dimostrato grande fiducia nella realizzazione della nuova infrastruttura digitale, con **28 aziende aderenti** tra cui i gli operatori delle telecomunicazioni e delle principali infrastrutture nazionali quali TIM, Leonardo, Eni ed Enel, oltre a Poste Italiane e Confindustria. A fine 2020, il sostegno è arrivato anche dall'allora Ministra per l'innovazione, Paola Pisano, che ha sottolineato l'importanza della nuova infrastruttura come strumento di autonomia digitale rispetto ai fornitori extra-europei e come acceleratore della transizione digitale in termini di crescita economica ed efficienza della PA italiana.

Il Summit ha anche visto l'ufficializzazione della partecipazione al progetto anche da parte di multinazionali e dei principali fornitori di cloud extra-europei. Nello specifico, parteciperanno a Gaia-X anche Amazon Web Service (Aws), Microsoft Azure, IBM, Google e Alibaba, nonché diversi operatori di telecomunicazioni e aziende leader nella diffusione della rete 5G, come Ericsson e Huawei. Si ambisce quindi a stabilire una cooperazione duratura e internazionale, dettata da regole e valori mirati a garantire concorrenza e sicurezza.

In vista del probabile lancio di una versione alpha nel 2021, il progetto Gaia-X prevede attualmente una articolazione in Hub regionali che avranno la funzione di far emergere caratteristiche e requisiti legati a specificità settoriali o locali. Al momento, tuttavia, non appare definito a chi spetti coordinare queste iniziative nazionali: se in Germania il lavoro sarà coordinato dal ministero dell'Economia, in Francia il ruolo sarà assolto dalle principali aziende pubbliche.

Pur in questa incertezza, **l'Italia è tra i primi Paesi – insieme a Francia, Finlandia e Germania – ad aver iniziato le attività per dotarsi di un Regional Hub sul suolo nazionale.** Nello specifico, una prima roadmap prevede che ciò avvenga entro la prima metà del 2021, dopo la realizzazione dei poli in Francia e Germania, e in parallelo con l'Olanda.

A differenza di altri Paesi, in cui è previsto il coordinamento da parte delle istituzioni pubbliche, sul nostro territorio il promotore dell'Hub è Confindustria. L'associazione degli industriali sta gestendo le attività per la realizzazione del Regional Hub italiano, forte del sostegno al progetto Gaia-X sin dalle origini e della strutturata rete capillare del proprio tessuto associativo, che consente di

avviare azioni di sensibilizzazione e coinvolgimento nei confronti delle aziende e dei player nazionali con l'obiettivo facilitare l'adesione al progetto e la condivisione di best practice.

2.4 LA GESTIONE DEI DATI TRA EUROPA E USA

2.4.1 Dal caso Microsoft vs. USA al Cloud Act. Le potenziali frizioni con la normativa europea

Il **Clarifying Lawful Overseas Use of Data Act** o **Cloud Act** (HR 4943) è una legge federale degli Stati Uniti emanata nel 2018 con l'approvazione del Consolidated Appropriations Act, 2018, PL 115-141, Divisione V.

Si tratta di un intervento dalla grandissima rilevanza con il quale, dopo i non riusciti tentativi di riforma rappresentati dal "Law Enforcement Access to Data Stored Abroad Act" (Legge LEADS) del 2015 e l'International Communications Privacy Act (ICPA) del 2017, è stato modificato lo Stored Communications Act (SCA), approvato dal Congresso degli Stati Uniti nel 1986 all'interno del più ampio Electronic Communications Privacy Act (ECPA), nell'ottica di consentire alle forze dell'ordine federali di obbligare le società tecnologiche con sede negli Stati Uniti tramite mandato o mandato di comparizione a fornire i dati richiesti archiviati sui server indipendentemente dal fatto che i dati siano archiviati negli Stati Uniti o su suolo straniero. Lo SCA, in particolare, vietava la divulgazione di dati relativi ai contenuti, mentre i dati non relativi ai contenuti potevano essere forniti su base volontaria[15].

[15] Tale esigenza di modifica è emersa, in particolare, nell'ambito di un'indagine sul traffico di droga del 2013, durante la quale l'FBI ha emesso un mandato SCA per le e-mail che un cittadino statunitense aveva archiviato su uno dei server remoti di Microsoft in Irlanda. A fronte di tale richiesta, Microsoft ha reso noti i dati immagazzinati nei server americani mentre ha opposto un deciso rifiuto con riguardo alle email archiviate in un server in Irlanda. Alla base di tale rifiuto la considerazione secondo cui l'art. 41 del SCA, non prevedendo la propria applicazione al di fuori del territorio americano, non potesse coprire i dati archiviati al di fuori degli Stati Uniti. È iniziata, dunque, un'aspra battaglia legale nella quale il Governo ha sostenuto che il mandato è rivolto all'impresa che gestisce il servizio internet e non al luogo dove sono situati i server e che tale mandato non è un comune mandato bensì un *subpoena*, ossia uno strumento che indica la capacità di un giudice di ottenere coattivamente una testimonianza o la produzione di elementi di prova con la previsione di una sanzione qualora tale prerogativa non venga rispettata. Tali argomentazioni, se hanno in primo grado trovato accoglimento, hanno successivamente visto la contrapposizione dei Giudici della Corte d'Appello che, al contrario, hanno accolto le motivazioni poste in essere dai legali della compagnia ritenendo che le leggi del Congresso, in mancanza di diversa indicazione, devono essere sempre intese come applicali solo all'interno della giurisdizione degli Stati Uniti così come stabilito anche nella sentenza della Corte Suprema nel caso Morrison contro National Australia Bank. A seguito di questa decisione il governo americano ha portato il caso alla Corte Suprema che ha trattato la

Entrando nel merito di **quanto previsto dal Cloud Act**, quest'ultimo parte dalla constatazione dell'importanza di assicurare alle autorità l'accesso tempestivo ai dati elettronici relativi o non relativi al contenuto in possesso dei fornitori di servizi di comunicazione per proteggere la sicurezza pubblica e combattere i reati gravi, compreso il terrorismo, dall'ostacolo rappresentato dall'impossibilità di accedere ai dati memorizzati al di fuori degli Stati Uniti che si trovano tuttavia sotto il controllo o possesso di fornitori di servizi di comunicazione soggetti alla giurisdizione statunitense ("*data stored outside the United States that is in the custody, control, or possession of communications service providers that are subject to jurisdiction of the United States*") ed evidenzia, al contempo, l'importanza, anche per le autorità straniere, di accedere, nella propria attività di contrasto ai reati, ai dati elettronici in possesso dei fornitori di servizi di comunicazione negli Stati Uniti.

Nel tentativo di far fronte a tali esigenze, il Cloud Act: a) consente alle autorità statunitensi, forze dell'ordine e agenzie di intelligenze di acquisire da fornitori di "*servizi di comunicazione elettronica o servizi di calcolo a distanza*", tra cui i CSPs, che siano sottoposti alla giurisdizione degli Stati Uniti dati informatici "*regardless of whether such communications, record or other information is located within or outside of USA*" ossia indipendentemente dal fatto che tali comunicazioni, registrazioni o altre informazioni si trovino all'interno o all'esterno degli Stati Uniti a condizione però che siano in custodia, controllo o possesso di fornitori di servizi di comunicazione soggetti alla giurisdizione degli Stati Uniti; b) si applica soltanto a dati ed informazioni strumentali alla protezione della sicurezza pubblica e a contrastare reati di particolare gravità, quali terrorismo, crimini di violenza significativa, sfruttamento minorile, criminalità organizzata transnazionale, frodi finanziarie di importanza rilevante; c) la richiesta di accesso ai dati digitali nei confronti del destinatario deve essere sempre supportata da una misura nazionale che si sostanzia, a seconda dei casi, in mandato, ordinanza o ordine di esibizione amministrativo che presupponga un'analisi circa la probabilità dell'esercizio dell'azione penale; d) vieta l'imposizione di obblighi di decriptazione e/o decifrazione dei dati secretati (ad es. mediante criptazione) a carico dei soggetti sottoposti cui il medesimo si applica; e) innova il meccanismo dei trattati di reciproca assistenza giudiziaria introducendo con un sistema imperniato su accordi bilaterali, i

causa il 27 febbraio del 2018. La Corte ha poi archiviato il processo il 17 aprile 2018, dopo essere stata informata dalle parti dell'adozione del Cloud Act che ha consentito l'emissione di un nuovo mandato per ottenere le informazioni necessarie da Microsoft.

cosiddetti *executive agreements* che l'esecutivo statunitense potrà stipulare con Stati stranieri in determinate circostanze e secondo requisiti sostanziali e procedurali di base e a meno che il Congresso non si opponga.

Lo stesso Cloud Act attribuisce al provider destinatario di un provvedimento di ostensione di "*contents of a wire or electronic communication of a subscriber or customer*" la possibilità di formulare - entro 14 gg dalla ricezione di tale provvedimento e salva proroga disposta dal tribunale su richiesta del provider - una richiesta di modifica o annullamento della stessa nel caso in cui ragionevolmente ritenga che il cliente o l'abbonato non sia un cittadino statunitense e non risieda negli Stati Uniti e sussista il rischio concreto che l'ottemperanza all'ordine determini la violazione del diritto di un "*qualifying foreign government*", intendendo con tale locuzione un governo straniero che abbia concluso con gli USA un executive agreement. Nel caso in cui non sia stato concluso alcun accordo esecutivo, sembra che la divulgazione possa essere contestata solo sulla base di un esame alla luce del principio di cortesia previsto dal common law.

Fatta salva la possibilità per l'ente governativo di apportare modifiche in conseguenza dell'**istanza del provider,** sulla base delle richiamate considerazioni relative alla violazione di leggi straniere ed alla residenza e nazionalità del cliente/abbonato, cui si aggiunge la verifica circa la sussistenza di circostanze e interessi della giustizia che impongano un ripensamento o l'annullamento della richiesta, il tribunale adito può, sulla base della valutazione di una serie di fattori puntualmente indicati dalla norma[16] **apportare modifiche o annullare la richiesta di ostensione inviata al provider**.

Lo stesso Cloud Act si occupa di individuare la complessa procedura, le condizioni per addivenire alla conclusione dell'executive agreement ed i contenuti essenziali dello stesso, prescrivendo, in particolare: 1) la previsione, da parte del diritto del governo straniero, di solide tutele sostanziali e procedurali per la privacy e le libertà civili, la garanzia del rispetto del principio di non discriminazione e dei diritti umani universali (ed. il diritto alla manifestazione del pensiero, il divieto di tortura e trattamenti disumani etc.); la previsione, da parte del governo straniero, di appropriate procedure per minimizzare l'acquisizione, la conservazione e

[16] Si fa riferimento a: gli interessi investigativi statunitensi e gli interessi del governo straniero, la nazionalità e residenza del cliente o abbonato del provider, le conseguenze del mancato o ritardato accesso all'informazione richiesta, il legame del provider con gli USA e gli interessi investigativi dell'autorità straniera nel caso in cui il procedimento sia stato dalla stessa avviato.

la diffusione di informazioni concernenti soggetti statunitensi sottoposti all'agreement; 3) il divieto di inserimento nell'agreement di previsioni che obblighino i provider ad essere in grado di decifrare i dati o limitino la loro attività di decifraggio; 4) che l'ordine di esibizione formulato da un governo straniero sia teso ad ottenere informazioni concernenti la prevenzione, l'indagine ed il perseguimento penale di gravi reati, incluso il terrorismo, identifichi con puntualità l'oggetto della richiesta (specifica persona, account, device etc.), sia conforme alla legge nazionale cui è sottoposto il provider, sia fondato su giustificati motivi, sia soggetto a controllo da parte di un organo giudiziario o di un'autorità indipendente; 5) che nel caso di un ordine di intercettazione di comunicazioni elettroniche o via cavo, esso sia per un periodo specifico e limitato e non superiore a quanto necessario per il raggiungimento degli obiettivi perseguiti, non sia possibile ragionevolmente ottenere la stessa informazione attraverso un metodo meno invasivo.

Dal punto di vista operativo, il Dipartimento di Giustizia degli Stati Uniti ha emesso nel dicembre 2017 una guida intitolata "*Seeking Enterprise Customer Data Held by Cloud Service Providers*" che consiglia ai pubblici ministeri di rivolgersi direttamente ai clienti piuttosto che ai fornitori di servizi, se ciò non compromette l'indagine.

Se questa è la cornice normativa, probabilmente è da ridimensionare l'ampio e acceso dibattito che si è scatenato a livello europeo e nazionale e che si è focalizzato sulla convinzione che la disciplina contenuta nel Cloud Act attribuisca alle autorità statunitensi un potere pressoché illimitato di accedere a dati personali di cittadini europei nella disponibilità di società soggette alla giurisdizione degli USA e che l'esercizio di tale potere, in un mercato come quello del Cloud, che vede competere pochi grandi player prevalentemente statunitensi, possa minare il set di garanzie faticosamente realizzato a livello di Unione e racchiuso nel GDPR, strumento poderoso e modello di tutela della privacy che ha suscitato e continua a suscitare ammirazione a livello globale.

Un'attenta analisi della disciplina contenuta nel Cloud Act suggerisce, invero, un supplemento di riflessione che tenga nella dovuta considerazione alcune circostanze che appaiono dirimenti per inquadrare in maniera corretta le questioni ed orientare così il dibattito ed il confronto tra gli stakeholders interessati e i policy makers.

La disciplina in esame, infatti, al fine – peraltro sotteso anche alle proposte di regolamento e direttiva formulate dalla Commissione nel 2018 in relazione agli ordini europei di produzione e conservazione di prove elettroniche in materia penale – di assicurare alle autorità l'accesso tempestivo

ai dati elettronici relativi o non relativi al contenuto in possesso dei fornitori di servizi di comunicazione, per proteggere la sicurezza pubblica e combattere i reati gravi, compreso il terrorismo, pone un obbligo di ostensione che concerne i dati conservati anche al di fuori del territorio USA ma che siano comunque in custodia, controllo o possesso di fornitori di servizi di comunicazione soggetti alla giurisdizione degli Stati Uniti.

Si tratta, sì, di un obbligo ampio e pervasivo ma che trova una serie di **importanti limitazioni e garanzie procedimentali**. E infatti, il Cloud Act individua minuziosamente i soggetti destinatari della disciplina, subordina l'accesso ai dati all'adozione di specifici provvedimenti che presuppongono già una valutazione dell'Autorità giudiziaria circa la possibilità di procedere penalmente per combattere reati gravi, quali terrorismo, crimini di violenza significativa, sfruttamento minorile, criminalità organizzata transnazionale, frodi finanziarie di importanza rilevante. Vieta l'imposizione di obblighi di decriptazione e/o decifrazione dei dati secretati (ad es. mediante criptazione) a carico dei soggetti sottoposti cui il medesimo si applica, assicura ai destinatari di tali richieste di accesso la possibilità di adire l'autorità giudiziaria per chiedere l'annullamento o la modifica del mandato ed introduce la possibilità di addivenire alla stipula di un *executive agreement* da cui discende l'acquisizione, da parte dell'altro stato contraente, della qualifica di "*qualifying foreign government*", molto rilevante in sede di eventuale ricorso presentato dal destinatario della richiesta per opporre la violazione del diritto di tale Paese.

Il *Cloud Act* si presenta, dunque, come uno strumento che introduce un modello di condivisione dei dati digitali agile con cui far fronte a specifiche e limitate esigenze connesse alla protezione della sicurezza pubblica, nel rispetto di garanzie procedurali tese a rendere effettivo il diritto di ricorso degli operatori cui si applica e a garantire dunque la tutela della privacy dei clienti, anche europei. Si tratta di un approccio certamente pragmatico che per certi versi si presenta anche meno *disruptive* di quello proposto a livello UE dalla Commissione e che si analizzerà *infra*. La proposta di direttiva del 2018 ed ancora in corso di discussione, infatti, prescrive a tutte le società che offrono servizi ai residenti dell'Unione Europea l'individuazione di un rappresentante con sede nell'Unione stessa, andando a determinare, sostanzialmente, un 'espansione della propria giurisdizione che non trova analoga misura all'interno del Cloud Act.

Se questo è il quadro USA, nella UE (per approfondimenti v. appendice C - *Il quadro normativo europeo e le proposte in discussione*) il **regolamento n. 679/2016**

(GDPR) rappresenta il baluardo della tutela della privacy dei cittadini europei fissando la cornice normativa generale in materia di tutela dei dati personali. Il Capo V, in particolare, ha ad oggetto i trasferimenti di dati personali verso Paesi terzi o organizzazioni internazionali, distinguendo le diverse tipologie di trasferimento (sulla base di una decisione di adeguatezza o trasferimento soggetto a garanzie adeguate), disciplinando il trasferimento o comunicazione non autorizzati dal diritto dell'Unione ed individuando le deroghe in specifiche situazioni.

Nell'ambito di questa cornice normativa generale, considerato che è in forte crescita il numero di reati commessi online o mediante l'utilizzo del canale informatico e che l'Unione europea deve affrontare il tema della raccolta e della conservazione delle prove elettroniche nel tentativo di rendere più rapide ed efficaci tali attività, il 17 aprile 2018 la Commissione ha pubblicato una **proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018) 225 final) e una proposta di direttiva (COM(2018) 226 final), per la definizione di norme sulla rappresentanza legale nell'Unione di determinati prestatori di servizi ai fini della ricezione, dell'ottemperanza e dell'esecuzione di decisioni e ordini emessi dalle autorità competenti degli Stati membri per acquisire prove nei procedimenti penali.**

Si tratta di proposte molto rilevanti che introducono norme in base alle quali un'autorità di uno Stato membro può ingiungere a un prestatore di servizi che offre servizi nell'Unione di produrre o conservare prove elettroniche, indipendentemente dall'ubicazione dei dati (facendo salva la facoltà delle autorità nazionali di ingiungere ai prestatori di servizi stabiliti o rappresentati nel loro territorio di ottemperare a misure nazionali dello stesso tipo) a patto che sussista - secondo specifici criteri puntualmente individuati - un **collegamento sostanziale** con l'Unione che si realizza certamente quando il prestatore di servizi ha uno stabilimento nell'Unione e che esista un **procedimento penale**, in fase sia preprocessuale che processuale. La proposta di regolamento individua la **competenza** ad emettere ordini di produzione riguardanti dati relativi agli abbonati o dati relativi agli accessi, alle operazioni o dati relativi al contenuto, nonché ordini di conservazione, fissa le **condizioni per l'emissione** di un ordine di produzione nonché i **contenuti dell'ordine** stesso, individua **procedure e tempistiche di risposta**, a fronte della ricezione di un ordine di produzione, individua i **casi di possibile opposizione da parte del destinatario di un ordine di produzione e conservazione**, descrive la

procedura di riesame da attivare nel caso di obblighi contrastanti basati su diritti fondamentali o interessi fondamentali di un paese terzo e fissa i principi da seguire nella fissazione delle sanzioni pecuniarie conseguenti alle violazioni della normativa.

La direttiva proposta, invece, prescrive agli Stati membri di provvedere affinché un prestatore di servizi che offre servizi nell'Unione ed un prestatore di servizi che offre servizi sul loro territorio ma che non è stabilito nell'Unione designi almeno un **rappresentante legale nell'Unione** ai fini della ricezione, dell'ottemperanza e dell'esecuzione di decisioni e ordini emessi dalle autorità competenti degli Stati membri per acquisire prove nei procedimenti penali prevedendo, per i casi di violazione della disciplina in esame, l'irrogazione di sanzioni efficaci, proporzionate e dissuasive e disponendo la designazione di un'autorità centrale o, laddove il loro sistema giuridico lo preveda, più autorità centrali competenti per garantire che la presente direttiva sia applicata in maniera coerente e proporzionata. Si tratta, a ben vedere, di una previsione di grandissimo impatto, attraverso la quale, di fatto, l'UE riuscirebbe ad assicurarsi la giurisdizione anche su quelle società che avendo una sede al di fuori del territorio UE risulterebbero sottratte a tale giurisdizione.

Posto che le proposte appena analizzate disciplinano il caso di determinati tipi di prestatori di servizi che forniscono servizi sul mercato dell'UE e che pertanto esiste il rischio di obblighi contrastanti con le leggi dei paesi terzi, al fine di affrontare tali possibili conflitti di legge e ridurre il ricorso alle procedure di riesame che pure le proposte prevedono, in linea con il principio di cortesia internazionale, il 5 febbraio 2019 la Commissione ha adottato una **raccomandazione di decisione del Consiglio (COM(2019) 70 final) che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale o l'avvio di negoziati**. Si tratta di un'iniziativa importante che fissa gli obiettivi da perseguire nell'ambito dei negoziati, richiede la puntuale definizione della natura e dell'ambito applicativo dell'accordo, individua le garanzie da assicurare e definisce la governance dell'accordo.

2.4.2 Dalla sentenza Schrems II alle raccomandazioni dell'EDPB

Le raccomandazioni dello European Data Protection Board (EDPB) - il Comitato europeo per la protezione dei dati - intervengono a colmare il vuoto normativo generato dalla **sentenza Schrems II**

pronunciata dalla Corte di giustizia dell'Unione europea lo scorso 16 luglio in merito al regime di trasferimento dei dati tra l'Unione europea e gli Stati Uniti che ha invalidato la decisione di adeguatezza del *Privacy Shield*.

Il *Privacy Shield*[17], in particolare, faceva seguito alle indicazioni della Corte di giustizia europea, che il 6 ottobre 2015 aveva dichiarato non valida la decisione della Commissione del 2000 sullo scambio di dati tra UE e USA, il cosiddetto **Safe Harbour** e, al fine di proteggere più efficacemente i diritti fondamentali delle persone nell´UE i cui dati personali vengano trasferiti negli Stati Uniti, aveva stabilito regole certe per le imprese che effettuano trasferimenti di dati al di là dell´Atlantico.

Ebbene, la **sentenza Schrems II ha posto**, in materia di trasferimento dei dati dall'UE verso Paesi terzi (USA nel caso di specie) **una serie di importanti punti fermi**[18] tra cui

[17] Si tratta, nello specifico, di un accordo che ha fissato obblighi più rigorosi in capo alle imprese statunitensi e più stringenti obblighi di vigilanza per le autorità americane e con il quale per la prima volta è stato garantito formalmente che l'accesso delle autorità pubbliche ai dati personali sarà oggetto a limiti e al rispetto di procedure e garanzie specifiche. Nello specifico, l'accordo ha definito obblighi di trasparenza per le aziende e meccanismi di controllo del rispetto delle regole introdotte, ha disposto sanzioni o esclusione dai benefici dell'accordo per le aziende che non lo rispettano, ha fissato condizioni più rigide per il trasferimento dei dati dalle imprese riceventi a destinatari ulteriori, mentre con riferimento all'Amministrazione USA, quest'ultima ha formalmente garantito che non saranno realizzate attività di sorveglianza indiscriminata o massiva.
A ciò si aggiunge la possibilità, per le aziende, di dichiarare il numero approssimativo di richieste di accesso ricevute e l'istituzione del "difensore civico", soggetto indipendente incaricato di ricevere e decidere i reclami presentati dagli interessati che rappresenta uno strumento di tutela giuridica importante, che si affianca alla possibilità di rivolgersi direttamente all'azienda (la quale è chiamata a rispondere al reclamo ricevuto entro 45 giorni), utilizzare meccanismi ADR e rivolgersi all'Autorità di protezione dati, rivolgersi al Privacy Shield Panel (Collegio arbitrale del Privacy Shield) per ottenere, nel caso nessun'altra soluzione abbia avuto esito positivo, una decisione esecutiva mediante un meccanismo di arbitrato. Al monitoraggio annuale sono preposti Commissione europea (chiamata a redigere una relazione annuale a Parlamento e Consiglio) e Department of Commerce USA con il coinvolgimento di esperti dei servizi di sicurezza americani e delle Autorità europee per la protezione dei dati.

[18] La sentenza Schrems II, in particolare, ha affermato che:

a) l'art. 2, paragrafi 1 e 2, del GDPR relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati deve essere interpretato nel senso che rientra nell'ambito di applicazione di tale regolamento un trasferimento di dati personali effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro verso un altro operatore economico stabilito in un paese terzo, nonostante il fatto che, durante o in seguito a tale trasferimento, i suddetti dati possano essere sottoposti a trattamento da parte delle autorità del paese terzo considerato a fini di sicurezza pubblica, di difesa e sicurezza dello Stato;

b) l'art. 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del GDPR devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati

l'invalidità della decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016 sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy che ha determinato un grave vuoto regolamentare da colmare.

A tal fine, a quattro mesi dalla pronuncia di tale sentenza, il 29 ottobre scorso lo European Data Protection Supervisor (EDPS) - il Garante europeo della protezione dei dati i cui poteri, competenze ed organizzazione sono definiti dallo stesso regolamento n. 1275/2018 - ha pubblicato la ***Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling***, volta a delineare un piano strategico per assicurare che i trasferimenti internazionali in corso e futuri siano effettuati in conformità a quanto previsto dalla Carta europea dei diritti fondamentali e dal Cap. V del regolamento n. 1725/2018.

