

Rassegna Stampa

di Lunedì 5 ottobre 2026



Centro Studi C.N.I.

Sommario Rassegna Stampa

Pagina	Testata	Data	Titolo	Pag.
Rubrica Professionisti				
10	Il Sole 24 Ore	05/10/2026	Il temporary manager entra nello studio legale (M.Carbonaro)	3
Rubrica Intelligenza Artificiale				
1+10	Il Sole 24 Ore	05/10/2026	AI, sull'alto rischio rinviati gli obblighi ma debutta il reato (G.Vaciago)	4
Rubrica Cybersecurity				
22	Italia Oggi Sette	05/10/2026	Le frodi cyber si affinano con l'IA (T.Cerne)	6



PANORAMA

TREND & BUSINESS

Il temporary manager entra nello studio legale



Lo studio Fazzini Holzmilller & Partners lancia il nuovo servizio alle imprese

Il temporary manager entra nello studio legale, per offrire un nuovo modello di assistenza alle imprese che mette in campo un mix di consulenza e attività operative. È con questo obiettivo che lo studio Fazzini Holzmilller & Partners lancia un servizio di Temporary management, affidandolo a Sergio Arcuri, che fa il suo ingresso nella firm come of counsel.

Il temporary manager non opererà da solo ma supportato da una realtà già specializzata nella consulenza alle imprese, a partire dalle Pmi, e lavorerà in team con i professionisti fiscali, legali ed esperti di M&A dello studio.

Nello spiegare l'ingresso di Arcuri, commercialista con esperienza di management e consulenza in istituzioni pubbliche e in aziende dei settori telecomunicazioni, energia e servizi, i partner Marco Fazzini ed Enrico Holzmilller hanno spiegato: «Nel nostro lavoro al fianco delle imprese abbiamo registrato l'esigenza di avere questo tipo di supporto in momenti specifici. Vogliamo espandere i servizi offerti dalla nostra firm, nella certezza della loro qualità».

Una strategia, quella di FHP che conferma quanto il servizio di temporary management sia in crescita in Italia. Secondo il rapporto sugli interim manager realizzato da Inima, l'associazione italiana dei temporary manager, insieme con Leading network, sono soprattutto le media imprese a rappresentare il core market di questo tipo di attività, intercettando il 55-60% degli incarichi complessivi in Italia. Nelle imprese sopra i 15-20 milioni di euro di fatturato si registra la crescita maggiore di progetti legati alla ristrutturazione delle filiere produttive e all'integrazione delle tecnologie Ai nei processi industriali. Dall'ultima indagine emerge che si sta diffondendo la modalità fractional del servizio: viene richiesto per uno o due giorni alla settimana e i professionisti gestiscono più incarichi in contemporanea, agendo su un portfolio di progetti.

— **Massimiliano Carbonaro**

© RIPRODUZIONE RISERVATA





PROFESSIONI

AI, sull'alto rischio rinviati gli obblighi ma debutta il reato

Il regolamento Digital omnibus ha rinviato alcune novità per i sistemi ad alto rischio ma occorre organizzare il percorso di adeguamento. Intanto, il decreto legislativo 160/2026 ha fatto entrare l'AI nel Codice penale.

Giuseppe Vaciago — a pag. 10

AI e imprese: rinviati gli obblighi sull'alto rischio, ma parte il reato

Compliance. Nei piani di adeguamento va considerato che il Digital omnibus Ue ha spostato solo alcune novità e con il decreto 160/2026 l'intelligenza artificiale entra nel Codice penale e nella «231»

Giuseppe Vaciago

«Hanno rinviato tutto, ne riparlano l'anno prossimo». È la frase con cui, in queste settimane, molte imprese stanno rimettendo nel cassetto i progetti di adeguamento all'AI Act. Poggia su un fatto vero e su una lettura sbagliata, che è bene che i professionisti che le assistono spieghino chiaramente.

Il regolamento Ue 2026/1744, l'omnibus digitale sull'AI in vigore dal 27 luglio, ha effettivamente spostato il debutto di alcune novità inizialmente previste per il 2 agosto di quest'anno. Nel dettaglio: al 2 dicembre 2027 gli obblighi sui sistemi ad alto rischio dell'Allegato III e al 2 agosto 2028 quelli sui sistemi integrati in prodotti già regolati. Ma dal 2 agosto scorso sono già applicabili gli obblighi di trasparenza previsti dall'articolo 50, la cui violazione è punita con sanzioni fino a 15 milioni di euro o al 3% del fatturato mondiale annuo. E dal 30 settembre in Italia è entrato in vigore il decreto legislativo 160/2026, che ha portato l'intelligenza artificiale nel Codice penale, nel catalogo dei reati 231 e nelle regole sul risarcimento del danno.

