Rassegna Stampa

di Lunedì 15 giugno 2026

Centro Studi C.N.I.

Sommario Rassegna Stampa

Pagina	Testata	Data	Titolo	Pag.
Rubrica	**Imprese**			
1+5	Il Sole 24 Ore	15/06/2026	*Software, mosaico di agevolazioni ma il cloud per ora resta fuori (G.Giordano/R.Villa)*	3
2	Italia Oggi Sette	15/06/2026	*Iperammortamento, imprese in slalom fra termini e requisiti (B.Pagamici)*	6
Rubrica	**Professionisti**			
14	Il Sole 24 Ore	15/06/2026	*Professioni tecniche, pressing per limitare la responsabilita' civile (G.Latour)*	8
1+5	Italia Oggi Sette	15/06/2026	*Via alle verifiche sui debiti fiscali per le fatture dei professionisti (G.Mandolesi/P.Ricciardo)*	9
Rubrica	**Cybersecurity**			
1+2	Italia Oggi Sette	15/06/2026	*Ora non c'e' piu' scusa che tenga (M.Longoni)*	11
1+7	Italia Oggi Sette	15/06/2026	*Priorita' cybersicurezza (B.Pagamici)*	12
Rubrica	**Space Economy**			
34	Corriere della Sera	15/06/2026	*IL RISCHIO DELLA DISCARICA SPAZIALE (R.Battiston)*	14

Il Sole 24 ORE

IMPRESE

Software, mosaico di agevolazioni ma il cloud per ora resta fuori

L'iperammortamento, attivo da venerdì scorso, si aggiunge al mosaico di misure settoriali che agevolano l'acquisto dei software da parte delle imprese. Le soluzioni via web e in abbonamento (cloud) restano però escluse da quest'ultima misura e sono incentivate solo da aiuti settoriali. Difficile per ora ipotizzare una estensione: c'è il nodo risorse.

Fotina, Giordano, Mazzucco e **Villa** —*a pag. 5*

Software, mix di incentivi ma il cloud per ora è fuori

La mappa. L'iperammortamento attivo da venerdì si aggiunge al mosaico di misure settoriali ma non si applica alle soluzioni gestite via web

Giuseppe Giordano
Umberto Mazzucco
Ranieri Villa

Un mosaico di incentivi al quale si è appena aggiunta l'ultima tessera, anche se priva della parte potenzialmente più interessante. È il quadro – frammentato per destinatari e finalità – delle misure attualmente operative per sostenere gli investimenti in software e digitalizzazione delle imprese italiane.

La tessera che per ultima si è aggiunta è l'iperammortamento, le cui domande sono aperte dalle 12 di venerdì scorso (si veda Il Sole 24 Ore dell'11 giugno). La ragione per cui è priva della parte potenzialmente più interessante è che lo strumento esclude i software as a service (Saas), cioè, in pratica, le soluzioni in base alle quali, invece di installare un software sui propri sistemi, l'utente accede via internet al software stesso pagando un canone. Ma andiamo con ordine.

Il contesto italiano

Secondo i dati Eurostat, nel 2025 solo il 16,4% delle imprese italiane utilizzava strumenti di intelligenza artificiale, contro il 26% della Germania e oltre il 40% dei Paesi nordici come Danimarca e Finlandia. L'Ocse segnala che gli investimenti italiani in asset intangibili – software, dati, ricerca e sviluppo – restano tra i più bassi dell'area euro, mentre nelle economie avanzate gli investimenti reali in software sono triplicati dal 2008 a fronte di una crescita aggregata di appena il 12% per i macchinari. La crescita della produttività si è spostata dagli asset fisici agli asset intangibili, con la conseguenza che il valore non nasce più solamente dalla macchina, ma dal software che la rende "intelligente".

I canoni non capitalizzabili

In questo contesto, l'iperammortamento reintrodotto dalla manovra 2026 è, sulla carta, un interessante incentivo per sostenere gli investimenti in beni strumentali tecnologici: una maggiorazione del costo di acquisizione fino al 180% per investimenti, aperta a tutte le imprese, di tutti i settori, di tutte le dimensioni, indipendentemente dall'ubicazione, senza bandi né graduatorie, operativa in dichiarazione dei redditi come variazione in diminuzione del reddito imponibile.

Come detto, però, l'agevolazione esclude i software as a service. Tecnicamente, i canoni Saas non sono capitalizzabili come immobilizzazioni immateriali: sono costi di esercizio imputati a conto economico, e l'iperammortamento si applica esclusivamente sui beni ammortizzabili.

Il decreto attuativo estende l'agevolazione anche ai beni acquisiti in leasing finanziario, ma non ai canoni di abbonamento. La logica contabile è corretta. Ma il problema è che i grandi vendor internazionali hanno abbandonato il modello della licenza perpetua on-premise. Oggi l'intelligenza artificiale, la cybersecurity, il monitoraggio predittivo, la gestione della supply chain sono erogati in abbonamento. Il software as a service rappresenta circa l'80% del mercato del cloud.

La questione non è nuova, e, peraltro è stata già anche risolta in passato. Infatti, nel 2017 la circolare

Il Sole 24 ORE

4/E dell'agenzia delle Entrate aveva escluso il Saas dall'iperammortamento 4.0 con la stessa logica. Il legislatore era poi intervenuto con la manovra 2019 (legge 145/2018, comma 229), aprendo i canoni cloud tra le spese agevolabili «per la quota imputabile per competenza», orientamento ribadito dalla circolare 8/E del 2019 e rimasto in vigore fino al 31 dicembre 2024.

Le altre misure

Chi cerca alternative trova, come detto, un sistema frammentato per destinatari e finalità (si veda la scheda in pagina). La Simest – nelle misure per Transizione Digitale ed E-commerce – ammette piattaforme cloud e software in abbonamento, ma solo nell'ambito di progetti di internazionalizzazione.

Il programma Digital Transformation di Mimit/Invitalia offre un mix di 10% a fondo perduto e 40% di finanziamento agevolato e copre anche i canoni per l'utilizzo di programmi informatici, ma è riservato alle sole Pmi.

Smart&Start Italia finanzia soluzioni digitali con prestiti a tasso zero fino all'80% delle spese ammissibili, ma è accessibile esclusivamente alle startup innovative con piani tra 100mila e 1,5 milioni di euro.

On-Oltre Nuove Imprese copre software gestionali e applicazioni di AI, blockchain e internet of things con agevolazioni fino al 90% delle spese, ma è rivolto a piccole imprese costituite da non più di 60 mesi la cui compagine societaria sia composta per oltre la metà da under 36 o da donne.

Nessuno di questi strumenti è accessibile a qualsiasi impresa italiana che voglia "solo" investire in software cloud o intelligenza artificiale per migliorare la propria produttività. Il risultato è un mosaico di misure che, prese singolarmente, hanno una loro coerenza, ma che nel complesso non coprono il mercato reale degli investimenti digitali.

L'iperammortamento potrebbe essere il "veicolo" giusto per agevolare i Saas creando così un sostegno universale, automatico e tecnologicamente neutro. La misura copre gli investimenti fino al 30 settembre 2028, perciò il tempo per intervenire c'è, prendendo spunto dal precedente normativo del 2019.