Al fine di individuare le azioni da mettere in campo, la strategia, in una logica di identificazione delle azioni di breve periodo, dopo aver invitato le istituzioni a focalizzare l'attenzione in via prioritaria sui trasferimenti

personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell'Unione europea. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo, in particolare quelli enunciati all'articolo 45, paragrafo 2, di detto regolamento;

c) l'art. 58, paragrafo 2, lettere f) e j), del GDPR deve essere interpretato nel senso che, a meno che esista una decisione di adeguatezza validamente adottata dalla Commissione europea, l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 di tale regolamento e dalla Carta dei diritti fondamentali, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo;

d) dall'esame della decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46/CE, come modificata dalla decisione di esecuzione 2016/2297 della Commissione, del 16 dicembre 2016, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali non è emerso alcun elemento idoneo ad inficiarne la validità;

e) la decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, è invalida.

diretti a soggetti privati in particolare negli USA, dà conto dell'adozione, da parte del Garante, di un **approccio fondato sull'analisi del rischio**, e dell'avvio (il 5 ottobre) da parte delle istituzioni europee, su disposizione dello stesso Garante, di **un'attività di mappatura ed inventario, di tutte le operazioni ed i contratti pendenti che comportino trasferimenti di dati verso paesi terzi**.

In una logica precauzionale, il Garante ha poi fornito un'esortazione piuttosto importante alle istituzioni: garantire che qualsiasi nuova operazione di trattamento o nuovo contratto con qualsiasi fornitore di servizi non comporti trasferimenti di dati personali verso gli Stati Uniti.

Se questo è quanto disposto per il breve periodo, con riferimento al medio, il Garante ha richiesto alle istituzioni europee di condurre **valutazioni di impatto del trasferimento (Transfer Impact Assessments – TIA)** per verificare se nel paese terzo di destinazione è garantito un livello di protezione sostanzialmente equivalente a quello previsto dall'UE ed adottare le conseguenti decisioni annunciando ulteriori iniziative ispirate dalla volontà di rafforzare i meccanismi di coordinamento e cooperazione (v. Appendice C).

In occasione della quarantunesima sessione plenaria tenutasi il 10 novembre 2020, il Comitato europeo per la protezione dei dati (EDPB), che riunisce i Garanti nazionali, ha pubblicato le ***"Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data"*** e le ***"Recommendations 02/2020 on the European Essential Guarantees for surveillance measures"***.

Si tratta di raccomandazioni che, al fine di agevolare gli esportatori (siano essi enti privati o organismi pubblici, che trattano dati personali nell'ambito di applicazione del GDPR) nel complesso compito di valutare i Paesi terzi e individuare, se necessario, adeguate misure supplementari, individuano una serie di **step procedimentali** da seguire, identificano i **fattori da valutare** e le **possibili misure** da mettere in campo tra cui spicca, per importanza, il **ricorso alla crittografia ed alla pseudonimizzazione**.

Con queste importanti iniziative si sta cercando di colmare il vuoto determinato dalla sentenza Schrems II. La strategia, in particolare, se da un lato ha l'indubbio merito di cercare di fare **chiarezza** sullo stato dell'arte mediante un'attenta opera di **mappatura** delle varie tipologie di trasferimenti diretti a soggetti privati in particolare negli USA e di promuovere un approccio – senz'altro condivisibile – fondato sull'**analisi del rischio** che certamente garantisce maggior adesione al principio di proporzionalità, dall'altro, nell'esortare le

istituzioni a garantire che qualsiasi nuova operazione di trattamento o nuovo contratto con qualsiasi fornitore di servizi non comporti trasferimenti di dati personali verso gli Stati Uniti, approda ad una soluzione draconiana che, sebbene ispirata da finalità di tipo precauzionale, desta alcune perplessità.

Per quanto concerne, invece, le raccomandazioni del Comitato, esse rappresentano certamente uno strumento utile che, in una logica di agevolazione degli esportatori di dati nel complesso compito di valutare i Paesi terzi ed individuare, se necessario, adeguate misure supplementari, descrive una serie chiara ed articolata di step procedimentali da seguire attraverso cui procedere all'attività di mappatura, all'identificazione dello strumento di trasferimento su cui si basa il trasferimento, alla verifica circa l'esistenza di elementi nella legge o nella prassi del paese terzo in grado di incidere sull'efficacia delle garanzie assicurate dagli strumenti di trasferimento applicabili al caso di specie ed all'identificazione e adozione di eventuali misure supplementari (di natura contrattuale, tecnica o organizzativa) necessarie per assicurare un livello di protezione dei dati sostanzialmente equivalente a quello garantito dall'UE.

Nell'identificare le misure da mettere in campo le raccomandazioni offrono una serie di indicazioni tra cui spicca, in termini di efficacia riconosciuta, il ricorso alla crittografia ed alla pseudonimizzazione. Rispetto al ricorso alla **crittografia**, in particolare, le raccomandazioni prescrivono che la cifratura sia "*implementata e convalidata in modo impeccabile*", richiedono che la robustezza dell'algoritmo di cifratura e della sua parametrizzazione sia valutata tenendo conto delle risorse e delle capacità tecniche a disposizione degli Stati e che le chiavi siano gestite in modo affidabile (generate, amministrate, conservate, se del caso, collegate all'identità di un destinatario previsto, e revocate) e conservate esclusivamente sotto il controllo dell'esportatore di dati, o di altri soggetti incaricati di questo compito che risiedono nel SEE o in un paese terzo, in una regione o presso un'organizzazione internazionale. Si tratta di indicazioni evidentemente molto rigorose e complesse che pongono importanti interrogativi in relazione agi adempimenti ed ai relativi costi, tanto più rilevanti per le piccole e medie imprese o per soggetti come gli istituti di ricerca, connessi all'analisi delle leggi e delle pratiche di decine di Paesi terzi, alla necessità di modificare il proprio fornitore di certificati digitali (con impatto anche si tale mercato) e di acquisire le necessarie competenze crittografiche, nonché, a livello più generale, al rischio che il timore connesso al trasferimento disincentivi le relazioni tra imprese UE ed extra-UE a scapito della competitività del mercato e dell'innovazione

A ciò si aggiungono **criticità irrisolte** e rigidità che potrebbero frapporre importanti ostacoli ai trasferimenti di dati. È il caso, in particolare, di cloud o data processor in Paesi ritenuti non sicuri. In tal caso, infatti, l'Annex 2 esclude, allo stato attuale dell'arte, la possibilità di individuare una misura tecnica efficace per garantire i diritti dell'interessato nelle ipotesi in cui il titolare del trattamento trasferisca i dati a un fornitore di servizi cloud o altro responsabile del trattamento e tale fornitore di servizi cloud (o altro responsabile) debba accedere ai dati in chiaro per eseguire il compito assegnato ed il potere concesso alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va oltre quanto necessario e proporzionato in una società democratica. Si tratta di una conclusione importante e che necessita ponderazione applicativa ove si consideri che un'applicazione rigorosa di tale raccomandazione potrebbe di fatto interrompere o comunque fortemente ostacolare una moltitudine di collaborazioni tra società europee e branch o intere società americane (si pensi solo all'impatto negativo che avrebbe potuto esercitare sulle ricerche condotte dalla società americana Pfizer con il partner tedesco, BioNTech, per lo sviluppo del vaccino COVID).

In un contesto di straordinaria complessità nel quale è necessario contemperare in maniera bilanciata tanti e diversi interessi concomitanti **è quanto mai dunque urgente addivenire alla stipula di un accordo UE-USA che disciplini in maniera chiara le modalità, i limiti e le garanzie sottese al trasferimento dei dati e all'accesso agli stessi da parte delle autorità e garantisca quella certezza del diritto indispensabile per garantire un ecosistema sicuro per gli individui ed al contempo favorevole agli investimenti delle imprese.**

3. SICUREZZA, CLOUD E DIGITALE IN ITALIA.

COME ACCELERARE LA TRASFORMAZIONE DIGITALE E PROMUOVERE LA COMPETITIVITÀ NAZIONALE

3.1 IL QUADRO NORMATIVO NAZIONALE SULLA SICUREZZA CIBERNETICA

3.1.1 Dal recepimento della direttiva NIS all'istituzione del Perimetro Nazionale di Sicurezza Cibernetica

Il tema della sicurezza dei servizi cloud non può prescindere dall'analisi del quadro normativo vigente ed in corso di definizione.

Dopo l'adozione, nel 2017, di alcuni provvedimenti propedeutici o preparatori all'adozione delle misure prescritte dalla direttiva NIS quali il Decreto del Presidente del Consiglio dei Ministri 17 febbraio 2017, "*Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali"* (il cosiddetto "DPCM Gentiloni"), che ha tra l'altro riorganizzato l'architettura per la protezione dello spazio cibernetico nazionale, ed il nuovo "*Piano nazionale per la protezione cibernetica e la sicurezza informatica*" (marzo 2017), che ha aggiornato gli indirizzi e le direttive stabilite col precedente Piano del 2013 proprio in vista delle indicazioni presenti nella direttiva NIS (attualmente in fase di modifica a livello UE), con il **D.Lgs. n. 65 del 18 maggio 2018** l'Italia ha recepito la direttiva NIS (attualmente sottoposta a procedura di revisione). Con tale decreto, in particolare, sono state adottate le seguenti misure: adozione di un elenco nazionale degli operatori di servizi essenziali presso il MISE; individuazione (all'art. 5) degli elementi da considerare ai fini della determinazione della rilevanza degli effetti negativi; declinazione dei contenuti della strategia nazionale; suddivisione delle competenze tra 5 ministeri (Sviluppo economico, Infrastrutture e trasporti, Economia, Salute e Ambiente) (art. 7) – incaricando il Dipartimento delle informazioni per la sicurezza (DIS) di svolgere le funzioni di punto di contatto unico ed istituendo, presso la Presidenza del Consiglio dei Ministri, un unico Computer Security Incident Response Team, detto CSIRT italiano –; riproposizione degli specifici obblighi in materia di sicurezza gravanti sugli operatori di servizi essenziali; prescrizione di obblighi di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali e declinazione di un set di sanzioni in relazione alle diverse possibili infrazioni che possono essere poste in essere dagli operatori di servizi essenziali e dai fornitori di servizi digitali, fino ad un massimo di € 150.000. Quanto al CSIRT, cui spettano importantissime funzioni tra cui la definizione delle procedure per la prevenzione e la gestione dei *cyber incidents* e la ricezione delle segnalazioni di incidente, nel mese di maggio si è provveduto all'ufficiale accorpamento del Computer Security Incident Response Team nel Dipartimento delle Informazioni per la Sicurezza (DIS).

In questo quadro generale si inquadra la disciplina relativa alla *golden share*, poi *golden power*. *La golden share*, in particolare, è propria della tradizione britannica e fa riferimento alla conservazione, da parte dello Stato, nell'ambito di procedure di privatizzazione di imprese in origine pubbliche, di una partecipazione azionaria con poteri esorbitanti rispetto a quelli spettanti ad un normale azionista.

Tale strumento è stato introdotto nel nostro ordinamento con il **decreto legge 31 maggio 1994, n. 332, convertito con legge 30 luglio 1994, n. 474** e rivisto, a seguito della Comunicazione n. C220 del 19/07/1997 della Corte di Giustizia – con la quale è stato precisato che l'esercizio di tali poteri deve comunque essere attuato senza discriminazioni, essere fondato su "*criteri obiettivi, stabili e resi pubblici*" ed essere giustificato da "*motivi imperiosi di interesse generale*" – con il **decreto legge 15 marzo 2012 n. 21, convertito con modificazioni con la legge n. 56 del 2012.** Tale decreto ha ridisegnato il quadro normativo segnando il passaggio dalla golden share al c.d. "***golden power***", locuzione con cui si fa riferimento ad una serie di poteri esercitabili nei settori della difesa e della sicurezza nazionale, nonché in alcuni ambiti di attività definiti di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni rispetto a tutte le società, sia pubbliche che private, che svolgono attività considerate di rilevanza strategica.

Con riferimento all'esercizio dei poteri speciali nei comparti della sicurezza e della difesa, la normativa esige la sussistenza di una **minaccia di grave pregiudizio per gli interessi essenziali della difesa e della sicurezza nazionale**. Al fine di valutare la minaccia di grave pregiudizio agli interessi essenziali della difesa e della sicurezza nazionale, il Governo considera, tenendo conto dell'oggetto della delibera, la rilevanza strategica dei beni o delle imprese oggetto di trasferimento, l'idoneità dell'assetto risultante dalla delibera o dall'operazione a garantire l'integrità del sistema di difesa e sicurezza nazionale, la sicurezza delle informazioni relative alla difesa militare, gli interessi internazionali dello Stato, la protezione del territorio nazionale, delle infrastrutture critiche e strategiche e delle frontiere, nonché gli elementi di cui al comma 3 e, nello specifico: a) l'adeguatezza, tenuto conto anche delle modalità di finanziamento dell'acquisizione, della capacità economica, finanziaria, tecnica e organizzativa dell'acquirente nonché del progetto industriale, rispetto alla regolare prosecuzione delle attività, al mantenimento del patrimonio tecnologico, anche con riferimento alle attività strategiche chiave, alla sicurezza e alla continuità degli approvvigionamenti, oltre che alla corretta e puntuale esecuzione degli obblighi

contrattuali assunti nei confronti di pubbliche amministrazioni, direttamente o indirettamente, dalla società le cui partecipazioni sono oggetto di acquisizione, con specifico riguardo ai rapporti relativi alla difesa nazionale, all'ordine pubblico e alla sicurezza nazionale; b) l'esistenza, tenuto conto anche delle posizioni ufficiali dell'Unione europea, di motivi oggettivi che facciano ritenere possibile la sussistenza di legami fra l'acquirente e paesi terzi che non riconoscono i principi di democrazia o dello Stato di diritto, che non rispettano le norme del diritto internazionale o che hanno assunto comportamenti a rischio nei confronti della comunità internazionale, desunti dalla natura delle loro alleanze, o hanno rapporti con organizzazioni criminali o terroristiche o con soggetti ad esse comunque collegati.

Dal punto di vista procedurale, il decreto legge ha disciplinato puntualmente **termini e procedure da osservare** per l'invio dell'informativa da parte dell'impresa e l'esercizio del potere di veto da parte del Presidente del Consiglio (15 gg. con possibilità di sospensione per una sola volta nel caso di richieste di informazioni ulteriori all'impresa da fornire entro 10 gg.), ricollegando all'inutile decorso di tale termine, il silenzio assenso e, dunque, la possibilità di procedere con l'operazione oggetto di notifica. Dalla violazione di tale disciplina la normativa fa discendere la nullità delle delibere o degli atti adottati, la facoltà, per il Governo, di ingiungere alla società ed all'eventuale controparte di ripristinare a proprie spese la situazione anteriore, nonché l'imposizione di una sanzione amministrativa pecuniaria fino al doppio del valore dell'operazione e comunque non inferiore all'uno per cento del fatturato cumulato realizzato dalle imprese coinvolte nell'ultimo esercizio per il quale sia stato approvato il bilancio.

Successivamente, con il **decreto legge n. 148/2017**, convertito con legge n. 172/2017, il legislatore è intervenuto sulla disciplina dettata dal decreto legge n. 21/2012, estendendo l'esercizio dei poteri speciali applicabili nei settori dell'energia, delle comunicazioni e dei trasporti agli asset "ad alta intensità tecnologica" riferendosi, a titolo esemplificativo: 1) alle infrastrutture "critiche" o "sensibili", tra cui immagazzinamento e gestione dati e strutture finanziarie; 2) alle tecnologie "critiche", compresa l'intelligenza artificiale, la robotica, i semiconduttori, le tecnologie con potenziali applicazioni a doppio uso, la sicurezza in rete, la tecnologia spaziale o nucleare; 3) alla sicurezza dell'approvvigionamento di input "critici"; 4) all'accesso a informazioni "sensibili" o capacità di controllare le informazioni "sensibili".

Tale elencazione offre la misura dell'importanza dell'intervento;

l'ampliamento del perimetro di azione ha rafforzato i poteri speciali del Governo ampliandone notevolmente il campo d'azione e rendendo certamente più difficoltosa la possibilità per gli operatori di prevedere le ipotesi - che secondo la disciplina previgente erano poche e facilmente verificabili (in particolare occorreva verificare che la società acquisenda o operasse nei settori della difesa militare e della sicurezza nazionale o possedesse uno dei pochi e puntualmente identificati asset nei settori dell'energia, dei trasporti e delle comunicazioni) - di soggezione a tali poteri speciali. A ciò si aggiungono altre due importanti novità, ossia che la disciplina di cui al decreto legge n. 148 trova applicazione principalmente nel caso in cui l'acquisto a qualsiasi titolo di partecipazioni in società che detengono gli asset "strategici" avvenga da parte di un soggetto esterno all'Unione europea e che il Governo può esercitare i poteri speciali non solo quando questo acquisto comporti una minaccia di grave pregiudizio agli interessi "essenziali" dello Stato (e, cioè, relativi alla sicurezza e al funzionamento delle reti e degli impianti e alla continuità degli approvvigionamenti), ma anche quando esso possa minare la sicurezza o l'ordine pubblico.

Il quadro normativo descritto è stato ulteriormente rivisto ad opera del **D.L. 25 marzo 2019, n. 22** (c.d. **Decreto Brexit**), convertito con modificazioni dalla Legge 20 maggio 2019, n. 41, che ha aggiunto all'ambito previsto dalla legge n. 56/2012 **l'art. 1 bis**, rubricato "*Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G*", con il quale sono stati inclusi, nelle attività di rilevanza strategica per il sistema di difesa e sicurezza nazionale, i servizi di comunicazione elettronica a banda larga basati sulla tecnologia 5G.

Da ultimo, la disciplina del golden power ha subito un'ulteriore ridefinizione ad opera del **D.P.C.M. n. 179 del 18 dicembre 2020,** con il quale, in attuazione di quanto previsto dall'art. 4 del Reg. n. 452/2019 che ha istituito un quadro per il controllo degli investimenti esteri diretti nell'Unione, sono stati individuati beni e rapporti di rilevanza strategica per l'interesse nazionale ulteriori nel settore dell'energia, dell'acqua, della salute, nel trattamento, nell'archiviazione e in materia di accesso e controllo di dati e di informazioni sensibili (tra cui figura anche il *Cloud Computing*), nel settore delle infrastrutture elettorali, nei settori dell'intelligenza artificiale, della robotica, dei semiconduttori, della cybersicurezza, delle nanotecnologie e delle biotecnologie, delle infrastrutture e delle tecnologie aerospaziali non militari, nel settore agroalimentare, nel settore della libertà e del pluralismo dei media.

Con il **D.P.C.M. n. 180 del 23 dicembre 2020** è stato invece adottato un Regolamento per l'individuazione degli **attivi di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni per l'esercizio dei poteri speciali** di cui all'art. 2 del D.L. 21/2012 (convertito con legge n. 56/2012). Per quanto concerne il settore delle comunicazioni, gli attivi di rilevanza strategica sono individuati nelle reti dedicate e nella rete di accesso pubblica agli utenti finali in connessione con le reti metropolitane, i router di servizio e le reti a lunga distanza, nonché negli impianti utilizzati per la fornitura dell'accesso agli utenti finali dei servizi rientranti negli obblighi del servizio universale e dei servizi a banda larga e ultra-larga, e nei relativi rapporti convenzionali, inclusi gli elementi dedicati, anche laddove l'uso non sia esclusivo, per la connettività (fonia, dati e video), la sicurezza, il controllo e la gestione relativi a reti di accesso di telecomunicazioni in postazione fissa.

Il 21 settembre 2019 segna un momento cruciale nella definizione del quadro normativo nazionale a tutela della sicurezza cibernetica. In tale data, infatti, è stato varato il **decreto legge n. 105/2019**, convertito con la legge n. 133/2019, recante **disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica.** Si tratta di un intervento di rilevanza straordinaria che all'art. 1 istituisce il perimetro di sicurezza nazionale cibernetica al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori (pubblici e privati aventi una sede nel territorio nazionale), da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. La medesima disposizione prevede l'adozione di due distinti DPCM, su proposta del Comitato interministeriale per la sicurezza della Repubblica (CISR), da sottoporre al parere delle Commissioni parlamentari competenti per materia (da rendere entro 30 gg.) e da aggiornare, secondo le procedure di seguito descritte, con cadenza almeno biennale: il primo, ai sensi del comma 2, da adottare entro **4 mesi** dalla data di entrata in vigore della legge di conversione (21 novembre 2019), su proposta del Comitato interministeriale per la sicurezza della Repubblica, con il quale individuare **le amministrazioni pubbliche, gli enti e gli operatori inclusi nel perimetro di sicurezza nazionale cibernetica e tenuti al rispetto delle misure e degli obblighi previsti**, **definire i criteri** con i quali i soggetti individuati predispongono e aggiornano con cadenza

almeno annuale un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza, comprensivo della relativa architettura e componentistica[19]; il secondo, da adottare entro **10 mesi** dall'entrata in vigore della legge di conversione del decreto legge, per la **definizione delle procedure di notifica degli incidenti** aventi impatto su reti, sistemi informativi e servizi informatici al Gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) italiano[20], **l'individuazione di misure** – da parte di MISE e Presidenza del Consiglio, d'intesa con il Ministero della difesa, il Ministero dell'interno, il Ministero dell'economia e delle finanze e il Dipartimento delle informazioni per la sicurezza – **volte a garantire elevati livelli di sicurezza delle reti, dei sistemi informativi e dei servizi informatici** relative alla struttura organizzativa preposta alla gestione della sicurezza, alle politiche di sicurezza e alla gestione del rischio, alla mitigazione e gestione degli incidenti e alla loro prevenzione, anche attraverso interventi su apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza, alla protezione fisica e logica e dei dati, all'integrità delle reti e dei sistemi informativi, alla gestione operativa, ivi compresa la continuità del servizio, al monitoraggio, test e controllo, alla formazione e consapevolezza ed all'affidamento di forniture di beni, sistemi e servizi di Information and Communication Technology (ICT), anche mediante definizione di caratteristiche e requisiti di carattere generale (di standard e di eventuali limiti).

La medesima disposizione, al comma 6, prevede l'adozione di un terzo regolamento, entro **dieci mesi** dalla data di entrata in vigore della legge di conversione del presente decreto, per la disciplina delle procedure, delle modalità ed i termini con i quali le **centrali di committenza che intendano procedere all'affidamento di forniture di**

[19] Quanto alla procedura di trasmissione di tali elenchi, la norma fissa in sei mesi dalla data di entrata in vigore del DPCM il termine per la trasmissione alla Presidenza del Consiglio ed al MISE di tali elenchi che da questi ultimi vengono inoltrati al Dipartimento delle informazioni per la sicurezza, anche per le attività di prevenzione, preparazione e gestione di crisi cibernetiche affidate al Nucleo per la sicurezza cibernetica, nonché all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione.

[20] Una volta ricevute le notifiche, la norma dispone il loro tempestivo inoltro, da parte del Gruppo di intervento, al Dipartimento delle informazioni per la sicurezza anche per le attività demandate al Nucleo per la sicurezza cibernetica ed il successivo inoltro, da parte di quest'ultimo, all'organo del Ministero dell'interno per la sicurezza e la regolarità dei servizi di telecomunicazione nonché alla Presidenza del Consiglio dei ministri, se provenienti da un soggetto pubblico o da un soggetto di cui all'articolo 29 del decreto legislativo 7 marzo 2005, n. 82, ovvero al Ministero dello sviluppo economico, se effettuate da un soggetto privato

beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici appartenenti a categorie individuate, sulla base di criteri di natura tecnica, con decreto del Presidente del Consiglio dei ministri, da adottare entro dieci mesi dalla data di entrata in vigore della legge di conversione del decreto, **danno comunicazione di tale decisione al Centro di valutazione e certificazione nazionale** (CVCN)[21], istituito presso il Ministero dello sviluppo economico ed **i soggetti individuati quali fornitori di beni, sistemi e servizi destinati alle reti, ai sistemi informativi e ai servizi informatici assicurano al CVCN la propria collaborazione** per l'effettuazione delle attività di test sostenendone gli oneri. Si noti che il CVCN ha poteri di segnalazione rispetto all'eventuale mancata collaborazione al MISE, nel caso di forniture a soggetti privati ed alla Presidenza del Consiglio nel caso di soggetti pubblici.

Con riferimento alle reti 5G, poi, l'art. 4 *bis* ha modificato il decreto legge n. 21 del 2012 in tema di poteri speciali del Governo nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni, ha puntualmente definito gli **elementi che il Governo deve considerare nella valutazione dell'acquirente** ed ha operato una serie di modifiche alle **modalità e delle tempistiche associate agli obblighi di notifica[22].**

3.1.2 L'iter di attuazione della disciplina sul perimetro di sicurezza: l'adozione del primo DPCM e la proposta di DPR su CVCN e CV

Sebbene in ritardo rispetto alla *timeline* delineata dal D.L. n. 105/2019, complice, certamente, anche l'emergenza sanitaria ancora in atto, lo scorso 21 ottobre è stato pubblicato sulla Gazzetta Ufficiale il decreto del Presidente del Consiglio del Consiglio dei Ministri 30 luglio 2020, n. 131 che ha formalmente dato avvio all'articolata e complessa procedura di attuazione della

[21] Il CVCN ha la facoltà, entro 45 gg. dalla ricezione della comunicazione (in caso di inutile decorso, si può procedere con la procedura di affidamento), prorogabili di quindici giorni, una sola volta, in caso di particolare complessità, di effettuare verifiche preliminari ed imporre condizioni e test di hardware e software da compiere anche in collaborazione con le centrali di committenza (e concludere entro 60 giorni), secondo un approccio gradualmente crescente nelle verifiche di sicurezza (nel caso di apposizione di condizioni o richieste di test i bandi devono contenere condizioni sospensive o risolutive collegate a quanto richiesto o apposto dal CVCN).