Il rinvio ha spostato la data della verifica, non il lavoro che la precede, né le responsabilità.

Cosa è slittato e cosa no

Il differimento riguarda gli adempimenti sull'alto rischio – gestione dei rischi, documentazione tecnica, valutazione di conformità – che nella maggior parte delle imprese toccano pochi sistemi, in alcuni casi nessuno. Restano in piedi, invece, le regole che riguardano quasi tutti: i divieti in vigore dal febbraio 2025 e la trasparenza, cioè avvisare chi dialoga con un chatbot che sta parlando con una macchina, dichiarare i deepfake, marcare i contenuti sintetici. Il 2 dicembre, poi, finisce il periodo transitorio per la marcatura dei contenuti dei sistemi generativi già sul mercato e scattano due nuovi divieti, sulle immagini intime non consensuali e sul materiale pedopornografico generati con l'AI.

Il tassello nazionale

Mentre il calendario europeo rallenta, quello italiano accelera. Il decreto legislativo 160/2026, attuativo della legge 132/2025, introduce l'articolo 437-bis del Codice penale: reclusione da uno a cinque anni per chi omette le misure tecniche di sicurezza previste per i sistemi ad alto rischio e per l'utilizzatore professionale che rinuncia

intenzionalmente alla sorveglianza umana, se ne deriva un pericolo per la vita o l'incolumità delle persone. Il reato entra nel catalogo 231 con il nuovo articolo 25-vicies – sanzioni fino a mille quote, oltre 1,5 milioni di euro, e sanzioni interdittive – insieme alla diffusione illecita di deepfake introdotta dalla legge 132/2025.

Sul piano civile, il danneggiato può ottenere l'esibizione di log e documentazione tecnica; se il danno deriva dalla violazione di un obbligo dell'AI Act il nesso causale si presume, salvo prova contraria; la conformità, anche certificata, non esclude di per sé la responsabilità; e l'azione può essere rivolta direttamente all'assicuratore.

Come le nuove fattispecie si coordinano con obblighi europei esigibili solo dal dicembre 2027 è il primo nodo interpretativo. Alcune conseguenze, però, sono già chiare: la presunzione può operare sugli obblighi in vigore, come la trasparenza; il deepfake illecito è da subito un rischio 231; e la qualificazione di un sistema di intelligenza artificiale come ad alto rischio non è più una questione solo documentale, perché delimita il perimetro di un reato.

Il paradosso del rinvio

Per questo l'inventario resta il collo di bottiglia. Il rinvio concede 16 mesi in



più sul risultato e zero mesi in meno sul lavoro che lo precede: censire i casi d'uso, capire chi li governa, classificarli e motivare la classificazione richiede lo stesso tempo nel 2026 e nel 2027. Se per costruire controlli, documentazione e presidi contrattuali servono due o tre trimestri, la classificazione va chiusa entro la primavera del 2027; e poiché anche l'inventario richiede mesi, deve partire adesso. Nemmeno la constatazione più frequente, vale a dire quella per cui «non abbiamo sistemi ad alto rischio», chiude la partita: l'esclusione va motivata e documentata, tanto che il regolamento "Digital omnibus" ha mantenuto, in forma semplificata, la registrazione nella banca dati europea per i fornitori che si avvalgono della deroga.

L'alfabetizzazione

Il regolamento "Digital omnibus" ha riscritto anche l'articolo 4, applicabile dal febbraio 2025: fornitori e utilizzatori non devono più garantire «nella misura del possibile un livello sufficiente» di alfabetizzazione, ma adottare misure che ne sostengano lo sviluppo. È un obbligo di mezzi, che però si giudica dalla qualità dei mezzi: il corso una tantum, uguale per tutti e senza traccia, è la risposta più esposta alla contestazione di formalismo. Servono percorsi calibrati per ruolo e per rischio, aggiornati e documentati. Con le nuove regole sulla prova, la formazione tracciata è anche la prima dimostrazione di diligenza.

Chi deve muoversi per primo

Tre situazioni meritano attenzione prima delle altre:

- le imprese che usano chatbot e assistenti virtuali nel rapporto con il pubblico, soggette alla trasparenza già da agosto;
- quelle che si affidano a fornitori extra-Ue su condizioni standard, spesso prive di clausole su documentazione, log e uso dei dati: sono proprio i documenti che il giudice potrà ordinare di esibire;
- gli enti dotati di un modello 231, chiamati ad aggiornare la mappatura dei rischi al nuovo articolo 25-vicies.

