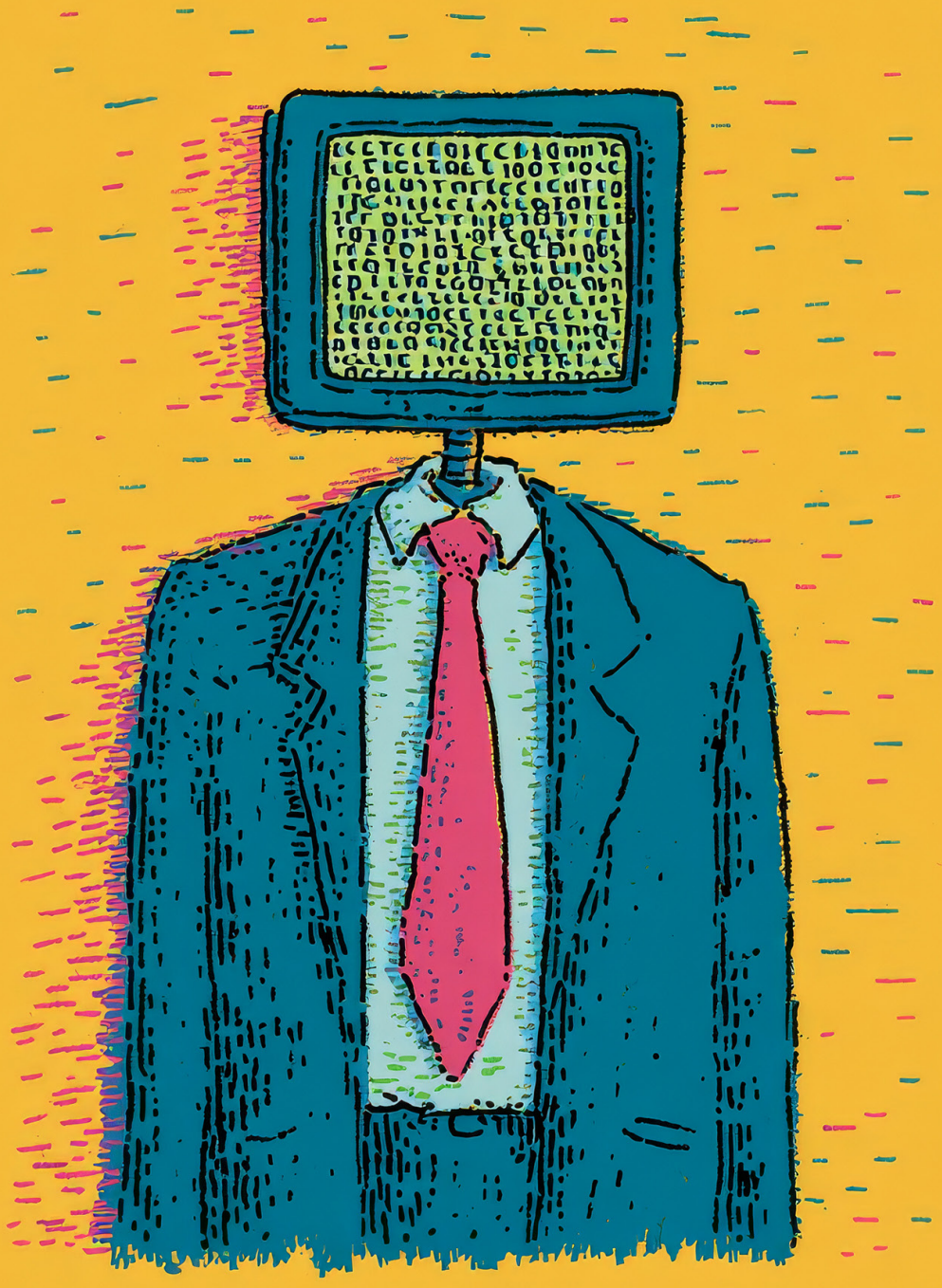
N. 1 - 2026 - ANNO 1 - RIVISTA QUADRIMESTRALE DEL REGISTRO .IT

dot.it

DOMAINS • OPINIONS • TRENDS



Registro.it

L'ANAGRAFE DEI DOMINI .IT

COORDINAMENTO EDITORIALE
Chiara Spinelli

COMITATO EDITORIALE
Valentina Amenta, Maurizio Martinelli, Chiara Spinelli

GRAFICA E IMPAGINAZIONE
Coesiva

COMITATO REDAZIONALE
Francesca Nicolini (coordinatore redazionale), Stefania Fabbri, Chiara Spinelli

HANNO COLLABORATO A QUESTO NUMERO
Giorgia Bassi, Arianna Del Soldato, Adriana Lazzaroni, Beatrice Lami, Daniele Sartiano, Gino Silvatici, Chiara Spinelli, Luca Albertario con Sonia Sbrana e Daniele Pancrazi (didascalie legali)
Michela Serrecchia (didascalie tecniche)
Silvia Giannetti (didascalie operative)

Si ringrazia il
Prof. Franco Bernabè per il contributo "I paradossi della regolazione"

FONTE DATI
Unità Sistemi e Sviluppo tecnologico del Registro .it

ELABORAZIONE DATI
Lorenzo Luconi Trombacchi, Michela Serrecchia (Unità Sistemi e Sviluppo tecnologico del Registro .it)
Luca Albertario, Daniele Pancrazi, Sonia Sbrana (Unità Aspetti legali e contenzioso)
Silvia Giannetti (Unità Operazioni e servizi ai Registrar)

A CURA DI
Unità Relazioni esterne, media, comunicazione e marketing del Registro .it

Via G. Moruzzi, 1
I-56124 Pisa
tel. +39 050 313 98 11
e-mail: info@registro.it
website: www.registro.it

RESPONSABILE DEL REGISTRO .IT
Andrea Passarella

Registro .it è gestito da:

Registro.it L'ANAGRAFE DEI DOMINI .IT | IIT ISTITUTO DI INFORMATICA E TELEMATICA CNR | Consiglio Nazionale delle Ricerche

01 **Anteprima | 4**

- DOT: dentro la rete che cambia, tra AI, trasformazioni di Internet e crescita dei domini .it 5

02 **Statistiche | 8**

- Crescita annuale del .it 9
- Crescita quadrimestrale del .it 10
- La top 10 delle regioni con più domini .it 11
- Le tipologie degli assegnatari dei domini .it 12
- Motivi opposizioni 13
- Rapporto Opposizioni - Riassegnazioni 14
- Andamento annuale Opposizioni - Riassegnazioni 15
- Risoluzione delle Opposizioni 16
- Verifica domini da parte del Registro 17
- Richieste Authinfo 18
- Richieste Autorità competenti 18
- Nomi riservati ai Comuni italiani 19

03 **News | 20**

- I primi 40 anni di Internet: una rivoluzione che guarda al futuro tra AI e Quantum 21
- Ludoteca del Registro .it - Laboratori di educazione digitale nelle scuole 25

04 **Approfondimenti | 28**

- I paradossi della regolazione 29
- Analisi dei rinnovi dei domini: il contributo del .it alla task force CENTR 38
- Dall'AI alla NIS2: le sfide del digitale per le imprese nelle dirette LinkedIn del Registro .it 46
- Educare alla cybersicurezza: in arrivo "Nel Mezzo dei Maghi", il nuovo gioco da tavolo della Ludoteca 50
- Rapporto Iocta 2026: dall'AI ai domini malevoli, l'allarme di Europol sul cybercrime 56
- Icann e l'impatto dell'intelligenza artificiale sul DNS 61

05 **Eventi | 66**

- Gli appuntamenti internazionali dal mondo della rete 67

01

Anteprima

Statistiche

News

Approfondimenti

Eventi

DOT: DENTRO LA RETE CHE CAMBIA, TRA AI, TRASFORMAZIONI DI INTERNET E CRESCITA DEI DOMINI .IT

Il digitale italiano e globale sta entrando in una fase in cui crescita, **infrastrutture, intelligenza artificiale, sicurezza e governance non possono più essere osservati come ambiti separati, ma come parti di un unico sistema in trasformazione**. Non si tratta più soltanto di misurare l'espansione delle presenze online o l'adozione di nuove tecnologie, ma di **comprendere come queste dimensioni si intreccino, ridefinendo il funzionamento stesso della Rete** e il suo ruolo nei sistemi economici e sociali.

Da questa consapevolezza nasce **DOT - Domains, Opinions, Trends**: dopo tredici anni, Quarter del Registro .it evolve e diventa DOT, inaugurando una nuova fase del proprio percorso editoriale. **Un nuovo nome** che, pur mantenendo la missione che ha accompagnato il quadrimestrale fin dall'inizio - informare, approfondire e interpretare i temi legati ai nomi a dominio, all'evoluzione di Internet e al digitale - ne **rafforza l'identità e la capacità di leggere un ecosistema sempre più interconnesso**.

