# Bending Spoons, il debutto al Nasdaq vale 24 miliardi: la più grande IPO non fintech dal 2021

**Bending Spoons** chiude il primo giorno di quotazione al Nasdaq con una capitalizzazione di circa 24 miliardi di euro. Una cifra che colloca la società milanese tra i maggiori gruppi italiani per valore di mercato e che dà alla quotazione un significato più ampio della sola operazione finanziaria.

Il debutto della società fondata da **Luca Ferrari, Matteo Danieli, Luca Querella** e **Francesco Patarnello** segna infatti uno dei passaggi più rilevanti per il tech italiano degli ultimi anni. Bending Spoons arriva al mercato americano con una storia costruita in meno di tredici anni, circa 2.500 persone e una posizione ormai riconosciuta anche fuori dall’Europa.




## Una quotazione che pesa più del prezzo

Secondo **Davide Dattoli Zhang**, fondatore di **Talent Garden**, Bending Spoons è oggi *“la 15esima società per capitalizzazione in Italia”* e vale più di **Leonardo**. Il dato, al di là del confronto tra settori molto diversi, serve a misurare la dimensione raggiunta da un’azienda nata come software company e cresciuta fino a diventare uno dei nuovi simboli della tecnologia europea.

La quotazione di Bending Spoons non è soltanto una notizia di Borsa. È una notizia industriale. In un Paese abituato a raccontare il successo imprenditoriale soprattutto attraverso moda, manifattura, lusso, design e meccanica, una società software italiana entra al Nasdaq con una valutazione da grande gruppo internazionale.

Dattoli Zhang ha sottolineato proprio questo punto: non il

valore economico in sé, ma il fatto che in Italia sia stata costruita da zero un’azienda tecnologica globale, riconosciuta anche nella Silicon Valley come un modello diverso di tech europeo.

Il paradosso è che il risultato arriva in un contesto nazionale che spesso fatica a riconoscere la portata delle proprie storie tecnologiche. Secondo Dattoli Zhang, la notizia avrebbe meritato “*prime pagine piene*” e maggiore attenzione pubblica, perché dimostra che anche dall’Italia può nascere una società digitale capace di competere sui mercati internazionali.

# Il nuovo tech italiano

Bending Spoons entra così in una categoria particolare: quella delle aziende italiane di prima generazione capaci di costruire valore globale partendo da una visione imprenditoriale forte. Nel confronto richiamato da Dattoli Zhang compaiono nomi come **Moncler**, **Luxottica**, **Brunello Cucinelli**, **Prada**, **Tamburi**, **Technogym** e **Mediolanum**.

La differenza è il tempo. Molti grandi gruppi italiani hanno impiegato decenni per raggiungere dimensioni internazionali. Bending Spoons ha superato la soglia dei 20 miliardi di valore in meno di tredici anni e punta a oltre un miliardo di EBITDA nel 2026.

# Le acquisizioni recenti

L’IPO arriva dopo una forte accelerazione nella strategia di acquisizioni. Fondata nel 2013 e con sede a Milano, Bending Spoons ha costruito un modello particolare nel panorama europeo: comprare prodotti digitali già affermati, spesso con una base utenti globale, per rilanciarli attraverso tecnologia, prodotto e nuova esperienza d’uso.

Tra il 2025 e l'inizio del 2026 il gruppo ha ampliato il proprio portafoglio con operazioni su piattaforme molto note. Tra queste **Komoot**, software per escursionismo e outdoor; **Harvest**, piattaforma per la gestione di tempi e progetti; **MileIQ**, app per il tracciamento dei chilometri percorsi; **Vimeo**, acquisita in un'operazione da 1,38 miliardi di dollari; **AOL**, rilevata per circa 1,5 miliardi di dollari; **Eventbrite**, acquistata per circa 500 milioni di dollari; e **Tractive**, società austriaca specializzata in dispositivi GPS e monitoraggio della salute per animali domestici.

A queste operazioni si aggiunge l'integrazione degli asset già rilevati negli anni precedenti, tra cui **WeTransfer**, **Issuu**, **Brightcove**, **Evernote**, **Meetup**, **StreamYard** e **Remini**. È questa combinazione tra prodotto, acquisizioni e capacità di esecuzione che ha trasformato Bending Spoons da software company italiana a piattaforma globale del digitale.

Per l'ecosistema italiano dell'innovazione, il debutto di Bending Spoons ha un peso che va oltre la singola società. Negli ultimi quindici anni, il dibattito sulle startup italiane è stato spesso dominato da due narrazioni opposte: da un lato l'entusiasmo per il potenziale, dall'altro lo scetticismo sulla capacità reale di creare campioni globali. Dattoli Zhang lo riassume così: *"Bending è la dimostrazione reale che si può fare"*.

**Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui**

Add as a preferred source on Google

**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/bending-spoons-il-debutto-al-nasdaq-vale-24-miliardi-la-piu-grande-ipo-non-fintech-dal-2021/578402/

# Il valore crescente delle certificazioni in cybersecurity nel 2026

Le certificazioni in cybersecurity rappresentano oggi uno strumento chiave per colmare i gap di competenze, validare le capacità professionali e rafforzare la resilienza dei team nell'era dell'intelligenza artificiale e della crescente complessità normativa. In questo articolo analizziamo come le certificazioni stiano ridefinendo la workforce della cybersecurity, il ruolo dell'AI nella trasformazione delle competenze e l'impatto della compliance sui modelli organizzativi.

La cybersecurity è entrata in una nuova fase. La sfida non è più soltanto assumere più persone, ma dimostrare che i team possiedono le competenze giuste, sono in grado di adattarsi ai cambiamenti introdotti dall'intelligenza artificiale e possono comprovare il proprio livello di preparazione in un contesto sempre più regolamentato. Nel 2026, le certificazioni diventano molto più di semplici credenziali professionali: sono uno strumento per validare le capacità, standardizzare i ruoli e creare fiducia tra team di sicurezza, executive, clienti, auditor e autorità regolatorie.

Il 2026 Cybersecurity Workforce Research Report di SANS | GIAC evidenzia chiaramente questo cambiamento: il 60% delle organizzazioni afferma che i gap di competenze rappresentano oggi una sfida più rilevante della carenza di personale, mentre l'81% segnala lacune nelle competenze cybersecurity richieste. Allo stesso tempo, il 74% dichiara che l'AI ha già

avuto un impatto sulle dimensioni dei team di cybersecurity o sulla struttura dei ruoli, e solo il 21% dispone di policy complete di sicurezza e governance dell'AI.