[22] Si prevede, nello specifico, la notifica alla Presidenza del Consiglio dei Ministri, entro dieci giorni dalla conclusione di un contratto o accordo, di un'informativa completa da parte dell'impresa che ha acquisito. È fissato in trenta giorni, prorogabile di ulteriori venti giorni, il termine per l'esercizio del potere di veto o l'imposizione di specifiche prescrizioni da parte del Presidente del Consiglio.

disciplina del perimetro di sicurezza cibernetica. Si tratta del primo atto, composto da 12 articoli, suddivisi in quattro Capi, con cui, sulla base anche di quanto rilevato dal Consiglio di Stato e dalle Camere nei pareri rilasciati rispettivamente nel mese di maggio e di luglio, sono state definite le **modalità e i criteri procedurali di individuazione dei soggetti** (amministrazioni pubbliche, enti e operatori pubblici e privati) inclusi nel perimetro di sicurezza nazionale cibernetica e che, pertanto, saranno tenuti al rispetto delle misure e degli obblighi previsti dal decreto-legge e sono stati individuati i **criteri con i quali i soggetti inclusi nel perimetro predispongono e aggiornano l'elenco delle reti, dei sistemi informativi e dei servizi informatici** di rispettiva pertinenza, comprensivo della relativa architettura e componentistica.

Tale decreto, in particolare, ha fornito una serie di importanti definizioni tra cui quella di "***pregiudizio per la sicurezza nazionale***", inteso come danno o pericolo di danno all'indipendenza, all'integrità o alla sicurezza della Repubblica e delle istituzioni democratiche poste dalla Costituzione a suo fondamento, ovvero agli interessi politici, militari, economici, scientifici e industriali dell'Italia, conseguente all'interruzione o alla compromissione di una funzione essenziale dello Stato o di un servizio essenziale serie e di "***analisi del rischio***", intendendo, in particolare, un processo che consente di identificare i fattori di rischio di un incidente, valutandone la probabilità e l'impatto potenziale sulla continuità, sulla sicurezza o sulla efficacia della funzione essenziale o del servizio essenziale, e conseguentemente di trattare tale rischio individuando ed implementando idonee misure di sicurezza. Molto rilevanti le definizioni tese all'individuazione, dal punto di vista tecnico, dell'ambito applicativo del decreto e, nello specifico, quella di **compromissione** ed **incidente**, nonché quella di **rete, sistema informativo, bene ICT ed architettura componentistica**.

Gli artt. 2 e 3 contribuiscono a delineare le modalità per **l'individuazione dei soggetti** inclusi nel perimetro oggetto del successivo Capo II, declinando i concetti di funzione e servizio essenziale. In particolare, in ossequio ai criteri generali fissati dal decreto legge, il decreto include nel concetto di **funzione essenziale** le attività tese ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia e la funzionalità dei sistemi economico e finanziario, e dei trasporti. Rientrano, invece, nel concetto di **servizio essenziale**, i soggetti che svolgono attività: a) strumentali all'esercizio di funzioni essenziali dello Stato;

b) necessarie per l'esercizio e il godimento dei diritti fondamentali; c) necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; d) ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

Quanto ai **settori di attività** in cui operano i soggetti da inserire nel perimetro di sicurezza cibernetica, l'art. 3 del decreto, facendo salva l'estensione ad altri settori in sede di aggiornamento, aderendo agli stimoli formulati dalla Camere, individua i soggetti operanti nel settore governativo, concernente, nell'ambito delle attività dell'amministrazione dello Stato, le attività delle amministrazioni CISR, nonché gli ulteriori soggetti, pubblici o privati, operanti nei seguenti settori di attività, ove non ricompresi in quello governativo: a) interno; b) difesa; c) spazio e aerospazio; d) energia; e) telecomunicazioni; f) economia e finanza; g) trasporti; h) servizi digitali; i) tecnologie critiche; l) enti previdenziali/lavoro.

Il Capo II, nel fissare le modalità di individuazione dei soggetti inclusi nel perimetro di sicurezza cibernetica, definisce le modalità ed i criteri procedurali di individuazione dei soggetti inclusi nel perimetro di sicurezza nazionale cibernetica, attribuendo alle amministrazioni competenti il compito di: 1**) identificare le funzioni e servizi essenziali** (di diretta pertinenza o esercitati da soggetti vigilati o da operatori pubblici e privati) **che dipendono da reti, sistemi informativi o servizi informatici la cui interruzione o compromissione possa arrecare un pregiudizio per la sicurezza nazionale**; 2) valutare, con riguardo agli **effetti di una interruzione della funzione o servizio essenziale**, estensione territoriale, numero e tipologia di utenti potenzialmente interessati, livelli di servizio garantiti e possibili ricadute economiche, mentre, in relazione agli **effetti della compromissione** dello svolgimento della funzione o servizio essenziale, le conseguenze della perdita di disponibilità, integrità o riservatezza dei dati e delle informazioni trattati, con riferimento alla tipologia e quantità degli stessi, alla loro sensibilità e allo scopo cui sono destinati; 3) **valutare la possibile mitigazione** – rispetto all'interruzione o alla compromissione dello svolgimento della funzione o servizio essenziale – considerando il tempo necessario per ripristinare lo svolgimento in condizioni di sicurezza, tenendo altresì conto della possibilità che la funzione o il servizio essenziale possano essere assicurati con modalità prive di supporto informatizzato, anche temporaneamente, ovvero parzialmente da altri soggetti.

Le amministrazioni individuano, poi, le funzioni o servizi essenziali per i quali sulla base dei suddetti criteri e delle conseguenti valutazioni - in caso di interruzione o compromissione – "*il pregiudizio per la sicurezza nazionale è ritenuto massimo e le possibilità di mitigazione minime*" e operano una graduazione in scala crescente. In fase di prima applicazione, sono individuati i soggetti titolari di tali funzioni o servizi per i quali un'interruzione delle relative attività comporterebbe il mancato svolgimento della funzione o del servizio. Le varie amministrazioni, all'esito delle descritte valutazioni, stilano un **elenco** di soggetti che viene trasmesso al CISR e al CSIR tecnico e poi formalizzato in un atto amministrativo, adottato e periodicamente aggiornato dal Presidente del Consiglio dei ministri, su proposta del CISR. È compito del **Dipartimento delle informazioni per la sicurezza (DIS)** darne comunicazione alle amministrazioni interessate.

Lo stesso decreto prevede poi l'istituzione di un **Tavolo interministeriale** per l'attuazione del perimetro di sicurezza nazionale cibernetica con funzioni di supporto del CISR, presieduto da un vice direttore del DIS, composto da due rappresentanti di ciascuna amministrazione CISR, un rappresentante per ciascuna delle due agenzie di informazioni (Agenzia informazioni e sicurezza esterna – AISE e Agenzia informazioni e sicurezza interna – AISI) e due rappresentanti dei ministeri di volta in volta interessati che sono chiamati a partecipare alle riunioni, anche su loro richiesta motivata, in relazione agli argomenti da trattare di cui almeno uno, in adesione ai rilievi espressi da Consiglio di Stato e Camere, in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica, che si riunisca periodicamente, e comunque almeno una volta ogni 6 mesi (senza alcun gettone di presenza, compenso o rimborso spese o altri emolumenti per la partecipazione alle riunioni).

Quanto, invece, ai criteri per la predisposizione e l'aggiornamento degli elenchi delle reti, dei sistemi informativi e dei servizi informatici il decreto prescrive ai soggetti inclusi nel perimetro di individuare i beni ICT necessari a svolgere la funzione essenziale o il servizio essenziale valutando, nello specifico, l'impatto di un incidente sul bene ICT (in termini sia di limitazione della operatività del bene stesso, sia di compromissione della disponibilità, integrità, o riservatezza dei dati e delle informazioni da esso trattati, ai fini dello svolgimento della funzione o del servizio essenziali) e la dipendenza con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti, ivi compresi quelli utilizzati per fini di manutenzione e gestione e predisporre ed aggiornare, con cadenza

almeno annuale, l'elenco di beni ICT di rispettiva pertinenza, con l'indicazione delle reti, dei sistemi informativi e dei servizi informatici che li compongono. In fase di prima applicazione, il decreto circoscrive tali adempimenti ai beni ICT che, in caso di incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale o una compromissione degli stessi con effetti irreversibili sotto il profilo della integrità o della riservatezza dei dati e delle informazioni.

L'art. 9 fissa in **sei mesi** dal ricevimento della comunicazione di avvenuta iscrizione nell'elenco il termine per procedere alla trasmissione degli elenchi appena descritti alla Presidenza del Consiglio o al Ministero dello sviluppo economico (ai quali sono attribuiti poteri di ispezione e verifica) e prevede che tale trasmissione avvenga mediante una piattaforma digitale costituita presso il DIS anche per le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al NSC, nell'ambito delle risorse finanziarie, umane e strumentali previste a legislazione vigente.

Se *l'iter* di adozione del primo DPCM si è concluso con la pubblica dello stesso in G.U. il 21 ottobre scorso, è ancora *in itinere* la procedura di adozione dello **schema di regolamento** indispensabile ai fini dell'operatività del CVCN, che in attuazione dell'art. 1 c. 6 del decreto istitutivo del perimetro, definisce le procedure, le modalità ed i termini da seguire ai fini delle valutazioni da parte dello stesso CVCN e dei centri di valutazione del Ministero dell'interno e del Ministero della difesa (CV), ciascuno nell'ambito delle rispettive competenze, in ordine all'acquisizione, da parte dei soggetti inclusi nel perimetro, di oggetti di fornitura rientranti nelle categorie individuate sulla base dei criteri dallo stesso indicati, i criteri di natura tecnica per l'individuazione delle categorie a cui si applica la procedura di valutazione delineata, le procedure, le modalità ed i termini con cui le Autorità competenti effettuano le attività di verifica e ispezione ai fini dell'accertamento del rispetto degli obblighi stabiliti nel decreto-legge e nei decreti attuativi.

La proposta, in particolare, si compone di 4 Capi che definiscono con puntualità le tipologie di beni, sistemi e servizi ICT oggetto della valutazione da parte del CVCN, le modalità ed i contenuti delle comunicazioni da effettuare in favore di CVCN o CV da parte dei soggetti inclusi nel perimetro, le tipologie di valutazioni, test e verifiche realizzabili, nonché le attività di verifica ed ispezione cui possono essere sottoposti i soggetti inclusi nel perimetro.

Molto rilevanti, in particolare, le disposizioni contenute nell'art. 4 che entra nel vivo dell'attività valutativa di CVCV e CV,

descrivendo il **procedimento di verifica e valutazione** dell'analisi documentale contenuta nella comunicazione, individuando le singole fasi ed i relativi termini. Nello specifico, la procedura si articola in: 1) verifiche preliminari, imposizione di condizioni e di test di hardware e di software da inserire nelle clausole del bando di gara o del contratto, da compiersi entro il termine di quarantacinque giorni dalla comunicazione (prorogabile una sola volta di quindici giorni nei casi di particolare complessità ed in particolare, quando l'oggetto di valutazione è costituito da beni, sistemi e servizi ICT integrati tra di loro, è basato su tecnologie di recente sviluppo per le quali non si dispone di metodologie di test consolidate o interagisce con componenti che erogano altre funzioni essenziali o servizi essenziali); 2) fase di preparazione all'esecuzione dei test, esecuzione dei test di hardware e di software e definizione di eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro; 3) esecuzione dei test di hardware e di software e definizione di eventuali prescrizioni di utilizzo al soggetto incluso nel perimetro (da concludersi entro sessanta giorni a partire dalla data in cui il soggetto incluso nel perimetro comunica che l'oggetto della valutazione è reso fisicamente disponibile per i test al CVCN o ai CV).

Lo schema, in una logica di semplificazione, prevede un meccanismo di **silenzio-assenso** per cui inutilmente decorsi i termini sopra indicati senza che CVCV o CV si siano pronunciati, i soggetti inclusi nel perimetro possono proseguire nella procedura di affidamento e nell'esecuzione del contratto.

La medesima disposizione prevede la condivisione da parte di CVCN, con i CV e i Laboratori accreditati di prova, indipendente dai soggetti inclusi nel perimetro e dai fornitori, che ha ottenuto l'accreditamento dal CVCN (LAP), le metodologie per l'effettuazione dei test, di cui si prescrive di garantire la riservatezza.

Quanto all'**individuazione di condizioni e test**, l'art. 5 prescrive a CVCV e CV di tener conto, nell'individuazione dei test da eseguire, dell'analisi del rischio e dei livelli di severità, demandando l'individuazione test corrispondenti ai livelli di severità derivanti dall'analisi del rischio all'atto che il CVCV dovrà adottare entro 60 gg. dall'entrata in vigore di tale decreto. Quanto alle tipologie di test richiedibili, si tratta di test di corretta implementazione delle funzionalità di sicurezza allo scopo di verificare che queste ultime si comportino secondo le relative specifiche di progetto e test di intrusione a supporto dell'analisi di vulnerabilità.

Quanto al **fornitore**, nel caso di imposizione di test, lo schema prescrive l'esecuzione, da parte dello stesso, di una serie di attività propedeutiche e indispensabili alla loro

esecuzione ed in particolare: a) fornire evidenza dell'idoneità delle funzioni di sicurezza e delle loro configurazioni a soddisfare i requisiti di sicurezza; b) provvedere all'allestimento di un ambiente di test adeguatamente rappresentativo della realtà di esercizio presso il laboratorio o, se necessario, presso il fornitore o presso il soggetto del perimetro; c) fornire una descrizione generale dell'architettura dell'oggetto di valutazione e delle sue funzioni; d) fornire una descrizione delle funzionalità di sicurezza implementate nell'oggetto di valutazione; e) fornire una descrizione di test funzionali e di sicurezza già eseguiti dal fornitore o dal produttore o da una parte terza, comprensivi dei relativi risultati.

3.1.3 Il DL Semplificazioni

In un contesto normativo ancora in corso di definizione, si inquadra il **decreto legge 16 luglio 2020, n. 76**, convertito con modificazioni dalla legge n. 120/2020 **(c.d. Decreto Semplificazioni)** recante misure urgenti per la semplificazione e l'innovazione digitale. Si tratta di un intervento di grandissima importanza con il quale sono state adottate misure impattanti su moltissimi settori e discipline (es. è stata rivista la disciplina in materia di contratti pubblici contenuta nel Codice degli Appalti, sono stati introdotti strumenti di semplificazione e altre misure in materia edilizia e per la ricostruzione pubblica nelle aree colpite da eventi sismici, sono state disposte ed individuate semplificazioni procedimentali e responsabilità, etc.) tra cui spicca per rilevanza, ai fini della presente analisi, il Titolo III, recante misure di semplificazione per il sostegno e la diffusione dell'amministrazione digitale (artt. 23 *bis* - 37).

Le disposizioni in esame, infatti, hanno introdotto misure tese a favorire l'affermazione della cittadinanza digitale e l'accesso ai servizi digitali, hanno disposto la semplificazione della disciplina in materia di conservazione dei documenti informatici e gestione dell'identità digitale, hanno introdotto una piattaforma per la notificazione digitale degli atti della pubblica amministrazione ed introdotto, all'art. 32, il Codice di condotta tecnologica, uno strumento importante che disciplina le modalità di progettazione, sviluppo e implementazione dei progetti, sistemi e servizi digitali delle amministrazioni pubbliche, nel rispetto del principio di non discriminazione, dei diritti e delle libertà fondamentali delle persone e della disciplina in materia di perimetro nazionale di sicurezza cibernetica e che dovrebbe garantire il coordinamento nello sviluppo dei sistemi informativi e dell'offerta dei servizi in rete delle pubbliche amministrazioni su tutto il

territorio nazionale. Molto importante anche l'istituzione, disposta dall'art. 34, di una **Piattaforma Digitale Nazionale Dati (PDND)**, gestita dalla Presidenza del Consiglio, finalizzata a favorire, mediante un'infrastruttura tecnologica che rende possibile l'interoperabilità, la conoscenza e l'utilizzo del patrimonio informativo detenuto, per finalità istituzionali, nonché la condivisione dei dati tra i soggetti che hanno diritto ad accedervi ai fini della semplificazione degli adempimenti amministrativi dei cittadini e delle imprese, in conformità alla disciplina vigente e agli accordi quadro (con esclusione dei dati attinenti a ordine e sicurezza pubblici, difesa e sicurezza nazionale, polizia giudiziaria e polizia economico-finanziaria e la previsione di meccanismi chiari di responsabilità per eventuali inadempimenti rispetto a tali obblighi a carico dei dirigenti competenti. La stessa disposizione affida poi a DPCM l'individuazione della **strategia nazionale dati** che dovrà identificare le tipologie, i limiti, le finalità e le modalità di messa a disposizione, su richiesta della Presidenza del Consiglio dei ministri, dei dati aggregati e anonimizzati dando priorità ai dati riguardanti gli studenti del sistema di istruzione e di istruzione e formazione professionale ai fini della realizzazione del diritto-dovere all'istruzione e alla formazione e del contrasto alla dispersione scolastica e formativa.

L'art. 35 contiene, invece, la disposizione centrale nell'ambito della presente analisi, ossia la previsione che, al fine di tutelare l'autonomia tecnologica del Paese, consolidare e mettere in sicurezza le infrastrutture digitali delle pubbliche amministrazioni, garantendo, al contempo, la qualità, la sicurezza, la scalabilità, l'efficienza energetica, la sostenibilità economica e la continuità operativa dei sistemi e dei servizi digitali, assegna alla Presidenza del Consiglio dei ministri la promozione dello sviluppo di **un'infrastruttura ad alta affidabilità localizzata sul territorio nazionale** per la razionalizzazione e il consolidamento dei Centri per l'elaborazione delle informazioni (CED) destinata a tutte le pubbliche amministrazioni.

Viene così introdotto l'obbligo per le pubbliche amministrazioni centrali di migrare i loro Centri elaborazione dati (Ced), che non hanno i requisiti di sicurezza fissati dall'Agenzia per l'Italia digitale (AgID), verso un'infrastruttura ad alta affidabilità, localizzata in Italia, il cui sviluppo è promosso dalla Presidenza del Consiglio o, in alternativa, verso soluzioni cloud per la Pubblica Amministrazione che rispettano i principi stabiliti dall'AgID. È possibile affidare i dati anche ai Data center, che rispettano i criteri AgID, delle in house regionali concretizzando il principio di sussidiarietà tecnologica. Stesso obbligo è posto a carico

delle amministrazioni locali che sono tenute a trasferire i propri servizi nella infrastruttura promossa dalla Presidenza del Consiglio o in altra infrastruttura presente sul territorio e in possesso dei requisiti di sicurezza o, in alternativa, verso soluzioni cloud per la Pubblica Amministrazione, nel rispetto dei requisiti fissati dall'AgID.

3.2 L'IMPATTO DELLA DIGITAL TRANSFORMATION E DEL CLOUD SULLE IMPRESE E SULLE PUBBLICHE AMMINISTRAZIONI

La trasformazione digitale è in grado di portare concreti benefici all'attività economica aziendale, con risparmi significativi sulle spese operative, migliorando in modo concreto efficienza, affidabilità, sicurezza e sostenibilità. La trasformazione digitale, applicata alla gestione sia dell'energia che dell'automazione, è in grado di produrre un valore ancora più grande per le aziende e di rendere i processi più coerenti ed efficienti all'interno di un'impresa, creando un vantaggio competitivo.

Quando si parla di **trasformazione digitale, tuttavia, si intende un processo più complesso della mera adozione di tecnologie più o meno avanzate**: sarebbe più corretto parlare dell'adozione di processi, prodotti e strumenti che si servono di tecnologie digitali per adeguarsi ai nuovi comportamenti dei clienti o utenti. In particolare, il cloud sta cambiando profondamente i modelli di business, rendendo l'azienda sempre più agile nell'adattarsi alla veloce trasformazione del mercato e degli obiettivi aziendali.

Le organizzazioni che intraprendono il processo di cambiamento, rendono la struttura dei propri costi più efficiente, migliorano i processi interni e rivedono la propria organizzazione per renderla sempre più flessibile e adattabile alle richieste del mercato.

3.2.1 L'analisi sulle imprese

I benefici che sta portando la digitalizzazione nel business alle imprese sono diversi e di grande portata. Maggiore flessibilità dei processi, capacità di gestione dei clienti, efficienza attraverso la riduzione dei costi operativi, pianificazione e programmazione in tempo reale dei processi, semplificazione e razionalizzazione dei flussi informativi, valorizzazione delle risorse umane sono i canali attraverso cui passa una maggiore competitività, che si traduce in maggiori ricavi.

In particolare, molti costi, relativi ad esempio all'acquisto di hardware, software, backup dei dati, ma anche di manutenzione e spesa IT tendono a ridursi fortemente una volta

passati al cloud[23]. Inoltre, la possibilità di accedere al cloud attraverso Internet migliora la mobilità dei lavoratori, mentre collaborazioni più efficaci e la migliore gestione degli aggiornamenti delle diverse versioni – grazie alla possibilità di condividere e lavorare contemporaneamente su uno stesso documento – tendono ad essere le principali ragioni dell'impatto positivo sulla produttività dei lavoratori[24].

Ne è prova l'incremento considerevole registrato nel grado di adozione del cloud da parte delle imprese (Fig. 3.1), particolarmente accentuato tra le imprese italiane, pari nel 2020 al 59% e quasi triplicato nel giro di 4 anni, rispetto alla media europea, pari al 35%, all'incirca il doppio del dato relativo al 2016. Non solo, ma le imprese stanno anche via via passando a livelli più "elevati" di complessità dei servizi di cloud computing: l'adozione di servizi di *cloud computing* di alto livello – quali applicazioni software, software di customer relationship management (CRM) e potenza di calcolo – rappresenta ormai la gran parte delle scelte di cloud (32% delle imprese italiane contro il 21% di quelle europee).

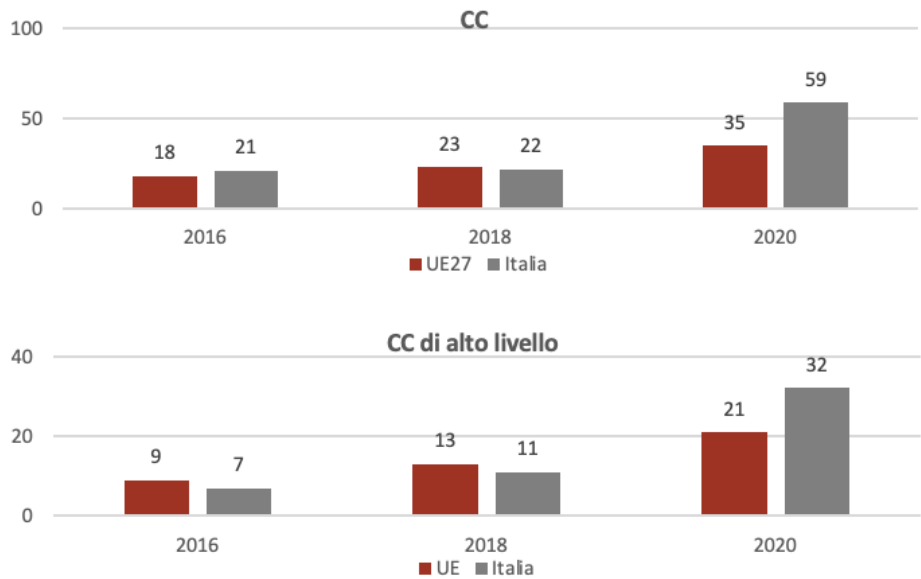


FIGURA 3.1 Adozione del cloud computing tra le imprese italiane e europee

Fonte: Eurostat

[23] ECB, "*Virtually everywhere? Digitalisation and the euro area and EU economies. Degree, effects, and key issues*", Occasional Paper Series, December 2020.

[24] Andrews et al., "*Going Digital: What determines technology diffusion among firms*?", OECD Economics Department Working Papers, n 1466, 2018.

I dati impiegati per l'analisi presentata in questa sezione sono microdati forniti da Istat. Si tratta di dati elementari raccolti nell'ambito della rilevazione sulle tecnologie dell'informazione e comunicazione nelle imprese (ICT), sviluppata congiuntamente dall'Eurostat e dagli Istituti nazionali di statistica dei paesi Ue. Il campione, costruito a partire da una popolazione di complessive 182.408 imprese, è costituito da 19.089 imprese. La rilevazione fornisce un insieme di informazioni relative all'utilizzo delle tecnologie dell'informazione nelle imprese italiane con almeno 10 addetti, tra cui l'utilizzo di servizi di enterprise resource planning (ERP), il customer relationship management (CRM) e l'analisi dei Big Data (BDA). Viene inoltre richiesto alle imprese se facciano uso di servizi di cloud computing a pagamento. Sono presenti, infine, alcune informazioni di carattere generale, quali la dimensione d'impresa per classe di addetti, l'area geografica in cui l'impresa risiede e il macrosettore di appartenenza.

Con riguardo a quest'ultimo, i macrosettori in cui sono raggruppate le imprese sono manifatturiero, energia, costruzioni e servizi non finanziari. Infine, per ciascuna impresa è indicata la classe di ricavi da vendita di beni e servizi.

Come sottolineato sopra, il **vero cambiamento è rappresentato dall'adozione di soluzioni cloud, che può rappresentare un *key enabler* della trasformazione digitale in senso ampio**. Dall'osservazione dei dati analizzati, risulta che attualmente il 30% del campione adotta soluzioni di cloud computing (Fig. 3.2), in particolare di cloud pubblico (18%). L'incidenza di imprese nelle classi di ricavi superiori (> 10 milioni di euro) è nettamente maggiore per le imprese che adottano il cloud (53,5% vs 32,6%) (Fig. 3.3).