DOT raccoglie l'eredità di Quarter, dunque, e ne prosegue il percorso, con l'intento di accompagnarne nel tempo l'evoluzione anche sul piano editoriale, in coerenza con i cambiamenti in atto nella dimensione digitale.

Il primo quadrimestre del 2026 restituisce l'immagine di un ecosistema in movimento, che **conferma la vitalità del tessuto digitale nazionale**. A fine aprile i domini registrati raggiungono quota **3.578.851**, con un **incremento dell'1,17% rispetto alla fine del 2025**, **più che doppio rispetto al ritmo di crescita osservato nello stesso periodo dell'anno precedente**. Un dato che conferma come la presenza online continui a rappresentare per imprese, organizzazioni e cittadini uno strumento strategico di identità, visibilità e relazione.

La crescita, tuttavia, racconta solo una parte della storia: per

essere compresa davvero, **va letta anche nella sua dimensione di stabilità e continuità**. In questa prospettiva si inserisce il contributo del Registro .it alla **Benchmarking Renewal Indicators Task Force** promossa da Centr (Council of European National Top Level Domain Registries), che ha analizzato circa 40 milioni di domini in scadenza nel 2024, mettendo a confronto dieci registri ccTLD. I risultati mostrano come il rinnovo sia strettamente legato a fattori quali l'età del dominio, quella del registrante e la sua categoria di appartenenza, offrendo una chiave di lettura importante: **la continuità digitale non è casuale, ma si costruisce nel tempo**. In questa prospettiva, **il rinnovo diventa una chiave di lettura del valore attribuito alla presenza online**, trasformando i dati in strumenti operativi che potranno, in prospettiva, supportare concretamente i Registrar nella gestione dei loro portafogli domini.

Accanto ai dati, **le grandi trasformazioni che stanno ridefinendo Internet trovano riscontro anche nelle dirette LinkedIn** organizzate dal Registro .it, in onda nei primi mesi del 2026 e dedicate all'impatto dell'intelligenza artificiale sui siti delle PMI, all'evoluzione del turismo digitale e alle implicazioni della direttiva NIS2. Ne emerge un quadro chiaro: **l'AI sta modificando profondamente la produzione dei contenuti, la ricerca delle informazioni e i meccanismi della fiducia online, ma non riduce la centralità del sito web e del dominio come presidio di identità e credibilità**. Allo stesso tempo, la sicurezza non è più un tema tecnico relegato agli specialisti, ma una responsabilità strategica che coinvolge governance, gestione della supply chain e organizzazione aziendale.

Lo sguardo sul presente e sul futuro di Internet attraversa anche una ricorrenza simbolica: **il quarantesimo anniversario del primo collegamento italiano alla Rete**, avvenuto il 30 aprile 1986. L'evento, organizzato a Pisa dall'Istituto di informatica e telematica del Cnr (Cnr-Iit), non è stato soltanto la celebrazione di una **tappa fondamentale della storia digitale nel nostro Paese, ma è stato soprattutto un'occasione per interrogarsi sul suo futuro**: una Rete sempre più integrata con l'intelligenza artificiale, distribuita, intelligente e orientata alla produzione di servizi e conoscenza. Nello stesso contesto si collocano le riflessioni di **Franco Bernabè**, con il suo **keynote - pubblicato integralmente in questo numero** - sul ruolo dell'Europa nella competizione tecnologica globale e sulla necessità di evitare nuove forme di dipendenza tecnologica.

Oltre ai dati, alle infrastrutture e alle tecnologie, **DOT racconta anche la dimensione culturale della trasformazione digitale**: dalle

attività di divulgazione e formazione alle nuove esperienze educative dedicate alla cybersicurezza della **Ludoteca del Registro .it**, **emerge con sempre maggiore evidenza la necessità di accompagnare le nuove generazioni verso un uso consapevole degli strumenti digitali**. In questo quadro, si inserisce il **nuovo gioco da tavolo "Nel Mezzo dei Maghi"**, **sviluppato dalla Ludoteca del Registro .it, in collaboraborazione con il CINI (Consorzio Interuniversitario Nazionale per l'Informatica) e l'IMT di Lucca**, per avvicinare i giovanissimi e le giovanissime ai temi della cybersecurity attraverso modalità sempre più partecipative ed esperienziali.

Completano il numero gli approfondimenti dedicati alla **sicurezza informatica, alla governance della Rete e all'impatto dell'intelligenza artificiale sugli ecosistemi digitali**, con attenzione anche alla dimensione regolatoria europea e internazionale. **Temi diversi, ma sempre più intrecciati tra loro, che restituiscono l'immagine di una Rete in trasformazione e confermano il ruolo centrale che i nomi a dominio continuano a svolgere al suo interno**. In questo scenario, sicurezza e governance si confermano dimensioni strutturali della dimensione online, in un contesto segnato dall'impatto crescente dell'intelligenza artificiale sui modelli di utilizzo di Internet.

DOT nasce per osservare e raccontare questo panorama digitale complesso e in continuo movimento: un "**punto**" nella Rete, ma anche un "**punto**" di osservazione privilegiato sui cambiamenti che stanno ridefinendo il digitale. L'obiettivo è quello di offrire alla comunità dei Registrar, ai professionisti, alle imprese e a tutti gli attori dell'ecosistema Internet, strumenti di lettura, approfondimento e confronto.

Buona lettura!