Il problema è che la maggior parte degli applicativi evoluti oggi sul mercato è in abbonamento

2028
La scadenza

La manovra 2026 ha previsto l'iperammortamento per gli investimenti effettuati fino al 30 settembre 2028.

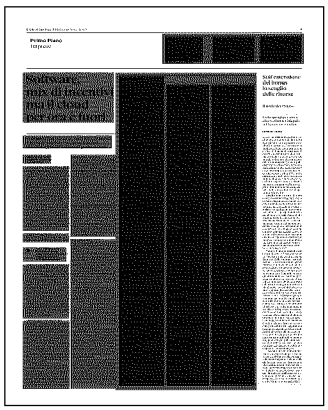
180%
Aliquota massima

Per gli investimenti di importo fino a 2,5 milioni di euro, l'iperammortamento ha l'aliquota più elevata (180%).

650 mln
Nuova Sabatini

È la dote con cui la manovra ha rifinanziato per il 2026-27 la misura che agevola gli interessi su finanziamenti e leasing.


Il Sole 24 ORE
Partite Iva, la salute batte il commercio



Il Sole 24 ORE

Le agevolazioni

1

NUOVO IPERAMMORTAMENTO

Normativa
Legge 199/2025, articolo 1, commi 427-436; Dl 38/2026

Periodo di applicazione
2026-30 settembre 2028

Ambiti tecnologici
Software acquistato (licenze perpetue), sistemi It, piattaforme digitali (Allegati IV-V: software 4.0/5.0, AI, automazione, cybersecurity software - solo se capitalizzabili come immobilizzazioni immateriali)

Saas ammissibile
No, solo software acquistato

Dimensioni aziendali
Tutte

Tipo agevolazione
Maggiorazione del costo d'acquisto, ai fini degli ammortamenti (deduzione fiscale)

Aliquota/importo
- 180% (fino 2,5 milioni di euro);
- 100% (2,5-10 milioni di euro);
- 50% (10-20 milioni di euro)

Note operative
Il cumulo è ammesso a condizione che il sostegno complessivo non copra le medesime quote di costo e non porti al superamento del costo totale sostenuto. La base di calcolo per la maggiorazione è assunta al netto di altre sovvenzioni o contributi già ricevuti per gli stessi investimenti.

2

SIMEST - TRANSIZIONE DIGITALE O ECOLOGICA

Normativa
Fondo 394/81 – disciplina Simest

Periodo di applicazione
Rifinanziamenti periodici

Ambiti tecnologici
Software (integrazione e sviluppo digitale dei processi aziendali), cloud computing, piattaforme digitali, transizione digitale, rafforzamento patrimoniale

Saas ammissibile
Sì

Dimensioni aziendali
Pmi, Mid-Cap, Grandi imprese (con vocazione internazionale)

Tipo agevolazione
Finanziamento a tasso agevolato + cofinanziamento a fondo perduto

Aliquota/importo
- Finanziamento a tasso agevolato (6-8 anni);
- Fondo perduto: 10% (max 100mila euro); 20% (max 200mila euro) per energivore e imprese con requisiti «energy» e 30% (Pmi in misura specifica «Energia per la competitività internazionale») sino al 31 dicembre 2026

Note operative
Almeno il 10% o 20% o 50% per investimenti digitali e il residuo per il rafforzamento patrimoniale; imprese esportatrici; rifinanziamenti periodici

3

SIMEST – E-COMMERCE

Normativa
Fondo 394/81 – disciplina Simest

Periodo di applicazione
Rifinanziamenti periodici

Ambiti tecnologici
Piattaforme e-commerce, software per la gestione degli ordini, circuiti di pagamento, servizi cloud, integrazioni con Erp, Crm, AI e realtà aumentata

Saas ammissibile
Sì

Dimensioni aziendali
Pmi, Mid-Cap, Grandi imprese (con vocazione internazionale)

Tipo agevolazione
Finanziamento a tasso agevolato + cofinanziamento a fondo perduto

Aliquota/importo
Finanziamento a tasso agevolato (4 anni); cofinanziamento a fondo perduto 10% (max 100mila euro) o 20% (max 200mila euro)

Note operative
Canoni SaaS ammessi se riferiti a piattaforme/servizi digitali direttamente connessi alla vendita su mercati esteri e sostenuti nel periodo di realizzazione del progetto

4

NUOVA SABATINI

Normativa
Legge 199/2025, articolo 1, comma 468 ha rifinanziato la misura con 650 milioni di euro per il periodo 2026 e 2027

Periodo di applicazione
2017-2027

Ambiti tecnologici
Software applicativi di proprietà e a titolo di licenza d'uso a tempo indeterminato o determinato, tecnologie digitali

Saas ammissibile
No

Dimensioni aziendali
Pmi

Tipo agevolazione
Finanziamento bancario/leasing agevolato + contributo in conto impianti (pari al valore degli interessi calcolati)

Aliquota/importo
- Finanziamento agevolato fino a 4 milioni di euro;
- contributo conto impianti (interesse annuo pari al 2,75-3,575%)

Note operative
Gestione tramite banca previa richiesta da parte della Pmi

5

DIGITAL TRANSFORMATION (MIMIT/INVITALIA)

Normativa
Dl 19/2024; gestione Invitalia

Periodo di applicazione
Dal 2020

Ambiti tecnologici
Software, costi sostenuti a titolo di canone per l'utilizzo dei programmi informatici, sistemi di e-commerce, di pagamento mobile e via internet, fintech, sistemi elettronici per lo scambio di dati, blockchain, intelligenza artificiale, internet of things

Saas ammissibile
Sì

Dimensioni aziendali
Micro, piccola e media impresa

Tipo agevolazione
Finanziamento agevolato, contributo diretto alla spesa e contributo in conto capitale

Aliquota/importo
- 10% contributo a fondo perduto;
- 40% finanziamento agevolato

Note operative
Procedura informatica, identificazione del compilatore tramite Spid o Cns o identità digitali di Invitalia

6

SMART&START ITALIA (INVITALIA)

Normativa
Dm 24 settembre 2014 (e successive modifiche)

Periodo di applicazione
Dal 2014

Ambiti tecnologici
Soluzioni digitali e tecnologiche delle startup innovative: componenti hardware e software, licenze relative all'utilizzo di software

Saas ammissibile
Sì

Dimensioni aziendali
Startup innovative

Tipo agevolazione
- Finanziamento a tasso zero;
- contributo a fondo perduto per le startup con sede nel Centro-Sud Italia

Aliquota/importo
- Finanziamento a tasso zero dell'80% delle spese ammissibili (90% se startup costituita interamente da donne e/o da giovani under 36);
- contributo a fondo perduto del 30%

Note operative
La misura finanzia piani di impresa con spese comprese tra 100mila euro e 1,5 milioni di euro

7

ON - OLTRE NUOVE IMPRESE A TASSO ZERO (INVITALIA)

Normativa
Dm 4 dicembre 2020 (e successive modifiche)