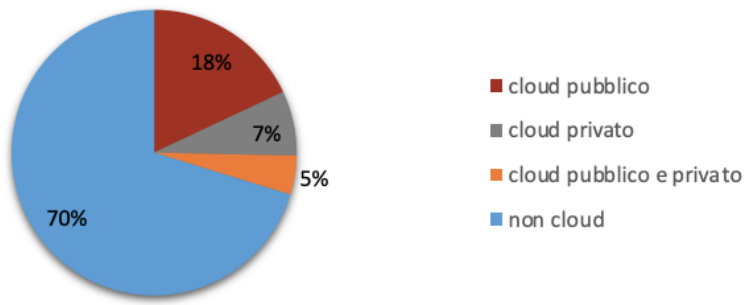


FIGURA 3.2 Diffusione del cloud computing tra le imprese (2016)

Fonte: Elaborazione I-Com su microdati Istat e dati Istat sul numero di imprese (2018)

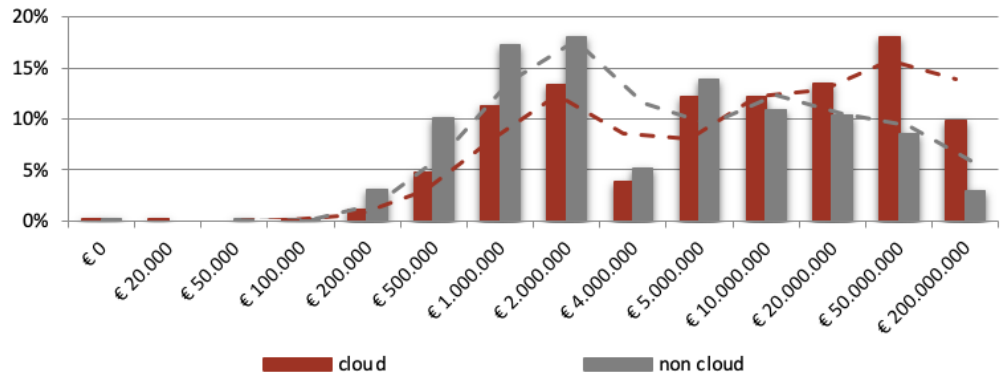


FIGURA 3.3 Distribuzione delle imprese per classe di ricavi (cloud vs non cloud) (2016)

Fonte: Elaborazione I-Com su microdati Istat

Sulla base dei risultati ottenuti impiegando un modello econometrico (per il quale si rimanda all'Appendice A), si è proceduto ad una stima del valore economico incrementale derivante dall'adozione del cloud computing da parte delle imprese che attualmente non ne fanno uso (i dettagli del metodo di stima vengono illustrati nell'Appendice B).

In particolare, si ipotizza che, qualora le imprese che attualmente non ne fanno uso cominciassero ad impiegare il cloud, una percentuale di queste imprese possa aumentare i propri ricavi, passando da una classe all'altra di fatturato[25]. Applicando il risultato ottenuto col modello descritto in Appendice

A alle imprese attualmente presenti in Italia[26], ne risulta che **l'adozione di soluzioni cloud** da parte di queste imprese **potrebbe comportare un aumento di fatturato per le imprese italiane fino a 620 miliardi di euro**, di cui oltre la metà a beneficio di piccole e medie imprese (Fig. 3.4).

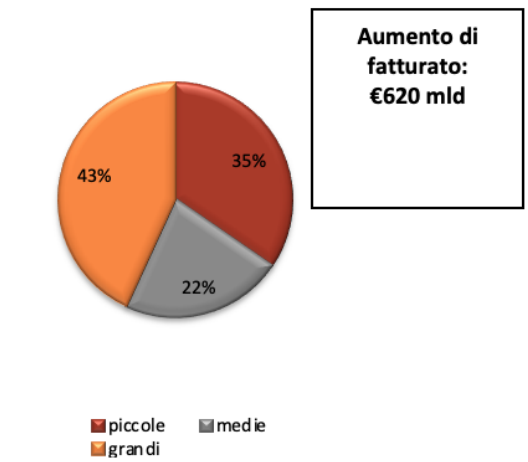


FIGURA 3.4 Aumento di fatturato stimato per le imprese italiane

Fonte: Elaborazione I-Com su microdati Istat

[25] Per i dettagli sulla percentuale di imprese e l'incremento di fatturato per impresa, si rinvia alle Appendici.

[26] Il dato sulle imprese presenti in ciascuna area geografica è aggiornato al 2018 (fonte: Istat).

Case study 5: Prysmian

Il passaggio alla piattaforma cloud ha permesso a Prysmian, impresa italiana leader mondiale nella produzione di cavi, di ottenere un'infrastruttura affidabile e scalabile a supporto delle sue attività in Nord America riducendo contestualmente i costi IT del 20%. L'azienda ha acquisito nel 2018, General Cable, una società statunitense, con la volontà allargare il proprio prodotti e fornire alla propria clientela le soluzioni più innovative e sostenibili presenti sul mercato. La fusione ha però rappresentato una sfida notevole a causa dell'estrema frammentazione dell'infrastruttura IT della società acquisita. L'integrazione dei sistemi IT era una priorità assoluta dell'azienda poiché solo così le attività aziendali potevano dirsi realmente integrate. L'ecosistema cloud di cui necessitava l'azienda doveva essere in grado di offrire risorse flessibili nonché supportare il carico di lavoro generato dal sistema SAP con cui operava la società acquisita. Inoltre, il sistema doveva essere in grado di ospitare una crescita organica delle istanze per i progetti futuri e fornire risorse aggiuntive a supporto delle attività di sviluppo e di test.

Il passaggio ad una soluzione in Cloud oltre a offrire all'azienda un'infrastruttura affidabile e scalabile a supporto del sistema SAP nordamericano ha portato un'importante evoluzione tecnologica permettendo l'introduzione delle tecnologie SAP S / 4HANA e SAP BW / 4HANA. Il sistema scelto è inoltre progettato per essere modulare, pronto a quindi a supportare anche nuove soluzioni SAP con il crescere dell'azienda.

Fonte: https://www.ibm.com/case-studies/prysmian-group-cloud-sap

3.2.2 L'analisi sulla PA

Se i benefici della trasformazione digitale per le imprese sono evidenti e di una certa portata, non meno rilevanti sono i **vantaggi che la trasformazione digitale può portare anche nella Pubblica Amministrazione**: un sistema più efficiente, la capacità di accorciare le distanze tra PA e utenti (siano essi cittadini o imprese), un maggiore e più facile accesso ai servizi.

Nel processo di trasformazione digitale della PA, un ruolo fondamentale può essere giocato dal cloud computing. Che, infatti, permette di fare cose altrimenti impossibili, come fornire servizi in aree remote (elemento cruciale per salute e scuola), creare nuove applicazioni sulla nuvola che sfruttano la dimensione online e sviluppare modelli di gestione che permettono una rapida espansione dell'utilizzo delle infrastrutture in periodi di intensa attività. **Le soluzioni di cloud computing appaiono, in effetti, ancor**

più vantaggiose per le PA di piccole dimensioni. Esse, infatti, oltre ad evitare la realizzazione e la gestione in casa delle infrastrutture IT – riducendo evidentemente in maniera drastica i costi di progettazione, installazione e gestione di queste ultime – abbattono altrettanto drasticamente i tempi di acquisizione delle tecnologie, che richiedono semplicemente la sottoscrizione di un contratto con il service provider. A ciò si aggiunga il venir meno degli investimenti nell'upgrade delle tecnologie acquisite necessari a contrastare l'obsolescenza dell'infrastruttura.

Inoltre, soluzioni simili comportano un rapido adeguamento dell'infrastruttura IT a seguito della variazione dei carichi di lavoro – con un chiaro beneficio per le PA di minori dimensioni, che non potrebbero permettersi infrastrutture IT on site oltre una certa portata – implicando una maggiore prontezza di risposta della PA alla crescente domanda di servizi. Il cloud computing può dunque fornire un importante vantaggio al settore pubblico, da un lato, consentendo riduzioni di costo, dall'altro lato, comportando un'espansione produttiva.

Data la disponibilità di soli dati aggregati a livello regionale, di seguito viene mostrata la relazione esistente tra la diffusione del cloud computing (% di amministrazioni comunali per ogni regione) e l'efficienza che la trasformazione tecnologica può apportare nella gestione delle amministrazioni pubbliche, misurata in termini di spesa per il personale; per tenere in debita considerazione la dimensione di ciascuna regione (e dunque il maggior livello di spesa che una maggiore dimensione comporta in termini assoluti), la spesa per il personale viene pesata per l'ammontare complessivo di spese correnti sostenute.

Di conseguenza, l'indicatore di efficienza consiste nell'ammontare di spese per il personale per ogni milione di euro di spese correnti sostenuto da tutti gli enti comunali appartenenti a ciascuna delle 20 regioni. L'assunzione di base è che l'impiego di soluzioni cloud permetta di semplificare, rendendo pertanto più efficiente, il lavoro svolto dai lavoratori del settore pubblico, e consenta di conseguenza di liberare risorse che possono essere più proficuamente impegnate in formazione e riqualificazione delle proprie competenze così da poter essere reimpiegate in altre attività. Questo, unitamente allo sblocco del turnover del personale, può portare ad un uso più razionale delle risorse umane, andando a migliorare la qualità dei servizi offerti.

Si stima una relazione positiva tra l'adozione di cloud computing e la produttività del personale della PA, grazie ad un miglioramento dell'efficienza: **da un**

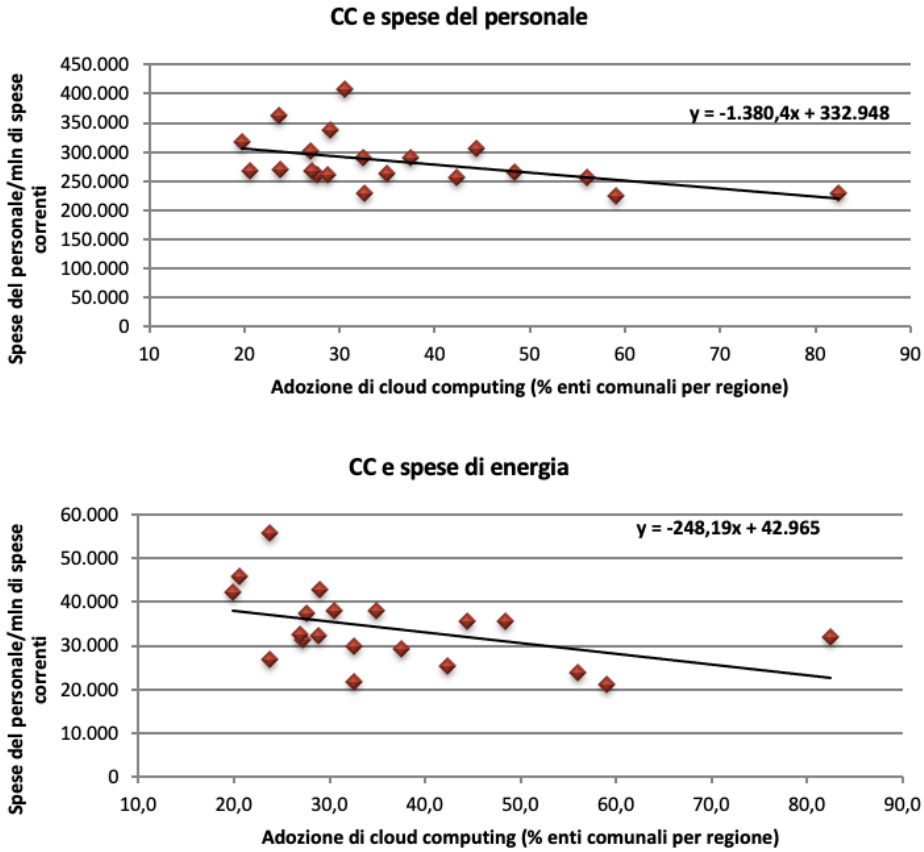


FIGURA 3.5 Relazione tra diffusione di cloud computing e le spese di personale e di energia per ogni milione di spese correnti (2018)

Fonte: Elaborazione I-Com su dati Istat (2018) e SIOPE (2018 e 2019)

aumento del 10% delle amministrazioni locali che adottano soluzioni cloud potrebbe derivare un risparmio pari a circa €13.800 per ogni milione di spese correnti sostenuto dalle stesse (Fig. 3.5).

Un secondo canale di risparmio riguarda la **spesa energetica**. La relazione tra grado di diffusione del cloud computing e risparmio in spese energetiche appare, infatti, positiva: **se il grado di adozione tra le amministrazioni comunali aumentasse del 10% si stima, che, mediamente, per ogni milione di spese correnti sostenute, le spese di energia si ridurrebbero di oltre €2.500 l'anno.**

Se si considera che **in Italia** le spese correnti nel 2019 ammontavano a €53,5 miliardi, stiamo parlando di un **potenziale risparmio complessivo in termini di spese per il**

personale, per le sole amministrazioni locali, di oltre €738,5 milioni, pari al 5,5% delle attuali spese per redditi da lavoro, e di quasi €133 milioni in sole spese di energia (l'8% della spesa complessiva in prodotti energetici nel 2019).

Assumendo che il margine di risparmio stimato per le amministrazioni comunali si possa applicare anche agli **enti regionali**, per questi ultimi si stima un potenziale risparmio di **oltre €290 milioni**, di cui circa €282 milioni in termini di maggiore efficienza e circa €8 milioni in minore spese energetiche.

Complessivamente, il risparmio stimato ammonta a circa €1,16 miliardi, di cui oltre €1 miliardo in termini di maggiore produttività e ulteriori €140 milioni in termini di minori spese di energia (Fig. 3.6).

3.3 LE CONSEGUENZE DELLA SOVRANITÀ DIGITALE SU COMPETITIVITÀ E TASSI DI INNOVAZIONE

Un tema che i decisori politici sono chiamati a non sottovalutare è legato alle conseguenze che le proprie scelte in materia di sovranità digitale avranno sulla competitività, intesa come futura capacità delle imprese multinazionali europee di competere sui mercati globali, e al rischio di un declino dell'influenza europea nei confronti di altre potenze mondiali.

La sovranità tecnologica, infatti, potrebbe **ridurre** la **competitività internazionale dell'Europa** e finire per dotare gli europei di tecnologie e imprese non competitive a livello globale. Un concetto di sovranità tecnologica mal applicato porterebbe al rischio di una **sovranità fittizia**: la UE sarebbe, cioè, libera di

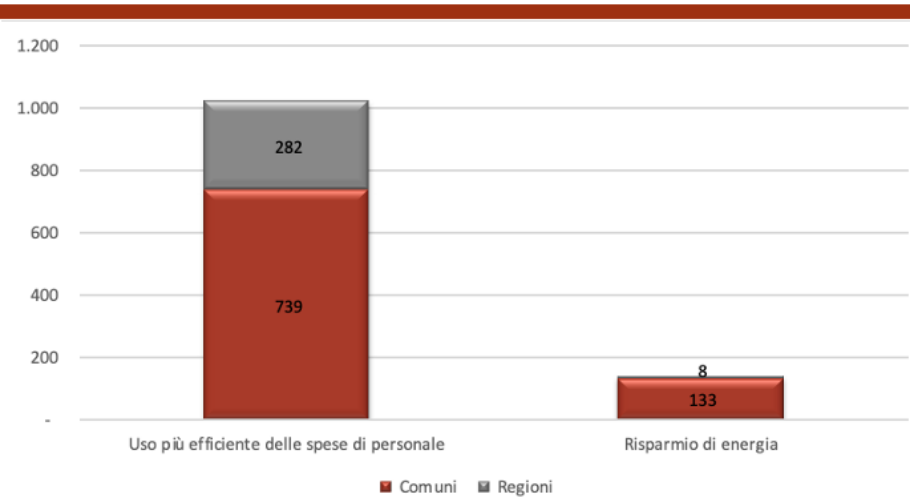


FIGURA 3.6 Risparmio stimato per le amministrazioni comunali e regionali italiane (mln €)

Fonte: Elaborazione I-Com su dati Istat e SIOPE

adottare le proprie tecnologie e i propri standard, ma ciò non produrrebbe i vantaggi economici e innovativi desiderati.

Si consideri che l'UE rappresenta solo il 10% della popolazione mondiale e la maggior parte dei dati nel mondo non è quindi di proprietà dell'UE. Come affermato dalla Presidente della Commissione Ursula von der Leyen, più dati abbiamo e più intelligenti sono i nostri algoritmi. Un'intuizione simile rende evidenti due aspetti importanti. Il primo è legato agli **inevitabili vantaggi che le soluzioni di provider globali hanno**, per le cosiddette economie di apprendimento: uno studio relativamente recente[27] mette in evidenza come i prezzi dei servizi cloud siano costantemente diminuiti negli ultimi anni e, al contempo, il mercato dei servizi cloud sia stato caratterizzato da frequenti introduzioni di prodotti nuovi e migliorati, sempre più spesso relative non tanto a caratteristiche osservabili (quali vCPU, memoria o storage) quanto alla tecnologia e alla potenza dei processori. Queste tendenze riguardano in particolare i grandi player globali – i c.d. hyperscaler – a testimonianza della forte concorrenza esistente nel mercato nonché della loro capacità di fare innovazione, un'innovazione che, a quanto pare, sarà sempre più incentrata su qualità e differenziazione dei prodotti anziché sui prezzi. Il secondo aspetto ha a che fare con l'importanza, per l'Unione, di avere accesso ai dati che sono fuori dei suoi confini. In quest'ottica, preoccuparsi esclusivamente del rischio di esporre i dati europei agli stranieri non basta ma occorrerebbe piuttosto occuparsi della sfida futura, che sarà **per l'Europa avere accesso ai dati degli stranieri**. L'indipendenza del digitale e dei dati non è una soluzione realistica per ottenere la sovranità rispetto alle tecnologie.

Una politica isolazionista potrebbe produrre un **vantaggio economico** per alcuni e **limitato ad un certo periodo di tempo**, ma potrebbe al contempo avere la pesante conseguenza di **minare invece la futura capacità dell'Europa di affrontare rischi specifici in materia di sicurezza e integrità dei dati**. Non solo, il protezionismo e l'autosufficienza dei dati o delle tecnologie ICT rischierebbe di ridurre la **competitività globale delle diverse industrie europee, ampliando i gap di investimento e produttività** che caratterizzano la UE nel confronto coi Paesi best performer a livello mondiale (Tab. 3.1), tra i quali peraltro il cloud computing costituisce un settore con gap a doppia cifra, con 11 miliardi l'anno di investimenti pubblici e privato in meno rispetto a Stati Uniti e Cina.

[27] Coyle D., Nguyen, D., "Cloud computing and National Accounting", ESCoE Discussion Papers, 2018

TABELLA 3.1 Gap di investimento* nella trasformazione digitale (mld € per anno)

Reti di comunicazione	42
HPC	6
Cloud	**11**
IA e blockchain	23
Tecnologie digitali verdi	6
Cybersecurity	3
Innovazioni digitali/Dati e Internet della prossima generazione	5
Semiconduttori/Fotonica	17
Skill digitali	9
Data spaces comuni europei	3

Fonte: Stime DG CNECT (2 maggio 2020)

*Stimato come la differenza tra gli investimenti di Stati Uniti e Cina e gli investimenti (pubblici e privati) dell'UE

In termini di spesa per ricerca e sviluppo, l'Europa, con una spesa di circa $411 miliardi, è in ritardo rispetto a Stati Uniti e Cina ($551 e $526 miliardi, rispettivamente). **In Italia**, la situazione appare ancor peggiore, con **solo $32,4 miliardi investiti in R&S, pari all'1,4% del PIL nazionale** (il 2% a livello UE).

Per quanto riguarda, poi, **la spesa per il cloud e la capacità dei data center su larga scala**, gli Stati Uniti sono leader indiscussi. L'Asia sta fortemente aumentando la capacità, con una previsione di crescita del 9,6% annuo tra il 2019 e il 2023, mentre si prevede che l'Europa la stia incrementando solo del 2,0%[28].

Al contrario, un approccio alla sovranità tecnologica basato sull'autonomia dovrebbe fondarsi sulla capacità dell'Europa di comprendere, accedere e utilizzare le nuove tecnologie e i nuovi modelli di business che tali tecnologie rendono possibili, preparandosi dunque ad accogliere la prossima ondata di innovazione in ambito ICT. Un programma simile dovrebbe inevitabilmente basarsi sulla **capacità di fornire istruzione e capitale umano** nonché di **abbattere le barriere normative** di un mercato unico europeo che ad oggi, anziché favorire, spesso impedisce il passaggio delle tecnologie tra Paesi.

In questo senso, se si interpreta la fornitura di un servizio cloud non come una mera operazione di acquisto – che punti magari a ridurre i costi di implementazione – ma

[28] Kearney, "The tipping point for European high-tech: catch up or lose out"

piuttosto come una **partnership col fornitore**, volta a massimizzare il valore del cloud nel lungo periodo, un simile rapporto di collaborazione con un provider internazionale genererebbe delle esternalità positive in termini di **distribuzione delle competenze sul territorio**, a beneficio dello **sviluppo di skill** che appare assolutamente necessario, sia a livello nazionale che europeo.

La capacità di innovare dei grossi provider affermati su scala globale è sicuramente indiscutibile. Una scelta che comporti l'esclusione (o una forte limitazione) dei grandi player globali – che da decenni investono in Europa, tanto in data center quanto nel talento europeo – priverebbe le amministrazioni pubbliche, le imprese e i cittadini italiani ed europei di innovazioni tecnologiche e digitali potenzialmente importanti, e limiterebbe inoltre la **libertà di scelta**, risultando il **ventaglio di servizi** (talvolta costruiti ad hoc sulle singole esigenze) **fortemente ridotto**.

In sintesi, possiamo dire che ostacolare l'accesso alle principali aziende tecnologiche non UE rischierebbe, dunque, di lasciare l'Europa con **meno concorrenza, meno scelta e meno accesso all'innovazione**.

3.4 IL CASO DEL CLOUD NAZIONALE

3.4.1 Il rischio di riduzione degli effetti benefici: economie di scala e tasso innovativo

Tutte queste considerazioni sono tanto più vere - e ancor più amplificate ne risulterebbero le conseguenze – laddove si ragionasse di infrastrutture cloud nazionali. In questo caso, infatti, sarebbe **ancor meno possibile sfruttare gli effetti di scala**, ne risulterebbe ulteriormente ridotto il grado di concorrenza e i **costi di duplicazione delle infrastrutture** renderebbero ancor meno efficienti i processi. Il **ventaglio di scelta** per i consumatori italiani, in particolare imprese e enti pubblici, risulterebbe **fortemente ridotto**, in particolare con riguardo a tutte quelle applicazioni che sono state già sviluppate, utilizzate, spesso migliorate, col rischio di rallentare i processi produttivi e operativi all'interno dei quali tali applicazioni sono ormai integrate.

Tali rischi sono al momento tutt'altro che remoti in quanto, anche se le ipotesi nazionali più estreme sembrano superate e l'indirizzo al momento pare essere orientato verso un coordinamento europeo, l'impostazione resta comunque molto frammentata all'interno dell'Unione, con la scelta di aderire o meno a progetti europei rimessa comunque ai singoli Stati membri.

La crisi pandemica ha messo alla prova la resilienza di tutti i Paesi europei e la

percezione della dipendenza dalle soluzioni tecnologiche straniere. I primi risultati indicano che le soluzioni nazionali non hanno funzionato meglio di quelle già esistenti, sia europee che internazionali[29].

Ad esempio, uno strumento di didattica a distanza del governo francese non è riuscito ad offrire supporto a tutti coloro che avevano bisogno di didattica online. Alcune soluzioni di prestigio nazionale hanno fallito – mostrando tutti i loro limiti in termini di capacità produttiva – mentre le soluzioni europee e globali esistenti, dall'infrastruttura cloud alle comunicazioni, dai sistemi di pagamento ai servizi di streaming, hanno continuato a funzionare in maniera efficace.

Le esigenze che un sistema IT governativo è chiamato ad affrontare sono molte e varie, e può essere molto difficile trovare un unico provider di cloud computing in grado soddisfare efficacemente tutte le necessità. Alcune di queste esigenze, poi, richiederanno l'impiego di cloud governativi – quali quelle legate alla sicurezza o alla privacy – mentre per altre applicazioni potrebbe risultare più conveniente far ricorso a cloud commerciali. Inoltre, **i sistemi IT dovranno essere** sufficientemente **flessibili e in grado di integrare tecnologie emergenti** come blockchain, AI e quantum computing che guideranno la prossima rivoluzione (e che interesseranno necessariamente anche gli apparati pubblici) per consentire un **ammodernamento a prova di futuro**. In questo senso, una prospettiva diversa inoltre può essere offerta dal cloud ibrido che abilita la creazione e la gestione di soluzioni che possano lavorare in cloud, on-premise e perfino alla periferia (edge computing), con una piattaforma comune, gestita da un singolo pannello di controllo. Questo consente l'archiviazione di dati sensibili ad esempio su un cloud privato e in contemporanea l'utilizzo di servizi di automazione e risorse computazionali avanzate di un cloud pubblico. Il cloud ibrido si adatta alle diverse esigenze, consentendo scelte diverse che si alternino ad esempio in tempi diversi a seconda dei diversi casi d'uso.

