Rassegna Stampa

di Lunedì 24 novembre 2025

Centro Studi C.N.I.

Sommario Rassegna Stampa

Quotidiano
24-11-2025
Pagina 1+6
Foglio 1 / 3

Il Sole 24 ORE

Imprese

SICUREZZA INFORMATICA: INCENTIVI FRENATI DALL'EFFETTO BUROCRAZIA

di **Ivan Cimmarusti**

—a pagina 6

Cybersicurezza: incentivi a metà fra burocrazia e spese escluse

Il quadro. Dal maxi ammortamento con detrazione dei costi al voucher del Mimit con plafond da 150 milioni: tutte le misure a sostegno delle imprese per il 2025-2026. Fuori gli oneri per servizi It. Procedure complesse e tempi di accesso frenano l'utilizzo

Pagina a cura di
Ivan Cimmarusti

Non è solo una questione di quanti soldi ci sono in campo. Il punto vero, quando si parla di cybersicurezza delle Pmi italiane, è come quelle risorse sono progettate, rese accessibili, strutturate nel tempo.

Le misure pubbliche oggi in vigore sono davvero adeguate a proteggere le imprese, mentre gli attacchi informatici si moltiplicano e diventano sempre più sofisticati? Quanto lo Stato accompagna concretamente queste realtà produttive nell'investimento – spesso oneroso – in infrastrutture di sicurezza? E soprattutto: gli strumenti messi sul tavolo sono davvero all'altezza della minaccia o stiamo combattendo ransomware e phishing con armi spuntate?

Per capire quanto e come il sistema pubblico stia aiutando le imprese in questa transizione, Tinexta – gruppo specializzato in trasformazione digitale e crescita delle Pmi – tramite le aziende del Gruppo Tinexta Cyber e Tinexta Innovation Hub ha elaborato per il Sole 24 Ore una mappa dettagliata di agevolazioni, contributi, finanziamenti e programmi Ue disponibili tra il 2025 e il 2026 per potenziare la cybersicurezza aziendale (si veda la tabella). Perché se è vero che una parte della partita si gioca sulla consapevolezza – riconoscere ed evitare un'email anomala resta essenziale – è altrettanto vero che non basta: senza investimenti in sicurezza informatica (sistemi aggiornati, infrastrutture, gestione professionale) il confine tra tentato attacco e disastro resta sottilissimo. La "geografia degli incentivi", pur rappresentando un punto di svolta, dimostra però un quadro incompleto.

Le misure in campo

Il perno è il nuovo maxi ammortamento 2026 – previsto allo stato dal Ddl di Bilancio –, che aumenta le quote deducibili per beni strumentali nuovi, inclusi software, sistemi e piattaforme per proteggere reti, dati e impianti, secondo gli allegati A e B della legge 232/2016 (legge di Bilancio 2017) in tema cyber. In base al testo attuale del Ddl, vale per investimenti effettuati nel 2026 (con possibile coda al 30 giugno 2027) e prevede maggiorazioni decrescenti, ma con intensità massima su investimenti fino a 2,5 milioni di euro. È la misura chiamata a rimpiazzare progressivamente Transizione 4.0 e 5.0, restando cumulabile con altri incentivi entro il costo del bene.

Sul fronte dei contributi diretti spicca il voucher "Cloud & Cybersecurity" del Mimit (2025), che rimborsa fino al 50% delle spese per servizi cloud e soluzioni di sicurezza (Mfa, firewall, cifratura, Siem, backup), con importi tra 4mila e 40mila euro per impresa e una dotazione di circa 150 milioni, rivolto a Pmi e microimprese.

Accanto a queste leve agiscono strumenti finanziari già noti ma orientabili al cyber: Nuova Sabatini (contributo in conto interessi su finanziamenti per tecnologie digitali); finanziamenti Simest per progetti di digitalizzazione per la competitività internazionale con quota a fondo perduto; Fondo di garanzia Pmi, che copre fino all'80% dei prestiti per progetti It, riducendo costi e assorbimento di capitale.

A livello locale, bandi regionali e camerali (ad esempio i Voucher digitali I4.0) coprono audit, consulenze e soluzioni di sicurezza con incentivi tra il 40% e il 60 per cento. Nei grandi contratti di sviluppo e nelle Zes/Zls, infine, la componente cyber è finanziabile se integrata nei progetti industriali sopra i 20 milioni di euro.

I nodi da sciogliere

Secondo Tinexta Innovation Hub, c'è grande attesa per i nuovi maxi ammortamenti 2026, che possono realmente alleggerire il peso degli investimenti tecnologici sui bilanci aziendali. E si iniziano finalmente a vedere misure specifiche, pensate proprio per la cybersicurezza delle Pmi.

Tuttavia, molte agevolazioni – pur citando la cybersicurezza tra gli obiettivi – non coprono in modo pieno tutte le spese effettivamente necessarie per garantire livelli ade-

Il Sole 24 ORE

guati di protezione. Restano spesso ai margini i costi ricorrenti per servizi It, attività di governance, gestione del rischio e servizi gestiti: elementi ormai indispensabili per un approccio maturo e continuativo alla sicurezza informatica.

Come ricordano gli esperti, la cybersecurity non è un intervento "una tantum", né un progetto che si conclude con la consegna di un software. È un processo continuo, che richiede prevenzione, monitoraggio costante e adattamento alle nuove minacce. Se gli incentivi non seguono questa logica, rischiano di mitigare solo parzialmente il problema.

A tutto questo si aggiunge un altro ostacolo ben noto agli imprenditori: la complessità delle procedure e i tempi di accesso alle misure. Bandi complicati, documentazione stratificata, finestre temporali ristrette e iter lunghi scoraggiano molte imprese, che spesso non hanno un ufficio interno dedicato solamente a intercettare e gestire incentivi pubblici.

Un quadro, insomma, che dovrà essere modellato. Anche perché c'è un livello più alto che inquieta: le intelligence europee registrano il proliferare di attacchi di natura "statuale". Sono offensive condotte da Paesi come Russia, Cina, Corea del Nord, Iran con l'obiettivo esplicito di indebolire le economie del continente europeo (secondo la società Crowdstrike l'Italia è tra i primi cinque Paesi europei per numero di attacchi). Una forma di guerra ibrida che colpisce al cuore i sistemi produttivi, con attacchi alle imprese, e mina la fiducia dei cittadini verso le istituzioni, anche attraverso campagne di disinformazione che tendono a mitizzare altre economie rivali, come nel caso della Russia. Temi oggetto del Consiglio supremo della difesa della scorsa settimana, presieduto dal presidente della Repubblica, Sergio Mattarella. Si pensi che secondo l'Agenzia per la cybersicurezza nazionale, nei primi sei mesi del 2025 gli eventi sono aumentati del 53% rispetto allo stesso periodo dello scorso anno.