Periodo di applicazione
Dal 2020

Ambiti tecnologici
Adozione di software digitali per la gestione e/o l'organizzazione aziendale e/o per la gestione della logistica; programmi informatici, tecnologie e applicazioni emergenti relativi a AI, blockchain e internet of things

Saas ammissibile
Sì

Dimensioni aziendali
Micro e piccole imprese costituite in forma societaria da non più di 60 mesi in cui i soci sono soggetti di età compresa tra 18 e 35 anni ovvero da donne

Tipo agevolazione
Finanziamento a tasso zero + contributo a fondo perduto

Aliquota/importo
Il mix di agevolazioni può coprire fino al 90% delle spese

Note operative
L'incentivo sostiene progetti fino a 3 milioni di euro

ItaliaOggi Sette

Dopo l'avvio della piattaforma Gse è corsa contro il tempo per l'ammissione alla deduzione

Iperammortamento, imprese in slalom fra termini e requisiti

Pagina a cura
DI BRUNO PAGAMICI

Fattore tempo decisivo per la corsa agli investimenti 2026 agevolabili con l'iperammortamento. Dopo una lunga attesa arriva il disco verde per l'operatività della maxi deduzione fiscale, ma l'apertura del 12 giugno 2026 della piattaforma Gse (disposta dal decreto direttoriale 11 giugno 2026 del ministero delle imprese e del made in Italy) a cui inviare le comunicazioni preventive, rischia di essere tardiva rispetto ai tempi necessari alla completa messa in funzione degli investimenti agevolabili che deve avvenire entro la fine di quest'anno. In altri termini, l'avvio a metà del 2026 dell'iter per beneficiare degli incentivi fiscali del nuovo Piano Transizione 5.0 rischia di complicare la vita alle imprese che puntano a ottenere il riconoscimento della maxi deduzione in sede di dichiarazione dei redditi 2027. Gli impianti a "vocazione energetica" agevolabili, infatti, devono essere consegnati, interconnessi e funzionanti (oltre a essere asseverati con perizie redatte dai tecnici abilitati nonché validati dal Gse) perentoriamente entro il 2026, come stabilito dall'art. 4 del decreto attuativo Mimit/Mef firmato il 7 maggio 2026 dai ministri Adolfo Urso e Giancarlo Giorgetti e reso attuativo dopo il visto della Corte dei conti. I tempi che ci separano dalla fine del 2026 sembrano pertanto insufficienti per portare a compimento gli investimenti tecnicamente più complessi (come sono quelli funzionali alla trasformazione tecnologica e digitale e all'autoproduzione di energia rinnovabile) nel rispetto di tutte le fasi richieste dalla normativa che disciplina l'accesso all'iperammortamento. Essendo il via libera del ministero intervenuto a metà del 2026, e cioè a ridosso del periodo feriale e considerando che per gli impianti tecnicamente complessi, come quelli appartenenti alla categoria energetica, occorreranno mesi per la consegna alle imprese, i tempi a disposizione per quest'anno sembrano essere insufficienti a garantire in sede di dichiarazione dei redditi 2027 i benefici dell'iperammortamento a valere sugli investimenti effettuati nel periodo d'imposta 2026.

Il rischio, pertanto, è che la piena funzionalità degli investimenti richiesta dal decreto 7 maggio 2026 Mimit/Mef ai fini agevolativi possa concretizzarsi non prima del 2027, con il conseguente slittamento dei benefici fiscali della maxi deduzione al 2028.

Non per ultimo va segnalato che nel decreto attuativo Mimit/Mef non rientrano, nonostante le richieste provenienti da più parti, le spese per i software in cloud "as a service" (per i quali si paga un abbonamento periodico) e che nelle ultime fasi della stesura del provvedimento sono state introdotte altre due comunicazioni, questa volta periodiche, ai fini del monitoraggio della spesa pubblica entro il 20 gennaio di ciascun anno (informazioni sugli investimenti effettuati) e entro il successivo 30 giugno (quote di ammortamento). Con apposito decreto verranno individuati i termini per la presentazione delle comunicazioni di conferma (per il pagamento del 20% del costo del bene).

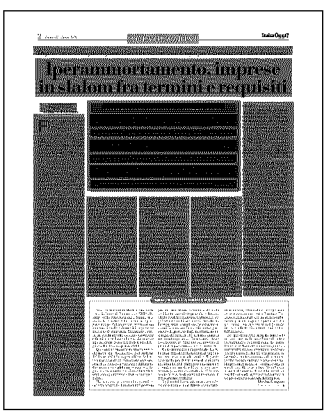
Quando scatta il beneficio. La maggiorazione del costo di acquisizione dei beni rileva, ai fini della determinazione delle imposte sui redditi, a decorrere dal periodo d'imposta nel quale l'impresa trasmette la comunicazione di completamento e il bene oggetto dell'investimento è entrato in funzione. Per l'utilizzo della detrazione occorrerà attendere di ricevere la comunicazione di esito positivo del Gse.

Le 5 comunicazioni. Per avviare la pratica di accesso al beneficio occorre trasmettere al Gse innanzitutto una comunicazione preventiva (dati identificativi, tipologia e l'ammontare degli investimenti previsti nei beni degli allegati IV e V, la data prevista di interconnessione e di entrata in funzione per i beni energetici), poi una comunicazione di conferma (data e importo del pagamento dell'ultima quota dell'acconto del 20% del costo di acquisizione di ciascun bene) che non può riguardare beni diversi o importi superiori rispetto a quelli comunicati nella fase precedente. Infine va trasmessa la comunicazione del completamento degli investimenti e dell'avvenuta interconnessione dei beni (non oltre il 15 novembre 2028). Quanto alla novità delle ulteriori due comunicazioni (periodiche), il decreto Mimit/Mef dispone che entro il 20 gennaio di ciascun anno l'impresa deve trasmette una comunicazione con le informazioni sugli investimenti effettuati, i costi sostenuti e la previsione di utilizzo del beneficio; entro il successivo 30 giugno va inoltre trasmessa una comunicazione integrativa recante il piano di ammortamento con l'indicazione delle quote dell'incentivo imputate in ciascun esercizio.

Gli investimenti agevolabili. La disciplina dell'iperammortamento prevede due categorie di investimenti agevolabili:

- beni strumentali funzionali alla trasformazione tecnologica e digitale delle imprese (di cui agli allegati IV e V alla legge 199/2025, come macchine interconnesse, robot, sistemi di manifattura additiva, software avanzati, ecc.);
- beni materiali finalizzati all'autoproduzione di energia rinnovabile destinata all'autoconsumo, riconducibili alla medesima struttura produttiva ovvero localizzati sulle stesse particelle catastali della struttura produttiva o connessi alla medesima tramite punti di prelievo (Point of delivery, Pod) esistenti come ad esempio i gruppi di generazione dell'energia elettrica e relativi impianti per lo stoccaggio dell'energia, impianti per la produzione di energia termica).