È indubbio che **il nostro Paese**, ancor più che l'UE nel suo complesso, **sconta un significativo svantaggio in campo tecnologico**: il settore ICT, in Italia, vale solo il 3,3% del PIL nazionale, un valore tra i più bassi a livello UE (peggio di noi solo Grecia, Lituania e Spagna) e, come già evidenziato, gli investimenti in R&S non migliorano la reputazione del Paese in quanto a capacità innovativa. Tagliare fuori dal mercato operatori che sinora hanno fortemente contribuito all'innovazione del nostro Paese

[29] ECIPE, "*Europe's Quest for Technology Sovereignty: Opportunities and Pitfalls*", Occasional Paper 02/2020.

pare una scelta rischiosa, oltre che antieconomica.

Il **rischio**, in definitiva, sarebbe quello **di vanificare parte dei benefici** importanti, evidenziati al precedente paragrafo 3.2, di cui sia le imprese che le Pubbliche Amministrazioni godono grazie all'**adozione del cloud**, e che spesso hanno a che fare anche con la capacità del fornitore, da un lato, di praticare prezzi vantaggiosi, dall'altro, di individuare le specifiche esigenze e fornire soluzioni mirate, soprattutto quando si tratta di piccole imprese – che nel nostro Paese rappresentano la stragrande maggioranza – o piccoli enti pubblici.

3.4.2 La potenziale limitazione nell'offerta di servizi cloud avanzati

Come già ricordato, il cloud è la principale piattaforme abilitante per la diffusione delle tecnologie proprie della trasformazione digitale sia per le imprese che per gli enti che fanno capo alla Pubblica Amministrazione. Si può osservare come la funzione di abilitatore di servizi del cloud sia identificabile anche nelle dinamiche di adozione da parte delle imprese (Tab.3.2).

Infatti, a livello nazionale, le imprese che utilizzano tecnologie e servizi cloud cresciute fino al 58%, a fronte del 23% che di quelle che utilizzano tecnologie e servizi propri dell'IoT e dell'8% che adotta soluzioni dell'area Big Data.

TABELLA 3.2 Acquisto di beni e servizi in aree tecnologiche da parte delle imprese, per settore (2020*, in %)

	imprese che acquistano servizi di cloud computing (CC) (incidenza %)	imprese che utilizzano IoT o sistemi interconnessi tramite Internet (incidenza %)	imprese che analizzano big data internamente o esternamente (incidenza %)
attività manifatturiere	59,09	23,63	5,99
energia, reti fognarie, rifiuti	65,29	35,81	13,7
costruzioni	58,56	23,92	6,18
commercio all'ingrosso e al dettaglio	60,72	24,53	9,86
attività professionali, scientifiche e tecniche	75,66	14,49	8,89
settore ict	82,29	26,62	19,86
totale	59,14	23,08	8,55

Fonte: Istat (2020)

* Imprese con più di 10 dipendenti

Analizzando il trend in relazione ai principali settori si osserva come tale correlazione si rispecchi in ognuno di essi e sia ancor più evidente tra le imprese del comparto ICT (in cui oltre l'80% già utilizza il cloud, 1/4 utilizza l'IoT e il 1/5 i Big Data) e delle attività professionali (74% cloud, 14% IoT e 9% Big Data). In generale, quindi, l'utilizzo del cloud risulta propedeutico all'uso di tutte le applicazioni tecnologiche più innovative. Tale dinamica è valida tanto per il settore privato, quanto per quello della Pubblica Amministrazione.

Relativamente ai servizi propri dell'Intelligenza artificiale, si osserva come questi si basino prevalentemente sulle capacità di apprendimento delle macchine, a loro volta distinte in due macro-categorie: machine learning e deep learning. I modelli che fanno capo al primo ambito consentono alle macchine di imparare a prendere decisioni senza essere preventivamente programmate, bensì basandosi su esempi o analizzando delle serie di risultati positivi e negativi. Sono riconducibili a tale modello strumenti quali il riconoscimento delle immagini, il riconoscimento vocale e la traduzione automatica dei testi. Le applicazioni che si basano sul deep learning sono attualmente quelle più avanzate: necessitano di reti neurali che, aggregando ingenti quantità di dati provenienti da fonti differenti (ad esempio stimoli sonori e visivi) permettono di effettuare elaborazioni su più livelli che consentono loro di prendere decisioni non direttamente attribuibili alle informazioni di input (come nel caso delle auto a guida autonoma).

Per quanto concerne i Big Data, considerata la grande capacità di calcolo richiesta per l'utilizzo di questi servizi anche da parte di imprese e organizzazioni che non sono in grado di investire nell'acquisto e nella manutenzione di infrastrutture ICT particolarmente dispendiose (o che intendono ridurre i costi totali di utilizzo), le piattaforme cloud risultano particolarmente strategiche, consentendo di abbattere i costi di acquisto di server e sistemi di storage ed elaborazione e di pagare solo per l'acquisto effettivo di servizi "chiavi in mano".

Anche i servizi che fanno capo all'Internet of Things, altra importante tipologia relativa alla possibilità per gli oggetti di inviare e ricevere informazioni dalla rete, diventando intelligenti e acquisendo la capacità di svolgere diverse funzioni che vanno dalla localizzazione, alla scannerizzazione e all'interazione con l'ambiente circostante finalizzata alla raccolta e all'elaborazione di dati e all'esecuzione di task, hanno bisogno di essere abilitati da piattaforme cloud.

Tutti questi servizi risultano quindi particolarmente strategici per innalzare la competitività di imprese e PA italiane. D'altro

canto, l'intervento previsto nell'ultima versione disponibile del PNRR, pubblicata a gennaio (cfr. paragrafo 3.4.6), sembrerebbe orientato prevalentemente alla creazione di un Polo nazionale dedicato alla gestione dei dati. Agendo in questa direzione, il rischio sembrerebbe quello di implementare una sorta di megastorage, senza focalizzarsi però sulla fornitura di servizi Saas avanzati sopradescritti, quali intelligenza artificiale, Big Data, IoT etc.

Al contrario, come mostrato nel paragrafo 1.3.3, i servizi cloud, in particolare offerti dalle piattaforme degli hyperscaler, includono non solo l'hosting ma anche servizi avanzati in modalità as a service, on demand e personalizzabili che si possono utilizzare al consumo a seconda delle necessità puntuali dell'utente.

Inoltre, a differenza dell'hosting puro, il cloud computing permette di utilizzare risorse hardware e software senza necessita di acquistarle o svilupparle, ed i servizi e le applicazioni offerte dai cloud provider seguono un processo di continua innovazione, crescendo e adattandosi alle esigenze del cliente.

Di conseguenza, per favorire la diffusione dei servizi avanzati e la loro adozione da parte di PA e PMI, anche nell'ottica di favorire una rapida digitalizzazione e sburocratizzare in particolare gli enti pubblici, appare opportuno favorire la diffusione di servizi cloud di mercato anche presso la Pubblica Amministrazione, senza limitarsi ad un eventuale fornitura di servizi offerti dal cloud di Stato.

Case study 6: Stevanato Group

Fondato nel 1949, Stevanato Group è il più grande produttore privato al mondo di packaging primario in vetro per l'industria farmaceutica. Il Gruppo padovano, che comprende una vasta gamma di competenze dedicate a servire l'industria biofarmaceutica e diagnostica, è una delle più importanti realtà industriali del nostro paese, e conta oltre 4.200 dipendenti e 14 impianti produttivi in 9 Paesi. Dall'inizio della pandemia il Gruppo è inoltre impegnato nella produzione di componenti in plastica per i test diagnostici e di flaconi in vetro necessari per i trattamenti di diversi candidati di vaccino anti Covid-19. Sebbene nell'ultimo biennio Stevanato avesse già adottato l'utilizzo di cloud per garantire vantaggi in termini di capacità di calcolo e per godere in tempo reale di una visione unica su processi di vendita e clienti, proprio durante questa fase di massima emergenza l'azienda ha consolidato il proprio utilizzo di tecnologie cloud e di altri servizi di ultima generazione. Il cloud computing si è infatti rivelato strategico per la continuità di business in questa fase

delicata, e ha permesso allo Stevanato Group di non interrompere mai la produzione e il supporto all'intero comparto dell'industria farmaceutica. In modo da rendere possibili i test di accettazione di fabbrica (FAT) e le ispezioni sui macchinari nei mesi di emergenza sanitaria, il Gruppo ha inoltre sviluppato un progetto di Virtual Audit grazie all'utilizzo di nuove tecnologie di Realtà Miste. Indossando dei visori olografici di ultima generazione, i dipendenti dell'azienda riescono a muoversi all'interno degli impianti, mostrando al cliente collegato da remoto sia i macchinari impiegati che i processi in atto. Questo ha permesso a Stevanato di superate le limitazioni nei viaggi e le misure di isolamento, assicurando l'eseguibilità, anche a distanza, di audit del sistema di qualità e di accertamenti dell'impianto. L'accettazione in remoto delle macchine di ispezione dei farmaci e del vaccino in sviluppo ha infatti permesso di velocizzarne la spedizione alle case farmaceutiche, un fattore critico in questo momento in cui l'azienda si trova a gestire alti volumi in tempi ristretti, garantendo all'azienda un vantaggio competitivo rispetto agli altri competitor del settore. Stevanato ha ora in programma di l'integrazione anche di tecnologie di AI sulle macchine da ispezione. Questo progetto, che verrà finalizzato nel 2021, consentirà alle aziende farmaceutiche di ulteriormente ridurre gli sprechi e garantire i migliori standard d'integrità dei contenitori per farmaci e vaccini. Quest'ultimo elemento risulta essenziale e, grazie all'interazione con gli strumenti IA, dovrebbe ridurre fino a 10 volte i falsi positivi e migliorare il detection rate del 5%. Questi progetti fanno parte del più ampio piano di Trasformazione Digitale di Stevanato Group, che si basa sul completamento del New Digital Ecosystem entro il 2022. In questo quadro le tecnologie cloud saranno fondamentali per l'elaborazione di analisi su big data e per la restituzione di risultati con massima rapidità. Un ulteriore significativo vantaggio riguarderà la massima garanzia di sicurezza e privacy, un aspetto strategico rilevante nel settore farmaceutico e nello sviluppo di brevetti dall'ingente valore economico, come quelli sul nuovo vaccino anti-Covid19.

Fonte: https://news.microsoft.com/it-it/2020/12/16/stevanato-group-e-microsoft-cloud-computing-e-sistemi-di-assistenza-in-remoto-per-far-fronte-alle-sfide-dellindustria-farmaceutica/

3.4.3 Il potenziale impatto di un eventuale cloud nazionale sulla cybersecurity

L'eventuale creazione di un cloud nazionale potrebbe avere delle ripercussioni, in particolare nel breve-medio periodo, anche sul livello di sicurezza complessivo di enti pubblici e aziende che si troverebbero ad

utilizzare servizi forniti dal provider di Stato rispetto a quelli forniti dai leader di settore o da un sistema aperto ad una molteplicità di soluzioni.

Il fenomeno del **cybercrime**, infatti, ha assunto negli ultimi anni contorni sempre più preoccupanti e impattanti sia a livello di sicurezza dei dati, sia a livelli di danni economici. La relazione sulla politica dell'informazione per la sicurezza 2019 indica che le **amministrazioni pubbliche sono il target privilegiato per i criminali informatici** (Fig.3.7) essendo state bersaglio nel 2019 del 73% degli attacchi informatici critici. I soggetti pubblici maggiormente attaccati sono stati i Ministeri, 34% nel 2019.

Per quanto riguarda i privati, invece, i soggetti più colpiti fanno capo al settore energetico (che nel 2019 ha subito il 13% degli attacchi complessivi), alle infrastrutture digitali (10%), alle telecomunicazioni (7%), e al settore bancario (anch'esso al 7%). Preoccupante è inoltre il fatto che il 34% degli attacchi critici nel 2019 abbia avuto come esito un esfiltrazioni di dati.

Secondo uno studio condotto da Comparitech, nel terzo trimestre del 2019, il 9,68% dei computer e il 3,04% dei dispositivi mobili utilizzati all'interno dell'Unione

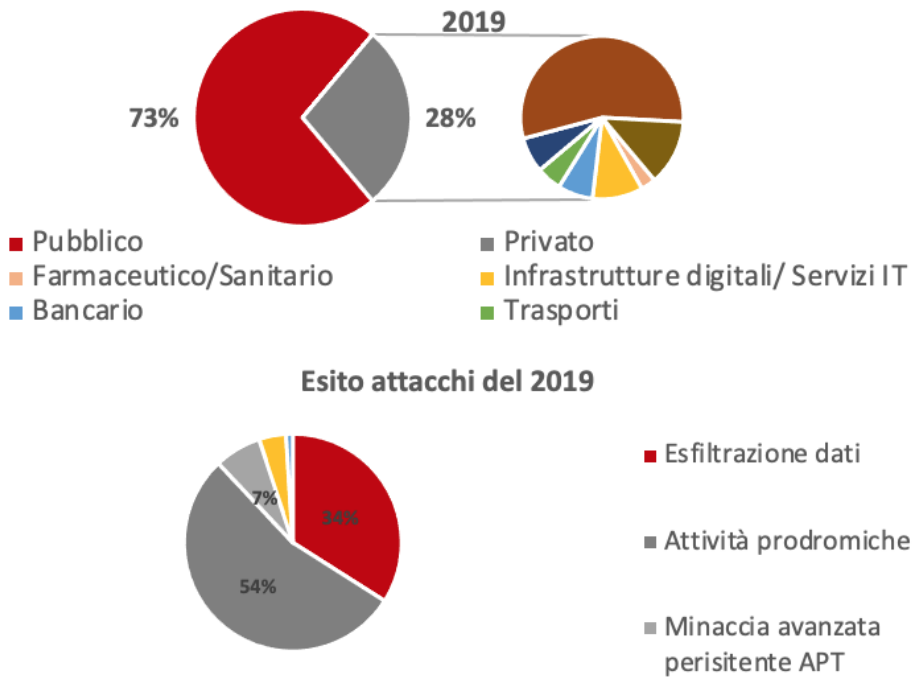


FIGURA 3.7 Attacchi informatici critici avvenuti in Italia per tipologia di Target ed Esito

Fonte: Relazione sulla politica dell'informazione per la sicurezza 2019 – Presidenza del Consiglio dei Ministri

Europea sono stati infettati da malware[30]. **Maggiore preoccupazione è data dal fatto che il nostro Paese presenta profili di rischio più alti sia rispetto alla media europea, sia in confronto a tutte le principali economie mondiali**. Infatti, i dati mostrano come l'Italia sia al primo posto in termini di computer compromessi con software malevoli (12,47%), davanti a Cina, Giappone, USA, Corea del Sud e Regno Unito. Per quanto riguarda i dispositivi mobili, invece, il dato sulle infezioni fatto registrare dall'Italia (5,01%) tra le aree geografiche considerate è secondo solo a quello degli USA (8,18%) ed è circa il 2% più elevato della media UE27 (Fig.3.8).

La quota estremamente rilevante di computer e device mobili corrotti mostra l'opportunità di conservare i dati all'interno di un cloud che dispone delle tecnologie di sicurezza più evolute e aggiornate disponibili, piuttosto che su dispositivi proprietari non costantemente aggiornati.

Inoltre, subire un attacco informatico che comporta la perdita di dati impatta sulle aziende sia dal punto di vista economico che su quello della perdita di fiducia da parte degli utenti. L'ultima versione dello studio annuale "*The Kaspersky Global Corporate IT Security Risks Survey 2020*", condotto dall'azienda specializzata in sicurezza informatica Kaspersky, ha cercato di stimare l'impatto

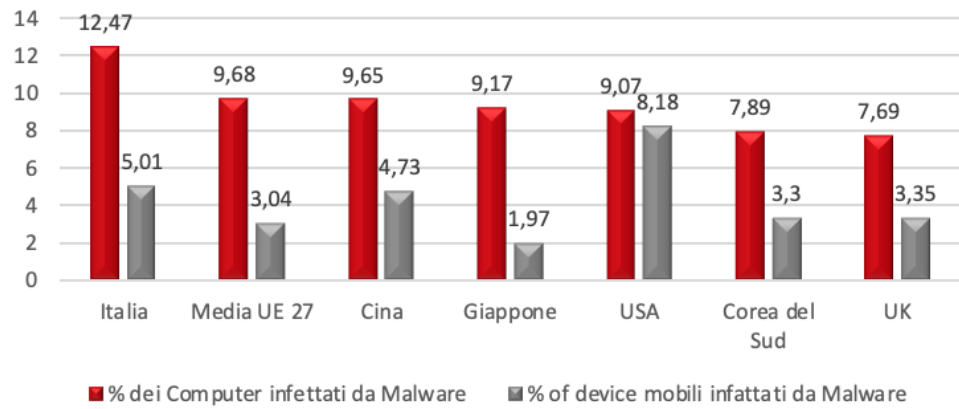


FIGURA 3.8 % di devices che hanno subito attacchi informatici per area geografica (2019)

Fonte: Comparitech, 2020

[30] Il malware, contrazione delle parole inglesi *malicious* e *software*, è un software malevolo in grado di intrufolarsi in un computer, in un dispositivo mobile o in una rete aziendale senza l'autorizzazione dell'utente con lo scopo di trafugare dati riservati, spiare le vittime o arrecare danni più o meno gravi al sistema informatico nel quale è in esecuzione (Cybersecurity 360).

finanziario medio di un data breach sia nelle PMI che nelle grandi imprese[31].

Dallo studio è emerso che **il costo medio delle violazioni si è attestato nel 2020 sui 101 mila dollari per le PMI e su 1,09 milioni per le grandi imprese** (Fig.3.9). Osservando l'impatto finanziario medio negli ultimi quattro anni è possibile notare che, sia per le PMI che per le grandi imprese, nel 2020 il danno economico è inferiore rispetto ai periodi precedenti. La ragione principale di questa decrescita, nonostante l'aumento dei punti potenzialmente vulnerabili, è legata al fatto che i nuovi sistemi di sicurezza informatica permettono alle aziende di rilevare e rispondere alle violazioni in un tempo notevolmente inferiore.

Secondo gli esperti intervistati da Kaspersky nel 2017 solo il 4% delle aziende disponeva di un sistema atto a prevenire e rilevare le intrusioni sulla propria rete contro il 10% del 2020. Inoltre, il peso della sicurezza informatica sul budget IT e cresciuto sia per le PMI, dal 23% del 2019 al 26% del 2020

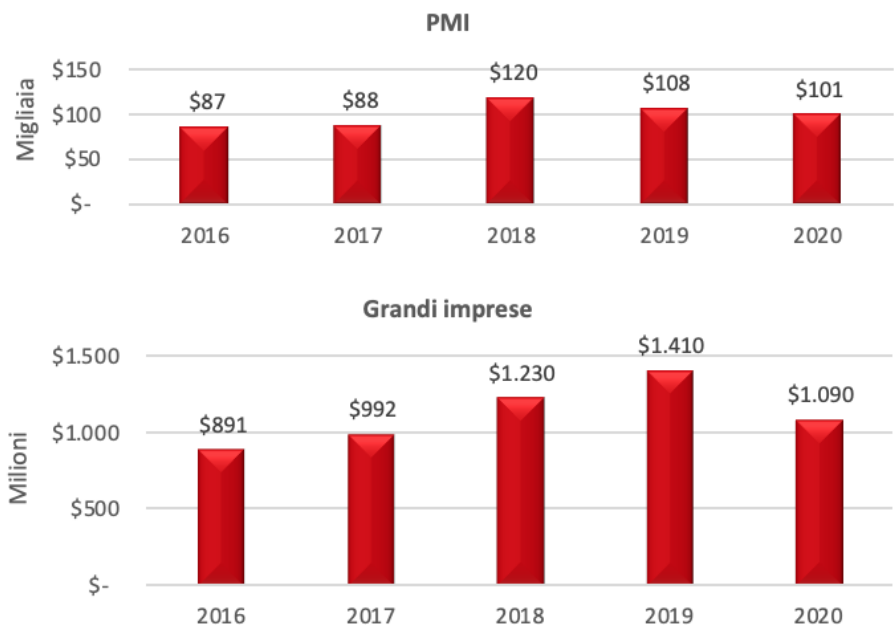


FIGURA 3.9 Impatto finanziario medio di un data breach nelle PMI e nelle grandi imprese (2016 - 2020)

Fonte: Kaspersky, 2020

[31] L'analisi è stata condotta intervistando 5.266 responsabili aziendali delle decisioni che riguardano l'IT provenienti da 31 Paesi. Sono state classificate come PMI le aziende tra i 50 e i 999 dipendenti a prescindere dal fatturato.

(raggiungendo i 275 mila dollari medi all'anno), sia per le grandi imprese, dal 26% al 29% (raggiungendo in media i 14 milioni di dollari annui).

Dai dati sopracitati risulta quindi evidente che **ad un aumento degli investimenti in sicurezza informatica equivale una riduzione del danno derivante da potenziali attacchi**.

Disporre di un sistema di sicurezza all'avanguardia riduce infatti sia la possibilità che una rete venga penetrata sia, in caso avverso, il tempo che i criminali informatici hanno a disposizione prima di essere scoperti ed estromessi.

Purtroppo, secondo il rapporto "NIS Investments" pubblicato dall'ENISA nel dicembre 2020, **la spesa media per la sicurezza IT delle organizzazioni Italiane (in relazione al budget IT) è inferiore sia alla media USA che a quella dell'UE27 (Fig.3.10)**. Infatti, in media le organizzazioni USA investono il 6% del proprio budget IT in sicurezza, quelle europee il 3,5% e quelle italiane il 3,1%.

Osservando nel dettaglio le tipologie di organizzazioni analizzate dall'ENISA emerge che i settori in cui viene investita in sicurezza la quota maggiore del budget in IT (Fig.3.11) sono i servizi bancari e finanziari (5,6%), il farmaceutico (5,5%) lo sviluppo di software e servizi Internet (4,7%).

Le pubbliche amministrazioni, che per propria natura detengono le informazioni sensibili di tutti i cittadini di un Paese, allocano alla sicurezza solo il 4% del budget IT.

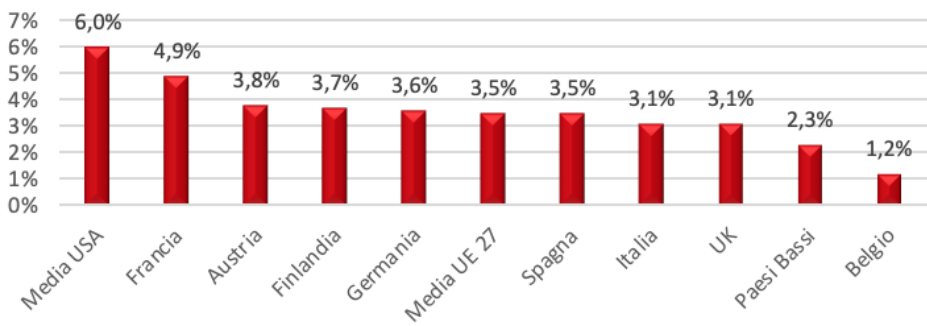


FIGURA 3.10 % della spesa in sicurezza informatica delle organizzazioni rispetto al budget IT per area geografica (2020)

Fonte: ENISA, 2020

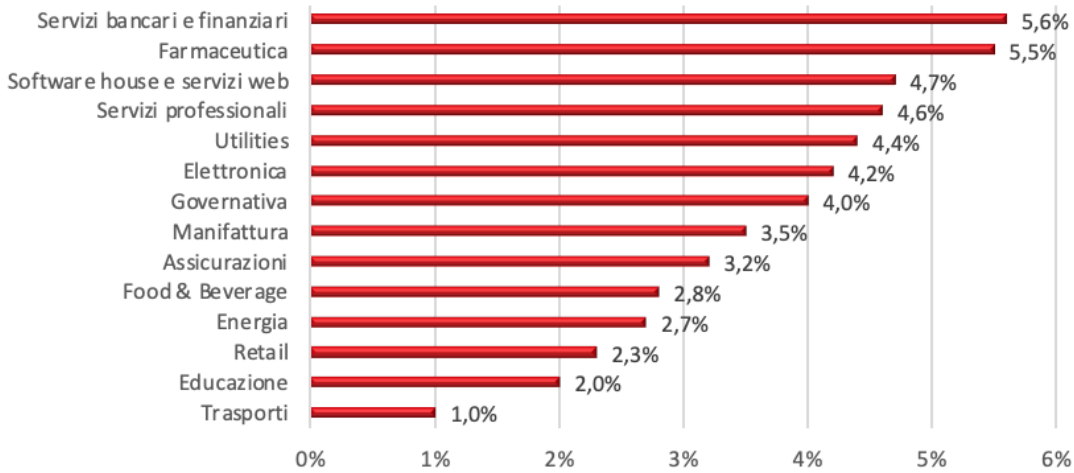


FIGURA 3.11 % della spesa in sicurezza informatica delle organizzazioni rispetto al budget IT per area settore (2020)

Fonte: ENISA, 2020

In conclusione, si rileva come la creazione di un cloud di Stato che escludesse l'utilizzo delle migliori soluzioni relative alla sicurezza rischierebbe di esporre, in particolare nel breve-medio periodo, gli eventuali utilizzatori (pubblici e privati) a maggiori vulnerabilità, rispetto ad un contesto in cui enti della PA ed imprese abbiamo la facoltà di scegliere le migliori soluzioni disponibili sul mercato.

Inoltre, alla luce dei dati presentati nel Piano Nazionale di Ripresa e Resilienza[32], le risorse dedicate alla sicurezza informatica del cloud nazionale (che ammontano ad una quota non definita rispetto agli € 1,25 miliardi che dovrebbero essere messi a disposizione per un progetto di tale portata) si osserva come queste potrebbero non essere sufficienti[33].