02

Anteprima

Statistiche

News

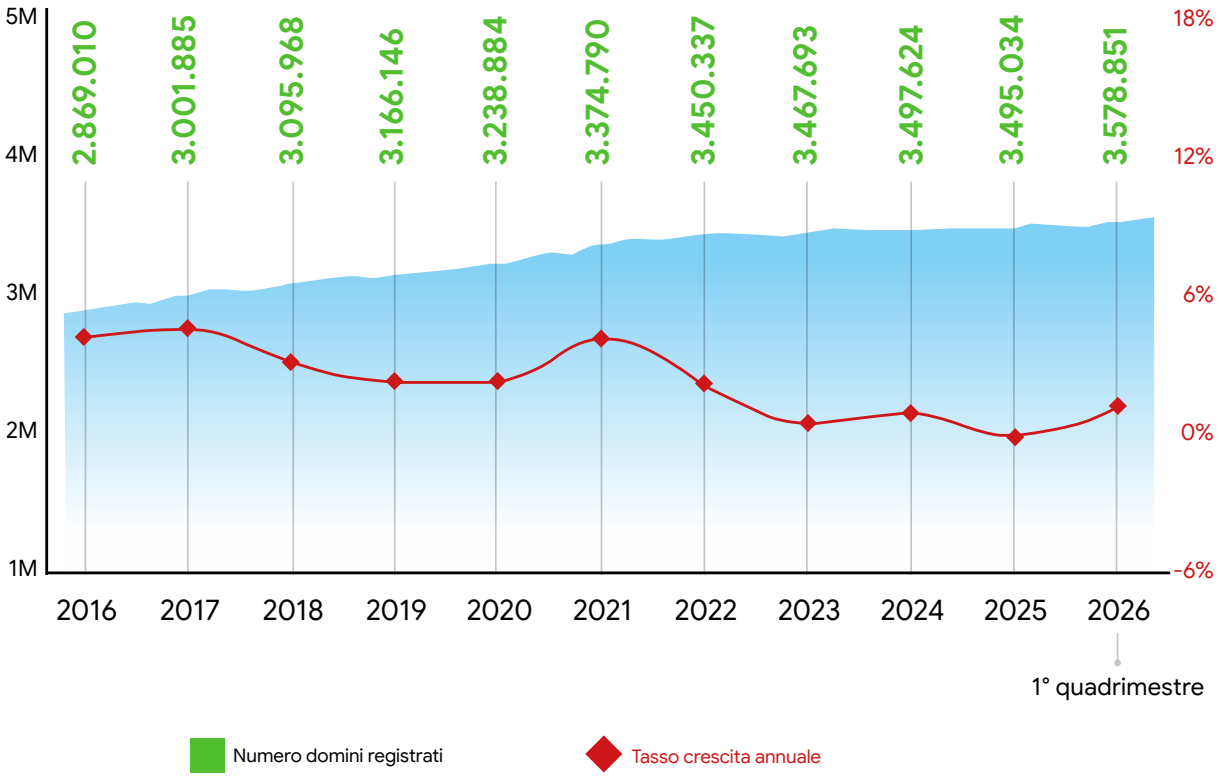
Approfondimenti

Eventi

CRESCITA ANNUALE DEL .IT

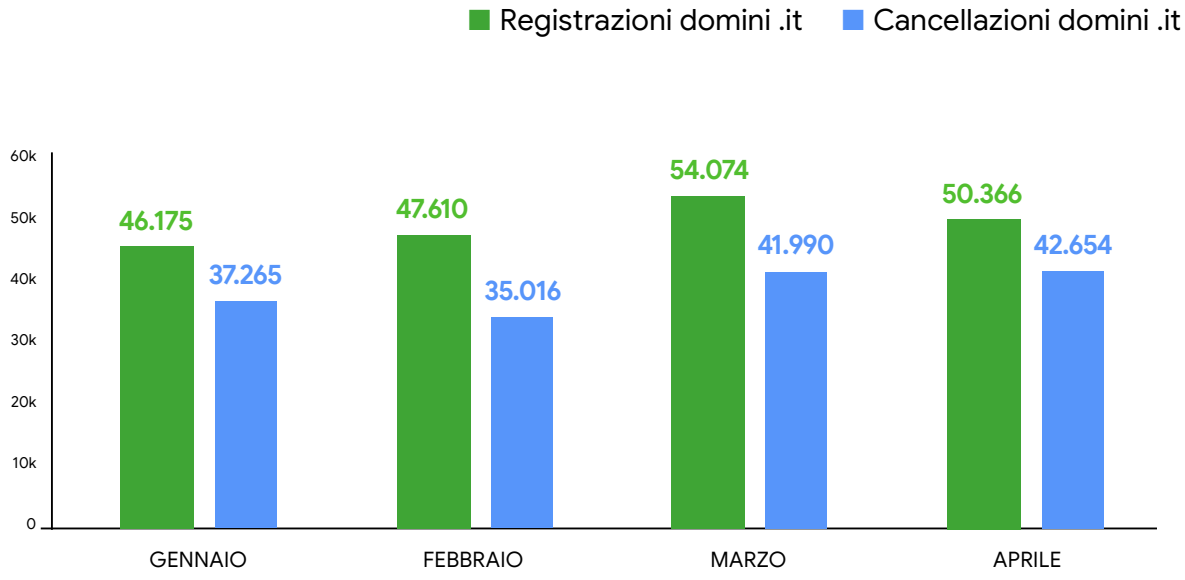
Alla fine del primo quadrimestre 2026, il **numero totale** dei domini .it raggiunge quota **3.578.851**, registrando un **incremento dell'1,17% (+41.300 domini) rispetto alla fine del 2025.** Tale risultato evidenzia una netta accelerazione rispetto allo stesso periodo dell'anno precedente, quando la crescita si era attestata allo 0,54% (+19.023 domini rispetto alla fine del 2024).

gennaio-aprile 2026



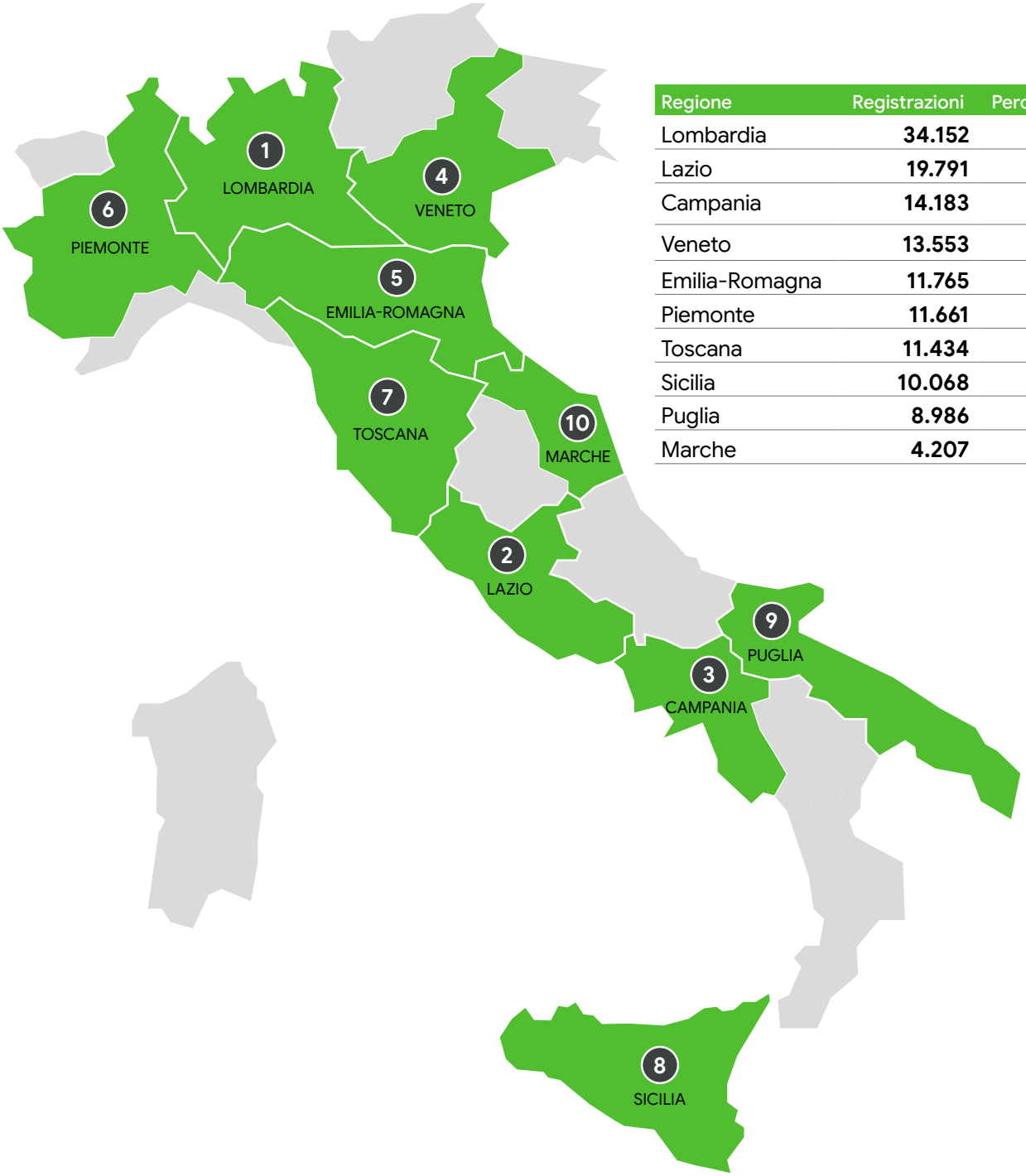
CRESCITA QUADRIMESTRALE DEL .IT

L'andamento delle registrazioni dei nomi .it, nei primi quattro mesi dell'anno, evidenzia un **saldo positivo tra nuovi domini e cancellazioni**, con un picco significativo nel mese di febbraio. Il bilancio complessivo del periodo esaminato supera le 41mila unità, un dato più che raddoppiato rispetto allo stesso quadrimestre del 2025, quando il saldo si era fermato a poco più di 19mila domini. **L'andamento risulta positivo sotto un duplice profilo: un incremento delle nuove registrazioni e una contestuale diminuzione delle cancellazioni** rispetto allo scorso anno.



LA TOP 10 DELLE REGIONI CON PIÙ DOMINI .IT

Nel primo quadrimestre, la **Lombardia si conferma leader** indiscussa **della classifica**: la percentuale delle nuove registrazioni resta stabile al 21%, rispetto allo stesso periodo dello scorso anno. **Il Lazio mantiene la seconda posizione**, anch'esso con una percentuale invariata al 12%. Ottima performance per **la Campania**, che **sale al terzo posto** raggiungendo il 9%, a spese del Veneto che, perdendo una posizione, scivola in quarta posizione. Perde terreno anche il Piemonte, che scende al sesto posto fermandosi al 7%.