## Dalla carenza di personale ai gap di competenze

Per anni, il dibattito sulla workforce cybersecurity si è concentrato soprattutto sulla mancanza di talenti. Oggi la conversazione si sta evolvendo. Le organizzazioni hanno ancora bisogno di persone, ma la domanda più urgente è se le persone già presenti siano davvero preparate per le attività che oggi vengono loro richieste. AI, adozione del cloud, esposizione della supply chain, ransomware e requisiti normativi sempre più complessi stanno generando una domanda crescente di competenze più profonde, più specialistiche e più misurabili.

È per questo che le certificazioni continuano ad avere un ruolo centrale. Offrono un metodo strutturato per valutare se un professionista sia in grado di operare rispetto a un corpus di conoscenze definito e, sempre più, se sappia applicare tali conoscenze in scenari pratici. Per i responsabili della sicurezza, questo consente di trasformare gli investimenti in formazione in una strategia visibile e difendibile di sviluppo delle capacità.

## L'AI sta ridefinendo i ruoli nella cybersecurity

L'AI sta cambiando entrambi i lati dell'equazione cybersecurity. I difensori la utilizzano per accelerare rilevamento, automazione, analisi e risposta, mentre gli attaccanti sfruttano le stesse tecnologie per scalare social engineering, scoperta di vulnerabilità e automazione malevola. Di conseguenza, i team cybersecurity devono capire non solo come proteggere i sistemi di AI, ma anche come utilizzare l'AI

in modo sicuro ed efficace nei propri flussi di lavoro.

Questo crea nuove aspettative in termini di pianificazione della workforce. Alcune attività entry-level potranno essere sempre più automatizzate, ma questo non elimina la necessità di sviluppare talenti. Cambia piuttosto le competenze che i professionisti junior e mid-level devono costruire: pensiero critico, uso sicuro degli strumenti di AI, validazione degli output automatizzati, consapevolezza della governance e capacità di operare in ambienti tecnici sempre più complessi.

SANS ha risposto con risorse pratiche pensate per aiutare le organizzazioni a costruire team di sicurezza capaci di operare nell'era dell'AI, tra cui il SANS AI Security Maturity Model, il Secure AI Blueprint, risorse formative dedicate all'AI, l'AI Cybersecurity Careers Guide e gli insight del SANS AI Survey. Nel loro insieme, queste risorse aiutano le organizzazioni a valutare la propria maturità, individuare i gap di competenze e definire passi concreti per governare, proteggere e rendere operativa l'AI in modo sicuro.

## La compliance sta ridefinendo il concetto di "qualificato"

Anche la regolamentazione sta cambiando l'equazione della workforce. NIS2, DORA, AI Act europeo, ISO 27001, ISO 42001, IEC 62443 e altri framework richiedono sempre più spesso alle organizzazioni di dimostrare che i rischi cyber siano gestiti da persone con competenze, responsabilità e supervisione adeguate.

Secondo la ricerca 2026 SANS | GIAC sulla workforce, il 68% delle organizzazioni segnala un impatto da moderato a estremo delle direttive regolatorie sulle decisioni di hiring, e il 53% afferma che sono necessari nuovi ruoli specialistici per soddisfare i requisiti normativi. Le certificazioni aiutano le organizzazioni a fornire evidenze del fatto che le persone

responsabili del rischio cyber, dell'incident response, della sicurezza cloud, degli ambienti industriali, della sicurezza AI o della governance siano state formate e valutate rispetto a standard riconosciuti.

Man mano che i ruoli cybersecurity diventano più specialistici, le organizzazioni hanno bisogno di un linguaggio comune per definire le capacità. Framework di workforce come NICE, l'European Cybersecurity Skills Framework (ECSF) e il framework dello UK Cyber Security Council offrono una struttura per mappare ruoli, competenze e percorsi di carriera. Le certificazioni completano questi framework fornendo alle organizzazioni un modo coerente per validare le competenze tra team, regioni e business unit.

Se utilizzato correttamente, questo approccio aiuta le organizzazioni a:

- Individuare i gap di competenze prima che diventino rischi operativi
- Allineare i piani di formazione a ruoli specifici e priorità di business
- Supportare decisioni di assunzione, promozione e sviluppo di carriera
- Dimostrare il livello di preparazione a executive, clienti, auditor e regolatori
- Costruire pipeline di talento sostenibili, invece di dipendere solo dall'assunzione esterna

# Le certificazioni in cybersecurity come strumento di validazione delle competenze

La certificazione resta uno dei metodi più utilizzati per validare le competenze cybersecurity. La ricerca 2026 SANS | GIAC sulla workforce ha rilevato che il 64% delle

organizzazioni utilizza le certificazioni per validare le competenze cybersecurity e che il 58% le considera molto importanti nei processi di selezione.

Il valore non risiede soltanto nella credenziale in sé, ma in ciò che essa rappresenta: conoscenze specifiche per ruolo, applicazione pratica e un benchmark coerente, comprensibile tra team e mercati diversi. In un contesto in cui le decisioni di hiring sono spesso prese a livello di senior leadership, le certificazioni aiutano anche a tradurre le capacità tecniche in un linguaggio comprensibile a executive e stakeholder non tecnici.

## Come devono evolvere le certificazioni nel 2026

Per restare rilevanti, le certificazioni devono continuare a evolvere insieme alla workforce. Le certificazioni di maggiore valore saranno:

- Pratiche e basate sulle competenze, con laboratori, simulazioni e scenari reali, non solo valutazioni teoriche
- Specifiche per ruolo, allineate alle responsabilità di analyst, engineer, incident responder, specialisti cloud, difensori OT, practitioner di sicurezza AI e cyber leader
- Aggiornate in modo continuo, per riflettere nuove minacce, tecnologie, strumenti e aspettative normative
- Accessibili ai talenti emergenti, a supporto dello skills-based hiring e di percorsi di crescita strutturati
- Allineate alle esigenze dell’organizzazione, aiutando i leader a collegare i percorsi di certificazione alla pianificazione della workforce e alla riduzione del rischio

# Cosa significa per i CISO

Per i CISO, la sfida è sempre più una questione di orchestrazione. Devono comprendere dove si trovano le competenze, dove i gap generano rischio, quali ruoli mancano e come dimostrare i progressi alla leadership. Fogli di calcolo, piattaforme GRC, dashboard, matrici di competenze e framework di workforce hanno tutti un ruolo da svolgere, ma sono realmente utili solo quando sono collegati a competenze validate e a percorsi di sviluppo chiari.

Nel 2026, una strategia matura per la workforce cybersecurity dovrebbe combinare pianificazione della workforce, governance dell'AI, mappatura dei ruoli, formazione pratica e certificazioni. Questo aiuta i responsabili della sicurezza a passare da decisioni formative isolate a un modello misurabile di capacità, in grado di sostenere resilienza e accountability.