22%
Obiettivo Europa
Secondo Crowdstrike, società Usa di cybersicurezza, le economie europee rappresentano il 22% degli obiettivi globali

+53%
Eventi
Per l'Agenzia per la cybersicurezza nazionale, in sei mesi del 2025 gli eventi cyber sono aumentati del 53% rispetto allo scorso anno

70%
Vulnerabilità
Secondo Tinexta Cyber, il 70% degli attacchi alle Pmi sfrutta vulnerabilità facili da intercettare

Il Fondo di garanzia Pmi copre fino all'80% dei prestiti per progetti It, riducendo costi e assorbimento di capitale


Il Sole 24 ORE
Flat tax
Per i dipendenti risparmi Irpef a 2 miliardi nel 2026
Cultura, ancora pochi lavoratori giovani


Cybersicurezza: incentivi a metà fra burocrazia e spese escluse

Il Sole 24 ORE

La mappa degli aiuti

Agevolazioni fiscali, contributi a fondo perduto, finanziamenti e programmi Ue per sostenere nel biennio 2025-2026 gli investimenti in sicurezza informatica delle imprese (in particolare Pmi)

MISURA	TIPOLOGIA	COSA PREVEDE	CYBERSECURITY AMMISSIBILE	INTENSITÀ/IMPORTI	NOTE/CUMULABILITÀ
Maxi ammortamenti 2026*	Agevolazione fiscale	Maggiorazione del costo di acquisizione dei beni strumentali nuovi (materiali e immateriali) con deduzione più alta di ammortamenti o leasing	Software, sistemi, piattaforme e applicazioni per protezione reti, dati, programmi e macchine (allegati A e B L. 232/2016)	+180% fino a 2,5 milioni di euro; +100% tra 2,5-10 milioni; 50% tra 10-20 milioni; premialità green fino 220%	Sostituisce progressivamente crediti d'imposta Transizione 4.0/5.0. Cumulabile nel limite del costo
Voucher "Cloud & Cybersecurity" (Mimit)	Contributo a fondo perduto	Fino al 50% per servizi cloud e cybersicurezza	Soluzioni di sicurezza It (Mfa, firewall, cifratura, Siem, backup e altri)	Importo massimo del contributo per impresa: 20mila euro. Importo minimo di progetto: 4mila	Gestione Mimit
Nuova Sabatini	Contributo in conto impianti	Contributo su finanziamenti-leasing per beni strumentali	Software e tecnologie digitali per sicurezza informatica	Contributo su interessi (parametrato alla tipologia di investimento)	Cumulabile con maxi ammortamenti
Simest – Transizione digitale/ecologica	Finanziamento agevolato con quota a fondo perduto	Sostegno a progetti di digitalizzazione a supporto dell'internazionalizzazione	Spese per cybersicurezza ammissibili a supporto della transizione digitale	Finanziamento agevolato con possibile quota a fondo perduto (percentuali variabili)	
Fondo di Garanzia per le Pmi	Garanzia pubblica su finanziamenti bancari	Garanzia fino all'80% su prestiti per progetti di sicurezza It, riducendo costo e assorbimento di capitale	Progetti digital-cyber	Copertura garanzia fino all'80% (in base alle regole vigenti)	Complementare a prestiti e altre misure
Digital Europe Programme 2025–2027	Programma Ue – bandi	Bandi su cybersicurezza, competenze digitali, infrastrutture dati. Partecipazione in consorzi	Linee-bandi specifici su cybersicurezza	Contributi a progetto secondo bando	Regole Ue; cumulabilità secondo bando
European Digital Innovation Hubs	Servizi	Servizi gratuiti o scontati	Assessment cyber, test-before-invest, formazione e supporto tecnico	Sconti/erogazione servizi (no contributi diretti)	Riduce costi di consulenza; complementare ad altre misure
Voucher Digitali I4.0 e bandi regionali/camerali	Contributo a fondo perduto	Spese per audit, consulenze e soluzioni di sicurezza informatica	Acquisto prodotti di cybersicurezza	Frequentemente 40-70%; importi: 5mila-10mila euro	Regole di cumulabilità definite dai bandi locali
Contratti di sviluppo / Zes / Zls	Agevolazioni per grandi investimenti	Sostegno a nuovi stabilimenti, ampliamenti, diversificazioni; la componente cyber è ammissibile se parte dell'investimento produttivo	Componente cyber integrata nell'investimento industriale	Secondo schema agevolativo previsto	Regole specifiche per ciascuno schema (Contratti/ Zes/Zls)

(*) Regole attualmente previste dalla bozza della legge di bilancio - Fonte: Tinexta Innovation Hub per il Sole 24 Ore

EURO-ECONOMIE SOTTO ATTACCO

Le analisi della Difesa

«Il comparto manifatturiero risulta particolarmente bersagliato, in gran parte a causa della prevalenza di piccole e medie imprese prive di strutture di difesa adeguate, che lo rendono uno dei settori più colpiti dai ransomware». È questo uno degli allarmi contenuti nel "Non paper" del ministero della Difesa, illustrato dal ministro Guido Crosetto nel Consiglio supremo della Difesa della scorsa settimana.
Il principale varco resta la posta elettronica: email costruite ad arte vengono usate per sottrarre informazioni sensibili, aprendo la strada al ricatto

Il comparto manifatturiero

In Europa, quest'anno, il ransomware è già cresciuto del 48% rispetto al 2024. Colpisce soprattutto i Paesi economicamente più appetibili: Regno Unito e Germania, con l'Italia terza seguita da Francia e Spagna. I dati sono della società di cybersicurezza Crowdstrike. Nel 92% dei casi l'incursione combina cifratura dei file ed esfiltrazione dei dati. I bersagli non cambiano: manifatturiero, servizi professionali e tecnologici, industria. Con sfumature locali. In Italia, i più colpiti sono manifatturiero, vendita al dettaglio, mondo universitario e industria

I Paesi ostili

I conflitti armati, dalla guerra in Ucraina alle tensioni in Medio Oriente, stanno alimentando l'ondata di attività cyber in Europa. I gruppi legati agli Stati - Russia, Corea del Nord, Cina, Iran, in particolare - usano soprattutto il cyberspazio per spiare governi ed eserciti, sostenere lo sforzo bellico e amplificare campagne di informazione e disinformazione.
In alcuni casi l'accesso alle reti viene "armato" per colpire infrastrutture critiche e funzioni essenziali dello Stato.
Parallelamente continuano le operazioni di spionaggio digitale e gli attacchi opportunistici a scopo di profitto

Quotidiano
24-11-2025
Pagina 20
Foglio 1

Il Sole 24 ORE

Sismabonus in salvo anche con asseverazione presentata in ritardo

Immobili

La Cgt di Bergamo ammette inoltre il ricorso sul diniego di autotutela facoltativa

Cristiano Dell'Oste

Ok al sismabonus anche se l'asseverazione del progettista non è allegata alla Scia o al permesso di costruire, ma viene presentata dopo. Così la Corte di giustizia tributaria di primo grado di Bergamo (sentenza 543/1/2025, giudice monocratico Rivello), in una vicenda che tocca anche l'impugnabilità del diniego di autotutela.