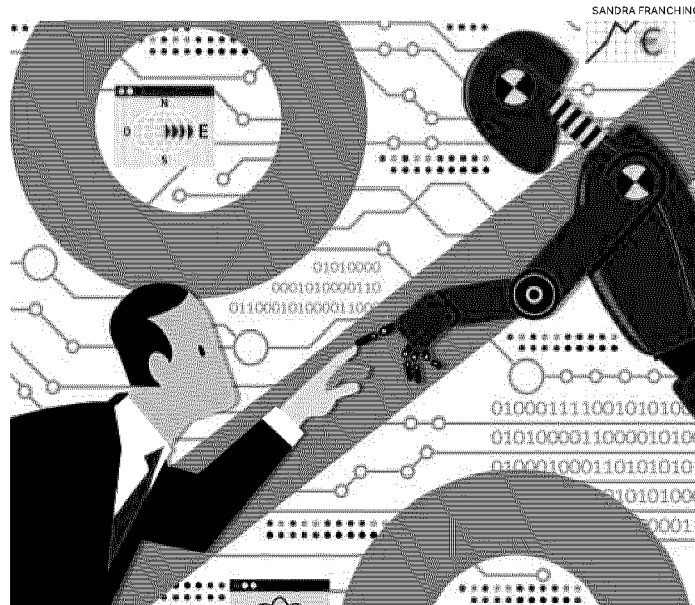
Tutti devono partire dagli stessi adempimenti:

- 1 realizzare un registro dei casi d'uso, anche in bozza, con sistema, fornitore, funzione aziendale e referente;
- 2 mappare gli obblighi già applicabili (trasparenza, divieti, formazione, contratti con i fornitori);

3 predisporre l'elenco di ciò che può attendere il 2027 e di ciò che non può.

Per le imprese, e per i professionisti che le assistono, il 2 dicembre 2027 è la data dell'esame, non quella in cui si comincia a studiare.

© RIPRODUZIONE RISERVATA



IL CALENDARIO

Già in vigore

Pratiche vietate (dal febbraio 2025), con sanzioni fino a 35 milioni o al 7% del fatturato mondiale. Alfabetizzazione, nella nuova formula del regolamento "Digital Omnibus". Obblighi dei fornitori di modelli di Ai per finalità generali (dall'agosto 2025).

2 agosto 2026

Trasparenza (articolo 50): chatbot, deepfake, contenuti sintetici; sanzioni fino a 15 milioni di euro o al 3 per cento. Poteri sanzionatori della Commissione sui modelli per finalità generali.

30 settembre 2026

In vigore il decreto legislativo 160/2026: reato dell'articolo 437-bis del Codice penale; Ai nel catalogo 231 (articolo 25-vicies);

esibizione delle prove e presunzione del nesso causale nelle cause di danno; azione diretta verso l'assicuratore.

2 dicembre 2026

Divieto dei sistemi che generano immagini intime non consensuali e materiale pedopornografico. Fine del periodo transitorio per la marcatura dei contenuti dei sistemi generativi già sul mercato.

2 dicembre 2027

Obblighi sui sistemi ad alto rischio dell'Allegato III (tra cui selezione del personale, istruzione, merito creditizio).

2 agosto 2028

Obblighi sui sistemi ad alto rischio dell'Allegato I (componenti di sicurezza di prodotti già regolati).

L'allarme dell'osservatorio Crif: nel I semestre oltre 2,5 milioni di dati esposti nel dark web

Le frodi cyber si affinano con l'IA

Italia nel mirino. In testa indirizzi e-mail e carte di credito

Pagina a cura
DI TANCREDI CERNE

Allarme rosso per la sicurezza informatica: l'Italia rappresenta, infatti, uno dei bersagli preferiti dal cybercrime di tutto il mondo. Nei primi sei mesi dell'anno, è stata il quarto Paese europeo (e sesto a livello mondiale) più colpito per numero di indirizzi e-mail compromessi e messi in circolazione sul dark web, e sesto in Europa (22° a livello globale) per numero di dati relativi a carte di credito in circolazione. Non solo. L'Italia si è posizionata anche al sedicesimo posto a livello europeo (51° al mondo) per rilevamento di numeri di telefono, che rappresentano un elemento chiave in molte truffe online, come lo smishing, una truffa informatica che usa messaggi di testo e sms per rubare dati personali e somme di denaro. Ancora più significativo il dato sugli infostealer, ovvero i malware progettati per sottrarre in modo automatico informazioni riservate dai dispositivi infettati: per account rubati e diffusi con questa tecnica l'Italia è terza nel mondo, dietro soltanto a Stati Uniti e Francia.