# Key finding del 2026 Workforce Study

Il 2026 Cybersecurity Workforce Research Report di SANS | GIAC evidenzia diversi key finding che dovrebbero guidare il modo in cui i CISO valutano le capacità nel 2026: i gap di competenze pesano ormai più della carenza di personale, l'AI sta già modificando dimensioni e struttura dei team, la compliance sta influenzando assunzioni e nuovi ruoli specialistici, la formazione resta critica ma è limitata da tempo e budget, e le certificazioni continuano a essere il principale strumento utilizzato dalle organizzazioni per validare le competenze cybersecurity. Nel loro insieme, questi risultati mostrano che la strategia di workforce non può più essere separata dalla gestione del rischio, dalla governance dell'AI e dalla readiness regolatoria.

| Finding | Why it matters |
|---|---|
| 60% say skills gaps are a bigger challenge than lack of staff | Workforce planning must focus on capability, not only headcount. |
| 81% report gaps in required cybersecurity skills | Training plans need to be more targeted and role-based. |
| 74% say AI has impacted team size or role structure | AI skills are becoming part of mainstream cybersecurity readiness. |
| 21% have comprehensive AI security and governance policies | Most organizations still need to mature AI governance and security practices. |
| 68% report hiring impact from regulatory directives | Compliance is increasingly shaping the definition of qualified talent. |
| 64% use certification to validate cybersecurity skills | Certifications remain a central mechanism for proving capability. |

# Continuare la conversazione in Italia

Per i lettori di ICT Security Magazine, questa conversazione proseguirà al Forum ICT Security 2026, in programma il 18 e 19 novembre 2026 a Roma. SANS sarà presente all'evento, dove CISO, executive, policy maker e professionisti della cybersecurity discuteranno di workforce readiness, sicurezza dell'AI, compliance e delle competenze necessarie per costruire organizzazioni di sicurezza resilienti.

# Conclusione

Le certificazioni cybersecurity stanno acquisendo sempre più valore perché la cybersecurity stessa sta diventando più

misurabile, regolamentata e guidata dalle competenze. L'AI sta ridefinendo i ruoli, le normative stanno alzando le aspettative e le organizzazioni hanno bisogno di evidenze che dimostrino che i loro team siano pronti ad agire. In questo contesto, le certificazioni aiutano a tradurre la formazione in capacità validate e offrono una base concreta per costruire team cybersecurity resilienti e pronti per il futuro.

## Risorse SANS utili

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/certificazioni-in-cybersecurity/

---

# Chat Control 2.0, gli esiti incerti della contestata proposta di regolamento europeo

Lunedì 29 giugno l'Unione Europea è tornata a discutere del Regolamento 2022/0155 CSAR (*Child Sexual Abuse Regulation*), più noto come **"Chat Control 2.0"**.

Presentato nel 2022, negli anni il testo è stato oggetto di numerosi *round* negoziali tra Parlamento, Consiglio e Commissione UE; allo stesso tempo è finito al centro di accese critiche legate al rischio di avallare forme di sorveglianza digitale sugli utenti.

Per meglio inquadrare l'esito dell'incontro, nel presente

articolo ripercorriamo l'*iter* normativo, i contenuti e le principali criticità della proposta di regolamento.

# L'iter della proposta CSAR

Il passaggio iniziale risale all'11 maggio 2022, quando la Commissione Europea annunciò di voler introdurre un regolamento mirato a *"prevenire e combattere l'abuso sessuale sui minori"*.

Alla luce dell'evoluzione delle tecnologie e del mutato panorama di rischio, la proposta si affiancava alla precedente Direttiva 2011/93 e abrogava il Regolamento 2021/1232 – noto come **"Chat Control 1.0"** – che prevedeva una deroga temporanea alla direttiva ePrivacy del 2002, per consentire agli erogatori dei servizi digitali la scansione volontaria delle conversazioni sulle proprie piattaforme a fini di rilevazione e rimozione del *Child Sexual Abuse Material* (CSAM).

La nuova formulazione assegnava ai gestori dei servizi un ruolo più stringente, prevedendo uno *scanning* non più volontario ed episodico ma preventivo e massivo, allo scopo di contrastare più efficacemente lo CSAM e i fenomeni di *grooming*.

Negli anni seguenti, tuttavia, diversi pareri e relazioni tecniche degli organi comunitari avrebbero evidenziato le possibili insidie di simili ingerenze nelle comunicazioni private dei cittadini.

Nonostante tali criticità, inizialmente gran parte degli Stati membri annunciò il proprio favore per l'adozione della normativa; ma in seguito si diffusero crescenti dubbi verso le misure proposte, tanto che le consultazioni avvenute nell'ottobre 2025 terminarono con esito negativo (mentre il 26 novembre il Consiglio avrebbe poi raggiunto una posizione comune).

Dopo una parziale revisione del testo, svoltasi sotto la Presidenza danese del Consiglio UE, alla fine del 2025 si è quindi aperto un processo negoziale – tuttora in corso – che ha coinvolto Parlamento, Consiglio e Commissione europea.

L'*iter* ha registrato un'evoluzione fondamentale a marzo, quando la Commissione Giustizia, Libertà civili e Affari interni (LIBE) ha respinto la deroga provvisoria alla direttiva ePrivacy con 28 voti favorevoli e 38 contrari; pochi giorni dopo, anche il Parlamento si sarebbe pronunciato a sfavore, portando alla scadenza della proroga il 3 aprile 2026.

## Il nodo della crittografia *end-to-end*

Uno dei principali nodi critici della proposta risiede nella previsione di una sorveglianza preventiva generalizzata, che permetterebbe alle aziende *tech* di accedere a chat di messaggistica ed email di milioni di persone senza necessità di alcun controllo giudiziario, così violando il principio di riservatezza della vita privata sancito dall'art. 8 della Convenzione Europea sui Diritti Umani (CEDU).

Questo richiederebbe di verificare i messaggi mediante il *client-side scanning*, analizzando i contenuti direttamente sul dispositivo dell'utente prima di applicare la crittografia *end-to-end* (E2E); ne deriverebbero serie implicazioni anche per le aziende responsabili dei servizi, costrette a monitorare costantemente i contenuti condivisi dai propri utenti alla ricerca di materiali illeciti.

È ovvio che l'unico modo per garantire tale monitoraggio su un'immensa mole di conversazioni sarebbe implementare forme di scansione automatizzata delegate a sistemi basati sull'AI, con quanto ne consegue in termini di falsi positivi ed errori dagli effetti potenzialmente molto gravi per la vita e la

reputazione dei cittadini coinvolti, come del resto aveva rilevato sin da subito il parere congiunto EDPB–EDPS n. 4/2022.