Ma andiamo con ordine. Nel 2017 una società avvia in un immobile di sua proprietà lavori di ristrutturazione antisismica, agevolati dal sismabonus ordinario. Le opere proseguono nel 2018, poi vengono sospese per la pandemia. La società intanto scarica le spese (detrazione annua: 4.110 euro).

Le Entrate effettuano un controllo formale (ex articolo 36-ter del Dpr 600/1973) per il 2019. Il contribuente non risponde e il 20 dicembre 2023 gli viene notificato un avviso di irregolarità con cui si recupera il bonus.

Il 5 agosto dell'anno seguente la società fa istanza di sgravio dell'atto impositivo, inoltrando all'ufficio l'asseverazione del progettista che certifica la classe di rischio sismico antelavori e quella raggiungibile dopo l'intervento progettato. La società sollecita l'Agenzia a ritirare l'atto, perché – afferma – si ricade in una delle ipotesi di autotutela obbligatoria previste dallo Statuto del contribuente dopo le modifiche del Dlgs 219/2023, attuativo della delega: si tratta in particolare dell'ipotesi di «mancanza di documentazione successivamente sanata, non oltre i termini ove previsti a pena di decadenza» (lettera g dell'articolo 10-quater della legge 212/2000).

L'ufficio risponde però con diniego espresso il 19 dicembre 2024, ricordando che il Dm 58/2017, all'articolo 3, comma 3, chiede che il progetto e l'asseverazione siano allegati alla Scia o al permesso di costruire quando vengono presentati. Inoltre, secondo la circolare 28/E/2022, diramata per il super-sismabonus, la mancanza dell'asseverazione blocca il beneficio.

Questo atto di diniego viene allora impugnato dal contribuente davanti al giudice bergamasco. Qui le Entrate chiedono innanzitutto che venga riconosciuta l'inammissibilità del ricorso, perché si ricadrebbe in un caso di autotutela facoltativa, non obbligatoria, e perché il contribuente è legittimato a impugnare l'eventuale rifiuto espresso o tacito all'istanza di autotutela, ma non l'esito del riesame.

Il giudice, invece, ammette il ricorso, anche se poi qualifica il caso come autotutela facoltativa. La sentenza richiama infatti la lettera g-ter dell'articolo 19 del Dlgs 546/1992, che ritiene impugnabile «il rifiuto espresso sull'istanza di autotutela nei casi previsti dall'articolo 10-quinquies» dello Statuto (norma che regola l'autotutela facoltativa).

Nel merito, il giudice afferma la prevalenza dei requisiti sostanziali richiesti dalla legge: «Il mero dato formale, rappresentato dalla tardività dell'invio dell'asseverazione, non costituisce elemento atto a comportare il disconoscimento del credito derivante dall'oggettiva realizzazione di lavori rientranti nell'alveo del sismabonus».


Bonus ricerca, stop ai controlli basati sul Manuale di Frascati per il 2013-19

Sismabonus in salvo anche con asserverazione presentata in ritardo

VALORE24

La nuova era della certificazione digitale

Settimanale
24-11-2025
Pagina 6
Foglio 1

L'Economia
del CORRIERE DELLA SERA

Il commento

A segno il primo attacco di un hacker artificiale: perché è una svolta

di MARIA ROSARIA TADDEO

Anthropic ha recentemente pubblicato un rapporto che documenta un evento spartiacque per la cybersicurezza: il primo attacco informatico condotto in modo sostanzialmente autonomo da un sistema di intelligenza artificiale (AI). L'operazione è avvenuta lo scorso settembre. Ed è attribuita al gruppo GTG-1002, presumibilmente legato al governo cinese, che ha sfruttato Claude Code per automatizzare quasi l'intero ciclo di attacco.

Seguendo i prompt degli attaccanti, l'AI ha individuato e sfruttato vulnerabilità in obiettivi di alto valore, tra cui grandi aziende tecnologiche e agenzie governative, conducendo un'ampia gamma di attività post-exploitation, dall'analisi dei sistemi all'escalation dei privilegi.

Il sistema ha eseguito autonomamente l'80-90% delle operazioni necessarie: ricognizione, identificazione delle vulnerabilità, exploitation, raccolta di credenziali, analisi ed esfiltrazione dei dati. Una volta ricevuti i prompt iniziali, Claude ha coordinato altri agenti artificiali operando con tempistiche e su scala impossibili per operatori umani. L'attacco ha utilizzato strumenti open source — scanner di rete, framework per database, tool di password cracking — coordinati attraverso il Model Context Protocol. Secondo Anthropic, gli attaccanti hanno lavorato tra i 2 e i 10 minuti. Si sono occupati della strategia, delegando all'AI la tattica.

A voler essere sarcastici, l'attacco è un caso impeccabile di «team ibrido». Gli hacker hanno sostenuto una parte minima, tra il 10% e il 20%, dello sforzo. Si sono occupati della parte strategica, creativa oserei dire — hanno eluso Claude passandosi per tecnici della sicurezza — lasciando all'AI l'esecuzione. Sarcasmo a parte, questo attacco segna un cambiamento della cybersicurezza, che pone rischi seri per le democrazie digitali.

Tre sono i rischi di particolare importanza. Il primo: gli attacchi contro l'AI sono manipolatori, mirano a cambiare il comportamento del sistema non a bloccarne il funzionamento. Nel caso di Claude, la manipolazione era a fini di spionaggio, ma immaginiamo un attacco che alteri il comportamento di un sistema AI per il riconoscimento delle immagini usato in battaglia. Non c'è bisogno di descrivere la gravità delle conseguenze dei limiti del controllo sull'AI.