Aliquote e tetti di spesa. Il decreto Mimit/Mef prevede che l'iperammortamento possa essere determinato sulla base delle


Iperammortamento, imprese in slalom fra termini e requisiti

ItaliaOggi Sette

spese agevolabili per gli investimenti (completati in ciascuna annualità) nella misura del 180% per investimenti fino a 2,5 milioni di euro, del 100% per investimenti oltre 2,5 milioni e fino a 10 milioni e nella misura del 50% per investimenti oltre 10 milioni e fino a 20 milioni.

Perizia tecnica asseverata. Le caratteristiche tecniche dei beni nonché il soddisfacimento delle caratteristiche relative ai beni finalizzati all'autoproduzione di energia da fonti rinnovabili per l'autoconsumo, dovranno essere comprovate da perizie rilasciate da un ingegnere o perito industriale dotato di idonee coperture assicurative (dottore agronomo o forestale per il settore agricolo).

È stata eliminata la possibilità di ricorrere all'autodichiarazione per gli investimenti di basso valore.

Perizia contabile. L'effettivo sostenimento delle spese ammissibili all'agevolazione deve risultare da apposita certificazione rilasciata da un revisore contabile (per tali spese non è previsto un rimborso).

Cosa prevede il decreto 7 maggio 2026

Per il riconoscimento della maxi deduzione fiscale in sede di dichiarazione dei redditi 2027 gli impianti devono essere consegnati, interconnessi e funzionanti (oltre a essere asseverati dai tecnici abilitati e validati dal Gse) entro il 2026

La maxi detrazione opera a decorrere dal periodo d'imposta in cui l'impresa trasmette la comunicazione di completamento al Gse e l'investimento è entrato in funzione

Nelle ultime fasi della stesura del decreto sono state introdotte due comunicazioni periodiche da inviare entro il 20 gennaio di ciascun anno (investimenti effettuati) ed entro il successivo 30 giugno (quote di ammortamento)

Nel decreto non rientrano le spese per i software in cloud "as a service" (per i quali si paga un abbonamento periodico)

Entro luglio il Mimit pubblicherà una circolare contenente chiarimenti specifici per l'operatività dell'iperammortamento 2026 e per risolvere i dubbi interpretativi che attengono all'applicazione della normativa

Il Gse ha pubblicato sul proprio sito tutti gli step per compilare e inviare correttamente la prima comunicazione (guida, modelli fac-simile e istruzioni operative)

Quotidiano
15-06-2026
Pagina 14
Foglio 1

Il Sole 24 ORE

PROPOSTA IN PARLAMENTO

Professioni tecniche, pressing per limitare la responsabilità civile

Riequilibrare la responsabilità civile dei professionisti tecnici: ingegneri, architetti, geometri, periti, geologi. Va in questa direzione la proposta di legge, a prima firma Andrea de Bertoldi (Lega), che sarà presentata formalmente domani alla Camera. E che è stata elaborata proprio con il contributo dei Consigli nazionali, a partire da quelli di ingegneri e architetti. Alla presentazione del testo interverranno, tra gli altri, il presidente degli ingegneri, Domenico Perrini, la vicepresidente degli ingegneri, Carla Cappiello e il presidente degli architetti, Alessandro Panci.

«È importante – spiega proprio de Bertoldi, raccontando lo spirito della proposta, che va nella direzione di altri testi già approvati in questi anni da Governo e Parlamento – definire in modo chiaro il perimetro delle responsabilità del progettista o del direttore dei lavori. Non è accettabile che i professionisti paghino anche per le imprese. Questo finisce per complicare il loro lavoro e contribuisce, in prospettiva, a rendere meno attrattive le professioni tecniche per i giovani».

Passando ai dettagli del disegno di legge, questo punta a riesaminare, ad ampio raggio, il tema della responsabilità civile dei professionisti, bilanciando meglio i diversi interessi contrapposti che si confrontano in varie situazioni. Viene, così, chiarito il confine della responsabilità solidale tra professionista e impresa esecutrice, soprattutto nelle attività di progettazione e direzione lavori, di coordinamento della sicurezza e collaudo. Un caso tipo è quello nel quale, a distanza di anni dall'intervento, le aziende che hanno eseguito le opere risultino fallite o cessate e, dunque, il professionista e i suoi eredi rimangano gli unici soggetti aggredibili in caso di richieste di risarcimento danni. La proposta di legge, su questo punto, delimita la responsabilità del professionista e degli eredi alla quota parte della loro condotta colposa accertata.

L'impresa esecutrice, in questo quadro, sarà sempre obbligata a produrre al committente un'idonea polizza assicurativa indennitaria decennale postuma a copertura dei danni derivanti da rovina totale o parziale dell'opera o da gravi difetti costruttivi (cosa che oggi accade soltanto in alcuni casi).

C'è, poi, la questione dell'azione di responsabilità professionale: in base alla proposta avrà una prescrizione di dieci anni dalla conclusione della prestazione, salvo che per dolo. In questo modo, l'obiettivo è evitare situazioni di incertezza a decenni di distanza. Ancora, per quanto riguarda gli eredi del professionista, il provvedimento interviene limitando il loro coinvolgimento solo circa i beni ereditati, salvaguardando il patrimonio personale degli eredi.

Infine, il capitolo delle assicurazioni, legato soprattutto all'obbligo che tutti i professionisti hanno di contrarre una polizza. La proposta, su questo fronte, ribadisce che la copertura deve essere adeguata all'entità delle prestazioni, ma soprattutto deve allungarsi almeno di dieci anni oltre la cessazione dell'attività professionale o il decesso del professionista. In questo quadro, in base alla proposta il danneggiato ha a disposizione un'azione diretta nei confronti della compagnia di assicurazione del professionista, anche se i danni sono accertati successivamente alla morte del professionista.

—**Giuseppe Latour**


Professioni 24

Valutazioni ad hoc e tracciate contro il rischio di riciclaggio

ItaliaOggi Sette

Via alle verifiche sui debiti fiscali per le fatture dei professionisti

Mandolesi e Ricciardo a pag. 5

In vigore dal 15 giugno le nuove disposizioni sui crediti verso la pubblica amministrazione

Compensi nel mirino del Fisco

Check preventivo dei debiti per le fatture dei professionisti

Pagina a cura
DI GIULIANO MANDOLESI
E PINA RICCIARDO

Dal 15 giugno 2026 le prestazioni dei professionisti verso la Pubblica amministrazione (Pa) diventano anche uno strumento rapido di riscossione fiscale.

Prima di liquidare il compenso ai professionisti, infatti, le amministrazioni pubbliche e le società a totale partecipazione pubblica dovranno verificare la posizione debitoria dello stesso e, in presenza di eventuali cartelle esattoriali non pagate, per un importo complessivo almeno pari a i 5.000 euro, saranno tenute a versare il dovuto al fornitore professionista direttamente all'Agente della riscossione fino a concorrenza del debito risultate dalla verifica e solo l'eventuale eccedenza al beneficiario.

Per gli altri soggetti che vantano crediti nei confronti dalla Pa il meccanismo è meno penalizzante rispetto a quello di nuova introduzione e strutturato ad hoc per i professionisti poiché - in presenza di pagamenti dovuti superiori a 5000 euro - la Pa deve effettuare la verifica presso il riscossore e in presenza di debiti rilevati over 5000 euro scatta solo una sospensione del pagamento.