Anche l'imposizione di meccanismi di *age verification* avrebbe serie conseguenze in termini di identificazione e profilazione degli utenti, portando a una sostanziale cancellazione del diritto all'anonimato online.

Soprattutto, minare la crittografia *end-to-end* significherebbe esporre a seri pericoli gruppi di persone già particolarmente vulnerabili alla sorveglianza digitale: come giornalisti investigativi, oppositori politici e perfino vittime di *cyber stalking*, che non potrebbero più contare su alcuna garanzia circa la segretezza delle proprie comunicazioni online.

## Gli attuali contenuti: "Chat Control 2.0"

Allo scopo dichiarato di proteggere i minori da ogni forma di abuso, il testo del regolamento abilita il *mass scanning* preventivo sulle email e i messaggi privati dei cittadini, rischiando di fatto di introdurre forme di sorveglianza digitale generalizzata sugli utenti europei.

Dopo la revisione avvenuta alla fine del 2025 si è tornati a parlare, come già nel Chat Control 1.0, di "scansione volontaria" e non obbligatoria; tuttavia, si continuano a prevedere misure obbligatorie di *risk assessment* (Art. 3) e *risk mitigation* (Art. 4) a carico delle aziende erogatrici di servizi di comunicazione digitale.

Si sancisce poi l'obbligo di introdurre meccanismi di verifica dell'età per i servizi di *hosting* e comunicazione, richiedendo l'esibizione di un documento d'identità o l'utilizzo di credenziali biometriche per accedere a servizi e piattaforme online.

Nel regolamento viene infine anticipata la costituzione di un nuovo centro di controllo europeo incaricato di coordinare le attività di prevenzione e contrasto della violenza sui minori, con cui le aziende tecnologiche saranno tenute a collaborare attivamente.

## La posizione dell'Italia sul Regolamento

Inizialmente tra i sostenitori della proposta, negli ultimi due anni l'Italia ha progressivamente sfumato la propria posizione sul regolamento CSAR.

Tuttavia, pur continuando a dichiararsi contraria alla previsione di forme di scansione massiva sulle comunicazioni private, nel Coreper di novembre il nostro Paese ha scelto non di esprimere un voto contrario ma di astenersi, come ha fatto anche la Germania.

Una scelta ambigua, che lascia aperte numerose domande sulla reale posizione del governo circa una normativa che potrebbe impattare profondamente la privacy dei propri cittadini.

## Le iniziative della società civile

Com'era prevedibile, nei quasi cinque anni trascorsi dalla sua proposizione il Regolamento non è rimasto esente da valutazioni negative.

Le più accese provengono dalle associazioni per i diritti digitali, le quali hanno lanciato una petizione contro l'approvazione della normativa, evidenziando che prevedere una scansione generalizzata su email e servizi di messaggistica equivale a sancire la fine della privacy come concepita in seno all'Unione Europea.

Anche numerosi esperti di cybersecurity si sono pronunciati

contro la proposta, ricordando come sancire l'aggirabilità della crittografia E2E significhi, tra le altre cose, aprire la porta ad ogni tipo di vulnerabilità sui dispositivi degli utenti.

E se i proponenti parlano di un "vuoto normativo" da colmare con urgenza, gli oppositori continuano a ricordare che esistono altre strade per combattere un fenomeno odioso come lo CSAM, senza necessariamente imporre a milioni di cittadini incolpevoli di rinunciare alla privacy delle loro comunicazioni digitali.

## Gli esiti dell'incontro del 29 giugno

Qualora nel trilogo di lunedì 29 giugno 2026 fosse stato raggiunto un accordo, l'adozione formale del regolamento CSAR sarebbe probabilmente arrivata entro la fine di luglio.

L'incontro non ha invece saputo individuare una posizione comune su tutti i punti in discussione, avendo come esito un'ennesima proroga dei lavori.

Si conferma l'esistenza di un consenso diffuso rispetto alla maggior parte delle misure proposte, come le definizioni del fenomeno da contrastare o le funzioni del futuro Centro Europeo per la protezione dei Minori; restano tuttavia irrisolti gli aspetti relativi alla scansione automatica dei messaggi privati, da sempre il punto più contestato della normativa.

Intanto, secondo quanto riportano alcune fonti (italiane ed estere), il Coreper avrebbe nuovamente calendarizzato un incontro per procedere a revisionare la versione del regolamento in cui era prevista la scansione delle comunicazioni su base volontaria oggetto della proroga scaduta ad aprile, ossia il noto "Chat Control 1.0".

Ciò significherebbe aggirare la volontà espressa dal Parlamento per riproporre una proposta ormai definitivamente decaduta: di fatto una lesione senza precedenti ai meccanismi democratici comunitari, che – se confermata – non mancherà di suscitare nuove critiche e reazioni, ulteriormente complicando la già lunga e travagliata strada per l'approvazione del regolamento CSAR.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/chat-control-2-0/

---

# Sports Fans Want Better Experiences, Not Better Algorithms


> The future of brands gets decided here. Join the industry's top marketers at Brandweek for the ideas, insights, and connections shaping what's next. **Get your ticket.**


***This post was created in partnership with EY Studio+***

## Key takeaways

- Sports organizations are inundated with data, which can fuel fan engagement if used properly.
- Sports and marketing leaders need to find the right balance between using data and AI tools and maintaining an emotional connection.

- AI can help personalize data for sports fans and make different sports easier for new fans to follow.

Sports organizations have more data than ever. The challenge is using it to strengthen fan connections without sacrificing the emotion at the center of sports.

During an ADWEEK House Cannes Lions group chat co-hosted with EY Studio+, leaders from sports, media, technology, and marketing discussed how AI is changing fan experiences, where personalization creates value, and why trust will shape the next phase of fan engagement.




(L-R) CAA Sports' Roman Di Somma, Fuse's Louise Johnson, EY Studio+'s Laurence Buchanan

## Data should deepen the experience, not distract

The discussion opened with a question about how data fuels fan engagement.

Hanne Jesca Bax, global vice chair – clients and industries at EY, noted that athletes have had access to performance data for years, but fans are now gaining access to many of the same insights. She also pointed to the broader role sports play in

building community.

“I think people have even more thirst to come together, and share in the passion that sports can bring,” Bax said. “Sports bring people together.”

As the conversation continued, participants discussed how data can add context to the fan experience without taking away the emotion.

“One of the greatest things about sport is the emotion, right? Because the emotion cannot be scripted, it’s authentic, and that’s what fans love,” shared Roman Di Somma, head of international talent at CAA Sports. “The key challenge for us is to use data not to fabricate the emotion, but to remove all the filters that are in between the audience and the emotion and serve it so that it can enhance the live experience of a sport.”