Del secondo rischio si parla da tempo e riguarda l'automazione delle dinamiche tra attaccanti e difensori: non è lontano il momento in cui sistemi di intelligenza artificiale risponderanno ad altri sistemi di AI, rischiando l'escalation. Gli attacchi informatici sono ormai parte integrante delle strategie geopolitiche, gli agentic cyberattacks introducono un fattore d'instabilità nei rapporti internazionali, proprio mentre gli equilibri si fanno più fragili.

Il terzo rischio riguarda gli utenti. O meglio, i cittadini. Il cyberspace favorisce l'attacco sulla difesa. Gli agentic cyberattacks amplificano questa asimmetria abbassando drasticamente i costi — umani, economici, tecnologici — degli attacchi. In risposta, la difesa adotta l'intelligenza artificiale per sviluppare sistemi più robusti e per il monitoraggio delle infrastrutture digitali e del comportamento degli utenti.

La sicurezza nel cyber non è una gara con traguardo, non si vince una volta per tutte. Si tiene solo il punteggio. Il rischio è che per provare a pareggiare, le difese usino l'AI per passare dal monitoraggio alla sorveglianza di massa.

In questo senso, l'AI non ridefinisce solo il panorama della cybersicurezza ma anche il prezzo della sicurezza in democrazia.

Docente
Mariarosaria Taddeo è docente di Digital Ethics and Defence Technology a Oxford e Defence Science and Technology Fellow all'Alan Turing Institute


Tecnologia
PROTEZIONE DIGITALE
A segno il primo attacco di un hacker artificiale: perché è una svolta
LA POLIZZA SMART

Settimanale
24-11-2025
Pagina 6
Foglio 1 / 2

ItaliaOggi Sette

Assonime spiega come applicare le semplificazioni privacy, effetto della sentenza della Cgue

Alias? Da maneggiare con cura

Il Gdpr è fuori solo se si è certi di non risalire all'interessato

Pagina a cura di
ANTONIO CICCIA MESSINA

Privacy semplificata per le imprese e le p.a. che usano dati pseudonimizzati. Ma solo se c'è la sicurezza che le persone non possono essere identificate. È questa la breccia aperta dalla sentenza della Corte di giustizia dell'Ue con la sentenza del 4/9/2025, resa nella causa C-413/23. La pronuncia ha importanti ricadute sull'operatività delle aziende e degli enti pubblici, sui rapporti tra imprese e tra p.a. e sugli adempimenti da svolgere per essere conformi alle norme sulla protezione dei dati personali. Ma, attenzione a non cadere nell'errore di illudersi che il Gdpr (regolamento Ue sulla privacy n. 2016/679) sia completamente accantonato. Questo perché i dati pseudonimizzati (alias o pseudonimi) si possono usare come anonimi (e, quindi, fuori ambito privacy) solo se la identificazione degli interessati non sia possibile con strumenti ragionevoli. Tutto ciò sembra quasi ovvio, ma così non è. La regola astratta comporta conseguenze in concreto: bisogna tradurre in pratica cosa vuol dire verificare la possibilità di attribuire un dato pseudonimizzato a un determinato individuo con il suo nome e cognome e, quindi, occorre stabilire quali documenti si devono scrivere e/o aggiornare. A dare una mano a districare questa complicata matassa è la nota n. 9/2025 di Assonime, diffusa il 13/11/2025, che spiega alle aziende come comportarsi, senza farsi ammaliare dal miraggio di semplificazioni che tali non sono.

La pseudonimizzazione. La nota di Assonime spiega, innanzitutto, che cosa è la pseudonimizzazione e qual è il cuore della sentenza citata.La pseudonimizzazione è una tecnica di sicurezza dei dati, che consiste nel trattare i dati personali in modo tale che non possano più essere riconducibili a un interessato specifico senza l'uso di informazioni aggiuntive, purché queste informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative volte a evitare l'identificabilità della persona cui il dato pseudonimizzato si riferisce.

La pseudonimizzazione è la stessa tecnica del "pen name" usato dagli scrittori ed è molto diversa dalla cifratura, perché non si usano chiavi di cifratura per mascherare e all'inverso per risalire al dato originario.

Concetti volatili. La sentenza, spiega Assonime, stabilisce che i dati pseudonimizzati qualche volta rimangono dati personali (con applicazione del Gdpr) e, invece, qualche altra volta sono da considerare come dati anonimi (senza applicazione del Gdpr). In particolare, si legge nella nota, i dati pseudonimizzati conservano la natura di dato personale solo se chi ne ha la disponibilità è ragionevolmente in grado di riferirli alla persona interessata, anche adottando mezzi ulteriori, quali un controllo incrociato con altri dati.

Quando, invece, il soggetto che ha in mano il dato pseudonimizzato non può, con mezzi ragionevoli, riferirlo a una persona identificata o identificabile, allora quel dato pseudonimizzato perde la sua connotazione di dato personale e di conseguenza può essere trattato come un dato anonimo.

In quest'ultimo caso, si può essere attratti dai vantaggi connessi al fatto che trattare dati anonimi esonera dal dover dare informative e chiedere consensi, dal dover rispondere a richieste di accesso e di esercizio degli altri diritti accordati agli interessati dal Gdpr e dal tenere il registro dei trattamenti e, inoltre, conforma in maniera diversa gli obblighi di sicurezza informatica e, infine e soprattutto, inibisce l'applicazione delle pesanti sanzioni previste dal Gdpr, le quali entrano in azione solo a fronte delle violazioni relative a dati personali.

Dribblare tutti questi adempimenti può essere una prospettiva appetibile e la sentenza delinea questo, a prima vista, favorevole scenario in relazione all'uso di dati pseudonomizzati.

La burocrazia dei dati pseudonimizzati. Peraltro, si deve considerare che non è tutto in discesa: anche l'uso di dati pseudonimizzati ha un suo apparato di adempimenti burocratici.

Si pensi attentamente già solo al fatto che uno stesso dato pseudonimizzato (in concreto una stessa parola o una stessa espressione numerica o alfanumerica) ha una qualifica volatile, che dipende dalle circostanze del caso concreto: come visto sopra, qualche volta e per qualcuno è un dato personale e qualche altra volta e per qualcun altro è assimilabile a un dato anonimo. Già questo dovrebbe far riflettere sul fatto se siamo di fronte a qualcosa che rende la vita più semplice o se, invece, siamo di fronte a uno scenario pieno di insidie e privo di certezze.