L'allerta è contenuta nell'ultimo osservatorio cyber realizzato da Crif da cui è emersa una crescente vulnerabilità del sistema Paese a fronte di minacce informatiche sempre più sofisticate. Basti pensare che nei primi sei mesi del 2026 quasi un terzo degli italiani (32,3% degli utenti monitorati) ha ricevuto almeno un alert relativo all'esposizione impropria dei propri dati sul web. Mentre la penetrazione dei malware silenziosi, favorita dal modello di diffusione stealer-as-a-service che abbassa le barriere d'accesso anche per criminali privi di competenze avanzate, ha alimentato un mercato nero in cui circolano oltre 2,5 miliardi di dati univoci. Una massa di informazioni che i cybercriminali possono incrociare per costruire profili dettagliati delle vittime, rendendo

più efficaci le truffe, i tentativi di phishing e i furti di identità.

«Le tecniche tradizionali, dal phishing via e-mail allo smishing via sms o app di messaggistica, dal vishing telefonico allo spear phishing con messaggi personalizzati, restano le minacce principali», hanno avvertito gli esperti del Crif secondo cui, a queste, si aggiungono anche gli attacchi basati sull'intelligenza artificiale, che sfruttano deepfake audio e video sempre più realistici e, in ambito aziendale, e-mail impeccabili, difficili da distinguere da comunicazioni autentiche. Così come avvenuto nei mesi scorsi a Fideuram con un raggio da 36 milioni di euro perpetrato attraverso il suo ex presidente, Paolo

Molesini, caduto nella rete dei truffatori per colpa di un finto messaggio di whatsapp a cui è seguita la telefonata di un finto legale la cui voce, grazie a strumenti di intelligenza artificiale, replicava ad arte quella di un noto avvocato di uno studio internazionale. In aggiunta, alcune mail, anche queste perfettamente contraffatte, che indicavano a Fideuram le coordinate di società e conti esteri sui quali operare i pagamenti per finalizzare una acquisizione internazionale richiesta, si pensava, dal Ceo di Intesa Sanpaolo. «Proteggere i propri dati personali è oggi più importante che mai. Le frodi online sono sempre più sofisticate e credibili, grazie a strumenti basati sull'intelligenza artificiale come deepfake, phishing personalizzato e tecniche avanzate di ingegneria sociale

che sfruttano informazioni personali spesso reperite online o provenienti da violazioni dei dati. In questo scenario, la consapevolezza personale rappresenta la prima linea di difesa», ha avvertito **Beatrice Rubini**, executive director di Crif per cui è importante promuovere la cultura della sicurezza digitale, supportando cittadini e consumatori nella tutela della propria identità e nell'adozione di comportamenti consapevoli per

riconoscere e prevenire le nuove minacce informatiche.

Umbria, Molise, Lazio i più a rischio. Tornando all'analisi dei dati messa a punto dal Crif, nel contesto nazionale, tra gennaio e giugno scorsi, la distribuzione geografica delle segnalazioni in Italia ha evidenziato, come regioni più colpite per volume di avvisi, la Lom-

bardia (15,7%), il Lazio (12,3%), la Sicilia (11,3%), l'Emilia-Romagna (9,7%) e il Piemonte (9,5%). Tuttavia, guardando alla proporzione rispetto alla popolazione residente, sono gli abitanti di Umbria, Molise, Lazio, Piemonte e Friuli-Venezia Giulia a registrare la frequenza relativa più elevata di notifiche. A livello di ripartizione macro-territoriale, invece, stando all'analisi del Crif, il sud ha raccolto il 29,2% degli alert complessivi, seguito a breve distanza dal nord ovest con il 27,5%. In termini demografici la platea degli utenti privati italiani avvisati dai servizi di protezione si concentra prevalentemente tra i 51 e i 60 anni (26,7%), tra i 41 e i 50 anni (26,6%) e nella fascia degli over 60 (20,3%), mentre sotto il profilo del genere la componente maschile rappresenta la mag-

gioranza schiacciante degli interessati, attestandosi al 64,3%. Ma quali sono i dati più appetibili per i cyber criminali? Al primo posto, secondo l'analisi del Crif, ci sarebbero le credenziali digitali che si confermano essere il bersaglio privilegiato: password, e-mail, nomi utente, numeri di telefono, nomi e cognomi.