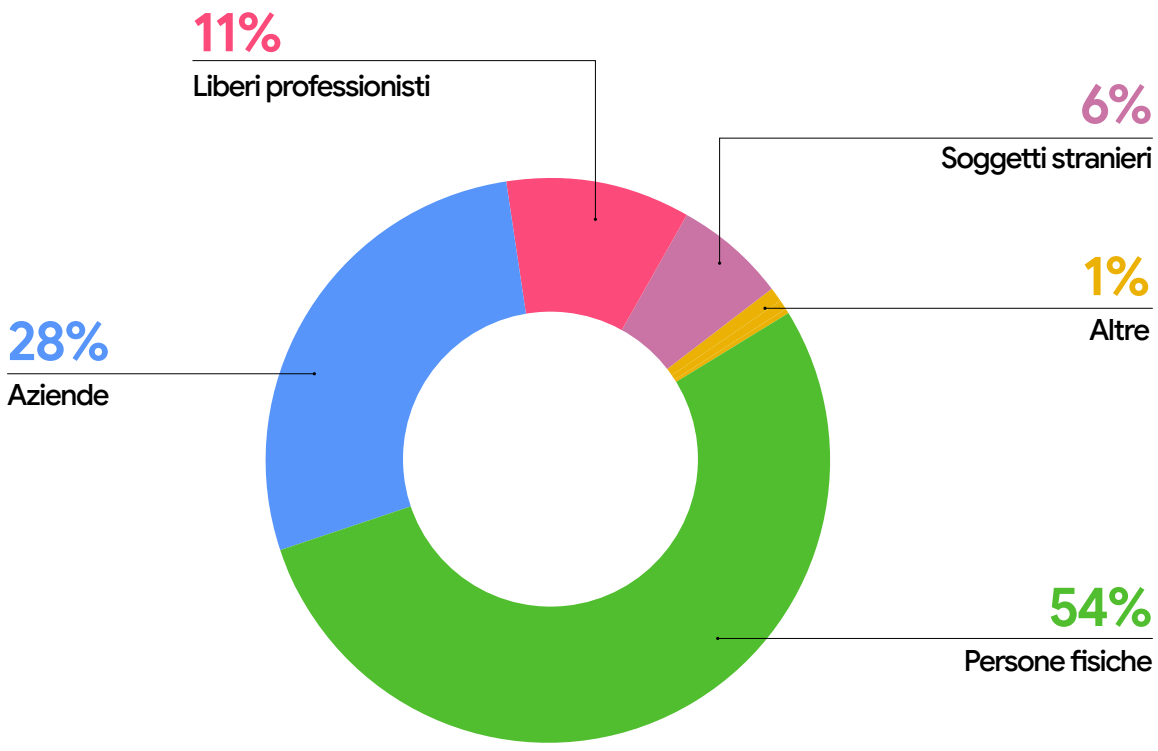


Regione	Registrazioni	Percentuale
Lombardia	**34.152**	20,79%
Lazio	**19.791**	12,05%
Campania	**14.183**	8,63%
Veneto	**13.553**	8,25%
Emilia-Romagna	**11.765**	7,16%
Piemonte	**11.661**	7,10%
Toscana	**11.434**	6,96%
Sicilia	**10.068**	6,13%
Puglia	**8.986**	5,47%
Marche	**4.207**	2,56%

LE TIPOLOGIE DEGLI ASSEGNATARI DEI DOMINI .IT

Rispetto al primo quadrimestre del 2025, **la percentuale di nuovi domini .it registrati da persone fisiche cresce di quattro punti** percentuali, raggiungendo il 54%. Calano invece **le imprese**, che **perdono due punti percentuali** scendendo al 28%. Si registra una leggera flessione anche per i liberi professionisti, la cui percentuale scende di un punto fermandosi all'11%.

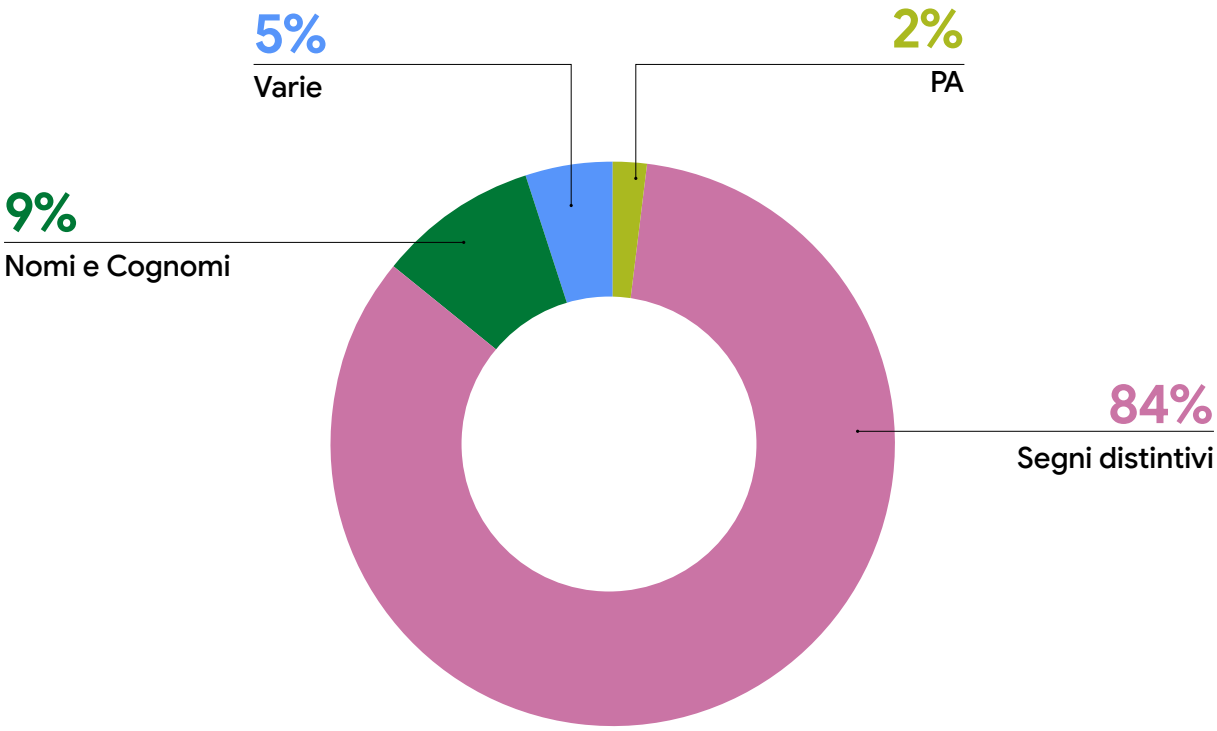
Nuove registrazioni gennaio-aprile 2026



MOTIVI OPPOSIZIONI

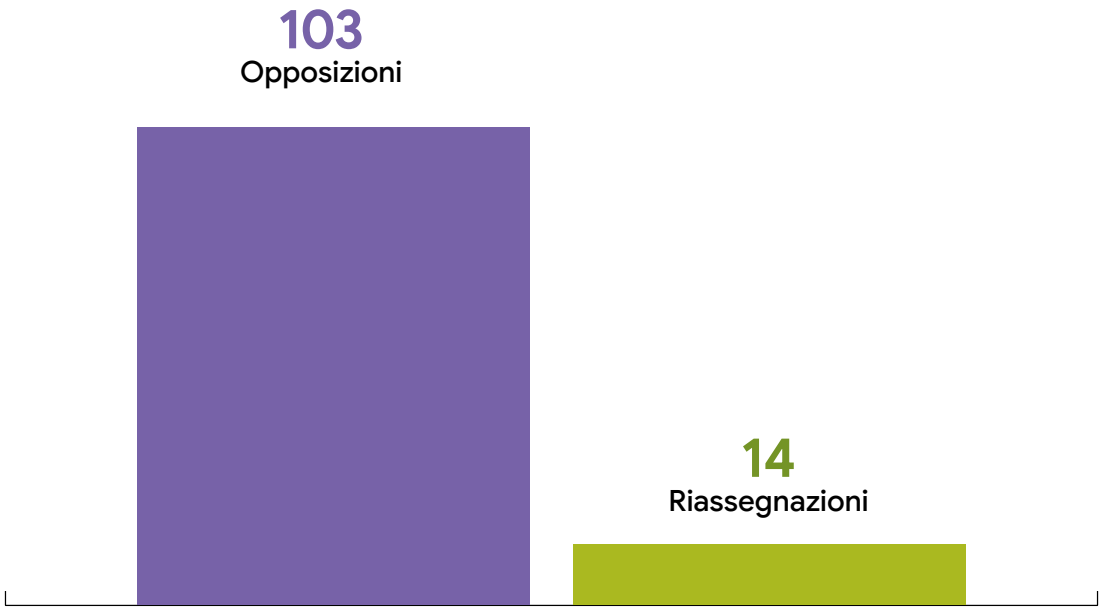
Nel primo quadrimestre, **le opposizioni per violazione dei segni distintivi rimangono prevalenti,** pur in lieve calo rispetto al 2025 (**84%** contro 89%). **Crescono invece le istanze relative a nomi e cognomi**, che passano **dall'8% al 9%**, mentre le opposizioni promosse dalle pubbliche amministrazioni raggiungono il 2%, a fronte dell'assenza di casi nell'anno precedente.
Le istanze riconducibili ad altre motivazioni si attestano infine al 5%, in aumento rispetto al 3% registrato nel 2025.