Si rifletta, poi, sul fatto che l'orientamento espresso dalla sentenza della Cgue costringe a misurarsi con concetti generici, vaghi e soggettivi, come la "ragionevolezza" degli strumenti da utilizzare per capire se si è in grado di identificare il soggetto cui è riferibile lo pseudonimo. Ciò che è ragionevole per chi ha convenienza a non applicare il Gdpr potrebbe non esserlo per chi vuole esercitare i diritti previsti dal Gdpr o chiedere i danni adducendo una violazione del Gdpr stesso.

La valutazione della identificabilità. Proseguendo nell'analisi della nota di Assonime, si legge che per stabilire se il dato pseudonimizzato possa essere considerato dato personale è necessario effettuare un'analisi delle ragionevoli probabilità che i dati pseudonimizzati possano essere associati alla persona cui si riferiscono. Assonime aggiunge che questa valutazione di identificabilità diventa un momento determinante per il trattamento dei dati, in quanto ne può rendere più agevole la circolazione.

Traducendo in un piano di lavoro le indicazioni di Assonime, tutto ciò significa che l'azienda (ma lo stesso discorso vale per le p.a. e per qualunque altro titolare del trattamento) deve effettuare uno specifico assessment, il cui esito è la produzione di un documento, la cui conclusione è, alternativamente, c'è oppure non c'è ragionevole possibilità di identificazione.

I parametri della ragionevolezza. In proposito, stando alla sentenza della Cgue, ai fini della valutazione ragionevole di identificazione si devono considerare i seguenti profili: costi e tempo necessari per l'identificazione, tecnologie disponibili al momento del trattamento e successivi sviluppi tecnologici.

Pertanto, il test di identificabilità dovrà riscontrare se i costi della identificazione sono ragionevoli e se lo sia il tempo occorrente alla verifica in rapporto agli strumenti disponibili in un contesto evolutivo. La necessità di porre attenzione a eventuali sviluppi tecnologici evidenzia, poi, che la valutazione di identificabilità va aggiornata periodicamente. Al riguardo, si pensi alle conseguenze che potranno derivare nell'immediato futuro dall'uso seriale e sistematico delle intelligenze artificiali, la cui capacità di rintraccio e incrocio di dati è enorme.

Un'operazione capziosa. Sul punto, Assonime constata che la valutazione della ragionevole possibilità di identificazione è, dunque, un'operazione il cui esito è condizionato non solo dai mezzi tecnologici a disposizione (soprattutto in termini di capacità di calcolo e di accessibilità di dati) ma anche dalle effettive capacità della persona che tratterà i dati pseudonimizzati.

Assonime, anzi, non esita a descrivere il reale stato delle cose e definisce l'assesment

ItaliaOggi Sette

sull'identificabilità "complesso" e "suscettibile di continua ridefinizione in base al mutare dei rischi reali".

Emerge, pertanto, la capziosità dell'intera operazione nonché la possibilità di uso strumentale del principio formulato dalla Cgue, con passaggio di dati pseudonimizzati a soggetti economici collegati e ciò al solo fine di bypassare gli adempimenti previsti dal Gdpr. Ma anche per chi agisce in buona fede e con correttezza la posizione è critica: Il giudizio sul fatto che taluno abbia usato ragionevolezza è altamente discrezionale e, quindi, bisogna andarci con i piedi di piombo.

In merito, un giudice o il Garante della privacy potranno ribaltare la valutazione che un'impresa ha fatto e infliggerle pesanti sanzioni per avere ingiustificatamente disapplicato il Gdpr.

L'informativa a monte. Un'ultima notazione della nota di Assonime riguarda il soggetto che detiene dati personali, li pseudonimizza e li trasmette a un'altra impresa. Quest'ultima è tenuta alla verifica di identificazione, mentre l'impresa a monte è obbligato a informare l'interessato circa il trasferimento dei suoi dati a soggetti terzi, a prescindere dal carattere, personale o no, che il dato assuma nel corso del trattamento. Chiarisce Assonime che, ai fini dell'applicazione dell'obbligo di dare l'informativa, l'identificabilità dell'interessato va valutata al momento della raccolta dei dati e dal punto di vista del titolare del trattamento, prima di qualsiasi eventuale trasferimento a terzi.

I dati pseudonimizzati qualche volta rimangono dati personali (con applicazione del Gdpr) e, invece, qualche altra volta sono da considerare come dati anonimi (senza applicazione del Gdpr)

Si deve considerare se i costi della identificazione sono ragionevoli e se lo sia il tempo occorrente alla verifica in rapporto agli strumenti disponibili

Il doppio regime dei dati pseudonimizzati

Possibilità di identificazione	I dati pseudonomizzati sono da trattare come dati personali	Si applica il Gdpr
Assenza di ragionevole possibilità di identificazione	I dati pseudonomizzati sono da trattare come dati anonimi	Non si applica il Gdpr

I punti del test di identificazione

Costi
Tempo
Tecnologie disponibili al momento del trattamento
Sviluppi tecnologici sopravvenuti


PRIVACY

Alias? Da maneggiare con cura

Il Gdpr è fuori solo se si è certi di non risalire all'interessato

Settimanale
24-11-2025
Pagina 47
Foglio 1

la Repubblica A&F

L'AZIENDA

Il prezzo giusto per farsi una casa green

Sette immobili su dieci sono in classe bassa: metterci mano costa fino a 500 euro al metro quadro. La scommessa di Casâbito: "Saremo l'Amazon dell'edilizia"

Simone Cosimi

In Italia 7 immobili su 10 restano in classe energetica F o G e naturalmente cresce l'interesse per la riqualificazione. Dopo il Superbonus con le sue degenerazioni, il mercato torna a muoversi da solo, e gli italiani scoprono che rendere una casa più efficiente è un investimento necessario ma che richiede pianificazione, fiducia e rigore. E peserà parecchio sulle tasche.

Negli ultimi tre anni sono stati chiusi più di un milione di interventi agevolati. Un'ondata che ha trasformato l'edilizia italiana, creando una consapevolezza diffusa sul peso dei consumi che generano impatti in bolletta. Ora che gli incentivi sono stati ridimensionati, diventa centrale la domanda: quanto costa davvero rendere una casa più efficiente?

Le stime fornite da Italsoft, gruppo veneto con 40 anni di esperienza nella digitalizzazione e nella governance dei processi edilizi, parlano chiaro. Per un appartamento medio di 100 metri quadrati passare da una classe energetica bassa come G o F a una media come C o D significa spendere tra 20 e 40mila euro, ovvero tra 200 e 350 euro al metro quadro. Chi punta alle classi A o B, invece, deve mettere in conto cifre ben più importanti: da 40mila a 100mila euro, fino a 500 euro al metro quadro per gli interventi più strutturali. L'isolamento termico resta la voce più pesante, seguito dalla sostituzione degli infissi e dall'installazione di pompe di calore o impianti fotovoltaici.