Paula Radcliffe, broadcaster and former marathon world-record holder, cautioned that more information is not always better. “I think there has to be a balance there,” Radcliffe said. “There can be too much data, and it can then become confusing and take away the emotions.”

Others agreed that data has value when it provides context and explanation rather than becoming the focal point of the experience itself.



EY’s Hanne Jesca Bax

## Fans care more about the experience than the technology

The conversation then turned to personalization and how AI can make sports easier to follow.

For Louise Johnson, global CEO of Fuse, the goal is to simplify the fan experience. “Fans don’t wake up and go, ‘Oh, hey, I want a sports algorithm,’” Johnson said. “They want to know more about sport.”

Johnson argued that AI is most useful when it removes friction, helping fans find content, follow teams, and engage with the sports they love.

Laurence Buchanan, global leader of EY Studio+, explained that the most effective applications of data are the ones that make stories more accessible. “It’s not the data, it’s the story that the data tells, and that’s the thing that’s driving engagement with fans,” Buchanan explained.

He pointed to younger audiences who often discover sports through gaming before they begin watching or playing.

Statistics and player data can become an entry point that helps fans connect with sports.

The group also discussed how data can make sports more accessible by helping newcomers distinguish between good and great performance.

“You can now be a fan of so many different sports, because it’s very easy for you to understand as a fan the difference between good and great, and data is what provides that insight,” said Jon Gieselman, chief growth officer of connectivity and platforms at Comcast.



(L-R) Paula Radcliffe, Comcast’s Jon Gieselman, ADWEEK’s Will Lee

## The fan journey is still fragmented

Participants also discussed one of the biggest challenges facing sports organizations today.

“Sport has a really unfair advantage, which is the loyalty of the customer,” shared Buchanan. “The challenge of sports and fan experience is fragmentation.”

Fans move between teams, leagues, broadcasters, sponsors, venues, retailers, and creators throughout a single experience. As those touchpoints continue to converge, organizations are working to create a more connected fan journey.

“I think the brands that will win will be able to join those dots from the live moment to the retail moment to the ecom moment, to the creator to the media to the event,” Johnson added.

## Trust will shape the future of fan engagement

The conversation closed with a focus on trust and the growing role data plays in relationships.

From an athlete’s perspective, Di Somma said trust is still the foundation for everything else. “I think trust is at the core,” he said.

That same principle applies to fan experiences. Personalization can create value when it feels useful. Problems arise when fans feel their information is being used in ways they did not expect.

“Passion buys you permission,” Di Somma said. “If you try new things, if you try new tools, if you try new AI, you will immediately see if fans lean in.”

Although technology was a major topic, the group repeatedly returned to the same conclusion: Sports remain powerful because they are unpredictable, emotional, and human. AI may help organizations create better experiences around those moments, but the moments themselves are what matter most.

**Featured Conversation Leaders**

- Hanne Jesca Bax, Global Vice Chair – Clients and Industries, EY
- Laurence Buchanan, Global Leader, EY Studio+

- Roman Di Somma, Head of International Talent, CAA Sports
- Jon Gieselman, Chief Growth Officer of Connectivity and Platforms, Comcast
- Will Lee, CEO, ADWEEK
- Louise Johnson, Global CEO, Fuse
- Paula Radcliffe, Broadcaster

Recommended videos
https://www.adweek.com/brand-marketing/sports-fans-want-better-experiences-not-better-algorithms/

---

# Google aumenta emissioni di CO2 (+18%), consumi energetici (+37%) ed idrici (+34%) per colpa dell'AI

## L'AI mette sotto pressione gli obiettivi climatici di Google: consumi record di energia elettrica ed acqua nel 2025

L'**intelligenza artificiale** (AI) sta cambiando il mondo digitale, ma sta anche cambiando, e non in meglio, il profilo ambientale delle Big Tech. A confermarlo è l'ultimo *Environmental Report* di **Google**, che fotografa un anno in cui la corsa alla costruzione di infrastrutture per l'AI ha portato **consumi di energia elettrica, utilizzo di acqua ed emissioni di gas serra** ai livelli più alti mai registrati

dall’azienda.

Il dato più significativo riguarda proprio l’energia. Nel 2025 **la domanda di elettricità di Google è aumentata del 37%** rispetto all’anno precedente, dopo un incremento già molto elevato del 27% registrato nel 2024. Se si guarda al periodo pre-boom dell’intelligenza artificiale, il confronto è ancora più eloquente: oggi il fabbisogno energetico dell’azienda è circa tre volte e mezzo superiore rispetto al 2019.

Non meno significativo è il dato sull’acqua. **I consumi idrici hanno raggiunto 10,9 miliardi di galloni, con un incremento del 34%** rispetto all’anno precedente e un volume più che raddoppiato rispetto al 2021. Gran parte di questa crescita è attribuita ai data center, dove l’acqua viene utilizzata per il raffreddamento delle infrastrutture informatiche, una risorsa sempre più critica soprattutto nelle aree soggette a stress idrico.

## L’efficienza energetica non compensa più i consumi, aumentano le emissioni di gas serra

La crescita dell’infrastruttura necessaria per addestrare ed eseguire i modelli di intelligenza artificiale sta infatti **superando i miglioramenti ottenuti sul fronte dell’efficienza dei data center**. In altre parole, i sistemi consumano meno energia per unità di calcolo, ma il numero di server, acceleratori e chip installati aumenta a una velocità tale da annullare i benefici ottenuti.

Anche il bilancio climatico peggiora sensibilmente. **Le emissioni di gas serra sono cresciute del 18%** in un solo anno, il maggiore incremento annuale mai riportato da Google. A pesare è soprattutto la produzione dell’hardware destinato all’AI, dai processori specializzati ai server che popolano i

nuovi data center. Non si tratta quindi soltanto dell'energia necessaria per far funzionare queste strutture, ma anche dell'impatto industriale legato alla loro costruzione.

## L'AI manda all'aria gli impegni di sostenibilità delle Big Tech, una "buona narrazione" non basta più

Questi numeri raccontano una contraddizione sempre più difficile da ignorare. Google è da anni una delle aziende tecnologiche che investono maggiormente nelle **energie rinnovabili** e continua a presentarsi come protagonista della **transizione energetica**. Nel solo ultimo anno ha sottoscritto accordi per circa **12 gigawatt di nuova capacità da fonti pulite**, un record per il gruppo, riuscendo inoltre a mantenere pressoché stabile la quota di elettricità priva di emissioni di carbonio utilizzata per alimentare le proprie attività. Le emissioni legate all'elettricità sono perfino diminuite del 3% rispetto all'anno precedente.