Tale sospensione, non concessa ai professionisti che invece subiscono direttamente il "giroconto" della somma all'Agenzia delle entrate Riscossione, consente ai creditori di verificare la propria posizione debitoria, di regolarizzarla anche attraverso dilazioni e di ricevere quindi successivamente a tali attività il saldo del pagamento del dovuto dalla Pa.

Questi sono gli effetti generati dalla nuova normativa introdotta dalla legge di bilancio 2026 (all'articolo 1 comma 725 della legge 199/2025) che ha modificato l'articolo 48-bis del dpr 602/1973.

Cosa cambia dal 15 giugno. La nuova disciplina, come anticipato, è contenuta nell'articolo 48-bis, comma 1-ter, del dpr 602/1973, introdotto dall'articolo 1, comma 725, della legge 30 dicembre 2025, n. 199 e successivamente modificato dall'articolo 2-ter del dl 27 marzo 2026, n. 38.

Va preliminarmente ricordato che l'articolo 48-bis al comma 1 prevede un meccanismo di tutela per l'erario qualora un contribuente, con debiti scaduti nelle mani del riscossore, debba ricevere un pagamento per una prestazione effettuata verso la pubblica amministrazione.

Secondo quanto stabilito al comma 1, infatti, le società a prevalente partecipazione pubblica, prima di effettuare, a qualunque titolo, il pagamento di un importo superiore a cinquemila euro, verificano, anche in via telematica, se il beneficiario è inadempiente all'obbligo di versamento derivante dalla notifica di una o più cartelle di pagamento per un ammontare complessivo pari almeno a tale importo e, in caso affermativo, non procedono al pagamento e segnalano la circostanza all'agente della riscossione competente per territorio, ai fini dell'esercizio dell'attività di riscossione delle somme iscritte a ruolo.

La disposizione di fatto quindi prevede una sorta di "sospensione" del saldo, momento che dà la possibilità al beneficiario del pagamento di regolarizzare la propria posizione debitoria attivando eventualmente dilazioni presso il riscossore e di ricevere poi integralmente il dovuto da parte della Pa che può riverificare la posizione debitoria e "liberare" la somma dovuta al fornitore.

La legge di bilancio 2026 ha, come detto, modificato questa disciplina prevedendo un meccanismo specifico per le somme di cui all'articolo 54 del dpr 917/1986 dovute dalla Pa gli esercenti arti e professioni per l'attività professionale dai medesimi svolta.

Il meccanismo, che si applica a decorrere dal 15 giugno 2026, è simile a quello "ordinario" ex comma 1 ma più rigoroso e penalizzante poiché prevede il pagamento diretto delle somme al riscossore senza il momento di sospensione qualora si riscontri il parametro dei debiti scaduti ed indipendentemente dal valore della prestazione se sopra o sotto i 5000 euro.

Nello specifico, il comma 1-ter prevede infatti che per somme dovute dalla Pa ai professionisti scatta l'obbligo di verifica indipendentemente dal valore della prestazione (anche se riferite al pagamento di importo entro i 5.000 euro) e, qualora si rilevino poi debiti scaduti riferiti a una o più cartelle per un valore complessivo almeno pari a 5000 euro viene soddisfatto preventivamente il riscossore fino a concorrenza del debito risultante dalla verifica e solo successivamente il beneficiario nei limiti delle somme eventualmente eccedenti l'ammontare del predetto debito.

ItaliaOggi Sette

La circolare del Ministero della Giustizia del 17 marzo 2026, avente ad oggetto proprio le nuove disposizioni in materia di verifica della regolarità fiscale e contributiva nei pagamenti effettuati dalla Pa in favore di esercenti arti e professioni, ha chiarito che la nuova disciplina opera secondo il criterio di cassa.

Nel documento viene infatti riportato che la disposizione si applica a tutti i pagamenti, di qualsiasi importo, da effettuare a decorrere dal 15 giugno 2026, indipendentemente dalla data di acquisizione dei documenti contabili o dalla riferibilità delle prestazioni professionali a periodi precedenti.

Pertanto, continua la circolare, anche i compensi relativi a prestazioni professionali pregresse, ove liquidati successivamente a tale data, sono soggetti alla nuova disciplina.

Rientrano nel perimetro della disposizione, citati come esempio nel documento del Ministero della Giustizia, anche gli avvocati in regime di patrocinio a spese dello Stato in sede processuale o nei procedimenti di mediazione e negoziazione assistita, ausiliari del giudice e periti di parte, professionisti incaricati in ambito civile, penale, amministrativo e tributario, nonché ogni altro soggetto rientrante nella nozione di esercente arti e professioni ai sensi dell'art. 54 del Testo unico delle imposte sui redditi (Tuir).

La disciplina dei lavoratori dipendenti. Una disciplina specifica è prevista anche per i lavoratori dipendenti. L'articolo 48-bis, comma 1-bis, del dpr 602/1973 estende infatti il controllo alle somme dovute a titolo di stipendio, salario e altre indennità relative al rapporto di lavoro o di impiego, comprese quelle corrisposte in occasione della cessazione del rapporto, quando il pagamento supera 2.500 euro.

Anche in questi casi la verifica riguarda l'eventuale presenza di cartelle di pagamento non saldate per un ammontare complessivo almeno pari a 5.000 euro. Continua tuttavia a trovare applicazione il meccanismo previsto dal comma 1 della stessa disposizione, fondato sulla sospensione del pagamento e sulla segnalazione all'Agente della riscossione. Diversamente, per i professionisti la verifica preventiva deve essere effettuata indipendentemente dall'importo del pagamento, con la conseguenza che anche compensi di modesto ammontare rientrano nell'ambito del controllo. Proprio questa differenza rispetto alla disciplina applicabile agli altri creditori della Pa ha alimentato le principali osservazioni formulate dalle categorie professionali.

Le questioni ancora aperte. Restano alcuni aspetti applicativi da chiarire. Uno dei principali riguarda i contribuenti in regime forfettario. Il nuovo comma 1-ter richiama espressamente le somme di cui all'articolo 54 del Tuir corrisposte agli esercenti arti e professioni e, il dubbio interpretativo, nasce dal fatto che i contribuenti che applicano il regime forfettario determinano infatti il proprio reddito secondo le regole speciali contenute nei commi 54 e seguenti dell'articolo 1 della legge n. 190/2014 e non secondo le disposizioni ordinarie dell'articolo 54 del Tuir. Questa circostanza ha portato parte della dottrina a ipotizzarne l'esclusione dall'ambito applicativo della nuova disciplina. Sul punto mancano indicazioni ufficiali.

Dubbi analoghi riguardano le Società tra professionisti (Stp) e le Società tra avvocati (Sta), che secondo una prima interpretazione continuerebbero a rientrare nella disciplina ordinaria prevista per gli altri creditori della Pubblica amministrazione, con verifica limitata ai pagamenti superiori a 5.000 euro.