3.4.4 Maggiori difficoltà di certificazione e compliance normativa

Nel caso di un'eventuale piattaforma di cloud di Stato, la limitazione dell'accesso ai soli operatori nazionali rischia, inoltre, di **rallentare le procedure di certificazione e**

[32] Ci si riferisce alla versione presentata in Consiglio dei Ministri il 12 gennaio 2021

[33] Le risorse verranno infatti spalmate su 5 progetti diversi, tutti di notevole importanza e per i quali, nella maggior parte dei casi, non sembra esserci una solida base su cui partire. Un esempio è costituito dal "Centro nazionale di ricerca e sviluppo in cybersecurity" non ancora esistente, ma che dovrebbe, entro la fine del 2024 (secondo la bozza del cronoprogramma del PNRR del 29 dicembre 2020), aver già uno spessore tale da garantire la sicurezza informatica dei dati che andranno a confluire nella piattaforma cloud di Stato.

compliance di norme e certificazioni in materia di cloud computing. Tale fattore è determinato dalla minore abilità e flessibilità di soggetti che operano su scala minore di adattare e far sottostare il funzionamento delle proprie tecnologie a specifiche norme e requisiti (in particolare se questi mutano rapidamente nel tempo). A tal proposito, infatti, si osserva come provider di dimensione globale o che comunque operano su una molteplicità di mercati abbiano un maggiore expertise nell'adattare la propria offerta di servizi a normative locali, schemi e certificazioni che spesso divergono tra una nazione e l'altra. Una possibile misura di questo fenomeno è rilevabile dall'elenco dei fornitori di servizi di cloud computing qualificati dall'AgID e disponibili sul cloud marketplace della PA (Tab.3.3).

TABELLA 3.3 Elenco dei fornitori qualificati per servizi SaaS, IaaS e PaaS

Servizi IaaS		Servizi PaaS		Servizi SaaS*			
CSP	N° servizi	CSP	N° servizi	Piattaforma CSP	N° totale servizi SaaS	N° servizi SaaS di 3e parti	N° Servizi SaaS del CSP
IBM	18	AWS	72	AWS	138	127	11
AWS	17	Google	35	Aruba	99	96	3
Google	10	IBM	25	Microsoft	45	42	3
Oracle	9	Oracle	13	Oracle	30	6	24
Microsoft	5	Microsoft	7	Cineca	24	0	24
Reevo	4	Filippetti	3	Google	17	15	2
Brennercom	4	Salesforce	2	IBM	14	3	12
Aruba	2	DXC	2	ServiceNow	8	1	7
Telecom Italia	2	CSI Piemonte	1	Salesforce	6	0	6
Irideos	2	LISPA	1	SAP	4	0	4
Altri	32	Altri	7	Altri	97	97	

*Il dato relativo ai servizi SaaS indica la somma tra servizi nativi della piattaforma e servizi di terze parti qualificati AgID e offerti tramite la medesima piattaforma.

**Sulla base dei nuovi criteri AgID, i servizi sottoposti all'Agenzia ricevono una qualifica "ex-ante", pertanto il numero effettivo dei servizi attivi sul Cloud Marketplace potrebbe essere leggermente difforme rispetto a quanto riportato in tabella.

Fonte: AgID, 14 settembre 2020

I dati mostrano come, per ogni tipologia di servizi offerti, **gli operatori globali siano i principali fornitori disponibili, pesando per 51% sui servizi SaaS, per il 56% sugli IaaS e per il 90% sui PaaS.**

Risulta inoltre utile notare, in relazione ai servizi SaaS, che gli operatori globali, oltre ad essere tra i principali fornitori diretti, sono le principali piattaforme utilizzate da operatori di dimensioni minori per offrire i propri servizi. Dall'analisi dei dati risulta infatti che su 387 servizi offerti tramite piattaforme terze, il 50% sia attribuibile ai provider extraeuropei di maggiori dimensioni.

Un'eventuale esclusione dei provider globali dal mercato nazionale, oltre a ridurre il numero dei servizi disponibili, rischierebbe anche di impattare sugli operatori interni, minandone il tasso di innovatività complessiva. Inoltre, questo condurrebbe ad un aumento del prezzo da parte delle piattaforme che rimarrebbero sul mercato, rischiando di creare un problema di concorrenza e mettendo l'Italia in una posizione di svantaggio competitivo rispetto alle altre principali economie globali.

Case study 7: Il Cloud pubblico nel settore bancario

La digitalizzazione ha avuto nel corso dell'ultimo decennio un effetto dirompente sull'evoluzione del sistema bancario. I portali web stanno infatti rapidamente sostituendo le filiali fisiche come mezzo principale di erogazione di servizi all'utenza. Il settore bancario è però chiamato a gestire, per sua natura una mole enorme di dati sensibili. Per migliorare il servizio offerto all'utenza e rendere i propri sistemi più stabili e sicuri numerosi attori del settore hanno deciso di farsi affiancare da un partner cloud. Vista la criticità delle informazioni gestite l'Autorità Bancaria Europea (EBA) ha divulgato nel 2018 una serie di raccomandazioni in materia di esternalizzazione a fornitori di servizi cloud. Per tenere conto delle specificità dell'outsourcing dei servizi di cloud computing le raccomandazioni includono indicazioni non solo sulla sicurezza informatica del dato ma anche sulla localizzazione e sulla sicurezza fisica dei data center. L'EBA consiglia inoltre di utilizzare, come ulteriore misura di sicurezza, sistemi di crittografia sia per i dati in transito che per quelli conservati in archivio. Il primo passo che un istituto bancario deve compiere se vuole avvalersi di un servizio di cloud pubblico è quindi una valutazione delle attività che vengono considerate rilevanti. Alla luce di ciò è necessario che gli istituti individuino le attività critiche per la continuità operativa dell'ente e per il mantenimento dei suoi obblighi nei confronti dei clienti. In seguito, le banche sono obbligate ad informare le autorità di vigilanza e garantire l'accesso ai dati migrati sul cloud all'ente deputato a svolgere il servizio di audit. Risulta

inoltre fondamentale che l'istituto bancario effettui una valutazione attenta sulla capacità del partner cloud di mantenere la sicurezza delle informazioni custodite e che effettui un monitoraggio continuo delle misure prese a tale scopo.

Risulta infine fondamentale che l'ente che esternalizza abbia la possibilità, laddove necessario, di recedere dal servizio cloud senza che ciò comporti un'indebita interruzione dell'erogazione di servizi all'utenza o pregiudichi la sua conformità al regime normativo. È quindi necessario che l'istituto elabori un piano di uscita che sia complessivo, documentato e sufficientemente sperimentato.

Fonte: EBA

3.4.5 Possibile riduzione dell'adozione del cloud da parte di PA e imprese

Come osservato in precedenza, l'implementazione di un cloud nazionale e la limitazione dell'accesso ai provider extra-europei, in particolare gli hyperscaler, rischia di ridurre sensibilmente la varietà, la qualità e l'adattabilità di servizi finali offerti, in particolare in relazione al minor numero di applicazioni, alla minore qualità e al fatto che queste siano già state utilizzate (e migliorate) da varie tipologie di enti e aziende.

Inoltre, una tale **limitazione della concorrenza e quindi del livello di innovazione rischierebbe di inficiare anche lo stesso tasso di adozione del cloud da parte di aziende e PA**, per via della minore capacità del cloud di Stato di soddisfare le esigenze degli utenti (intesi come enti e aziende) con servizi e applicazioni già altamente performanti, customizzate e pronti all'uso.

A tal proposito, la dinamica di adozione del cloud da parte degli enti pubblici è stata analizzata da Sallehudin et al. (2018) in Malesia, utilizzando la teoria della diffusione dell'innovazione di Rogers (2003)[34]. Quest'ultima ha identificato i principali fattori di adozione delle innovazioni secondo cinque caratteristiche delle tecnologie (Fig.3.12): vantaggio relativo, compatibilità, complessità, testabilità (trialability, ovvero il grado in cui un'innovazione può essere sperimentata su una base limitata) e osservazione[35].

I risultati dell'analisi, effettuata su un campione di 169 organizzazioni tra Ministeri, Dipartimenti e Agenzie del Paese[36], mostrano

[34] Rogers, E. M. (2003). *Diffusion of innovations*. 5th edition, New York: Free Press.

[35] La natura di una tecnologia è caratterizzata anche dai principali obiettivi di contesto della stessa tecnologia (ad es. la tecnologia del cloud computing), piuttosto che dal contesto in sé, come la natura del decisore e gli altri fattori normativi e ambientali (interni o esterni).

[36] Il campione include 169 risposte valide, di cui il 36,1% proveniva da agenzie federali, il 17,8% da agenzie

come il **vantaggio relativo costituisca la caratteristica più rilevante per l'adozione del cloud computing da parte degli enti pubblici**, in particolare per quanto concerne sia la fase di avvio, sia in relazione all'implementazione effettiva. Inoltre, il vantaggio relativo era risultato una variabile significativa dell'adozione delle tecnologie anche in studi precedenti condotti su organizzazioni e aziende in particolare relativi ad applicazioni di e-commerce, tecnologie di e-business, RFID e dello stesso cloud computing (Alam et al., 2017).

In particolare, sia osserva come i fattori che compongo l'indicatore del vantaggio relativo, individuati da Rogers e testati dallo studio, siano a loro volta 5, ovvero:

- *il grado di redditività economica,* che nel caso del public cloud è determinato dalle ampie economie di scala degli operatori globali, che possono garantire prezzi più competitivi, e dall'apertura del mercato;
- *il basso costo iniziale*, che nel caso del cloud è tendente allo zero, in considerazione dello spostamento dei costi da Capex a Opex;
- la *diminuzione dell'impatto* (sull'organizzazione o l'impresa che adotta la tecnologia), che appare maggiore nei servizi offerti da un numero maggiore di operatori, inclusi quelli globali, grazie alla maggiore customizzazione e sperimentazione già effettuata su un vasto numero di soggetti;
- il *risparmio di tempo e fatica*, anche in questo caso maggiore per servizi offerti su mercati aperti, che includono tutte le tipologie di operatori, grazie alla maggiore facilità d'uso determinata da maggiori investimenti nell'usabilità;
- *l'immediatezza della ricompensa*, che appare percepibile in misura più consistente grazie alla maggiore quantità e qualità di servizi offerti su mercati aperti.

Secondo quanto emerge dalla ricerca, **questi 5 fattori sono direttamente implicati nella maggiore o minore adozione di tecnologie cloud da parte degli enti della Pubblica amministrazione**. Questo set di indicatori, peraltro, è adattabile anche al contesto aziendale, poiché è su questo che la teoria di Rogers è stata di fatto costruita.

Di conseguenza, anche alla luce degli studi sperimentali condotti sull'adozione del cloud,

statali, 16,6% da enti statali, il 16% da autorità locali e il 13,6% da altri enti.

è ragionevole ritenere che una **limitazione della concorrenza**, in tale settore, in particolare restringendo l'accesso agli operatori maggiormente performanti e innovativi, e che investono più risorse in R&S, **si concretizzi in un tasso di adozione verosimilmente più lento da parte degli enti pubblici e probabilmente anche delle imprese.**

Case study 8: Comune di Milano

Centro industriale ed economico del Paese, con 1,35 milioni di abitanti e quasi 300 mila imprese, Milano è un modello per sperimentazione di servizi e di pratiche innovative. Nel 2016, con lo slogan "da smart city a smart citizen", il Comune ha avviato un nuovo processo di unificazione dei servizi e dei dati attraverso una piattaforma cloud in cui ha fatto convergere tutti i servizi al cittadino erogati attraverso il sito istituzionale del Comune, l'infoline "020202" e gli sportelli fisici. Questo nuovo sistema unificato di Citizen Relationship Management, ha sensibilmente semplificato e velocizzato la gestione delle richieste dei cittadini. Con l'obiettivo di aumentare i canali di ascolto e di interazione con i cittadini, garantendo contemporaneamente una maggiore efficacia ed efficienza dei servizi erogati, la piattaforma ha ora in gestione le oltre 20 direzioni del Comune di Milano, con circa un milione di ticket emessi, e 250.000 appuntamenti prenotati.

Significative migliorie sono anche state riportate a livello manageriale e di governance della Pubblica Amministrazione. In questo campo la gestione unificata consente di monitorare i servizi della città in tempo reale, usufruendo di dashboard efficaci alimentati dai dati provenienti dal CRM. Questa gestione centralizzata dei dati, insieme alla varietà di canali di interazione con i cittadini, ha inoltre consentito al Comune di Milano di affrontare le difficoltà legate all'emergenza derivante dalla pandemia da Covid-19 senza dover ricorrere ad una brusca interruzione dei servizi. È infatti stata garantita una totale continuità dell'offerta per i cittadini, nel pieno rispetto del distanziamento sociale e delle misure derivanti dal lockdown. Oltre a un rafforzamento della infoline 020202, l'emergenza ha spinto il Comune ad estendere a tutti gli uffici dell'amministrazione la possibilità di prenotare gli appuntamenti online, precedentemente limitata alla richiesta delle carte di identità elettroniche, e ad incrementare il numero di certificati scaricabili online (che negli ultimi mesi hanno raggiunto quota 80%). Inoltre, è stata integrata nel sistema uniformato anche l'App del Fascicolo del Cittadino, un nuovo servizio avviato dall'Amministrazione nel maggio

2020, che consente la gestione di pratiche e servizi direttamente dallo smartphone.
In modo da sviluppare ulteriormente le forme di interazioni e la qualità del CRM, il Comune intende ore utilizzare il cloud per integrare le interazioni provenienti dai social network, e in particolare da Facebook, che sono oggi essenziali per captare il sentiment di cittadini e utenti. Attraverso procedure automatizzate e funzionalità di intelligenza artificiale, l'Amministrazione punta a utilizzare il servizio cloud per aumentare la capacità di gestione dei problemi e velocizzarne la soluzione.

Fonte: https://customers.microsoft.com/en-us/story/860179-comune-di-milano-government-dynamics365-it-italy

3.4.6 Il Cloud di Stato nel PNRR

I due elementi cardine attorno al quale ruota il Piano Nazionale di Ripresa e Resilienza italiano (PNRR), come da indicazioni europee, sono la digitalizzazione e la sostenibilità. In particolare, la missione "Digitalizzazione, innovazione, competitività e cultura" si pone come obiettivo la transizione digitale del Paese, sia per quanto riguarda la Pubblica Amministrazione che per il tessuto produttivo. A tale scopo, in attesa di conoscere le modifiche che verranno apportate al Piano da parte del Governo Draghi, la versione aggiornata del PNRR dello scorso 12 gennaio 2021 pone una notevole enfasi sulla necessità di sviluppare un cloud di Stato che possa funzionare in sinergia con il progetto europeo GAIA-X. Il passaggio al paradigma cloud viene infatti definito "una delle sfide più importanti per la digitalizzazione del Paese", in quanto costituisce il substrato tecnologico che abilita lo sviluppo e l'utilizzo di nuove tecnologie.

La Missione sopracitata si articola in 3 componenti:

- Digitalizzazione, Innovazione e sicurezza della PA;
- Digitalizzazione, Innovazione e competitività del Sistema Produttivo;
- Turismo e Cultura 4.0.

Il progetto atto alla creazione del Cloud di Stato italiano è parte integrante della componente Digitalizzazione, Innovazione e sicurezza della PA. Il programma d'azione delineato nel piano prevede stanziamenti economici da destinare alla creazione di uno o più Poli Strategici Nazionali verso cui migrare i Data Center delle Amministrazioni pubbliche centrali. Questa scelta nasce dalla volontà di superare l'attuale stato di frammentazione delle dotazioni infrastrutturali cloud in forza alla PA. Attraverso la razionalizzazione ed il consolidamento delle infrastrutture il piano mira a potenziare l'erogazione dei servizi e a ridurre i costi operativi necessari alla

manutenzione e aggiornamento dei data center. Le risorse momentaneamente previste per questo progetto equivalgono a 1,25 miliardi di euro (Tab.3.4), di cui 50 milioni sono già stati stanziati per la realizzazione di un data center del ministero dell'interno e per il potenziamento delle reti di connettività delle strutture operatici del Corpo Nazionale dei Vigili del Fuoco.

Per rendere fruibile l'ecosistema cloud a tutte le amministrazioni centrali e periferiche, è previsto che le basi dati presenti nei data center di stato siano interoperabili e accessibili, secondo vari livelli di autorizzazione, attraverso un catalogo di API che consenta di attingere ai dati del cloud, di elaborarli e di fornire servizi a cittadini e imprese. È previsto inoltre un investimento destinato all'implementazione del Single Digital Gateway (Sportello Digitale Unico europeo), che dovrebbe garantire l'accesso ai servizi erogati dalla PA italiana a tutti i cittadini europei, nonché della digitalizzazione e reingnerizzazione del Sistema Informativo Agricolo Nazionale (SIAN). Le risorse per questo progetto, che include anche i vari interventi delle amministrazioni centrali che hanno avviato progetti di digitalizzazione degli archivi e del patrimonio attualmente su supporto analogico e percorsi di digitalizzazione dei processi operativi, equivalgono a circa 1,13 miliardi di euro.

TABELLA 3.4 Risorse destinate alla componente "Digitalizzazione, Innovazione e sicurezza della PA" della missione "Digitalizzazione, innovazione, competitività e cultura"

Digitalizzazione della Pubblica Amministrazione	7,95
Infrastrutture digitali e cyber security	1,25
Dati e interoperabilità	1,13
Cittadinanza Digitale, Servizi e Piattaforme Abilitanti	5,57
Modernizzazione della PA	1,57
PA capace: reclutamento di capitale umano	0,21
PA Competente: rafforzamento e valorizzazione del capitale umano	0,72
PA semplice e connessa: semplificazione delle procedure amministrative, digitalizzazione dei processi	0,48
PA Smart: creazione di Poli Territoriali per il reclutamento, la formazione, il co-working e lo smart-working	0,1
Innovazione organizzativa della Giustizia	2
Risorse umane per il rafforzamento dell'ufficio del processo nuove posizioni organizzative	0
Totale	**20,98**

Fonte: Bozza PNRR, 12 gennaio 2021

All'interno del piano è, inoltre, prevista la realizzazione di un Cloud Enablement Program con lo scopo di favorire l'aggregazione e la migrazione delle PA centrali e locali verso soluzioni cloud e fornire alle stesse PA procedure, metodologie e strumenti di supporto utili a questa transizione.

4. CONCLUSIONI E SPUNTI DI POLICY

Come osservato nei precedenti capitoli dello studio, il contesto che circonda l'adozione ed il pieno sfruttamento delle tecnologie cloud è piuttosto variegato e include aspetti che spesso sono stati considerati in maniera lievemente distorta o non completamente rispondente rispetto alle reali condizioni del mercato, al corretto dispiegamento dell'innovazione e all'effettiva gestione dei rapporti tra Governo, Pubblica Amministrazione, imprese e cittadini nel contesto internazionale.

In questa sezione conclusiva si è proceduto a sintetizzare le principali risultanze emerse e a sistematizzarle per fornire un set di raccomandazioni utili per l'azione del Governo in questo campo, volte a ottimizzare il rapporto tra la regolamentazione dei vari ambiti connessi al passaggio verso il nuovo paradigma del cloud computing e alla massimizzazione dell'impatto positivo verso il sistema-Paese nel suo complesso.

A tal fine, le proposte di policy sono state suddivise secondo tre filoni principali: **impatto economico e apertura del mercato**; **sicurezza e protezione dell'utente**, inteso come enti pubblici e imprese private; e **resilienza complessiva del sistema**.

Rispetto a questi tre filoni, inoltre, le policy sono state classificate rispetto a quattro diversi domini: **infrastrutture e servizi; competenze; norme; principi di gestione e prassi operative**.

4.1 IMPATTO ECONOMICO E APERTURA DEL MERCATO

Il primo e principale tema è relativo all'impatto economico che può essere sprigionato in Italia grazie a un pieno utilizzo delle tecnologie cloud. A tal proposito, l'analisi ha mostrato come una tale diffusione potrebbe comportare fino ad oltre **1 miliardo** di risparmi l'anno per la Pubblica Amministrazione e un fatturato aggiuntivo di oltre **600 miliardi** per le imprese, in particolare **fungendo da piattaforma abilitante per tutti i benefici connessi ad una piena trasformazione digitale**.

Per conseguire un tale risultato appare necessario, in primo luogo, completare la **rete di accesso ad alta velocità** distribuita su tutto il territorio nazionale, sia mediante il Piano Bul, di cui si sta predisponendo una revisione, sia incentivando investimenti degli operatori anche attraverso lo stimolo alla domanda di servizi (si attendono in tal senso gli effetti della I° fase del Piano voucher), così come la diffusione delle antenne 5G e dei relativi servizi da parte degli operatori mobili.

In secondo luogo, si rileva l'opportunità di incentivare lo **sviluppo e l'adozione di soluzione cloud interoperabili** che

favoriscano la partecipazione e l'integrazione, in modo da aumentare il livello di innovazione del Paese, anziché vincolare la fornitura di tecnologie ad un numero limitato di fornitori. A tal proposito, si è osservato come una riduzione nella libertà di scelta priverebbe le amministrazioni pubbliche, le imprese e i cittadini italiani ed europei di innovazioni tecnologiche e digitali potenzialmente importanti, risultando il ventaglio di servizi (talvolta costruiti *ad hoc* sulle singole esigenze) sensibilmente ridotto, e ciò determinerebbe un contesto con meno concorrenza e un accesso all'innovazione nettamente inferiore.

Parallelamente, è importante garantire il **pieno controllo sui dati** attraverso modalità di localizzazione allineate agli standard europei e di mercato. In questo quadro, la partecipazione dell'Italia al progetto **Gaia-X**, in qualità di infrastruttura di dati federata e trasversale nell'UE, capace di garantire determinati standard di privacy e sicurezza e, al contempo, di sfruttare al meglio le opportunità economiche derivanti dal mercato dei dati, sembra essere ampiamente auspicabile. In particolare, appare importante la creazione di un framework comune, capace di promuovere parità di condizioni per tutti coloro che accettino i princìpi comuni, e prevenire i possibili effetti negativi derivanti da protezionismo e innalzamento di barriere di mercato, e discriminazioni geografiche, consentendo l'accesso anche alle aziende extra-europee che decidono di sottoscrivere gli standard e i valori della UE.

Sempre in tema di caratteristiche abilitanti, una menzione e una pianificazione operativa vanno necessariamente riferite all'ambito delle **competenze digitali**. L'Italia, come noto, è il fanalino di coda in Europa secondo l'indice Desi in questo ambito e non può prescindere dall'impegnarsi nel creare un Piano integrato per lo sviluppo delle competenze digitali a 360°, a supporto dagli attori sia pubblici sia privati. Per quanto riguarda i primi, appare necessaria una mappatura delle competenze di manager e dipendenti della PA, al fine di predisporre un piano formativo adeguato per colmare le possibili lacune che dovessero emergere dal censimento. In relazione al settore privato, apposite iniziative dovrebbero essere rivolte agli studenti (attraverso il potenziamento degli Istituti Tecnici Superiori e incentivando l'incremento dei laureati STEM - Science, Technology, Engineering and Mathematics, lavoratori (aggiornamento e riqualificazione delle competenze e Lifelong Learning) e cittadini (formazione per l'accesso quantomeno ai servizi di base, in particolare per le categorie meno digitalizzate).

Per quanto concerne le **possibili policy finalizzate a ottimizzare l'impatto**

economico e l'apertura del mercato, queste sono individuabili in 7 azioni:

- assicurare un'elevata competitività del mercato del cloud con la partecipazione di tutti i cloud service provider nazionali ed internazionali, in modo da favorire maggiori investimenti, italiani ed esteri, in innovazione, infrastrutture e tecnologie sul territorio nazionale e innalzare il livello di sviluppo e di conoscenze interno, promuovendo una **collaborazione basata su valori e principi comuni, senza discriminazioni geografiche.** A tal proposito, si osserva come i decisori politici siano chiamati ad adottare molta cautela nel fare determinate scelte in materia di sovranità tecnologica, poiché queste potrebbero comportare conseguenze negative per la **competitività del Paese** – la quale sconta un innegabile svantaggio tecnologico nei confronti dei Paesi più avanzati – rischiando di finire per **ampliare i gap di investimento e produttività** di cui soffre e lasciarlo con **meno concorrenza, meno possibilità scelta e minore accesso all'innovazione**;

- appare opportuno **favorire maggiori investimenti in innovazione e tecnologie sul territorio nazionale**, italiani ed esteri, in modo da innalzare il livello di sviluppo e di conoscenze interno relativo a tali ambiti;

- **incoraggiare l'interoperabilità dei servizi e la portabilità di dati e applicazioni**, l'utilizzo di standard aperti, favorendo la partecipazione, l'integrazione e la flessibilità, in modo da aumentare il livello di innovazione del Paese e la condivisione di tecnologie e best practice capaci di migliorare il livello complessivo di innovatività del sistema;

- proseguire e **intensificare i programmi nazionali** (in particolare il Piano Transizione 4.0, evoluzione di Impresa 4.0) e **gli incentivi per un'accelerazione della trasformazione digitale delle PMI tramite il cloud computing.**
  Si ritiene utile, in particolare, incentivare l'adozione di soluzioni cloud da parte delle Piccole e Medie Imprese italiane, con particolare attenzione per le funzioni strategiche e i servizi ad elevato valore aggiunto. Appare importante, inoltre, promuovere la transizione verso il **cloud come elemento di riferimento** nelle scelte delle PMI che vogliono accedere alle risorse del **Piano**

Transizione 4.0, volto a incentivare e supportare la competitività delle nostre imprese e valorizzare il Made in Italy;

- **promuovere la diffusione del cloud presso la PA accelerando la roadmap sulla *cloud-first policy*** previsto dal Piano Triennale per l'ICT pubblico sin dal 2018, secondo un modello di cloud ibrido, con l'obiettivo di migrare le migliaia di data center oggi dispersi e inefficienti che non riescono a garantire standard di sicurezza adeguati. In particolare, definire un Piano di Migrazione della Pubblica Amministrazione sul cloud di orizzonte triennale, accelerando il consolidamento delle infrastrutture IT esistenti anche in modalità ibrida e facendo leva sulle piattaforme di mercato offerte da tutti i cloud service providers certificati da AgID, potrebbe consentire una decisa semplificazione nelle attività della PA italiana, aumentando la sua efficacia nell'erogazione di servizi a cittadini e imprese, oltre a consentire sensibili risparmi. La sfida per la PA è quella di riuscire a creare una infrastruttura cloud a prova di futuro (flessibile, per potersi adattare alle evoluzioni del contesto, e aperta), per poter incorporare le innovazioni che possono arrivare dal mercato;
- promuovere l'utilizzo di fondi con cui valorizzare le esperienze e le capacità presenti nella Pubblica Amministrazione **evitando la centralizzazione su unico operatore privato di mercato per la gestione in partnership dei PSN** (i **Poli Strategici Nazionali**) ma rafforzando l'infrastruttura pubblica esistente al fine di utilizzarla per le applicazioni non migrabili al cloud di mercato;

- **favorire l'accompagnamento** alle nuove tecnologie e la **modernizzazione** delle **applicazioni** attraverso forme di incentivi che **premino** l'adozione di percorsi sinergici di migrazione e la scelta di operatori che facciano della **sostenibilità** un impegno concreto;

- nell'ambito delle azioni di **coordinamento** da intraprendere a livello internazionale, prevedere **armonizzazioni** di settore per i principali data space e business ecosystem, nel solco tracciato dal **progetto Gaia-X**, e assicurare l'armonizzazione con altri sistemi giuridici e di regolazione (anche alla luce delle Raccomandazioni del Comitato europeo della protezione

dei dati in seguito alla sentenza Schrems II).