La media nazionale, tra costi e tipologie di abitazioni, si ferma poco sotto i 30mila euro a unità. Ma dietro i numeri si nasconde un quadro ancora critico e sostanzialmente irrisolvibile: circa il 70% delle case italiane resta in classe F o G mentre solo una piccola parte – meno del 15% – rientra nelle fasce più virtuose. Il patrimonio immobiliare del paese continua dunque a disperdere energia, valore e fiducia. Nodi che, con le normative europee, prima o poi verranno al pettine dei proprietari.

È proprio sulla fiducia che si gioca la nuova partita della ristrutturazione. Perché, come sanno milioni di proprietari, rifare casa in Italia è spesso un percorso a ostacoli: burocrazia, preventivi che non tengono conto di tutti i costi effettivi, imprese introvabili e spesso inaffidabili, ritardi cronici. Da questa realtà nasce Casâbito, un progetto che prova a ribaltare la prospettiva, trasformando la ristrutturazione in un'esperienza misurabile, tracciabile e, soprattutto, affidabile. L'idea è proprio di Italsoft. Dalla joint venture con Apple negli anni '80 fino alla gestione di oltre un miliardo di euro di interventi, il gruppo veneto con oltre 6mila cantieri alle spalle lancia un modello nuovo: store diffusi sul territorio che coprono una fascia d'interventi con ticket medio tra 80 e 120mila euro, fino a un massimo di 250mila euro, un solo interlocutore per ogni cliente e un processo interamente tracciato che assicura il rispetto di tempi e costi. Il primo negozio è a Pescara ma il piano è ambizioso: 60 punti vendita entro il 2026, un investimento di 14,5 milioni e ricavi stimati, a regime, tra 120 e 180 milioni di euro. Ogni progetto viene seguito da un project manager dedicato che coordina architetti, fornitori e imprese locali e monitorato in ogni fase, dalla progettazione alla chiusura amministrativa. Gli store sono spazi fisici dove il cliente può toccare materiali, visualizzare in 3D la propria abitazione e sapere quanto spenderà e quando finirà il cantiere.

«In Italia la casa è il cuore delle famiglie ma ristrutturarla è sempre stato un percorso difficile - spiega Andrea Brigo, fondatore di Italsoft e di Casâbito - con questo progetto vogliamo restituire serenità e affidabilità alle persone unendo solidità industriale, tecnologia, fattore umano e prossimità territoriale». Brigo non è un imprenditore nato nel digitale, ma nei cantieri. Figlio di costruttori, negli anni '80 scelse di non seguire le orme del padre, preferendo fondare una software house per cambiare il modo di costruire.

Quarant'anni dopo, la sua Italsoft punta a chiudere con 100 milioni il 2025 e a far diventare Casâbito qualcosa come "l'Amazon dell'edilizia": «Un ecosistema in cui ogni servizio – dal software alla finanza, dalla progettazione alle certificazioni sino alla gestione integrata dei condomini – diventa parte di una stessa esperienza. Non per complicare la vita alle imprese, ma per renderla più semplice, più redditizia, più sicura».

ANDREA BRIGO
Fondatore di Italsoft negli anni '80 e di Casâbito

60

NEGOZI

La nuova avventura di Italsoft prevede 60 punti vendita e ricavi di 120-180 milioni

ItaliaOggi7 Affari Legali

L'investimento fatto dal governo italiano per sostenere lo sviluppo della Space Economy

Spazio, un'avventura da 7,5 mld

DI ROBERTO MILIACCA

La nuova corsa allo Spazio del terzo Millennio è partita. L'Italia è il primo paese europeo ad aver approvato una legge quadro sullo Spazio e sulla Space economy, la legge 13 giugno 2025, n. 89, che, tra le altre cose, si pone l'obiettivo di promuovere gli investimenti privati nel settore, favorendo l'accesso degli operatori privati e introducendo una disciplina di favore per le piccole e medie imprese e le start-up e creando un Fondo pluriennale a sostegno di queste aziende ai programmi pubblici. «Abbiamo scelto di destinare allo Spazio oltre 7,5 miliardi di euro. Un investimento record destinato alle infrastrutture, alle tecnologie, alla ricerca e alle competenze. Risorse nazionali e Pnrr, che si traducono in catene del valore più solide, in una filiera industriale più competitiva, in servizi migliori per cittadini e imprese», ha detto poche settimane fa il presidente del Consiglio, Giorgia Meloni, in occasione della seconda edizione degli Stati Generali della Space Economy promossi dall'Intergruppo Parlamentare, a cui hanno partecipato tutti i players nazionali ed europei del settore, compresi alcuni dei maggiori studi legali italiani che hanno deciso di attivare delle practice dedicate, con un approccio multidisciplinare al tema. Perché nella legge ci sono molti aspetti che hanno bisogno di esperti per poter avere attuazione, specie tra le aziende: la legge 89 regolamenta infatti l'intero ciclo delle attività spaziali, dall'accesso allo spazio allo smaltimento, ponendo al centro l'autorizzazione preventiva, i requisiti stringenti di sicurezza, di resilienza informatica, di sostenibilità ambientale e la necessità di dotarsi di adeguate coperture assicurative. Insomma, come spiegano gli studi che sono già partiti, la complessità del settore, la sua natura interdisciplinare e il contesto internazionale rendono fondamentale l'assistenza di professionisti specializzati per affrontare questioni come contrattualistica, governance dei dati, cybersecurity e conformità normativa, in vista anche del futuro EU Space Act.

la Repubblica A&F

L'editoriale

Transizione 5.0, tutto quello che non si deve fare

Walter Galbiati

Una toppa è una toppa. E quando se ne mette una sopra un'altra non sono altro che due toppe. È il caso di Transizione 5.0 che nelle mani di Adolfo Urso è diventato un esempio di tutto quello che non si deve fare quando si vogliono offrire incentivi all'industria.

segue a pag. 26

L'EDITORIALE

TRANSIZIONE 5.0 TUTTO QUELLO CHE NON SI DEVE FARE

Walter Galbiati

segue dalla prima pagina

Il piano non è decollato e poi quando lo stava per fare è stato abbattuto per decreto. Con il risultato che le imprese italiane, che hanno bisogno come non mai di fare investimenti per restare competitive, si sono trovate o a metà del guado o senza la possibilità di attivarli, creando quanto di più dannoso ci possa essere per le imprese stesse: l'incertezza.