Sul piano operativo restano da definire le procedure informatiche e le modalità attraverso le quali le amministrazioni dovranno effettuare il versamento diretto delle somme all'Agente della riscossione. Occorrerà inoltre chiarire le modalità di gestione dei casi in cui il debito iscritto a ruolo risulti inferiore al compenso da liquidare o sia nel frattempo oggetto di definizione agevolata.

Permangono infine interrogativi sulla tutela del contribuente nei casi in cui il debito sia oggetto di contestazione, rateizzazione o contenzioso ancora pendente.

I controlli sui pagamenti della Pa a confronto

Categoria	Quando scatta il controllo	Effetti della verifica
Imprese e fornitori	Pagamenti superiori a € 5.000	In presenza di cartelle scadute pari almeno a € 5.000 il pagamento viene sospeso e la situazione segnalata all'Agente della riscossione
Lavoratori dipendenti	Stipendi, salari, indennità e somme dovute alla cessazione del rapporto superiori a € 2.500	Si applica il meccanismo della sospensione del pagamento previsto dal comma 1 dell'art. 48-bis
Professionisti	Qualsiasi importo del compenso professionale	Verifica obbligatoria su ogni fattura. Se emergono debiti iscritti a ruolo pari almeno a € 5.000, le somme sono versate direttamente all'Agente della riscossione fino a concorrenza del debito
Avvocati in patrocinio a spese dello Stato, periti e ausiliari del giudice	Qualsiasi importo del compenso	Rientrano espressamente nell'ambito applicativo della nuova disciplina
Forfettari	Ambito applicativo incerto	Parte della dottrina ne ipotizza l'esclusione per il richiamo all'art. 54 Tuir; mancano chiarimenti ufficiali
Stp e Sta	Da chiarire	Secondo una prima interpretazione continuerebbero ad applicare la disciplina ordinaria prevista per gli altri creditori della Pa

ItaliaOggi Sette

Ora non c'è più scusa che tenga

DI MARINO LONGONI

L'attacco informatico non è più un incidente tecnico: è un fallimento di governance. È questo il punto che le imprese italiane farebbero bene a mettere in agenda subito, prima che a ricordarglielo siano un pubblico ministero, l'Agenzia per la cybersicurezza nazionale o un tribunale civile.

Il documento pubblicato dal Consiglio nazionale dei commercialisti sulla "Cybersecurity e Modello 231" segnala un passaggio importante, che cioè la sicurezza digitale è entrata ufficialmente nel cuore delle responsabilità degli amministratori e degli organi di controllo. Quindi, se l'azienda subisce un ransomware, una fuga di dati o una frode informatica, non basterà più dire "ci hanno hackerato". Ora qualcuno chiederà se sono stati predisposti adeguati assetti organizzativi per prevenire e gestire quel rischio.

continua a pag. 2

Marino Longoni

SEGUE DALLA PRIMA PAGINA

Negli ultimi anni infatti le norme europee e italiane, dalla direttiva NIS2 alla legge sulla cybersicurezza, hanno trasformato il rischio cyber in un obbligo di governance. Gli amministratori devono valutare i rischi informatici, approvare politiche di sicurezza, finanziare i controlli, verificare che esistano procedure efficaci e che l'azienda sappia reagire agli incidenti. Non è più materia da delegare soltanto al responsabile IT.

Qui entra in gioco il concetto chiave richiamato dal documento. Nel sistema del decreto 231, la responsabilità dell'ente nasce quando un reato viene commesso nell'interesse o a vantaggio dell'azienda e manca un modello organizzativo adeguato a prevenirlo. E i reati informatici, oggi, sono pienamente dentro quel perimetro.

Ma la novità più scomoda riguarda il collegio sindacale. I sindaci non possono più limitarsi al controllo contabile o alla verifica formale delle procedure. Devono vigilare sull'adeguatezza degli assetti organizzativi anche sotto il profilo della cybersicurezza: controllare che esistano sistemi di sicurezza, flussi informativi, procedure di gestione degli incidenti, monitoraggi dei fornitori tecnologici, piani di continuità operativa. In sostanza, devono chiedersi se l'impresa sia davvero in grado di reggere un attacco informatico.

È un cambio di ruolo profondo. La cybersicurezza diventa materia di vigilanza societaria, non solo tecnica. E questo vale anche per l'Organismo di vigilanza del Modello 231, chiamato a monitorare in modo continuo i rischi cyber, aggiornare la mappa delle vulnerabilità e verificare che le misure di prevenzione siano effettivamente applicate.

Oggi infatti il vero patrimonio aziendale non sono solo i macchinari o il magazzino, ma i dati, il know-how, la reputazione, le relazioni con clienti e fornitori. Tutti asset immateriali che un attacco informatico può distruggere in poche ore. Magari senza lasciare tracce nel bilancio, ma con effetti devastanti sul valore dell'impresa.

Per questo la cybersecurity non è solo un costo, ma anche una forma di tutela patrimoniale e reputazionale. Le aziende che la trattano come un adempimento burocratico stanno leggendo il problema con dieci anni di ritardo. Gli attacchi informatici continueranno ad accadere, perché nessun sistema è invulnerabile. Ma per amministratori, sindaci e organismi di controllo la vera linea di confine sarà poter dimostrare di aver fatto tutto il possibile, in modo organizzato, documentato e proporzionato ai rischi dell'impresa.


CIÙ CIÙ
ItaliaOggi
CIÙ CIÙ
Priorità cybersicurezza


Iperammortamento, imprese in slalom fra termini e requisiti

Settimanale
15-06-2026
Pagina 1+7
Foglio 1 / 2

ItaliaOggi Sette

Priorità cybersicurezza

In caso di attacchi informatici la mancata previsione di misure adeguate espone amministratori e sindaci al rischio di risarcire personalmente i danni. E al penale

Se l'omessa valutazione dei rischi cyber e la mancata previsione di misure adeguate favoriscono illeciti da parte di terzi (frodi informatiche, danneggiamento dati, ecc.), gli amministratori delle società possono essere chiamati a rispondere personalmente per i danni causati all'azienda, ai soci o ai creditori, in casi gravi anche in sede penale. E per i sindaci la mancata segnalazione di carenze critiche può configurare una responsabilità civile per culpa in vigilando.

Pagamici a pag. 7 e nell'inserto da pag.33

Nel documento Cndcec-Fnc le linee guida sulle responsabilità nell'ambito della governance

Cyber risk, vigilanza d'obbligo

Amministratori e sindaci rispondono degli eventuali danni

Pagina a cura
DI BRUNO PAGAMICI

Se l'omessa valutazione dei rischi cyber e la mancata previsione di misure adeguate consentono di favorire illeciti da parte di terzi (frodi informatiche, danneggiamento dati, ecc.), gli amministratori delle società possono essere chiamati a rispondere personalmente per i danni causati all'azienda, ai soci o ai creditori, in casi gravi anche in sede penale. E per i sindaci la mancata segnalazione di carenze critiche nei sistemi di sicurezza informatica può configurare una responsabilità civile per culpa in vigilando.