Segni distintivi gennaio-aprile 2026



RAPPORTO OPPOSIZIONI - RIASSEGNAZIONI

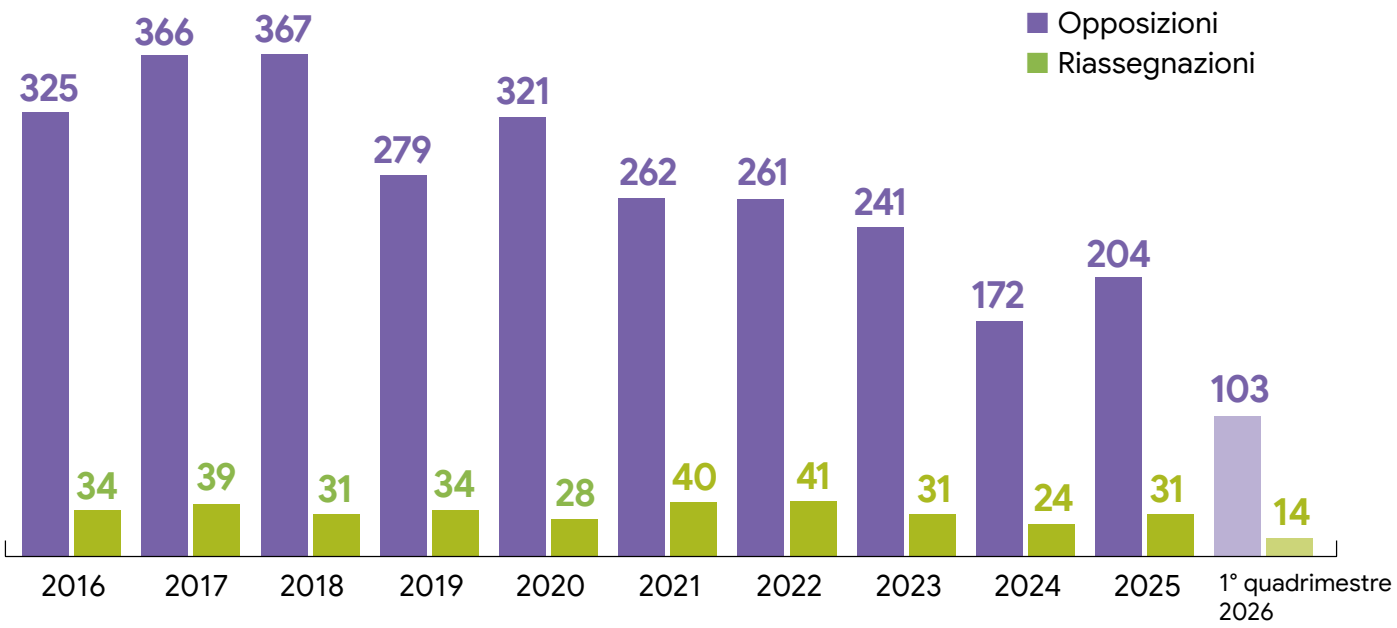
Nel periodo esaminato, sono **103 le opposizioni attivate, in aumento rispetto alle 83** dello stesso quadrimestre **del 2025**, con una media mensile passata da 21 a 26 attivazioni. Marzo è stato il mese più attivo con 34 opposizioni, mentre febbraio quello con il valore più basso (22).
Dal punto di vista geografico, **38 procedure hanno coinvolto esclusivamente soggetti italiani**; tra gli assegnatari/resistenti prevale il Nord (17), seguito da Sud (13) e Centro (8), mentre tra gli opponenti/reclamanti il Nord registra 23 soggetti, contro 10 del Centro e 5 del Sud. Il quadro si completa con **48 casi in cui opponenti italiani hanno agito contro assegnatari stranieri,** 4 opposizioni di opponenti esteri contro assegnatari italiani e 13 procedure interamente estere.
Sono state introdotte **14 procedure di riassegnazione** presso i PSRD (Prestatori del Servizio di risoluzione delle dispute): 4 interamente nazionali (assegnatari/resistenti e opponenti/reclamanti italiani), 2 tra soli soggetti esteri, 2 avviate da opponenti/reclamanti italiani contro assegnatari/resistenti esteri e 6 con assegnatari/resistenti italiani e opponenti/reclamanti esteri.



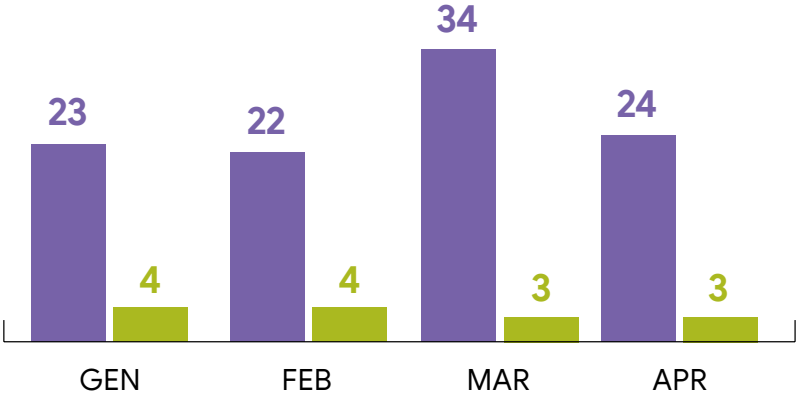
ANDAMENTO ANNUALE OPPOSIZIONI - RIASSEGNAZIONI

Nei primi quattro mesi dell'anno, si registra un **aumento complessivo delle opposizioni rispetto al 2025**, pur in presenza di dinamiche mensili differenziate. Gennaio e aprile mostrano una crescita di +5 opposizioni ciascuno (da 18 a 23 e da 19 a 24 rispettivamente), marzo passa da 23 a 34 con +11 casi, mentre febbraio registra una lieve flessione (-1), passando da 23 a 22 procedure.

Le procedure di riassegnazione passano da 9 a 14. La maggior parte dei ricorsi è stata accolta (8 trasferimenti di dominio a favore degli opponenti/reclamanti), mentre un solo caso è stato respinto e mantiene l'assegnazione originale. Una procedura si è conclusa per estinzione e 4 procedimenti sono ancora pendenti, in attesa di decisione da parte del Collegio.