Ancora più eloquente è l'analisi delle combinazioni. Il numero della carta di credito, con i dati di sicurezza e la data di scadenza, compare insieme nel 99,8% dei casi, ed è un dato in forte crescita che pesa sul rischio di frodi finanziarie. La password è associata all'e-mail nel 95,9% dei casi e allo username nel 96%, a conferma che il furto dell'account resta l'obiettivo primario. Il numero di telefono è abbinato alla password nel

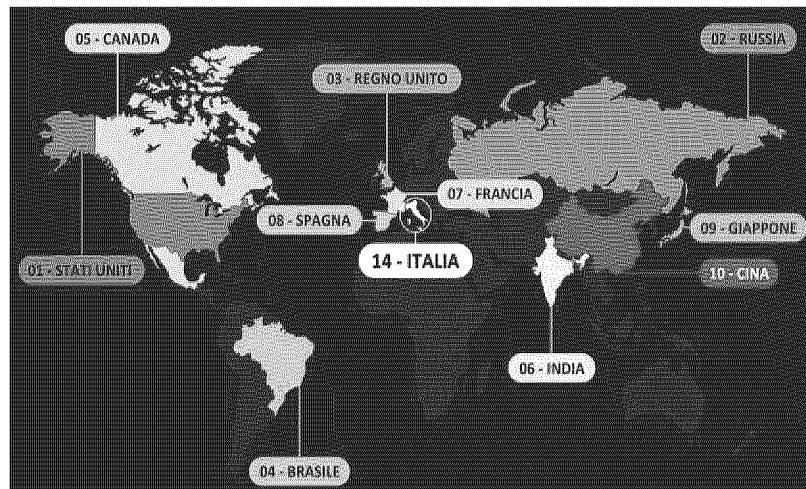


61,7% dei casi e a nome e cognome nel 18,8%, mentre l'indirizzo completo viaggia insieme al telefono nel 73,8% dei casi. L'incrocio di queste informazioni rende molto più efficaci gli attacchi di ingegneria sociale, compresi lo spear phishing e le truffe di tipo Bec, come la cosiddetta truffa del Ceo, in cui i criminali si fingono dirigenti per convincere i dipendenti a disporre bonifici o a condividere informazioni riservate.

I dati nel mirino dei criminali. Ma quali sono i dati più vulnerabili presenti oggi in rete? Stando alle indicazioni degli esperti di Crif, escludendo la posta elettronica e le password, i cyber criminali sarebbero sempre più a caccia di username associati soprattutto ad account di servizi, come portali di offerte di lavoro e di notizie, con una quota del 26,6%, seguiti dai social network (20,8%) e da forum e siti web (16,3%), ma anche dalle piattaforme di e-commerce (12,4%), dai servizi di streaming (5,8%), dai servizi finanziari (4,4%), dal comparto gaming (3,9%) e dagli enti pubblici o istituzioni (3,8%). Inoltre, dall'esame dei domini di posta coinvolti è emersa una netta prevalenza per gli indirizzi personali, che rappresentano il 92,1% del totale, mentre gli account business si attestano appena al 7,9%. Uno scarto che suggerisce come gli utenti privati continuino a prestare un'attenzione insufficiente alla sicurezza digitale, costituendo il bersaglio privilegiato dei cybercriminali. Detto questo, quale uso viene fatto delle credenziali sottratte? Gli esperti del Crif non sembrano avere dubbi: le credenziali sottratte possono servire a entrare negli account delle vittime, a usare servizi in modo fraudolento, a inviare richieste di denaro o link di phishing, a diffondere malware o ransomware.

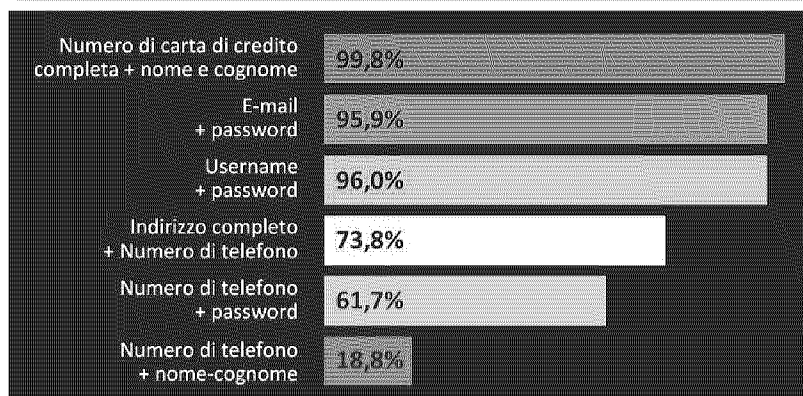
© Riproduzione riservata

Dove vengono rubati i dati delle carte di credito



Fonte: Osservatorio Cyber - Crif-Mister Credit

Le combinazioni di dati più esposte



Fonte: Osservatorio Cyber - Crif-Mister Credit