Sono queste alcune delle conseguenze in termini di responsabilità a carico dei vertici aziendali che anche il Consiglio nazionale dei dottori commercialisti e degli esperti contabili (Cndcec) ha messo in evidenza nel documento "Cybersecurity e Modello 231: integrazione dei rischi informatici nella governance dell'impresa" pubblicato a maggio 2026 in collaborazione con la Fondazione nazionale commercialisti (Fnc), che rappresenta una guida operativa per i professionisti che svolgono l'attività di vigilanza (si veda inserto da pag. 35).

Ciò in quanto la sicurezza informatica attualmente non è un mero adempimento aggiuntivo, ma una componente strutturale della governance d'impresa.

Lo studio analizza le intersezioni tra la sicurezza IT (la pratica che consiste nel proteggere sistemi informatici, reti, dispositivi digitali, e dati di un'organizzazione da accessi non autorizzati, violazione dei dati, attacchi informatici e altre attività dannose) e la responsabilità amministrativa ex dlgs 231/2001.

In pratica, gli amministratori sono tenuti a integrare la gestione del rischio cyber all'interno dei sistemi di controllo Mogc (Modello di organizzazione, gestione e controllo ex dlgs 231/2001) trattando la sicurezza informatica non più solo come tema tecnico, ma come pilastro fondamentale della conformità aziendale per prevenire i reati informatici.

In altri termini, sul piano della sicurezza informatica gli amministratori hanno un ruolo strategico e di garanzia e devono valutare l'impatto sul sistema aziendale delle nuove tecnologie e dell'intelligenza artificiale, sia come strumento di difesa che come vettore di nuove minacce.

Pertanto omissioni o inadeguatezze nella predisposizione dei sistemi organizzativi potrebbero esporre gli amministratori a diretti profili di responsabilità civile e penale (c.d. "colpa di organizzazione").

Sul piano dei controlli circa l'adeguatezza dell'assetto organizzativo e amministrativo, nelle Pmi tale funzione può essere svolta dai sindaci che possono assumere in toto le funzioni dell'Organo di vigilanza (Odv) e che rischiano di incorrere in responsabilità per omessa o insufficiente vigilanza se non hanno verificato la presenza, l'adeguatezza e l'aggiornamento dei protocolli di sicurezza informatica dell'impresa.

In pratica l'Odv, o il Collegio sindacale, deve assicurare che il Mogc – anche attraverso l'importante ruolo dell'attività di formazione del personale – contenga procedure e protocolli specifici per prevenire reati informatici e violazioni. Inoltre, a fronte di attacchi, nuovi standard tecnologici (inclusa l'IA) o modifiche normative l'Organo deve sollecitare l'aggiornamento del Modello e dei protocolli decisionali, nonché verificare che la gestione della cybersecurity sia coordinata con gli altri sistemi di compliance (es. privacy, normative antiriciclaggio) evitando sovrapposizioni e lacune.

L'Odv, o il Collegio, inoltre, deve assicurarsi che l'ente metta a disposizione un budget per acquisire competenze specialistiche nel caso in cui non disponga al suo interno delle conoscenze tecniche necessarie per valutare i rischi cyber e deve verificare che l'azienda adotti misure di risk assessment aggiornate affinché vengano segnalati tempestivamente eventuali incidenti di sicurezza o falle.

Modello 231 e cybersecurity. Da quanto emerge dallo Studio di Cndcec e Fnc, la progressiva digitalizzazione dell'economia e l'utilizzo dell'IA hanno reso la sicurezza informatica una variabile strategica della vita d'impresa non più confinabile al perimetro della gestione tecnica dei sistemi IT. Le minacce cyber colpiscono oggi con effetti dirompenti la continuità operativa, il patrimonio informativo, la reputazione e la solidità patrimoniale delle organizzazioni, indipendentemente dalla loro dimensione o dal settore di appartenenza.

Il dlgs 231/2001 (concepito come strumento di contrasto alla criminalità economica d'impresa) rivela una particolare attitudine a governare anche il rischio informatico, grazie alla sua architettura fondata sulla "prevenzione mediante organizzazione" e sulla logica del risk assessment strutturato. L'intersezione tra il Mogc e la cybersecurity si sviluppa lungo tre direttrici fondamentali: la gestione del rischio informatico come componente organica del Modello 231; l'analisi dei rischi e la mappatura delle aree sensibili; il ruolo del Codice etico e dei protocolli specifici quale presidio comportamentale e procedurale. Il tutto delinea un sistema integrato di compliance in cui la si-

ItaliaOggi Sette

curezza informatica non è un adempimento aggiuntivo, ma una componente strutturale della governance d'impresa.

Adeguati assetti e prevenzione. Sotto il profilo operativo, l'integrazione del rischio informatico nel Modello 231 richiede che l'ente adotti un risk approach strutturato collocabile nel più ampio contesto degli adeguati assetti organizzativi, amministrativi e contabili (Oac) ex artt. 2381, 2403 e 2086, 2° comma c.c.; tali riferimenti hanno visto assurgere le best practices aziendali al rango di norme di legge (trend a cui è ormai indirizzato tutto il diritto d'impresa).

Secondo lo studio di Cndcec e Fnc, la logica degli adeguati assetti e del sistema 231 condividono un medesimo fondamento e cioè la prevenzione mediante organizzazione. Di conseguenza il Mogc è ormai sistematicamente ascritto nel novero dei fattori che qualificano l'adeguatezza degli assetti, fermo restando il principio di proporzionalità secondo la natura e la dimensione dell'impresa. Gli Oac costituiscono l'infrastruttura attraverso cui l'impresa individua, valuta e governa i rischi rilevanti, inclusi quelli penalmente, economicamente e reputazionalmente significativi.

Il risk approach, inteso come metodo ordinatore della gestione, trova nel principio di corretta amministrazione e nei relativi assetti Oac la propria concreta attuazione e comprende a titolo esemplificativo la mappatura dei processi, l'identificazione delle aree sensibili, le gap analysis, la tracciabilità delle decisioni, i flussi informativi strutturati e sistemi di controllo interno. L'obiettivo è determinare quali vulnerabilità siano accettabili, quali richiedano un intervento immediato e quali possano essere gestite mediante meccanismi di trasferimento del rischio, come polizze cyber liability o contratti di outsourcing con Service level agreement (Sla) adeguati. Il Modello deve essere aggiornato periodicamente in relazione all'evoluzione dell'attività e del contesto normativo, requisito che in ambito cyber si traduce nell'obbligo di riesaminare la mappa dei rischi informatici almeno annualmente.

I flussi informativi verso l'Odv. In coerenza con le Linee Guida Cndcec del novembre 2025, l'Odv deve ricevere informazioni adeguate, tempestive e strutturate che gli consentano di esercitare la propria funzione di vigilanza sull'effettività del Modello 231 anche con riferimento ai presidi di cybersicurezza.

L'Odv deve ricevere con cadenza periodica:

- il "piano formativo annuale" in materia di cybersicurezza, con indicazione dei contenuti, dei destinatari, delle modalità di erogazione e del calendario;
- il "report di partecipazione e completamento", con evidenza dei tassi di adesione, dei test superati/non superati, delle eventuali criticità;
- i "risultati delle simulazioni di phlshing", disaggregati per funzione aziendale e con indicazione delle azioni correttive intraprese;
- le "variazioni al piano formativo", con la motivazione delle modifiche apportate.