Sempre in tema di armonizzazione, relativamente ai principi di gestione e prassi operative, si suggerisce l'opportunità di **definire modalità di gestione dei trasferimenti *cross-border*** e le relative modalità di protezione.

Sul punto, nel valutare ed orientare le relazioni UE-USA, è indispensabile che il dibattito attualmente in atto nell'Unione europea e a livello nazionale sia correttamente rimodulato ed incentrato sulla constatazione che gli obblighi di ostensione da esso attribuiti, seppur ampi, incontrano una serie di **importanti limitazioni e garanzie procedimentali che prevedono l'intervento delle Autorità giudiziarie, impongono un attento bilanciamento degli interessi coinvolti e attribuiscono ai destinatari degli ordini di esibizione specifici poteri di opposizione a tutela degli interessi degli Stati e degli individui**.

Tale dibattito si inquadra in un momento molto delicato in cui l'Unione Europea si trova ad affrontare un momento di grandissima complessità legato al fatto che, come noto, la recente sentenza Schrems II ha dichiarato invalida la decisione di adeguatezza del Privacy Shield, creando un vuoto regolamentare tanto ampio quanto grave.

Per far fronte a tale condizione di incertezza, il Comitato europeo della protezione dei dati (EDPB) ha formulato una strategia specifica da seguire per realizzare compliance ed enforcement mentre il Comitato europeo per la protezione dei dati personali ha fornito una serie di importanti raccomandazioni che forniscono indicazioni circa gli step procedurali da seguire nell'effettuare i trasferimenti di dati e declinano anche le possibili misure da adottare tra cui la crittografia assume un ruolo da protagonista. Si tratta di iniziative di particolare rilevanza che se, da un lato, hanno il pregio di perseguire obiettivi di chiarezza, dall'altro, come evidenziato nel corso dell'analisi, lasciano irrisolte alcune questioni che invece esigono un rapido chiarimento ed al contempo pongono molti interrogativi circa la proporzionalità delle misure proposte rispetto agli obiettivi perseguiti rendendo quanto mai evidente, ed urgente, un approfondimento di riflessione e confronto con gli stakeholder nella logica di assicurare un equo bilanciamento di tutti gli interessi coinvolti.

4.2 SICUREZZA, PROTEZIONE DELL'UTENTE E RESILIENZA

Un secondo tema fondamentale, indicato nello schema operativo, riguarda la **sicurezza dei dati** e la **protezione dell'utente**, inteso sia

come ente pubblico, sia come soggetto privato. A tal proposito, il primo e fondamentale aspetto è costituito dalle **infrastrutture**, rispetto alle quali si ritiene importante rendere disponibili forme di localizzazione dei dati e dei relativi processi di gestione nell'Unione Europea, nonché modalità evolute di segregazione delle informazioni:

- la **segregazione dei dati**, in particolare, concerne le varie modalità e sistemi di sicurezza offerti gli utenti, sia pubblici che privati, per garantire solo a quest'ultimi l'accesso ai dati. Tra le procedure di segregazione dati si identificano infatti forme di **cifratura, regolazione degli accessi e controllo delle identità;**

- questo tipo di tecnologie, inoltre, è particolarmente importante perché **tutela gli utenti pubblici** e **privati anche in caso di eventuali richieste di accesso ai dati effettuate ai provider internazionali da parte di Stati extra-europei**, dal momento che il criptaggio garantisce l'impossibilità di utilizzo dei dati a chiunque non possieda la chiave, inclusi gli stessi fornitori.

A livello **normativo**, anche alla luce delle disposizioni previste nella legge sul perimetro di sicurezza cibernetica, si sottolinea l'importanza delle seguenti azioni:

- effettuare una **classificazione di dati e asset strategici** per valutare quali sono quelli che necessitino di un particolare livello di protezione, con criteri che garantiscano il migliore trade-off tra sicurezza e competitività del mercato. A tal proposito, il caso del Regno Unito, che rappresenta il Paese maggiormente attivo in Europa nel campo della digitalizzazione e dell'economia dei dati in termini di investimenti, di valore, e di formazione, è di forte interesse per gli altri Stati membri dell'Unione. Con la Data Classification Strategy, infatti, è stato introdotto un sistema di classificazione che tiene conto sia della gestione digitale ed uniforme delle informazioni e dei dati della PA, sia dell'effettivo grado di informazioni sensibili all'interno di esse, identificando quelle meritevoli delle massime misure di protezione. Il **caso britannico** mostra quindi l'opportunità di effettuare una **classificazione** dati in modo da distinguerli per **livello di rischio** e conseguentemente per **livello di protezione**;

- caratterizzare l'infrastruttura cloud come "**infrastruttura critica estesa**" a contesti operativi diversi all'interno dei quali sia utile/necessario definire baseline operative condivise che possano consentire la gestione di un ecosistema, fermo restando il disposto normativo sul Perimetro di Sicurezza Cibernetica e la correlata definizione di infrastrutture critiche;

- garantire il **pieno controllo sui dati** – attraverso modalità di governo degli stessi – allineate agli standard europei e di mercato e la diffusione di **Codici di Condotta** – come ad esempio quello di CISPE (Cloud Infrastructure Services Providers in Europe) – che aiutino soggetti pubblici e privati ad assicurarsi che il fornitore della loro infrastruttura cloud utilizzi standard appropriati per la protezione dei dati che siano conformi al Regolamento generale sulla protezione dei dati (GDPR)

- **definire** e rendere noti **eventuali obblighi di trasferimento transfrontaliero** dei **dati**;

Per quanto concerne l'armonizzazione dei **principi di gestione** e delle **prassi operative**, si suggerisce di valutare la possibilità di:

- **stabilire procedure trasparenti e definite per la migrazione al cloud**, in modo da garantire e rassicurare in particolare Pubblica amministrazioni e PMI sulle operazioni da svolgere;

- **eseguire controlli sistematici e procedure di sicurezza rigorose per prevenire accessi non autorizzati e manipolazione di dati**, applicazioni e algoritmi, così come di definire gli ambiti e le modalità di accesso consentite alle forze dell'ordine.

Per garantire una completa protezione, infine, un aspetto da non sottovalutare riguarda anche il **fattore umano**. A tal proposito, appare opportuno promuovere **programmi ad hoc per la formazione in materia di sicurezza informatica presso dipendenti della PA e delle PMI**, relativi in particolare a conoscenze e prassi volta a ridurre notevolmente il livello di rischio che spesso deriva da pratiche non corrette e poco consapevoli.

Per quanto concerne il tema della **resilienza**, la cui importanza è stata evidenziata anche dalla rinnovata presa di coscienza circa la necessità di irrobustire il sistema per prevenire o fronteggiare eventuali situazioni di crisi:

- si osserva ulteriormente l'opportunità del passaggio al cloud, rispetto

all'attuale gestione di centinaia di data center, in particolare per quanto concerne le PA locali;

- inoltre, appare prioritario **assicurare a livello infrastrutturale la continuità dei servizi cloud** in particolare tramite **ridondanza** delle soluzioni, portabilità e interoperabilità, tracciamento e recuperabilità dei dati. Questo, come evidente, è direttamente collegato alla possibilità per le stesse PA locali, nonché di quelle centrali e delle stesse aziende, di accedere alla più vasta gamma di soluzioni, senza limitazioni di sorta, in particolare relative alle migliori e tecnologicamente più avanzate soluzioni disponibili sul mercato internazionale.

Il sostegno e la promozione di infrastrutture e tecnologie resilienti sono auspicabili anche tramite interventi normativi. A tal proposito:

- si sottolineano favorevolmente previsioni come quelle contenute nel dl **Curaitalia**, finalizzate a **semplificare l'acquisto di soluzione cloud da parte della PA contrastare la situazione emergenziale determinata dalla diffusione del Covid19** favorendo il lavoro agile[37];

- si evidenzia l'opportunità di **supportare** ulteriormente la **diffusione di tecnologie abilitanti flessibili** e capaci di organizzare soluzioni adatte anche a **contesti emergenziali**.

A livello di principi di gestione e prassi operative, appare opportuno **predisporre procedure formalizzate per la ripartenza delle operazioni, il recupero dei dati e la segnalazione e l'analisi degli incidenti di sicurezza,** di concerto con le autorità preposte e nel solco tracciato dalla legge sul perimetro di sicurezza cibernetica e dai relativi decreti attuativi in corso di redazione.

Un'ultima menzione, è relativa alle **competenze digitali atte a favorire la resilienza del sistema.** A tal proposito, si ritiene opportuno:

- favorire forme di **alfabetizzazione informatica finalizzata all'utilizzo di applicazioni flessibili e adattabili a diversi contesti di lavoro**, insieme all'adesione e al consolidamento di pratiche di **smart working;**

[37] In particolare, l'art. 75 del Curaitalia, al fine di agevolare la diffusione del lavoro agile, autorizzava le PA, sino al 31 dicembre 2020, ad acquistare beni e servizi informatici, preferibilmente basati sul modello cloud SaaS, "*mediante procedura negoziata senza previa pubblicazione di un bando di gara […] selezionando tra almeno 4 operatori economici, di cui almeno una «start-up innovativa»*".

- **coinvolgere sulla formazione le stesse imprese hi-tech**, sia italiane, sia internazionali, nell'ottica di mettere a sistema le best practice disponibili e alfabetizzare i lavoratori di PA e imprese all'utilizzo di soluzioni cloud che possano garantire, al contempo, maggiore sicurezza, flessibilità e massimo dispiegamento del potenziale che una piena trasformazione digitale porta con sé.

4.3 UNO SCHEMA OPERATIVO PER IL DIBATTITO

Infine, allo scopo di sintetizzare in modo organico gli spunti e le proposte emerse dall'analisi delle molteplici sfaccettature relative alla relazione tra sovranità digitale e cloud computing, i principali temi sono stati riassunti nella Fig. 4.1.

In particolare, la figura presenta una **dimensione verticale,** che racchiude gli ambiti che fungono da **abilitatori**, quali infrastrutture, servizi e competenze, e quelli che operano in qualità di **armonizzatori**, in particolare le norme, i principi di gestione e le prassi operative; ed una **dimensione orizzontale,** che individua il livello di **competitività e innovazione,** insistendo sui principali temi su cui ragionare in termini di policy, quali l'impatto economico e l'apertura del mercato, la sicurezza e la protezione dell'utente e la resilienza.

Il diagramma così costituito è finalizzato al duplice obiettivo di dettagliare, da un lato, i diversi campi nei quali indirizzare la discussione e, dall'altro, fornire una visione d'insieme finalizzata ad ottimizzare la ricerca del miglior trade-off tra la regolamentazione dei vari ambiti connessi al cloud e l'impatto complessivo sul sistema-Paese.

		Competitività e innovazione		
		Impatto economico e apertura del mercato	**Sicurezza e Protezione dell'utente (pub/pri)**	**Resilienza**
Abilitazione e armonizzazione	**Infrastrutture e servizi**	Completare la rete di accesso ad alta velocità su tutto il territorio nazionale (Piano Bul, diffusione 5G)	Rendere disponibili forme di localizzazione dei dati e dei relativi processi di gestione nella Unione Europea nonché modalità evolute di segregazione delle informazioni (es. cifratura)	Assicurare a livello infrastrutturale continuità di servizio (ridondanza delle soluzioni, portabilità e interoperabilità, tracciamento e recuperabilità dei dati)
		Incentivare lo sviluppo e l'adozione di soluzioni cloud interoperabili che favoriscano la partecipazione e l'integrazione		
		Garantire il pieno controllo sui dati attraverso modalità di localizzazione allineate agli standard europei e di mercato	Assicurare sicurezza enterprise grade basata su standard elevati, l'apertura delle soluzioni infrastrutturali, l'interoperabilità dei servizi e la portabilità di dati e applicazioni	

	Competenze	Creare un Piano integrato per lo sviluppo delle competenze digitali a 360°, supporto dagli attori privati dell'innovazione, rivolto a studenti (potenziamento ITS e incremento laureati STEM), lavoratori (aggiornamento e riqualificazione delle competenze e Lifelong Learning) e cittadini.	Promuovere programmi ad hoc per la diffusione di conoscenze e pratiche in materia di sicurezza informatica presso dipendenti della PA e delle PMI	Favorire l'utilizzo di applicazioni flessibili e adattabili a diversi contesti di lavoro insieme all'adesione e al consolidamento di pratiche di smart working
			Favorire la partecipazione di manager e dipendenti di PA e PMI a corsi di upskilling, reskilling e utilizzo di tecnologie cloud finalizzati ad aumentarne produttività e adattabilità	
	Norme	Assicurare la competitività del mercato mantenendone alta l'attrattività e garantendone l'apertura promuovendo una collaborazione basata su valori e principi comuni, senza discriminazioni geografiche	Classificare dati e asset strategici per valutare quali sono quelli che necessitano di un particolare livello di protezione, con criteri che garantiscano il migliore trade-off tra sicurezza e competitività del mercato	Favorire la diffusione di tecnologie abilitanti flessibili e capaci di organizzare soluzioni adatte anche a contesti emergenziali
		Favorire maggiori investimenti in innovazione e tecnologie sul territorio, italiani ed esteri		
		Favorire l'interoperabilità dei servizi e la portabilità di dati e applicazioni	Definire l'infrastruttura cloud come "infrastruttura critica estesa"	
		Proseguire e intensificare i programmi nazionali (Transizione 4.0) e gli incentivi per un'accelerazione della trasformazione digitale delle PMI tramite il cloud computing		
		Favorire la diffusione del cloud presso la PA accelerando la roadmap sulla Cloud-first policy in modo da migrare al cloud tutta l'infrastruttura ICT pubblica.	Definire e rendere noti eventuali obblighi di trasferimento transfrontaliero dei dati	
		Promuovere l'utilizzo di fondi con cui valorizzare le esperienze e le capacità presenti nella Pubblica Amministrazione evitando la centralizzazione su unico operatore privato di mercato per la gestione in partnership dei PSN ma rafforzando l'infrastruttura pubblica esistente al fine di utilizzarla per le applicazioni non migrabili al cloud di mercato		
		Favorire l'accompagnamento alle nuove tecnologie e la modernizzazione delle applicazioni attraverso forme di incentivi		

	che premino l'adozione di percorsi sinergici di migrazione e la scelta di operatori che facciano della sostenibilità un impegno concreto.		
	Prevedere armonizzazioni di settore per i principali data space e business ecosystem		
	Assicurare l'armonizzazione con altri sistemi giuridici e di regolazione	Definire un Codice di Condotta per la erogazione dei servizi cloud allineato agli standard europei (es. CISPE)	
Principi di gestione e prassi operative	Definire modalità di gestione dei trasferimenti cross-border e le relative modalità di protezione	Stabilire procedure trasparenti e definite per la migrazione al cloud	Predisporre procedure formalizzate per la ripartenza delle operazioni, il recupero dei dati e la segnalazione e l'analisi degli incidenti di sicurezza
		Eseguire controlli sistematici e procedure di sicurezza rigorose per prevenire accessi non autorizzati e manipolazione di dati, applicazioni e algoritmi	
		Stabilire gli ambiti e le modalità di accesso consentite alle forze dell'ordine	
		Assicurare trasparenza sull'utilizzo dei dati ed eventuali forme di rewarding per il loro utilizzo	

FIGURA 4.1 Proposte per un quadro organico di policy e raccomandazioni

Fonte: Elaborazione I-Com su varie

icom istituto per la competitività

APPENDICE A - IL MODELLO DI STIMA DELL'IMPATTO DEL CLOUD SULLE IMPRESE ITALIANE

METODOLOGIA E DESCRIZIONE DELLE VARIABILI

Il modello impiegato è un modello logit ordinale che consente di stimare l'effetto delle variabili indipendenti (adozione delle tecnologie) sulla probabilità che la variabile dipendente (classe di ricavi) appartenga ad una categoria superiore, mostrando se e quanto l'impiego delle tecnologie sopra menzionate aumenti la probabilità di un'impresa di appartenere ad una classe di ricavi superiore. La scelta di questa modello è dettata dalla caratteristica della variabile dipendente, la classe di ricavi cui l'impresa appartiene, che per sua definizione non dà un'indicazione puntuale dei ricavi di ciascuna impresa ma solo dell'appartenenza ad una classe piuttosto che ad un'altra. In altre parole, non si tratta di una variabile continua, ma di una variabile categorica – che può assumere, nel nostro caso, 14 valori, tante quante sono le classi di ricavi. Questa caratteristica rende inappropriato l'utilizzo di un modello di regressione lineare e rende più opportuno l'impiego di un modello logistico38.

Le variabili indipendenti impiegate sono: l'utilizzo di cloud computing (cc), di sistemi di Enterprise Resource Planning (erp), di Customer Relationship Management (crm) e di Big Data Analysis (bda). Al fine di depurare l'effetto di queste variabili da eventuali effetti fissi legati esclusivamente alla dimensione d'impresa oppure all'appartenenza ad un determinato settore o ad una certa area geografica, vengono altresì impiegate delle variabili di controllo, nello specifico: macrosettore per il settore di appartenenza, area geografica per l'area geografica di appartenenza e cl_addetti per la dimensione dell'impresa in base al numero di addetti.

I RISULTATI

Dal modello logistico impiegato risulta un impatto positivo di tutte le tecnologie prese in esame, tenendo conto del macrosettore di appartenenza e della dimensione d'impresa (Tab.5). Le imprese che fanno uso del cloud mostrano, infatti, una probabilità superiore di circa il 34%, rispetto a chi non impiega soluzioni cloud, di appartenere ad una classe di ricavi superiore. Si tratta di un impatto superiore alla media nazionale (27%).

Un risultato simile si ottiene con riferimento al CRM e al BDA (sebbene non statisticamente significativo), mentre molto maggiore è l'effetto di soluzioni ERP: chi le impiega ha una probabilità quasi tripla di appartenere ad

[38] Per ulteriori dettagli sul modello logit ordinale, si veda http://local.disia.unifi.it/grilli/files/Papers/Ordered_Logit.pdf

una classe di ricavi superiore rispetto a chi non impiega soluzioni di questo tipo.

Viene poi suddiviso l'intero campione di imprese del Nord Ovest in 3 sotto-campioni, per piccole, medie e grandi imprese, sulla base della classe di addetti di appartenenza. Viene così replicata l'analisi sui 3 sotto-campioni, al fine di valutare se l'adozione delle tecnologie digitali possa avere un impatto differente su imprese di diversa dimensione. In questo caso, si stima un impatto superiore, pari al 52% circa, mentre per le medie e piccole imprese l'impatto è comunque positivo e significativo, ma inferiore (31% e 28,5%, rispettivamente) (Tab. A.1). Risultati altrettanto importanti si registrano anche per l'enterprise resource planning e per il big data analysis.

TABELLA A.1 L'impatto di cloud e tecnologie digitali sui ricavi delle imprese

VARIABLES	Totale imprese ricavi	Piccole imprese ricavi	Medie imprese ricavi	Grandi imprese ricavi
1.cc	1,270***	1,223***	1,147**	1,557***
	-0,038	-0,048	-0,068	-0,118
1.erp	2,447***	2,306***	2,447***	3,809***
	-0,077	-0,089	-0,16	-0,399
1.crm	1,289***	1,120***	1,463***	1,941***
	-0,039	-0,044	-0,088	-0,151
1.bda	1,267***	1,252***	1,223***	1,408***
	-0,049	-0,073	-0,087	-0,114
2.macrosettore	1,316***	2,076***	0,788**	0,651**
	-0,076	-0,154	-0,092	-0,109
3.macrosettore	0,508***	0,571***	0,638***	1.063
	-0,023	-0,031	-0,064	-0,269
4.macrosettore	0,830***	1,158***	0,683***	0,485***
	-0,027	-0,052	-0,042	-0,04
2.cl_addetti	10,606***	-	-	-
	-0,5			
3.cl_addetti	35,760***	-	-	-
	-1.831			
4.cl_addetti	161,281***	-	-	-
	-9.516			
2.area_geografica	1,501***	1,402***	1,534***	1,838***
	-0,085	-0,098	-0,18	-0,329
3.area_geografica	1,510***	1,334***	1,734***	1,905***
	-0,08	-0,088	-0,183	-0,318

4.area_geografica	1,544***	1,394***	1,731***	1,939***
	-0,084	-0,094	-0,192	-0,338
Observations		11.818	4.387	2.687

Standard errors in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Fonte: Elaborazione I-Com su microdati Istat

icom istituto per la competitività

APPENDICE B - METODO DI STIMA DELL'AUMENTO DI FATTURATO DELLE IMPRESE

Per la stima dell'impatto economico del cloud computing sulle imprese, si suppone che la probabilità stimata dal modello econometrico sia interpretabile come l'incidenza delle imprese che, una volta adottato il cloud, sono in grado di spostarsi da una classe di ricavi a quella immediatamente successiva. Volendo essere conservativi, si assume che ciascuna impresa si assesti sul valore minimo della nuova classe di appartenenza.

Nello specifico, per il sotto-campione di piccole imprese (10-49 addetti), per ciascuna, delle classi di fatturato, si ipotizza che il 22,3%[39] delle imprese che non impiegano soluzioni cloud aumenti i propri ricavi in maniera tale da passare nella successiva classe di fatturato, mentre il restante 77,7%, pur impiegando soluzioni cloud, continui a far parte della stessa classe di fatturato. A queste ultime e alle imprese che già risultano fare uso di cloud viene associato un valore di fatturato pari alla media dei valori estremi della classe di ricavi di appartenenza. Si procede in questo modo per ciascuna classe di fatturato e, a seguire, per il sotto-campione di imprese di medie dimensioni (50-249 addetti) e per quello di imprese di grandi dimensioni (>249 addetti). Il valore incrementale così stimato per il campione di imprese viene suddiviso per il numero di imprese facenti parte del campione stesso, distinguendo tra piccole, medie e grandi imprese, così da calcolare un valore incrementale medio per ciascuna categoria d'impresa. Quest'ultimo viene, a questo punto, moltiplicato per il numero di imprese appartenenti all'intera popolazione delle imprese, sempre distinguendo per dimensione d'impresa. La somma dei tre valori così ottenuti dà un'idea del valore economico – in termini di fatturato aggiuntivo – associabile all'impiego del cloud computing da parte delle imprese nelle tre regioni oggetto d'indagine.

[39] Ossia il coefficiente stimato dal modello logistico di cui all'Appendice A

icom istituto per la competitività

APPENDICE C - IL QUADRO NORMATIVO EUROPEO E LE INIZIATIVE ADOTTATE DOPO LA PRONUNCIA DELLA SENTENZA SCHREMS II

DAL GDPR ALLE PROPOSTE DEL 2019 SUGLI ORDINI EUROPEI DI PRODUZIONE E DI CONSERVAZIONE DI PROVE ELETTRONICHE IN MATERIA PENALE

Il Regolamento n. 679/06 ha rappresentato un punto di svolta per la tutela dei dati personali nell'UE definendo in maniera dettagliata la cornice normativa generale ed apprestando quel set di tutele e rimedi sulla cui efficacia e raffinatezza giuridica vi è concordia a livello globale.