Nell'ambito del Pnrr, il piano Transizione 5.0 era nato con una dotazione finanziaria di 6,3 miliardi di euro e l'obiettivo di transitare le industrie, soprattutto manifatturiere, verso processi di produzione più efficienti sotto il profilo energetico e un modello più sostenibile, basato sulle energie rinnovabili. La misura consisteva in un regime di crediti d'imposta pari al 35% o al 55% degli investimenti sostenuti e la domanda doveva essere presentata entro il 31 dicembre 2025 per accedere poi al rimborso nel periodo compreso tra il primo gennaio 2025 e il 31 agosto 2026. In un Paese come il nostro dove l'energia è cara, il piano aveva senso anche perché secondo le stime avrebbe potuto far risparmiare 0,4 milioni di tonnellate equivalenti di petrolio nel periodo 2024-2026. Che ai costi attuali, vuol dire più o meno mezzo miliardo di bolletta energetica in meno.

La misura sarebbe dovuta partire con la finanziaria scritta nel 2023 per coprire gli investimenti del biennio 2024-2025. I decreti attuativi, però, sono arrivati tardi, ad agosto del 2024, ed erano scritti talmente male che in pochissimi hanno avviato le pratiche. Fino a maggio 2025 erano stati chiesti fondi per meno di un miliardo.

Quando sotto la pressione degli imprenditori, il ministro ha finalmente semplificato il groviglio legislativo, in meno di quattro mesi le richieste sono volate a 2,8 miliardi di euro. Ma ecco che arriva la sorpresa, perché Urso dà corpo alla rinegoziazione del Pnrr fatta in sede europea da Foti con Fitto e dirotta 3,7 miliardi di Transizione 5.0 al servizio della Legge di Bilancio.

E blocca al 7 novembre le domande per il piano, quando invece c'era tempo fino al 31 dicembre. Un disastro, perché molte imprese che avevano avviato la pratica restano fuori sia per la riduzione dei fondi (da 6,3 a 2,5 miliardi) sia per l'accorciamento dei tempi. La settimana scorsa con un nuovo decreto Urso ha prorogato la scadenza fino al 27 novembre e ha promesso che ci saranno le coperture per tutti. Ad oggi le richieste per Transizione 5.0 ammontano a 3,9 miliardi. Il numero potrà salire ancora un po', ma anche così sarà un fallimento perché alla fine è stato attivato meno del 65% dei 6,3 miliardi inizialmente previsti. Un esempio di come non fare e un'occasione persa per l'Italia che nel 2025 crescerà solo dello 0,5%.

L'OPINIONE

> Il piano non è decollato e quando poi lo stava per fare è stato abbattuto per decreto. Con il risultato che le imprese si sono trovate o a metà del guado o senza la possibilità di investire

Quotidiano
24-11-2025
Pagina 1+11
Foglio 1 / 2

Il Sole 24 ORE

ATENEI

Nei nuovi concorsi universitari spunta il sorteggio dei commissari

Dopo la manovra l'aula del Senato esaminerà il Ddl sui concorsi universitari, che sostituisce l'abilitazione scientifica nazionale con l'autocertificazione per accedere alle selezioni locali. Tra le novità commissari sorteggiati e prova didattica.

Eugenio Bruno —*a pag. 11*

Concorsi universitari: sorteggio dei commissari e verifica didattica

La riforma Bernini. Dopo la manovra è atteso in aula al Senato il Ddl che elimina dopo 15 anni il filtro dell'abilitazione scientifica nazionale: al suo posto autocertificazione dei requisiti minimi e cattedre assegnate dalle selezioni locali

Eugenio Bruno

Il mondo dell'università guarda già oltre la manovra 2026. Non solo perché la legge di Bilancio all'esame del Senato dedica poco spazio all'istruzione superiore anche negli emendamenti segnalati dalla maggioranza. Ma anche perché, dopo il suo varo, l'aula di Palazzo Madama esaminerà il disegno di Legge che riforma l'accesso alla cattedra e manda in pensione l'abilitazione scientifica nazionale (Asn) introdotta dalla legge 240 del 2010: una sorta di "patentino", distinto in prima e seconda fascia, che gli aspiranti prof universitari dovevano conseguire per accedere ai concorsi locali e che sembra destinato a sparire. Tra le preoccupazioni del mondo accademico (su cui si veda altro articolo in pagina).

Anche dopo l'esame in commissione, il Ddl approvato in Cdm il 19 maggio scorso su input della ministra Anna Maria Bernini sostituisce - di fatto - l'Asn con un'autocertificazione del possesso di requisiti minimi uguali per tutti, decisi centralmente e distinti tra professori ordinari o associati. Con alcune novità però. Ad esempio è stata snellita la lista di condizioni che ogni aspirante docente dovrà dichiarare di possedere per accedere alle selezioni locali. In base alla nuova formulazione i requisiti indispensabili andranno sempre individuati entro 90 giorni dall'approvazione della legge per ciascun gruppo scientifico disciplinare, con decreto del Mur, su proposta dell'Anvur e sentito il Cun, ma riguarderanno esclusivamente «l'attività di didattica e ricerca in Italia e all'estero, la titolarità, la contitolarità o la partecipazione a progetti di ricerca di base o applicata finanziati sulla base di bandi competitivi nazionali, europei e internazionali, nonché il raggiungimento degli indicatori minimi di quantità, continuità e distribuzione temporale dei prodotti della ricerca». Spariscono, invece, i riferimenti all'«organizzazione o la partecipazione come relatore a convegni di carattere scientifico in Italia o all'estero» e ai risultati di trasferimento tecnologico indicati nel testo originario.

Cambiano poi le commissioni d'esame. Anziché stabilire, come deciso inizialmente, che l'accesso al ruolo di professore di prima o seconda fascia del singolo ateneo sia affidato a un "esaminatore" interno e a quattro esterni sorteggiati dall'università «tra i docenti disponibili a livello nazionale, afferenti al settore scientifico-disciplinare di cui al bando di concorso» viene introdotta una lista di 40 aspiranti commissari per ciascun gruppo scientifico disciplinare che sarà redatta dal ministero in base a richieste corredate da curriculum consultabili online e dalla quale saranno estratti i quattro commissari esterni. Più un quinto individuato dall'ateneo tra gli interni o - altra novità - tra quelli stabilmente impegnati «all'estero in attività di ricerca o di insegnamento con una posizione accademica almeno equipollente» a quella ricercata. Le commissioni scenderanno a tre membri, di cui due esterni e uno interno, per i gruppi scientifico disciplinari più piccoli (dove le liste di partenza avranno meno di 40 nomi).