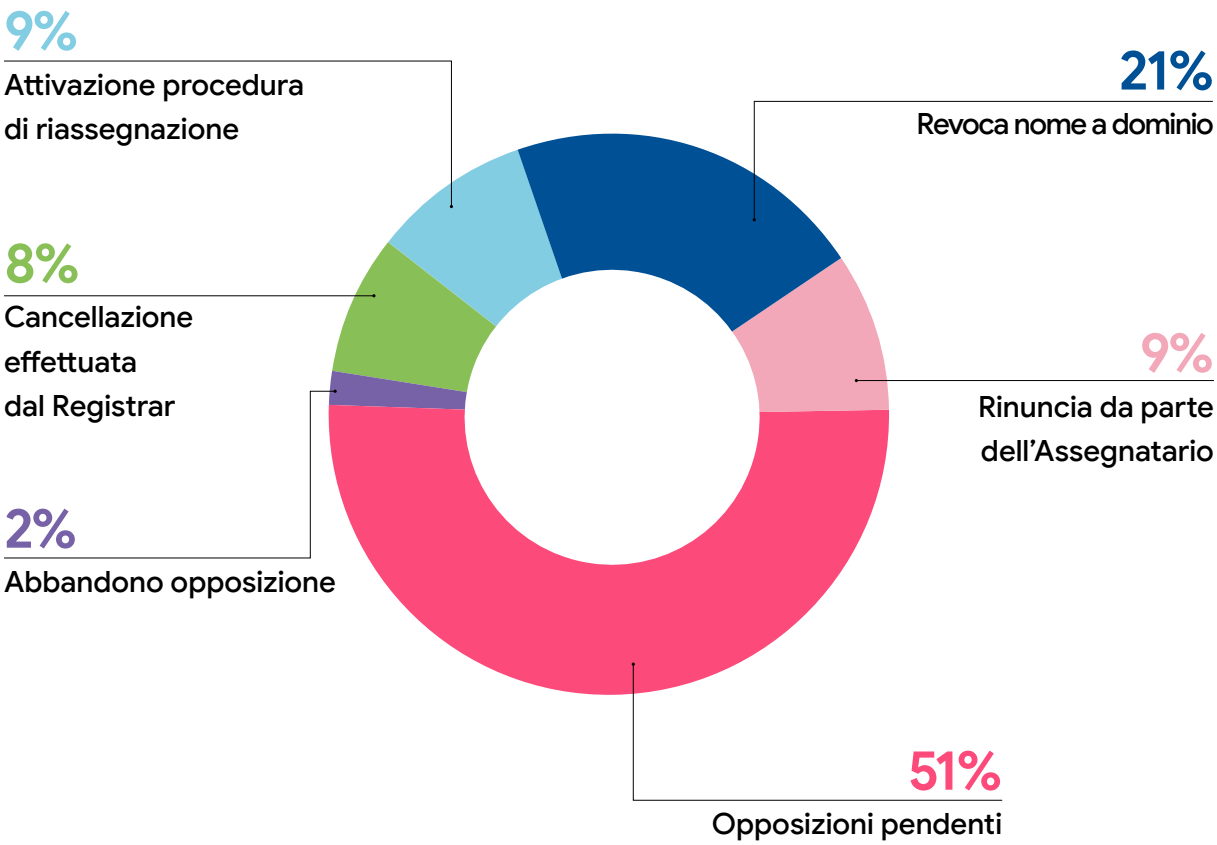


Andamento quadrimestre



RISOLUZIONE DELLE OPPOSIZIONI

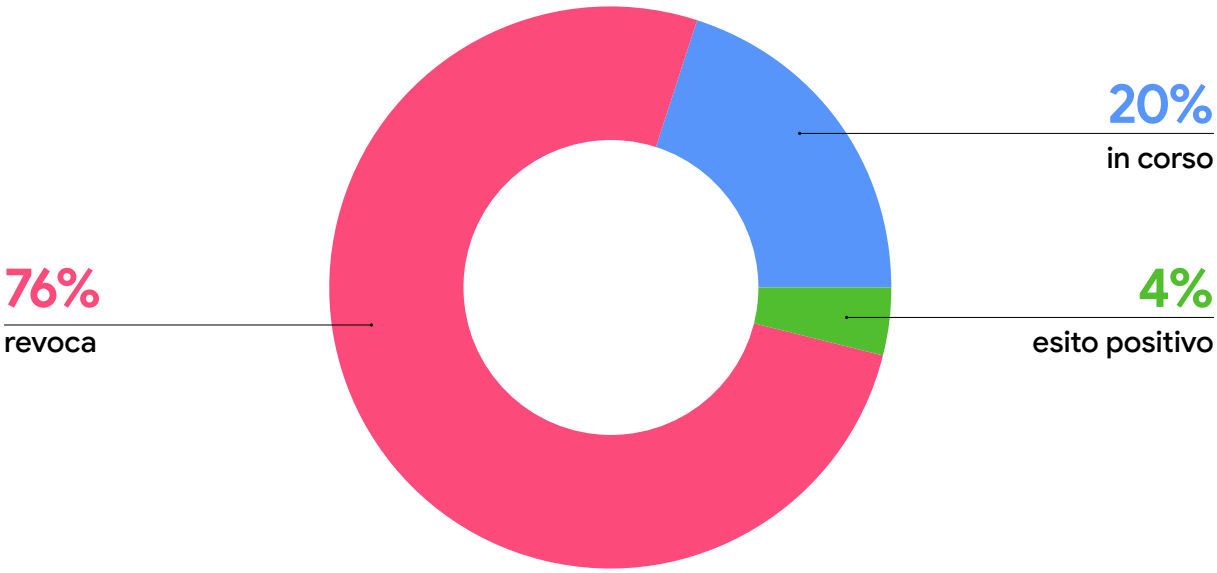
Il 51% delle 103 opposizioni risulta ancora **pendente. Tra quelle concluse**, la fattispecie più frequente è la **revoca** dei nomi a dominio a seguito della verifica dei requisiti soggettivi **(21%)**. Seguono, entrambe con il **9%**, le **cancellazioni** su richiesta degli assegnatari al Registro .it e le procedure di riassegnazione avviate dagli opponenti presso un PSRD. **Nell'8% dei casi il dominio è stato cancellato dal Registrar**, mentre nel **restante 2% l'opponente ha** formalmente **rinunciato alla prosecuzione dell'opposizione.**
Nel periodo considerato non si registrano casi di estinzione per mancato rinnovo, poiché l'opposizione rimane pendente per 180 giorni lavorativi.



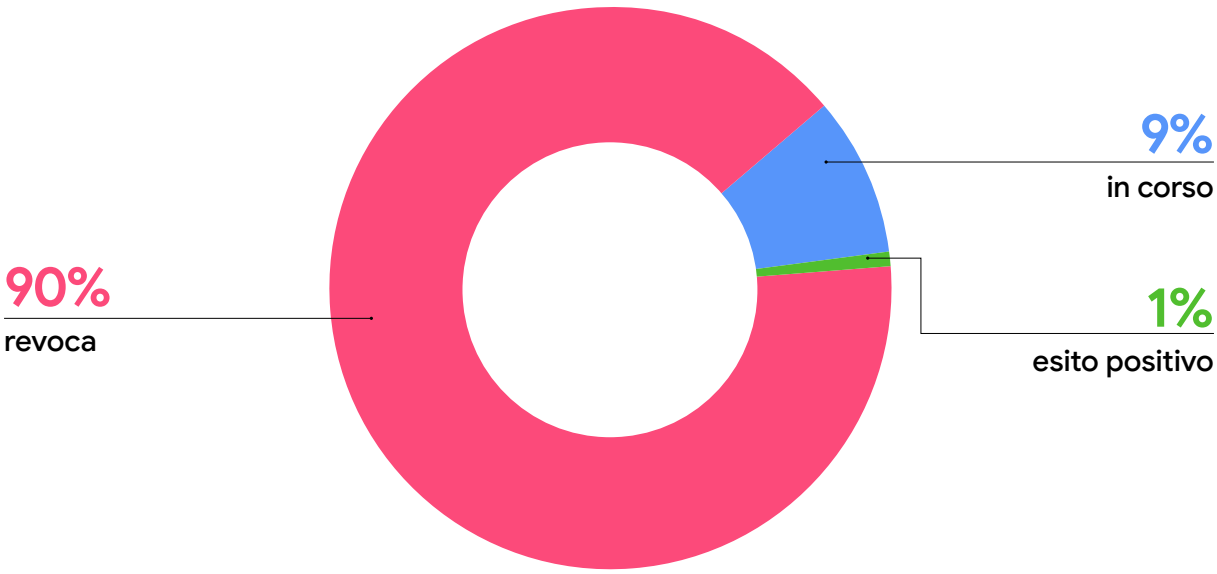
VERIFICA DOMINI DA PARTE DEL REGISTRO

Per verificare la correttezza dei dati dei Registranti presenti nel Database Whois, il Registro .it ha avviato **109 procedure di verifica relative a 270 nomi a dominio.** Di questi, 242 sono stati revocati, 4 hanno avuto esito positivo, mentre 24 risultano ancora in fase di verifica.

Verifiche gennaio-aprile 2026



Domini coinvolti gennaio-aprile 2026



RICHIESTE AUTHINFO

Nel primo quadrimestre, il Registro .it ha rilasciato **45 codici AuthInfo** direttamente ai Registranti, a tutela dei titolari nei casi di Registrar non più attivi. I Registrar coinvolti sono stati 8.

45



Richieste codici Authinfo

45



Domini

8



Registrar coinvolti

RICHIESTE AUTORITÀ COMPETENTI

Nei primi quattro mesi dell'anno, **le Autorità competenti** - nel rispetto delle prerogative di legge - **hanno inviato 25 richieste di informazioni relative a 28 nomi a dominio** registrati nel ccTLD .it.

25



Richieste

28



Domini coinvolti

NOMI RISERVATI AI COMUNI ITALIANI

I nomi a dominio appartenenti a questa categoria possono essere registrati esclusivamente dai Comuni italiani (ad es. comune.roma.it, comune.pontedera.pi.it, ecc.). Nel periodo considerato **sono stati registrati 13 nomi a dominio**. Il Piemonte risulta la regione con il maggior numero di registrazioni (3).



03

Anteprima
Statistiche
News
Approfondimenti
Eventi

I PRIMI 40 ANNI DI INTERNET: UNA RIVOLUZIONE CHE GUARDA AL FUTURO TRA AI E QUANTUM



Il 30 aprile 2026, a quarant'anni dal primo collegamento italiano a Internet, il Consiglio Nazionale delle Ricerche di Pisa ha celebrato l'anniversario che segnò l'ingresso del nostro Paese nella rete globale. Era **il 30 aprile 1986** quando, dall'istituto Cnuce del Cnr di Pisa, **partì il primo "ping" verso gli Stati Uniti**, ricevendo la risposta "ok" da un nodo di Arpanet in Pennsylvania: un evento simbolico che rese l'**Italia il quarto Paese europeo connesso a Internet**, dopo Regno Unito, Norvegia e Germania.



Sopra, l'Auditorium dell'Area della ricerca del Cnr di Pisa, sede dell'evento del 30 aprile 2026. In alto a destra, **Andrea Passarella**, Direttore dell'Istituto di informatica e telematica del Cnr e Responsabile del Registro .it



La celebrazione si è svolta presso l'Auditorium dell'Area della ricerca del Cnr di Pisa, su iniziativa dell'Istituto di Informatica e Telematica (Cnr-Iit), oggi punto di riferimento nazionale e internazionale per la ricerca sulle reti. Dall'ecosistema di quell'esperienza pionieristica, **un anno dopo quel primo collegamento** alla Rete, sempre a Pisa nel 1987, **nacque anche il Registro .it**, l'anagrafe dei nomi a dominio italiani, tuttora gestita dal Cnr-Iit.