Il **Capo V**, in particolare, disciplina i trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali prevedendo, come principio generale, il rispetto della disciplina contenuta in tale capo e la verifica circa la garanzia, da parte del paese terzo, del territorio o di uno o più settori specifici all'interno del paese terzo, o dell'organizzazione internazionale, di un livello di protezione adeguato. In particolare, gli artt. 45 e 46 individuano due tipologie di trasferimento: **1) Trasferimento sulla base di una decisione di adeguatezza**. L'art. 45, nello specifico, dispone che in presenza di una decisione di adeguatezza adottata dalla Commissione sulla base della valutazione di una serie di parametri e condizioni (relativi al quadro normativo vigente nel Paese in materia di diritti e libertà fondamentali e privacy, alla disponibilità di strumenti di ricorso effettivo, all'esistenza di una o più autorità di controllo indipendenti ed agli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione in relazione alla protezione dei dati personali), il trasferimento non necessiti di autorizzazioni specifiche. Premesso che le decisioni di adeguatezza sono sottoposte ad un riesame periodico almeno ogni quattro anni, è fatta salva, medio tempore, la possibilità per la Commissione di revocare, modificare o sospendere nella misura necessaria la decisione adottata nel caso emerga che lo stato o l'organizzazione non garantiscono più un livello di protezione adeguato; **2) Trasferimento soggetto a garanzie adeguate** (art. 46). In mancanza di una decisione di adeguatezza, il titolare del trattamento o il responsabile del trattamento può trasferire dati personali verso un paese terzo o un'organizzazione internazionale solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi. La stessa disposizione fornisce un elenco di possibili strumenti in grado di assicurare garanzie adeguate (uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici, le norme vincolanti d'impresa, le clausole tipo di protezione dei dati adottate dalla Commissione oppure adottate da un'autorità di controllo e approvate dalla Commissione ex art. 93, un codice di condotta approvato, unitamente all'impegno

vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati o un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati).

L'art. 48 disciplina, invece, il **trasferimento o comunicazione non autorizzati dal diritto dell'Unione**, prevedendo che le organizzazioni non sono legittimate a trasferire dati personali verso un paese terzo sulla base di una sentenza o di una decisione amministrativa a meno che non si fondino su un accordo internazionale, come un mutuo trattato di assistenza legale (strumento peraltro previsto dallo stesso Cloud Act).

Il successivo art. 49 individua le **deroghe in specifiche situazioni** in presenza delle quali è ammesso il trasferimento o un complesso di trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale (esplicito consenso dell'interessato, trasferimento necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato, per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato, per importanti motivi di interesse pubblico, per accertare, esercitare o difendere un diritto in sede giudiziaria, per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso, il trasferimento sia effettuato a partire da un registro).

In caso di inapplicabilità degli artt. 45 e 46 ed in mancanza, nel caso di specie, di deroghe in specifiche situazioni, il trasferimento verso un paese terzo o un'organizzazione internazionale è ammesso soltanto se non è ripetitivo, riguarda un numero limitato di interessati, è necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare e del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali.

Nell'ambito di questa cornice normativa generale, considerato che è in forte crescita il numero di reati commessi online o mediante l'utilizzo del canale informatico e che l'Unione

europea deve affrontare il tema della raccolta e della conservazione delle prove elettroniche nel tentativo di rendere più rapide ed efficaci tali attività, il 17 aprile 2018 la Commissione ha pubblicato una **proposta di regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018) 225 final) e una proposta di direttiva (COM(2018) 226 final), per la definizione di norme sulla rappresentanza legale nell'Unione di determinati prestatori di servizi ai fini della ricezione, dell'ottemperanza e dell'esecuzione di decisioni e ordini emessi dalle autorità competenti degli Stati membri per acquisire prove nei procedimenti penali.**

Quanto all'ambito applicativo, il regolamento proposto stabilisce le norme in base alle quali un'autorità di uno Stato membro può ingiungere a un prestatore di servizi che offre servizi nell'Unione di produrre o conservare prove elettroniche, indipendentemente dall'ubicazione dei dati (facendo salva la facoltà delle autorità nazionali di ingiungere ai prestatori di servizi stabiliti o rappresentati nel loro territorio di ottemperare a misure nazionali dello stesso tipo).

Per prestatore di servizi si intendono, in particolare, le persone fisiche o giuridiche che offrono servizi di comunicazione elettronica (come definiti dal codice europeo delle Comunicazioni elettroniche), servizi della società dell'informazione (come definiti all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio), per i quali la conservazione dei dati è una componente propria del servizio fornito all'utente, tra cui i social network, i mercati online che agevolano le operazioni tra utenti e altri prestatori di servizi di hosting e servizi di nomi di dominio internet e di numerazione IP, quali i prestatori di indirizzi IP, i registri di nomi di dominio, i registrar di nomi di dominio e i connessi servizi per la privacy o proxy.

Ai fini dell'applicabilità del regolamento, si richiede la **sussistenza di un collegamento sostanziale con l'Unione che si realizza certamente quando il prestatore di servizi ha uno stabilimento nell'Unione**. In mancanza, la proposta dispone la verifica dell'esistenza di un collegamento sostanziale che si intende esistente, ad esempio, in presenza di un numero significativo di utenti in uno o più Stati membri, o dell'orientamento delle attività verso uno o più Stati membri (da verificare sulla base di tutte le circostanze pertinenti, tra cui l'uso di una lingua o di una moneta generalmente usata nello Stato membro in questione o la possibilità di ordinare prodotti o servizi, la disponibilità di un'app nell'apposito negozio online nazionale, la fornitura di pubblicità a livello locale etc.). Presupposto per l'emissione di un

ordine di conservazione o di produzione è l'esistenza di procedimenti penali, in fase sia preprocessuale che processuale.

La **competenza ad emettere ordini di produzione riguardanti dati relativi agli abbonati o dati relativi agli accessi, alle operazioni o dati relativi al contenuto, nonché ordini di conservazione** spetta ad un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero competente nel caso interessato o a qualsiasi altra autorità competente, definita dallo Stato di emissione che, nel caso di specie, agisca in qualità di autorità inquirente nel procedimento penale e sia competente a disporre l'acquisizione di prove in conformità del diritto nazionale la quale ha bisogno di convalida da un giudice, un organo giurisdizionale, un magistrato inquirente o un pubblico ministero nello Stato di emissione (in tal caso il soggetto convalidante sarà riconosciuto come autorità di emissione).
La proposta fissa altresì le **condizioni per l'emissione di un ordine di produzione nonché i contenuti dell'ordine stesso**, prescrivendo, a livello generale, che l'ordine sia necessario e proporzionato ai fini del procedimento penale sottostante e sia disponibile una misura dello stesso tipo, per lo stesso reato, in una situazione nazionale comparabile nello Stato di emissione e precisando che mentre l'ordine europeo di produzione di dati relativi agli abbonati o dati relativi agli accessi può essere emesso per qualsiasi reato, l'ordine europeo di produzione di dati relativi alle operazioni o dati relativi al contenuto possa essere emesso solo reati punibili nello Stato di emissione con una pena detentiva della durata massima di almeno 3 anni oppure per altri specifici e particolarmente gravi reati, puntualmente identificati dalla disposizione di cui all'art. 5, c. 4 lett. a), b) e c).

Dal punto di vista procedurale, la stessa proposta attribuisce all'Autorità di emissione la **facoltà di consultare le autorità dello Stato membro nel quale il destinatario risiede o è stabilito prima di emettere l'ordine di produzione** qualora abbia motivo di ritenere che i dati richiesti relativi alle operazioni o al contenuto siano protetti con immunità e privilegi o che la loro divulgazione possa incidere su interessi fondamentali di tale Stato membro, come la sicurezza e la difesa nazionali. L'ordine europeo di conservazione può invece essere emesso per qualsiasi reato a condizione che sia necessario e proporzionato per impedire la rimozione, la cancellazione o la modifica di dati in vista di una successiva richiesta di produzione dei medesimi tramite l'assistenza giudiziaria, un ordine europeo d'indagine o un ordine europeo di produzione.

Dal punto di vista della procedura e delle **tempistiche di risposta**, a fronte della

ricezione di un ordine di produzione, il destinatario deve provvedere entro 10 gg. (o nel minor tempo eventualmente indicato nell'ordine, 6 ore in caso di emergenza) a meno che non si trovi nell'impossibilità di dare riscontro ad es. perché trattasi di dato previamente eliminato oppure per incompletezza o erroneità dell'ordine (da segnalare senza ritardo. In tal caso l'autorità dovrà fornire riscontro entro 5 gg.).
Nel caso invece di ordine di conservazione, il destinatario provvede, senza indebito ritardo, a conservare i dati richiesti per un periodo massimo di 60 giorni, a meno che l'autorità di emissione confermi che è stata avviata la successiva richiesta di produzione (è sempre fatta salva la possibilità di dare motivazioni circa l'impossibilità di procedere alla conservazione e di evidenziare incompletezze o errori che riguardino l'ordine).

All'inosservanza delle disposizioni la proposta collega **sanzioni pecuniarie** – la cui fissazione è rimessa agli Stati – che devono essere effettive, proporzionate e dissuasive.

La proposta di regolamento declina secondo il principio di tassatività i **casi di possibile opposizione da parte del destinatario di un ordine di produzione e conservazione** e descrive la **procedura di riesame** da attivare nel caso di obblighi contrastanti basati su diritti fondamentali o interessi fondamentali di un paese terzo, prevedendo che: 1) l'opposizione sia motivata e contenga tutte le informazioni pertinenti sul diritto del paese terzo, sulla sua applicabilità al caso di specie e sulla natura dell'obbligo contrastante; 2) l'autorità di emissione riesamini l'ordine europeo di produzione sulla base dell'obiezione motivata; 3) l'organo giurisdizionale competente dello Stato membro dell'autorità di emissione riesami l'ordine nel caso quest'ultima decida di confermarlo. In tal caso, il giudice competente dovrà valutare innanzitutto se esista un contrasto, esaminando a) se, in base alle circostanze specifiche del caso di specie, si applica il diritto del paese terzo e, in caso affermativo, b) se il diritto del paese terzo, ove applicato alle circostanze specifiche del caso, vieta la divulgazione dei dati in questione nonché esaminare se il diritto del paese terzo, anziché tutelare i diritti fondamentali o interessi fondamentali del paese terzo connessi alla sicurezza o alla difesa nazionali, intenda manifestamente tutelare altri interessi o proteggere attività illecite dalle richieste delle autorità di contrasto nell'ambito delle indagini penali. Nel caso ravvisi un contrasto, la proposta disciplina modalità e tempistiche entro cui l'autorità centrale del paese terzo deve dare riscontro all'organo giurisdizionale opponendosi o meno all'ordine.

La proposta disciplina, inoltre, la **procedura di riesame** in caso di obblighi contrastanti basati

su altri motivi prevedendo, anche in tal caso, l'intervento del competente organo giurisdizionale nel caso di conferma dell'ordine da parte dell'autorità di emissione e precisando che quest'ultimo, nel decidere se confermare o ritirare l'ordine si basi su alcuni elementi specifici.
La proposta prescrive, infine, che gli indagati e gli imputati i cui dati siano stati ottenuti tramite un ordine europeo di produzione abbiano il diritto a un ricorso effettivo contro tale ordine durante il procedimento penale per il quale l'ordine è stato emesso.

Al fine di affrontare tali possibili conflitti di legge e ridurre il ricorso alle procedure di riesame che pure le proposte prevedono, in linea con il principio di cortesia internazionale, il 5 febbraio 2019 la Commissione ha adottato una **raccomandazione di decisione del Consiglio (COM(2019) 70 final) che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale o l'avvio di negoziati**. Si tratta di un'iniziativa importante che fissa gli obiettivi da perseguire nell'ambito dei negoziati, richiede la puntuale definizione della natura e dell'ambito applicativo dell'accordo, individua le garanzie da assicurare e definisce la governance dell'accordo.

Quanto agli **obiettivi** da perseguire, la raccomandazione evidenzia l'importanza di: a) fissare norme comuni e affrontare i conflitti di legge relativi agli ordini per l'ottenimento di prove elettroniche sotto forma di dati relativi al contenuto e dati non relativi al contenuto emessi da un'autorità giudiziaria di una Parte contraente e rivolti a un prestatore di servizi soggetto alla legge dell'altra Parte contraente al fine di ridurre il rischio di frammentazione ed accrescere la certezza; b) consentire un trasferimento di prove elettroniche direttamente su base di reciprocità da parte di un prestatore di servizi a un'autorità richiedente; c) assicurare il rispetto dei diritti e delle libertà fondamentali e dei principi generali del diritto dell'UE come sanciti dai trattati e dalla Carta dei diritti fondamentali dell'Unione europea.

In termini di **garanzie**, invece, la raccomandazione suggerisce l'adozione di garanzie aggiuntive in materia di protezione dei dati e della vita privata che, in particolare, dovrebbero, tra l'altro, interessare la specificazione delle finalità per le quali i dati personali e i dati delle comunicazioni elettroniche possono essere richiesti e trasferiti, il requisito che l'ordine sia limitato ai dati personali e ai dati delle comunicazioni elettroniche necessari e proporzionati in funzione della finalità per i quali l'accesso è autorizzato, la previsione di specifiche

procedure di notifica ed autorizzazione preventiva da parte dell'autorità giudiziaria per l'uso e la divulgazione dei dati ad autorità statunitensi non vincolate dall'accordo, il requisito che i trasferimenti successivi ad altri paesi terzi possano essere effettuati solo nei confronti delle autorità di contrasto responsabili della prevenzione, indagine, accertamento e perseguimento di reati, compreso il terrorismo, e dovrebbero essere soggetti all'obbligo di notifica e autorizzazione preventiva da parte dell'autorità giudiziaria competente designata dallo Stato membro in cui il prestatore di servizi è stabilito o rappresentato (fatta salva la possibilità di prendere in esame le circostanze eccezionali e le garanzie richieste laddove un ulteriore trasferimento possa avvenire senza autorizzazione preventiva, in caso di minaccia grave e imminente per la sicurezza pubblica di uno Stato membro o di un paese terzo).

Quanto, infine, alla **governance**, si richiede la previsione di una verifica periodica congiunta delle Parti che verifichino la sua applicazione ed esaminino come renderne più efficace l'uso.

LE INIZIATIVE ADOTTATE DOPO LA SENTENZA SCHREMS II

A quattro mesi dalla pronuncia di tale sentenza, il 29 ottobre scorso lo European Data Protection Supervisor (EDPS) - il Garante europeo della protezione dei dati i cui poteri, competenze ed organizzazione sono definiti dallo stesso regolamento n. 1275/2018 - ha pubblicato la ***Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling***, volta a delineare un piano strategico per assicurare che i trasferimenti internazionali in corso e futuri siano effettuati in conformità a quanto previsto dalla Carta europea dei diritti fondamentali e dal Cap. V del regolamento n. 1725/2018.

Al fine di individuare le azioni da mettere in campo, la strategia, in una logica di identificazione delle azioni di breve periodo, dopo aver invitato le istituzioni a focalizzare l'attenzione in via prioritaria sui trasferimenti diretti a soggetti privati in particolare negli USA, dà conto dell'adozione, da parte del Garante, di un **approccio fondato sull'analisi del rischio**, e del successivo avvio (il 5 ottobre) da parte delle istituzioni europee, su disposizione dello stesso Garante, di **un'attività di mappatura ed inventario, di tutte le operazioni ed i contratti pendenti che comportino trasferimenti di dati verso paesi terzi**. Le medesime istituzioni sono state inoltre chiamate a compiere, entro il 15 novembre, una relazione circa gli specifici rischi e le carenze individuate nello svolgimento di tale attività di mappatura con specifico riferimento a tre tipologie di

trasferimenti: a) trasferimenti illegali che non si fondano su alcun strumento di trasferimento; b) trasferimenti basati sulla disciplina di cui all'art. 50 del Reg. n. 1725/2018; c) trasferimenti ad "alto rischio" verso gli USA a soggetti chiaramente soggetti alla Sezione 702 FISA o ad un executive order e che comportano operazioni di trattamento su larga scala o complesse o il trattamento di dati sensibili o di dati di natura altamente personale. Il tutto per consentire al Garante, sulla base di questo primo esercizio di segnalazione, di intraprendere azioni esecutive per rendere tali trasferimenti conformi al regolamento o sospenderli, se del caso.

In una logica precauzionale, il Garante ha poi fornito un'esortazione piuttosto importante alle istituzioni: garantire che qualsiasi nuova operazione di trattamento o nuovo contratto con qualsiasi fornitore di servizi non comporti trasferimenti di dati personali verso gli Stati Uniti.

Se questo è quanto disposto per il breve periodo, con riferimento al medio, il Garante ha richiesto alle istituzioni europee di condurre **valutazioni di impatto del trasferimento (Transfer Impact Assessments – TIA)** per verificare se nel paese terzo di destinazione è garantito un livello di protezione sostanzialmente equivalente a quello previsto dall'UE ed adottare le conseguenti decisioni (prevedendo, se necessario, misure supplementari o salvaguardie aggiuntive e verificando che sia applicabile, ad alcuni dei trattamenti esaminati, le deroghe contenute nell'art. 50 del Reg. n. 1725/2018). A tal fine, il Garante ha annunciato la formulazione, sulla base delle linee guida previste dal Comitato europeo per la protezione dei dati (EDPB), di un elenco di domande preliminari per i responsabili del trattamento da sottoporre agli importatori dei dati nell'ambito di tali valutazioni. Sulla base delle risultanze emerse a seguito delle TIA, le istituzioni dovranno inviare al Garante una relazione, nel corso della primavera 2021, sulla base del quale lo stesso Garante, in collaborazione con il Comitato, formulerà le priorità di conformità da seguire per il 2021.

Il Garante ha inoltre annunciato l'avvio di un'analisi tesa a verificare la possibilità di operare valutazioni congiunte *(joint assessments*) del livello di protezione dei dati personali offerto nei paesi terzi e le modalità di coordinamento tra autorità, responsabili del trattamento e altre parti interessate per fornire orientamenti e garantire il rispetto dei principi affermati nella sentenza Schrems II. A ciò si aggiunge l'impegno del Garante a cooperare con le altre autorità operanti nell'Area Economica Europea per la definizione di linee guida e raccomandazioni per agevolare l'individuazione delle misure supplementari per assicurare un livello di

protezione sostanzialmente equivalente a quello previsto dalla UE quando si trasferiscono dati a Paesi terzi.

In occasione della quarantunesima sessione plenaria tenutasi il 10 novembre 2020, il Comitato europeo per la protezione dei dati (EDPB), che riunisce i Garanti nazionali, ha pubblicato le **"*Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*"** (sottoposte a consultazione pubblica fino al 30 novembre) e le **"*Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*"**.

Si tratta di raccomandazioni che perseguono il fine di agevolare gli esportatori (siano essi enti privati o organismi pubblici, che trattano dati personali nell'ambito di applicazione del GDPR) nel complesso compito di valutare i paesi terzi ed individuare, se necessario, adeguate misure supplementari, mediante la definizione di una serie di step procedimentali da seguire che si sostanziano: 1) nello svolgimento di un'attività di **mappatura**, tesa ad individuare tutti i trasferimenti di dati personali verso paesi terzi per verificare la sostanziale equivalenza del livello di protezione assicurato nei vari paesi destinatari del trasferimento e verificare che i dati trasferiti siano adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali vengono trasferiti e trattati nel paese terzo; 2) nell'identificare lo **strumento di trasferimento** su cui si basa il trasferimento, tra quelli elencati nel capitolo V GDPR andando, in particolare, a verificare se la Commissione abbia già adottato una decisione di adeguatezza ai sensi dell'articolo 45 GDPR (o della precedente Direttiva 95/46) applicabile al caso di specie e se tale decisione sia ancora valida, oppure, in assenza di una decisione di adeguatezza, fare ricorso ad uno degli strumenti di trasferimento elencati all'articolo 46 GDPR per i trasferimenti che sono regolari e ripetitivi. Solo in alcuni casi di trasferimenti occasionali e non ripetitivi si può fare affidamento su una delle deroghe previste dall'articolo 49 GDPR, se appaiono soddisfatte le condizioni definite da tale disposizione; 3) nel valutare se esistono **elementi** nella legge o nella prassi del paese terzo in grado di incidere sull'efficacia delle garanzie assicurate dagli strumenti di trasferimento applicabili al caso di specie. Nello svolgimento di tale valutazione ed in considerazione delle specifiche responsabilità gravanti sulle autorità che dispongono il trasferimento verso il paese terzo, particolare attenzione va riservata alle ipotesi di assenza, ambiguità o non accessibilità al pubblico della legislazione che disciplini le circostanze in cui le autorità pubbliche possono accedere ai dati personali. Nel caso in cui l'autorità decida comunque di procedere al trasferimento, il

Comitato incentiva ad utilizzare la dovuta diligenza e a documentare accuratamente la decisione adottata; 4) nell'identificare ed adottare (con la dovuta diligenza e fornendo la relativa documentazione a sostegno) le eventuali **misure supplementari** (di natura contrattuale, tecnica o organizzativa) necessarie per assicurare un livello di protezione dei dati sostanzialmente equivalente a quello garantito dall'UE, tenendo a mente che ciascun paese terzo ed ogni trasferimento di dati presenta peculiarità specifiche, che potrebbe rivelarsi efficace l'impiego congiunto di diverse misure e che nel caso in cui nessuna misura supplementare dovesse risultare adeguata, si dovrà evitare, sospendere o interrompere il trasferimento per evitare di compromettere il livello di protezione dei dati personali.

Nell'identificare le misure da mettere in campo il Comitato raccomanda la **valutazione di una serie di fattori** ed in particolare, il formato e la natura dei dati da trasferire, la lunghezza e la complessità del flusso di elaborazione dei dati, nonché il numero di attori coinvolti e le relazioni tra essi esistenti e la possibilità che i dati possano essere oggetto di trasferimenti successivi, all'interno dello stesso paese terzo o anche verso altri paesi terzi.

Dal punto di vista qualitativo, le raccomandazioni offrono una serie di indicazioni circa le possibili misure da mettere in campo tra cui spicca, per importanza, il **ricorso alla crittografia ed alla pseudonimizzazione**. Rispetto al ricorso alla crittografia, in particolare, le raccomandazioni prescrivono che la cifratura sia "implementata e convalidata in modo impeccabile", richiede che la robustezza dell'algoritmo di cifratura e della sua parametrizzazione sia valutata tenendo conto delle risorse e delle capacità tecniche a disposizione degli Stati e che le chiavi siano gestite in modo affidabile (generate, amministrate, conservate, se del caso, collegate all'identità di un destinatario previsto, e revocate) e conservate esclusivamente sotto il controllo dell'esportatore di dati, o di altri soggetti incaricati di questo compito che risiedono nel SEE o in un paese terzo, in una regione o presso un'organizzazione internazionale; 5) nel definire le procedure formali necessarie per adottare le misure supplementari; 6) nel rivalutare e monitorare, ad intervalli temporali appropriati, in ossequio al principio di responsabilità che richiede una vigilanza continua sul livello di protezione dei dati personali, il livello di protezione dei dati trasferiti in paesi terzi e verificare se ci sono stati o ci saranno sviluppi in grado di influire su di essi.

Nonostante tali raccomandazioni rappresentino, in linea di principio, uno strumento di ausilio utile per assicurare

trasferimenti in linea con il diritto europeo, residuano criticità irrisolte e rigidità che potrebbero frapporre importanti ostacoli ai trasferimenti di dati. È il caso, in particolare, di cloud o data processor in Paesi ritenuti non sicuri. In tal caso, infatti, l'Annex 2 esclude, allo stato attuale dell'arte, la possibilità di individuare una misura tecnica efficace per garantire i diritti dell'interessato nelle ipotesi in cui il titolare del trattamento trasferisce i dati a un fornitore di servizi cloud o altro responsabile del trattamento e tale fornitore di servizi cloud (o altro responsabile) deve accedere ai dati in chiaro per eseguire il compito assegnato ed il potere concesso alle autorità pubbliche del paese destinatario di accedere ai dati trasferiti va oltre quanto necessario e proporzionato in una società democratica.

A completamento di tali raccomandazioni, nella stessa data il Comitato ha pubblicato le "***Recommendations 02/2020 on the European Essential Guarantees for surveillance measures***", in cui viene affrontata la questione dell'accesso ai dati personali da parte di autorità pubbliche di paesi terzi ed identificate, alla luce della giurisprudenza della Corte di Giustizia europea, le seguenti quattro garanzie europee essenziali da predisporre per porre limitazioni ai diritti al rispetto della vita privata e della vita familiare ed alla protezione dei dati di carattere personale riconosciuti dalla Carta dei diritti fondamentali dell'UEA: 1) il trattamento dovrebbe basarsi su regole chiare, precise e accessibili; 2) si deve dare dimostrazione della necessità e della proporzionalità del trattamento rispetto ai legittimi obiettivi perseguiti andando a valutare, da un lato, la gravità dell'ingerenza e, dall'altro, l'importanza dell'obiettivo di interesse pubblico perseguito ed escludendo che la normativa che consenta alle autorità pubbliche di accedere in modo generalizzato al contenuto delle comunicazioni elettroniche sia conforme al diritto fondamentale al rispetto della vita privata; 3) predisposizione di un meccanismo di controllo indipendente realizzato da un tribunale o un'autorità amministrativa indipendente che verifichi, con una decisione vincolante, l'esistenza di una situazione che giustifica il provvedimento ed il rispetto delle condizioni e delle garanzie previste; 4) disponibilità di rimedi efficaci per gli interessati.

icom
istituto per la competitività

icom
istituto per la competitività

Roma
Piazza dei Santi Apostoli 66
00187 Roma, Italia
Tel. +39 06 4740746

Bruxelles
Rue de la Science 14B
1040 Bruxelles, Belgio
Tel. +32 (0)2 880 3695

info@i-com.it
www.i-com.it
www.icomRU.eu