Accanto alla conferma che i docenti in cattedra verranno giudicati ogni tre anni in base a nuove linee guida sulla valutazione affidate all'Agenzia Anvur, con conseguenti benefici premiali in termini di contributi per l'università che li ha reclutati, vanno segnalati un altro paio di cambiamenti rilevanti rispetto al Ddl di partenza. Da un lato, l'introduzione di una prova didattica ex ante rispetto al momento della nomina del vincitore da parte del dipartimento; dall'altro, una correzione sulla mobilità. I passaggi tra atenei potranno avvenire se l'istituzione ricevente non ha problemi di bilancio e senza che il diretto interessato si porti dietro i punti organico (cioè gli spazi assunzionali) come immaginato inizialmente. A patto che l'assemblea del Senato confermi l'articolato uscito dalla commissione e tenendo presente che dopo Palazzo Madama toccherà anche a Montecitorio pronunciarsi sul testo.

Il Sole 24 ORE

STOP AND GO SUL TESTO
Il 19 maggio scorso il Consiglio dei ministri ha approvato un Ddl presentato dalla ministra dell'Università, Anna Maria Bernini, che supera l'attuale abilitazione scientifica nazionale. Il testo ha avuto l'ok della VII commissione del Senato a fine ottobre e andrà in aula dopo la manovra. Dopodiché passerà alla Camera.

L'ADDIO

Il sistema attuale
La legge 240 del 2010 aveva introdotto l'abilitazione scientifica nazionale come "filtro" che precedeva i concorsi universitari. In base al sistema tuttora in vigore prima di accedere alle selezioni bandite dai singoli atenei gli aspiranti prof di prima e seconda fascia devono dotarsi di abilitazione. Il Ddl Bernini all'esame del Senato, di fatto, la sostituisce con l'autocertificazione di requisiti minimi decisi centralmente

Liste centralizzate di 40 nomi per gli aspiranti esaminatori divisi per gruppo scientifico disciplinare

ADOBESTOC

Commissioni d'esame. Previsto un membro interno e quattro esterni sorteggiati


Il Sole 24 ORE
Flat tax
Per i dipendenti risparmi Irpef a 2 miliardi nel 2026
Cultura, ancora pochi lavoratori giovani


Concorsi universitari: sorteggio dei commissari e verifica didattica
DIGITAL POS NUMIA.

Il Sole 24 ORE

ACCESSI 2024

Ingegneri e architetti, mai così pochi iscritti

Ha toccato il minimo storico dalla nascita degli Albi nel 2002 il numero di giovani abilitati alle professioni di ingegnere e architetto: l'anno scorso, infatti, hanno superato l'esame di stato 4.229 candidati per la professione di ingegnere e 1.383 candidati per quella di architetto. A segnalare questo record (negativo) è l'analisi del Centro studi ingegneri sull'accesso alla professione. Non basta a spiegare il fenomeno la frenata del tasso di successo per entrambe le figure, che comunque da un anno all'altro è sceso per gli ingegneri dal 88,1% del 2023 all'84,2%, e per gli architetti dal 63,9% al 53,9 per cento. «È proprio la libera professione a non risultare più attrattiva - segnala il Cni - per una serie di motivi, tra cui il livello reddituale e gli oneri connessi alla gestione amministrativo-fiscale ed ordinistica». Basti pensare che i 4.229 abilitati rappresentano solo il 13,6% dei laureati magistrali 2024. Va peggio per gli architetti: da un anno all'altro il numero dei candidati all'esame si è ridotto del 40 per cento. Il presidente del Cni, Angelo Domenico Perrini, vuole intervenire subito semplificando l'accesso: «Insistiamo nella richiesta di introdurre, durante il percorso accademico, un tirocinio formativo con una prova pratica che, se conclusa con esito positivo, contempli l'abilitazione».


Professioni 24
Sostenibilità, oltre 6mila revisori abilitati per certificare i bilanci

ItaliaOggi7 Affari Legali

CONS. DI STATO
Accesso civico senza ingolfare gli uffici

Cirasa a pag. V

Istanze manifestamente onerose o sproporzionate sono state bocciate dal Consiglio di stato

Accesso civico con moderazione

Legittimo il diniego se la richiesta carica di lavoro gli uffici

DI PAOLO CIRASA

E' legittimo il diniego di accesso civico generalizzato che risulti manifestamente oneroso o sproporzionato e cioè tale da comportare un carico irragionevole di lavoro, idoneo a interferire con il buon andamento della pubblica amministrazione. Come nel caso di richiesta massiva contenente un numero rilevante di dati o documenti, ovvero di richieste massive plurime, pervenute in un arco temporale limitato da parte dello stesso soggetto o da soggetti comunque riconducibili a un unico centro di interesse. Lo afferma il Consiglio di Stato con sentenza del 10 ottobre 2025 n. 7973.

Dalla normativa di riferimento, rilevano i giudici di Palazzo Spada, si evince un principio generale di necessaria composizione tra il diritto alla trasparenza e l'esigenza di non pregiudicare, mediante un uso improprio dell'accesso, il buon andamento dell'azione amministrativa, evitando di imporre alla p.a. un carico operativo eccessivamente gravoso e incompatibile con i principi di funzionalità, economicità e tempestività dell'azione pubblica.

La valutazione circa la ragionevolezza delle istanze, precisa inoltre la decisione in commento, deve tenere conto non solo delle risorse organizzative e umane da impiegare (commisurate in termini di ore/lavoro) per soddisfare la richiesta di accesso, ma anche della rilevanza dell'interesse conoscitivo perseguito.

Pur non trattandosi di un requisito di legittimazione all'accesso, la scarsa rilevanza dell'interesse rappresentato concorre a motivare la legittimità del diniego opposto, proprio sotto il profilo della oggettiva e ingiustificata gravosità dell'attività istruttoria richiesta per dare seguito all'istanza.

Dal tenore dell'istanza sottoposta alla sua attenzione, conclude il collegio, emerge un interesse conoscitivo disallineato dalle finalità tipiche dell'accesso civico generalizzato, quali sono l'informazione e la formazione dell'opinione pubblica, il controllo sull'esercizio delle funzioni istituzionali, la verifica dell'impiego delle risorse pubbliche e la promozione della partecipazione democratica.

L'interesse sotteso all'istanza risulta, piuttosto, di natura individuale e privatistica, e di conseguenza legittimante il diniego opposto.


ItaliaOggi7 Affari Legali
Capital
Spazio, un'avventura da 7,5 mld


Accesso civico con moderazione
Legittimo il diniego se la richiesta carica di lavoro gli uffici