L'evento ha avuto un taglio scientifico e istituzionale di alto profilo e **ha riunito rappresentanti delle istituzioni, del mondo accademico e dell'industria per riflettere sull'evoluzione di Internet e sulle sue prospettive future.** I lavori sono stati aperti dal direttore del Cnr-Iit e responsabile del Registro .it, **Andrea Passarella**, e hanno visto la partecipazione, tra gli altri, del Presidente del Cnr **Andrea Lenzi**, del Sottosegretario alla Presidenza del Consiglio con delega all'informazione e all'editoria **Alberto Barachini**. Dal punto di vista scientifico, ricercatori ed esperti di rilievo internazionale nei settori dell'intelligenza artificiale e delle tecnologie quantistiche si sono alternati in un confronto dedicato all'evoluzione di Internet e alle traiettorie che ne delineeranno il futuro.



Ospite dell'evento è stato anche **Franco Bernabè**, Presidente del Consiglio di Amministrazione dell'Università di Trento e già AD di Telecom e ENI, che ha tenuto un keynote dal titolo **"I paradossi della regolazione"**.

Al centro della giornata, non solo la memoria storica del primo "ping", ma soprattutto una **riflessione sul futuro di Internet e sul ruolo che la ricerca è chiamata a svolgere nei prossimi anni**. Gli interventi

Dall'alto, il Presidente del Consiglio Nazionale delle Ricerche **Andrea Lenzi. Sen. Alberto Barachini**, Sottosegretario alla Presidenza del Consiglio dei ministri con delega all'editoria e all'informazione



hanno messo in evidenza come Internet stia evolvendo da semplice infrastruttura di comunicazione a piattaforma strategica per l'innovazione, sempre più integrata con intelligenza artificiale e tecnologie quantistiche. Il cambiamento in atto riguarda sempre meno la connettività in sé e sempre più la **capacità della Rete di generare, integrare ed elaborare informazioni e servizi,** attraverso infrastrutture digitali che combinano calcolo, dati e interazione con il mondo fisico, **dando forma a un ecosistema intelligente e distribuito.**



Il confronto ha offerto una lettura articolata delle trasformazioni in corso di Internet, mettendo in evidenza le implicazioni delle **tecnologie quantistiche sulla sicurezza delle comunicazioni e delle infrastrutture critiche**, insieme all'evoluzione dei modelli di intelligenza artificiale e delle architetture digitali. Ampio spazio è stato dedicato anche ai temi della **sovranità digitale** e dell'**autonomia tecnologica**, in un contesto globale segnato da forti dinamiche di competizione industriale, geopolitica e di controllo delle infrastrutture strategiche. Al tempo stesso, è stato sottolineato il valore del **trasferimento tecnologico e** della **collaborazione tra ricerca pubblica, università e imprese**



In alto a sinistra, **Roberto Baldoni**, Senior Advisor for Technology and Cybersecurity Policy presso l'Ambasciata d'Italia negli Stati Uniti, sotto, **Rita Cucchiara**, Rettrice dell'Università di Modena e Reggio Emilia. A piè di pagina, da sinistra, Andrea Passarella, i quattro protagonisti all'epoca del primo collegamento (Stefano Trumpy, Gianfranco Capriz, Luciano Lenzini, Blasco Bonito) e il giornalista Alessio Jacona

come leva fondamentale per trasformare i risultati scientifici e le tecnologie di frontiera in applicazioni capaci di produrre innovazione concreta, crescita e sviluppo sostenibile.

Quarant'anni dopo, a Pisa si torna a discutere di **Internet**, non come oggetto di memoria, ma **come questione aperta di ricerca, innovazione e responsabilità.** L'anniversario ha offerto l'occasione per segnare un passaggio di prospettiva: dalla celebrazione di un'infrastruttura che ha connesso il mondo, alla riflessione sui nuovi modelli di Rete, sul futuro che verrà e su come governare oggi una tecnologia che incide su sicurezza, autonomia tecnologica, modelli industriali e assetti globali. **Una sfida che chiama in causa il ruolo della ricerca pubblica nel guidare l'evoluzione della Rete in modo consapevole e sostenibile.**



Da sinistra: **Alessandro Zavatta**, Presidente di QTI S.r.L, **Martina Ottavi**, Head of Quantum Communication Systems Solutions and Technologies presso Thales Alenia Space, **Marco Gori**, Professore presso l'Università di Siena, **Rita Cucchiara**, e **Alessio Jacona**

LUDOTECA DEL REGISTRO .IT
LABORATORI DI EDUCAZIONE DIGITALE NELLE SCUOLE



A partire dai primi mesi del nuovo anno, l'**offerta formativa della Ludoteca del Registro .it** per le scuole primarie si è focalizzata, come nei precedenti anni scolastici, sulle tematiche della **cittadinanza digitale**, proponendo laboratori basati sulla **web app Internetopoli.** Complessivamente, hanno partecipato alle attività **180 alunni e alunne**. Per quanto riguarda le scuole secondarie di primo grado, il tema privilegiato degli incontri organizzati dalla Ludoteca è stato la **cybersecurity**, introdotta e approfondita attraverso laboratori basati sul **videogioco educativo "Nabbovaldo e il ricatto dal cyberspazio".** Gli studenti e le studentesse a Pisa e provincia hanno raggiunto un totale di 335.



Da sinistra: **Beatrice Lami**, staff Ludoteca del Registro .it, **Giorgia Bassi**, referente del progetto Ludoteca del Registro .it

PROGETTI FORMAZIONE SCUOLA LAVORO

Nell'ambito della **formazione** rivolta agli **istituti secondari di secondo grado**, sono stati attivati **due progetti FSL** (Formazione Scuola Lavoro): "Cybersecurity4Teens" (CS4T) e il progetto "Educazione decisionale per le competenze digitali".

CS4T è un percorso formativo, proposto anche nei precedenti anni scolastici, di 8 ore in presenza, interamente **dedicato alla sicurezza informatica** (6 ore di introduzione teorica e 2 ore di esercitazione pratica), che prevede anche la partecipazione, come docente, di Ilaria Matteucci, ricercatrice dell'Unità Trust Security and Privacy dell'Istituto di informatica e telematica del Cnr (Cnr-lit). Quest'anno hanno aderito al progetto due classi terze dell'IIS "Fascetti-Da Vinci" di Pisa, con il quale è stata rinnovata anche la convenzione triennale per le attività di FSL.

Il progetto **"Educazione decisionale per le competenze digitali"** rappresenta una nuova proposta formativa della Ludoteca, ideata e realizzata in collaborazione con la società benefit Onoblo srl, specializzata in servizi e consulenza in ambito formativo, con un **focus sugli strumenti dell'educazione decisionale.** Obiettivo di questa proposta, che ha coinvolto una classe quarta del Liceo di Scienze umane "G. Carducci", è promuovere consapevolezza critica nell'uso di strumenti digitali (social media, app, piattaforme online, contenuti e informazioni online). Il progetto ha previsto anche una parte di formazione per il personale della Ludoteca, utile per acquisire nuove skill di metodologia didattica ed educazione decisionale, con l'obiettivo di rendere l'esperienza replicabile.



Giorgia Bassi

PARTECIPAZIONE A EVENTI E INIZIATIVE

Anche quest'anno la Ludoteca ha partecipato a **Fiera Didacta Italia 2026**, il più importante evento dedicato alla formazione e all'innovazione nel mondo della scuola, che si è svolto a Firenze dall'11 al 13 marzo.

L'11 marzo, nello stand del Cnr, un talk dedicato al divario di genere nelle **STEM** (Science, Technology, Engineering and Mathematics), con un focus sulla rubrica video **"Donne&Informatica"**, dedicata a figure di informatiche pioniere, poco conosciute o non valorizzate come avrebbero meritato.

Il 13 marzo si è svolto, invece, il workshop immersivo **"La piattaforma**



SuperCyberKids per la cybersecurity education", con l'obiettivo di presentare ai docenti il **progetto Erasmus Plus "SuperCyberKids"**, dedicato alla formazione e alla sensibilizzazione sulla sicurezza informatica.
I partecipanti hanno potuto esplorare la piattaforma web educativa del progetto, utilizzare i relativi strumenti e le risorse didattiche basate su un approccio di **"game based learning"**, oltre che simulare lo svolgimento di un "lesson plan" di approfondimento.
Il 24 marzo si è svolto l'evento **"Giocando e riflettendo impariamo il valore dei nostri dati personali"**, organizzato dall'Associazione Protezione Diritti e Libertà privacy APS, membro - come la Ludoteca - del**l'Advisory Board del Safer Internet Centre-Generazioni Connesse, Ministero Istruzione e Merito (MIM).** L'iniziativa, pensata per favorire il dialogo tra generazioni diverse e metterle a confronto si è articolata in due sessioni, una mattutina e una pomeridiana.
In quella mattutina, riservata alle classi (per un totale di 120 alunni) e ai docenti delle classi dell'Istituto secondario di primo grado "Sms Teresa Franchini", attraverso giochi e attività di gruppo, il pubblico ha potuto riflettere sull'importanza di tutelare i propri dati online.
La sessione pomeridiana è stata dedicata, invece, all'educazione alla sicurezza informatica, interpretata come dialogo costruttivo tra generazioni. A questo incontro, hanno partecipato alla tavola rotonda gli esperti e le esperte dell'Associazione Protezione Diritti e Libertà Privacy APS, della Ludoteca del Registro .it e Università Politecnica delle Marche.