Tuttavia, questi risultati non bastano più a compensare la **crescita impetuosa della domanda di calcolo imposta dall'intelligenza artificiale**. Lo stesso report riconosce apertamente questa realtà, sottolineando che la rapida espansione del fabbisogno energetico rappresenta una sfida da gestire attivamente e che la crescita dell'AI non può diventare un pretesto per abbassare gli standard ambientali.

È proprio qui che emerge il paradosso delle Big Tech, come spiegato da Amy Harder su *Axios*. Per anni i rapporti di sostenibilità sono stati soprattutto strumenti attraverso i quali **raccontare, "attraverso una buona narrazione", i progressi nella riduzione delle emissioni e negli investimenti in energia pulita**. Oggi, invece, gli stessi documenti ufficiali mostrano come la rivoluzione dell'intelligenza artificiale stia mettendo sotto pressione quegli obiettivi

climatici che le aziende avevano indicato come prioritari.

## Obiettivi di sostenibilità al ribasso, mentre cresce l’impatto dei data center sui territori: il prezzo da pagare per l’AI?

L’impressione è che il parametro di riferimento sia cambiato. **Non si parla più di ridurre le emissioni in valore assoluto**, ma di limitarne la crescita rispetto a quella che sarebbe stata senza gli investimenti in fonti rinnovabili. Una differenza sostanziale che modifica il significato stesso degli impegni ambientali.

Il tema assume un peso ancora maggiore perché **la costruzione di nuovi data center è ormai al centro del dibattito pubblico e politico** soprattutto negli Stati Uniti. In molti territori **le comunità locali guardano con crescente attenzione a infrastrutture che richiedono enormi quantità di elettricità e di acqua**, incidendo sulle reti energetiche, sulle risorse idriche e sull’uso del territorio.

Secondo un recente **rapporto** dell’**United Nations University Institute for Water, Environment and Health (UNU-INWEH)**, entro il **2030** i data center mondiali potrebbero arrivare a consumare **945 terawattora (TWh)** di elettricità all’anno. Per comprendere l’ordine di grandezza, si tratta di un volume quasi triplo rispetto al consumo elettrico annuo combinato di **Pakistan, Bangladesh e Nigeria**, tre Paesi che insieme ospitano oltre **650 milioni di persone**.

## Una transizione green che perde

# credibilità

La domanda non riguarda più soltanto i benefici economici e tecnologici dell'intelligenza artificiale, ma anche **il prezzo ambientale** necessario per sostenerne la diffusione. Prendiamo l'ondata di calore record che ha travolto tutta l'Europa in questo inizio estate, secondo diversi studi condotti negli Stati Uniti, i data center hanno un impatto sul microclima locale da non sottovalutare in termini di aumento delle temperature medie.

Google continua a sostenere che l'AI potrà contribuire, nel medio periodo, a ridurre le emissioni in altri settori dell'economia, dall'ottimizzazione delle reti elettriche all'efficienza industriale. Almeno per ora, però, **il bilancio ambientale raccontato dai dati ufficiali va nella direzione opposta**.

Paradossalmente, i report di sostenibilità delle Big Tech stanno diventando uno degli indicatori più osservati per capire se la promessa di uno sviluppo digitale sostenibile riuscirà davvero a convivere con la gigantesca espansione infrastrutturale richiesta dall'intelligenza artificiale.

**Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui**




**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/google-aumenta-emissioni-di-co2-18-consumi-energetici-37-ed-idrici-34-per-colpa-dellai/578369/

# Why Peacock’s Love Island USA Makes a Perfect Partner for Advertisers



The future of brands gets decided here. Join the industry’s top marketers at Brandweek for the ideas, insights, and connections shaping what’s next. **Get your ticket.**

Peacock’s Love Island USA continues to bring the heat in Season 8, and advertisers are feeling the love.

Love Island USA ranked as the No. 1 series on streaming during its first two weeks of Season 8, according to Nielsen. It garnered a combined 2.3 billion minutes viewed during the weeks of June 1 and June 8, up 50% from the previous season’s first two weeks.

The show’s continued popularity has also been a draw for advertisers, with Peacock forging several new partnerships for the current season.

Among the advertising highlights, Season 8 has featured seven integrated partners, six of which are returning from the previous season, including CeraVe, Coffee-Mate, Cuervo, Maybelline, Motorola, and PepsiCo.

Recommended videos
https://www.adweek.com/convergent-tv/peacock-love-island-usa-makes-perfect-partner-advertisers/

---

# SSPM: la sicurezza dei SaaS che usi ma non controlli

SSPM è l’acronimo di SaaS Security Posture Management, e nasce da uno spostamento che ha cambiato in silenzio dove vive il rischio. L’attività di un’organizzazione oggi non gira più su server che configura e custodisce, ma su decine, spesso centinaia, di applicazioni in modalità software come servizio: la posta, i documenti, il CRM, le risorse umane, lo sviluppo, la collaborazione. Di queste applicazioni l’organizzazione non possiede l’infrastruttura e non ne scrive il codice. Ne controlla soltanto una cosa, la configurazione, ed è esattamente lì che si è trasferito il problema di sicurezza.

La logica è la stessa che governa il cloud, ma portata un passo più in là. Il fornitore del SaaS si occupa di proteggere la piattaforma e di tenerla aggiornata; al cliente resta la responsabilità di come quella piattaforma è impostata: chi può

accedere, cosa è condiviso con l’esterno, quali account hanno privilegi da amministratore, a quali applicazioni di terze parti si è dato il permesso di collegarsi. L’SSPM è la disciplina che verifica, in modo continuo, che la postura di tutto questo parco di applicazioni sia sicura, perché nessun fornitore lo farà al posto del cliente.

## La responsabilità che si è spostata

Conviene fissare bene questa divisione, perché è la fonte di gran parte degli incidenti. Nel modello del software come servizio il fornitore garantisce la sicurezza della piattaforma, ma la configurazione del singolo ambiente, il cosiddetto *tenant*, è interamente nelle mani del cliente. È il punto in cui si annidano le esposizioni: una regola di condivisione troppo permissiva che rende un documento accessibile a chiunque, un controllo amministrativo lasciato aperto, l’autenticazione a più fattori non imposta a tutti. Sono errori di impostazione, non difetti del prodotto, ed è il cliente a doverli trovare.

Il guaio è che la superficie di configurazione è enorme e diversa per ogni applicazione. Ciascuna piattaforma, dalla suite di produttività al CRM, ha centinaia di impostazioni di sicurezza con una propria logica, e quasi nessuna organizzazione le verifica in modo sistematico e ricorrente. La configurazione si fa una volta, all’avvio, e poi si muove da sola: nuovi utenti, nuovi permessi, nuove integrazioni, nuove derive rispetto allo stato sicuro di partenza. Senza un controllo continuo, lo scostamento cresce invisibile, fino al giorno in cui qualcuno si accorge che un dato che doveva restare interno era raggiungibile da fuori.