L'Odv deve essere tempestivamente informato in caso di:

- "incidenti di sicurezza informatica" di qualsiasi natura;
- "data breach" ai sensi del Gdpr con indicazione dell'impatto e delle comunicazioni effettuate al Garante privacy e agli interessati;
- "esiti negativi delle simulazioni di phishing";
- "segnalazioni whistleblowing" riconducibili a condotte in ambito informatico;
- "modifiche normative" o "provvedimenti delle autorità competenti" (Garante privacy, Anac, ecc.) che incidano sugli obblighi formativi dell'ente.

Odv e formazione. L'Odv inserisce nel proprio piano di vigilanza verifiche specifiche in materia di formazione sulla cybersicurezza, volte ad accertare: l'effettiva erogazione della formazione secondo il piano approvato; la completezza e l'aggiornamento dei contenuti formativi; il rispetto delle periodicità previste; la coerenza tra i risultati della formazione e la politica di gestione del rischio cyber dell'ente; l'adozione di misure correttive a fronte di criticità emerse dalle simulazioni, dagli incidenti o dagli audit; l'adeguatezza dei flussi informativi ricevuti.

La Cybersecurity nella governance d'impresa

Il rischio cyber come reato 231	Gli attacchi informatici (furto dati, frodi) non sono più solo problemi tecnici, ma possono configurare reati che fanno scattare la responsabilità amministrativa dell'impresa
Valutazione e adeguatezza	Il Cda deve verificare che l'organizzazione adotti presidi, procedure, risorse e responsabilità interne idonee a prevenire e gestire i rischi informatici (art. 2086 c.c.)
Aggiornamento del Mod. 231	Il Cda deve aggiornare costantemente il Mogc inserendo i reati informatici (art. 24-bis, dlgs 231/2001) e i rischi connessi alle nuove tecnologie come l'IA
Gestione incidenti	Il Cda deve assicurare la capacità di reazione aziendale agli attacchi e agli incidenti cyber per tutelare il patrimonio informativo e garantire la continuità operativa
Supervisione e aggiornamento	L'Odv o il Collegio sindacale non gestisce la sicurezza in prima persona ma deve accertarsi che il Mod. 231 preveda protocolli adeguati contro accessi abusivi, danneggiamenti, frodi, ecc.
Valutazione rischi emergenti	Odv o Collegio deve monitorare l'impatto di nuove tecnologie inclusa l'Ia sui sistemi aziendali e sulla tenuta del Mod. 231

Quotidiano
15-06-2026
Pagina 34
Foglio 1

CORRIERE DELLA SERA

DATA CENTER: IL VERO PROBLEMA NON È L'ENERGIA, MA I DETRITI

IL RISCHIO DELLA DISCARICA SPAZIALE

di **Roberto Battiston**

Quando Elon Musk parla di data center orbitali, vuole portare i computer nello spazio, alimentarli con il Sole, liberare la Terra da consumo di energia e acqua. Al di là del fatto che l'energia solare sulla terra è abbondante, il 2% del Sahara potrebbe sopperire a tutta l'energia elettrica del mondo, prima di chiederci se funzioneranno i server, dobbiamo chiederci se reggerà l'orbita. Nei documenti depositati alla FCC si parla addirittura di un sistema fino a un milione di satelliti per data center nello spazio. Per capire l'ordine di grandezza del rischio, basta però fermarsi a un caso molto più prudente: 80 mila satelliti, una scala comparabile alla richiesta di Starcloud da 88 mila satelliti, circa otto volte il numero di satelliti attualmente operativi. Anche così, i numeri diventano enormi.

Il rischio va diviso in tre categorie.

La prima riguarda i satelliti della costellazione. Finché sono operativi, comunicano e manovrano, non sono detriti. Ma se si guastano diventano oggetti passivi lanciati a 7-8 chilometri al secondo. In una flotta di 80 mila satelliti, anche l'1% di fallimenti significa 800 corpi morti in orbita. Un modello per satelliti con grandi radiatori, circa 120 metri quadrati ciascuno, dà circa 1.900 collisioni «naturali» l'anno in assenza di controllo attivo. Non significa che avverranno tutte: significa che il sistema di guida deve evitarle quasi tutte. Se sbagliasse un caso su mille, resterebbero quasi due collisioni catastrofiche l'anno; uno su diecimila vorrebbe dire circa una ogni cinque anni.

La seconda categoria è lo scontro con detriti tracciabili: vecchi satelliti, stadi di razzi, frammenti abbastanza grandi da essere visti da radar e telescopi. In teoria si evitano. In pratica una costellazione da 80 mila satelliti genererebbe fra 0,7 e 3,1 milioni di avvisi di congiunzione all'anno nella fascia 400-800 chilometri di altezza, con un picco intorno a 500-550 chilometri. Anche a 800 chilometri si parla di circa un milione di eventi da analizzare ogni anno. Non sono «un milione di incidenti», ma sono un milione di decisioni: manovrare o no, consumare propellente o no, fidarsi dei dati o no. Intensissimo traffico spaziale senza un vero codice della strada.

La terza categoria è la più seria: i detriti non tracciabili. Sono frammenti da millimetri a pochi centimetri. Non li vediamo in tempo e non possiamo evitarli. Eppure un centimetro, a 10 chilometri al secondo, può distruggere un componente critico. Con 80 mila satelliti e 120 metri quadrati esposti ciascuno, l'area bersaglio totale è 9,6 milioni di metri quadrati. Le stime danno, a 500 chilometri, 120-300 impatti l'anno da oggetti sopra il centimetro considerando tutta l'area come vulnerabile; a 800 chilometri si sale a 1.200-3.000 l'anno. I frammenti millimetrici sono molti di più: non sempre uccidono un satellite, ma bucano, degradano, riducono la vita utile.

Il punto è politico. Lo spazio vicino alla Terra non è vuoto: è un'infrastruttura comune. ESA stima circa 1,2 milioni di oggetti tra 1 e 10 centimetri e oltre cento milioni tra 1 millimetro e 1 centimetro. Sopra certe quote, soprattutto tra 700 e 900 chilometri, i rottami possono restare per decenni o secoli. Ogni collisione produce nuovi frammenti, cioè nuove probabilità di collisione: è la sindrome di Kessler.

La domanda da porre a Musk, e a chiunque voglia industrializzare l'orbita, non è solo «sapete lanciare questi satelliti?». È invece: «sapete anche pulire dai rifiuti?». Servono obblighi di rientro rapido, tracciamento indipendente, responsabilità economica per i satelliti morti e fondi per rimuovere i detriti già presenti. Altrimenti costruire data center nello spazio significa usare una risorsa comune come una discarica ad alta velocità. E il conto, prima o poi, lo pagheranno tutti.


L'ULTIMO SALOTTO DELL'OCCIDENTE
IL RISCHIO DELLA DISCARICA SPAZIALE