## Il ventre molle: le integrazioni

## SaaS-to-SaaS

C’è un fronte, in particolare, che sfugge a quasi tutti, ed è quello delle connessioni tra applicazioni. Ogni volta che si collega un’app di terze parti a una piattaforma SaaS, attraverso un consenso OAuth, si concede a quell’app un accesso ai propri dati che è ampio, persistente e raramente rivisto. È, a tutti gli effetti, una identità non umana con permessi spesso eccessivi rispetto a ciò che le serve, concessa con un clic e poi dimenticata. Moltiplicato per le centinaia di integrazioni che un’organizzazione accumula nel tempo, questo intreccio di connessioni da applicazione ad applicazione diventa una rete che nessuno ha mai inventariato.

È un ventre molle pericoloso perché aggira il perimetro. Un attaccante che comprometta un’app di terze parti con un consenso valido raggiunge i dati custoditi nella piattaforma principale senza dover violare nulla del cliente: usa una porta che il cliente stesso ha aperto. Lo ha mostrato in modo netto la compromissione dell’integrazione Drift di Salesloft, nell’agosto 2025: token OAuth sottratti a quell’app di terze parti hanno dato accesso ai dati Salesforce di oltre settecento organizzazioni, aggirando l’autenticazione, e da lì gli attaccanti hanno cercato credenziali per spostarsi verso altri servizi. È la dimostrazione di come una via legittima, una volta compromessa, diventi un’autostrada. L’SSPM affronta proprio questo, tracciando le applicazioni connesse, valutando gli ambiti e i permessi che hanno ottenuto, e segnalando le integrazioni rischiose o sovradimensionate prima che diventino il percorso di un attacco.

## SSPM non è CSPM e non è CASB

Per collocare bene questa disciplina serve distinguerla da altre con cui viene spesso confusa. La gestione della postura degli ambienti cloud, il CSPM, protegge l’infrastruttura su cui si costruisce, le macchine, le reti, gli archivi dei

fornitori di servizi infrastrutturali. L’SSPM protegge invece la configurazione delle applicazioni che si consumano già pronte. I due mondi si somigliano nel concetto, postura, scostamento, librerie di regole, ma poggiano su interfacce completamente diverse, al punto che le regole dell’uno non si possono trasferire all’altro: lo spiega bene chi ha mappato chi protegge cosa tra le varie sigle. Il CNAPP, semmai, non è una categoria contrapposta ma la piattaforma più ampia che consolida diverse di queste capacità, il CSPM tra le altre, e che in alcuni casi arriva a inglobare lo stesso SSPM come componente.

Diversa ancora è la funzione di un CASB, che lavora sul traffico: osserva e controlla l’uso delle applicazioni, blocca caricamenti, ispeziona i dati in transito, agendo come un intermediario sul flusso. L’SSPM non sta sul flusso, sta dentro l’applicazione, e governa la configurazione, le identità e gli accessi delle terze parti. Non sono alternative, sono strati complementari: il CASB sorveglia come gli utenti usano i SaaS, l’SSPM verifica come i SaaS sono impostati. Trattarli come la stessa cosa lascia scoperto proprio il livello, quello della postura, su cui questa disciplina lavora.

## Cosa guarda l’SSPM

In concreto, l’SSPM tiene sotto controllo alcune dimensioni ricorrenti su tutto il parco applicativo. Le configurazioni errate, come le condivisioni pubbliche e le impostazioni deboli. Le identità, con gli amministratori dormienti, l’autenticazione a più fattori non imposta, i ruoli sovraprivilegiati. Le applicazioni di terze parti collegate e gli ambiti che hanno ottenuto. E lo scostamento rispetto ai requisiti di conformità. Lo fa attraverso le interfacce delle piattaforme, senza agenti da installare, e soprattutto lo fa in continuazione, perché in un ambiente che cambia ogni giorno una verifica una tantum invecchia nel giro di una settimana.

## Perché conta adesso

La spinta che rende il tema urgente è la proliferazione stessa del software come servizio. Le organizzazioni adottano un numero di applicazioni molto superiore a quello che la sicurezza riesce a censire, e una quota consistente è *shadow SaaS*, sottoscritta dai singoli reparti senza passare da nessun controllo centrale. A questo si aggiunge l'arrivo degli assistenti basati sull'intelligenza artificiale dentro le stesse piattaforme, che ottengono accesso ai dati aziendali e allargano ulteriormente la superficie da governare. Il perimetro, in pratica, non è più una rete da difendere, ma un insieme di centinaia di ambienti che qualcuno ha configurato, spesso in fretta, e che da allora vivono di vita propria.

In definitiva, l'SSPM risponde a una domanda che vent'anni fa non aveva senso porsi, quando il software stava sui server di casa: le applicazioni che noleggio ma non gestisco sono configurate in modo sicuro, e a chi ho dato silenziosamente le chiavi dei miei dati. Più l'attività si sposta nei SaaS, più questi si collegano tra loro e all'intelligenza artificiale, e più la postura di quel parco di applicazioni diventa la vera superficie d'attacco, quella che il cliente possiede per intero e che, paradossalmente, quasi nessuno sorveglia. L'SSPM è il modo per smettere di darla per scontata.

## Fonti

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/cyber-security/sspm-saas-security-posture-management/

# WPP Bolsters Enterprise Services in Bid to Be an AI One-Stop Shop




In February, WPP CEO Cindy Rose made a big bet that the holding company could take a pole position in AI transformation when she unveiled WPP Enterprise Solutions, one of the four linchpins in her Elevate28 revitalization plan.

On Wednesday, the unit took a step toward realizing that goal by launching a portfolio of AI-powered solutions.

That portfolio includes five services: AI Transformation Consulting; Agentic Commerce, to shape how AI agents discover and recommend brands; Owned Intelligence, to help clients use their own data to create AI-ready assets; Real-time Relationships, to personalize customer interactions and drive loyalty; and Intelligent Content, to plan and develop content.

Recommended videos
https://www.adweek.com/agencies/wpp-bolsters-enterprise-unit-in-bid-to-be-an-ai-one-stop-shop/

# FiberCop, le telco bocciano i nuovi listini

*Oggi in primo piano la lettera di **Fastweb + Vodafone**, **WindTre**, **iliad** e **Sky** inviata ad **Agcom** per contestare gli aumenti dei prezzi di accesso all'ingrosso alla rete di **FiberCop**. Sotto esame gli impatti del modello "**wholesale only**" approvato dal regolatore. Si riaprirà il dossier?*

*Poi la nostra analisi sulla decisione della **Corte Suprema** americana che di fatto toglie l'**indipendenza** alle principali agenzie federali del Paese, sottoponendole al controllo del **Presidente degli Stati Uniti**.*

*Tra queste c'è la FTC, l'Antitrust USA. In virtù di questo radicale cambiamento delle agenzie, non più indipendenti, l'attivista austriaco per la privacy Max Schrems scrive all'UE: "Cancellare l'accordo sul Data Privacy Framework".*

Leggi le notizie della notra dailyletter

**Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui**




**Leggi le altre notizie sull'home page di Key4biz**

https://www.key4biz.it/fibercop-le-telco-bocciano-i-nuovi-listini/578315/

# Saldi, sabato al via in quasi tutta Italia ma ribassi già iniziati

(Adnkronos) – Al via sabato i saldi estivi in quasi tutta Italia, tranne per Bolzano e Trento. Attesi da famiglie ed esercenti gli sconti arrivano in una fase di ripresa del reddito disponibile delle famiglie e dei consumi che, secondo l'Istat, segnano rispettivamente +1,6% e +1,4% nel primo trimestre rispetto al precedente. Da vedere se questo rinnovato slancio si tradurrà in una crescita delle spese o del risparmio.

Ma le promozioni di fatto sono già partite: secondo un'indagine Ipsos per Fismo, la Federazione Italiana Settore Moda Confesercenti, più di un terzo degli italiani, il 36%, ha acquistato a prezzo scontato prima dell'apertura ufficiale. Ad acquistare in anticipo è soprattutto il Mezzogiorno, dove la quota sale al 42%, contro il 33% del Nord e il 32% del Centro. Nel dettaglio territoriale il picco è al Sud e nelle Isole (42%) e nel Nord-Est (40%), più contenuto il Nord-Ovest (28%). Per fasce d'età l'anticipo riguarda quasi un under 35 su due (48%), contro il 31% degli over 35; tra gli uomini (38%) di poco più che tra le donne (35%). Un fenomeno diffuso che, per Fismo, misura un sistema da rivedere.

Sullo sfondo, un comparto in sofferenza strutturale. Tra il 2019 e il 2025 hanno chiuso oltre 18mila negozi di abbigliamento e calzature, un calo del 13,5%, con circa 17mila posti di lavoro persi. La spesa delle famiglie per moda e calzature è scesa dal 7% al 3,7% dei consumi. I negozi indipendenti, che restano circa la metà dei punti vendita,

oggi pesano per il 20-25% del mercato, contro oltre il 75% degli anni Ottanta.

Calendario alla mano, i saldi dureranno al massimo fino al primo settembre. Nel distretto di Bolzano, Oltradige e Bassa Atesina l'intervallo per beneficiare degli sconti andrà dal 16 luglio al 13 agosto; in alcuni comuni, tra i quali Ortisei, dal 21 agosto al 18 settembre. Mani libere in Trentino, la regione autonoma non è tenuta ad una data unica di inizio delle svendite. Intanto c'è grande attesa tra gli esercenti romani: secondo le stime della Confcommercio oltre 8 cittadini su 10 si avvarranno dei saldi (81,4 %).

E la stagione degli sconti quest'anno si apre sotto la spinta anche della tassa di tre euro sui pacchi extra-Ue, accolta con favore dagli esercenti per contenere l'ondata dell'ultra fast fashion, come Shein. "I saldi estivi sono uno degli appuntamenti più attesi da famiglie, turisti e imprese con l'obiettivo di sostenere i consumi, valorizzare il commercio di prossimità e rafforzare un pilastro fondamentale della filiera della moda", sottolinea in una nota il presidente di Federmoda-Confcommercio Giulio Felloni. "Anche l'introduzione, da oggi, 1° luglio, del dazio di 3 euro sui piccoli pacchi extra Ue è un segnale importante per riequilibrare il mercato all'insegna del principio 'stesso mercato stesse regole'. Una misura che Federazione Moda Italia-Confcommercio ha fortemente voluto a livello europeo e che va nella direzione di contrastare gli squilibri generati dall'ultra fast fashion", aggiunge, annunciando per domani la presentazione di un pacchetto di proposte in occasione dell'incontro sul retail della Moda al ministero per le Imprese ed il Made in Italy.

Ma sulla ripresa del reddito e della spesa delle famiglie, al +1,6% e +1,4% nel primo trimestre secondo l'Istat, c'è la diffidenza dei consumatori che parlano di dati superati ed 'erosi' dal caro-energia. "Nel primo trimestre 2026 non si erano ancora dispiegati gli effetti nefasti dovuti all'effetto Iran. A marzo l'inflazione era ancora contenuta, sotto il 2%:

1,7%, da 1,5% di febbraio. E’ da aprile che è decollata da 1,7 a 2,7, con un’inflazione congiunturale dell’1,1%, un primato su base mensile che non si aveva addirittura dall’ottobre del 2022 al tempo della guerra in Ucraina”, osserva il presidente dell’Unione nazionale dei consumatori Massimiliano Dona. “Nel secondo trimestre questi dati, ora relativamente positivi, sono destinati, purtroppo, a peggiorare. Senza contare che comunque – avverte – non possono essere considerati entusiasmanti. Il fatto che il reddito disponibile salga più dei consumi, vuol dire che anche le famiglie che potrebbero permettersi di spendere di più, preferiscono mettere i soldi sotto al materasso e risparmiare, per mancanza di fiducia nel loro futuro, a scopo precauzionale”.

Dai cambi ai pagamenti, i decaloghi anti-fregatura danno una serie di indicazioni per non incorrere in brutte sorprese. Tra questi la possibilità di sostituire un capo dopo l’acquisto, entro il massimo di un mese, a meno che il prodotto non sia stato danneggiato. Nel caso di prodotto difettoso il negoziante è tenuto alla sostituzione o il rimborso se impossibilitato a sostituirlo. Nell’e-commerce invece si può chiedere il rimborso del prodotto in ogni caso, quando anche non è difettoso. Sul fronte dei pagamenti, il negoziante è tenuto ad accettare le carte ove richiesto. Quanto al prodotto in vendita, deve avere carattere stagionale e non dovrebbe essere un’occasione per ‘svuotare’ il magazzino. D’obbligo la massima trasparenza sui prezzi: sul cartellino va indicato il prezzo normale di vendita, lo sconto e il prezzo finale. (di Luana Cimino)

–

economia

webinfo@adnkronos.com (Web Info)

**Novità su Google, per aggiungere Key4Biz tra le tue fonti preferite, clicca qui**




**Leggi le altre notizie sull’home page di Key4biz**

https://www.key4biz.it/saldi-sabato-al-via-in-quasi-tutta-italia-ma-ribassi-gia-iniziati/578293/