Infine, il 25 marzo, **Ludoteca ed EURid hanno partecipato a "All digital weeks"**, una delle principali campagne di sensibilizzazione paneuropee sulle competenze digitali per l'inclusione, l'empowerment e l'occupazione: il seminario congiunto presso il Liceo scientifico "F. Buonarroti" (Pisa) è stata l'occasione per far conoscere a studenti e studentesse il mondo dei nomi a dominio, il ruolo dei Registri TLD, proponendo un focus su sicurezza informatica e hacking etico.

04

Anteprima
Statistiche
News
Approfondimenti
Eventi

I PARADOSSI DELLA REGOLAZIONE

Perché l'Europa è diventata una colonia digitale degli Stati Uniti e come evitare che lo resti nell'era dell'Intelligenza Artificiale

di **Franco Bernabè**

Keynote speech tenuto all'evento "40 anni di Internet in Italia" - Pisa, 30 aprile 2026, Area Territoriale di ricerca del CNR di Pisa

Internet di cui oggi ricordiamo il 40° anniversario del primo collegamento dell'Italia è diventata **la più importante infrastruttura del mondo moderno**. Il suo successo a partire dagli anni novanta non è solo il frutto di una serie di importanti innovazioni tecnologiche. È la conseguenza di un disegno politico visionario e ambizioso concepito da Al Gore e da Bill Clinton e perseguito con coerenza da tutte le amministrazioni successive.

Rispetto alle promesse iniziali, oggi appaiono in tutta evidenza non solo i benefici ma anche i problemi che la rivoluzione di internet ha prodotto: in termini di controllo sociale, di dipendenza, di sicurezza e di concentrazione della ricchezza. Tuttavia, mentre gli Stati Uniti hanno enormemente beneficiato sul piano geopolitico e commerciale della tecnologia, **per quasi quaranta anni l'Europa ha subito l'iniziativa americana e si trova oggi senza un vero presidio tecnologico autonomo. All'Europa non mancano certo le competenze tecnico scientifiche e imprenditoriali**



Franco Bernabè, Presidente del Consiglio di Amministrazione dell'Università di Trento e già AD di Telecom e ENI

per reggere il confronto ma il gap che si è creato è cosi profondo da essere difficilmente recuperabile.

Contrariamente ad una opinione diffusa non è stato l'eccesso di regolazione a penalizzare la crescita europea nel settore della tecnologia, ma esattamente il contrario. È stata l'assenza o l'inefficacia della regolamentazione europea prima della recente approvazione del Digital Services Act e del Digital Markets Act che ha permesso alle piattaforme americane di conquistare il mercato europeo realizzando una concentrazione di potere di mercato senza precedenti.

Non è stato l'eccesso di regolazione a penalizzare la crescita europea nel settore della tecnologia, ma esattamente il contrario

I **quattro elementi che hanno consentito il predominio americano in Europa** sono stati **l'accesso senza controllo ai dati personali degli europei** che hanno favorito la penetrazione sul mercato degli Hyperscalers della Silicon Valley, **l'immunità da responsabilità civili e penali delle piattaforme, la proliferazione di contenuti** che creano dipendenza e la **dottrina antitrust americana** che ha consentito operazioni di concentrazione inammissibili in Europa. Tutti questi fattori hanno decisamente aiutato le Big Tech americane, ma **l'Europa avrebbe potuto costruire i propri campioni digitali anche in presenza di quei vantaggi americani** se avesse avuto un mercato dei capitali integrato, un mercato digitale unico, una cultura aperta a sostenere il rischio imprenditoriale, una capacità avanzata di trasferimento tecnologico e appalti pubblici orientati all'innovazione. In quaranta anni su questi temi l'Europa ha fatto molto poco, la sfida di oggi è fare tesoro della esperienza e degli errori del passato ed evitare che all'alba di una nuova rivoluzione, quella dell'Intelligenza Artificiale, l'Europa arrivi impreparata.

Tutto parte dalla **intuizione originaria di Al Gore** agli inizi degli anni novanta di **diffondere internet promuovendone l'utilizzo commerciale** allora fortemente avversato dalla National Science Foundation, titolare dell'internet backbone.
Gore attribuiva alla rete una funzione civica e internazionale. Nelle sue parole, la Global Information Infrastructure doveva servire ad estendere conoscenza e prosperità, rafforzare la partecipazione democratica e rendere più difficile sopprimere la libertà d'espressione. Il processo di creazione degli Information Superhighways prese concretezza con la privatizzazione della rete posseduta dalla NSF nel 1995, e il Telecommunications Act del 1996 che smantellava la struttura fisica e regolamentare dei vecchi monopoli delle telecomunicazioni e apriva la strada alle nuove piattaforme della banda

larga che potevano agire senza vincoli regolatori.

Mentre gli Stati Uniti costruivano un sistema basato sull'autoregolamentazione, l'Europa seguiva una filosofia radicalmente diversa. **La Direttiva Europea sulla Protezione dei Dati 95/46/CE**, adottata nell'ottobre 1995 e divenuta pienamente applicabile il 24 ottobre 1998, all'articolo 25 **vietava il trasferimento di dati personali dai paesi membri dell'UE verso qualsiasi paese che non offrisse un livello di protezione "adeguato"**. Poiché gli Stati Uniti non soddisfacevano tale standard, **la prima cosa di cui gli americani si preoccuparono fu quello di fare accettare anche dall'Europa i principi che erano stati stabiliti negli USA**. Si arrivò così nel 2000 alla firma dell'**accordo di Safe Harbour** con il quale le aziende americane potevano dichiarare la propria conformità a principi di privacy derivati dalla Direttiva europea, e ottenere così il diritto a ricevere dati dall'UE. Le aziende che si autocertificavano venivano inserite in un registro pubblico tenuto dal Dipartimento del Commercio, e gli stati membri dell'UE erano obbligati a riconoscerle come "adeguate" ai sensi della regolamentazione europea.

Il coordinamento delle autorità nazionali europee per la privacy aveva ripetutamente avvertito, all'epoca, che **i principi erano troppo deboli, le eccezioni troppo ampie e l'enforcement troppo dipendente dall'autoregolamentazione**. Il difetto più grave era però di natura strutturale: **le leggi sulla sicurezza nazionale americana** — in particolare quelle che autorizzavano la sorveglianza di massa

Mentre gli Stati Uniti costruivano un sistema basato sull'autoregolamentazione, l'Europa seguiva una filosofia radicalmente diversa

da parte della NSA — **prevalevano su qualsiasi impegno Safe Harbour, rendendo i dati dei cittadini europei accessibili ai servizi di intelligence americani** senza alcun rimedio giuridico.

L'accordo sopravvisse fino al 6 ottobre **2015, quando la Corte di Giustizia dell'UE lo invalidò nella sentenza Schrems .vs Facebook Ireland** perché le pratiche di sorveglianza di massa americane di cui si erano registrati numerosi esempi erano incompatibili con i diritti fondamentali europei, e **i cittadini UE non disponevano di alcun rimedio giurisdizionale effettivo.**

Dopo l'invalidazione del Safe Harbour, la Commissione europea e gli Stati Uniti annunciarono il 2 febbraio 2016 un nuovo quadro per i trasferimenti transatlantici, il **Privacy Shield**, presentato come risposta ai rilievi della Corte. Ma in realtà **nemmeno questo risolveva i problemi sollevati da Schrems** che infatti riformulò il reclamo contro Facebook Ireland

sostenendo che, anche caduto il Safe Harbour, **i trasferimenti verso gli Stati Uniti restavano incompatibili con il diritto UE** perché il diritto e le pratiche USA non garantivano una protezione sufficiente contro l'accesso delle autorità pubbliche.

Anche questa volta la Corte dette ragione a Schrems invalidando Il Privacy Schield con la sentenza del 16 luglio 2020.
L'ulteriore risposta politica dell'UE fu il **Data Privacy Framework** del 2023: il 10 luglio 2023 la Commissione adottò una nuova decisione di adeguatezza affermando che gli Stati Uniti avevano introdotto garanzie vincolanti per limitare l'accesso dell'intelligence a quanto "necessario e proporzionato" e un nuovo meccanismo di ricorso per gli interessati europei. In sostanza, **Bruxelles tentò una terza architettura giuridica per preservare i flussi di dati**, mantenendo il modello dell'adeguatezza ma cercando di rispondere ai due difetti che avevano fatto cadere Safe Harbour e Privacy Shield, cioè sorveglianza e tutela giurisdizionale.

In realtà **Data Privacy Framework non impedisce all'intelligence americana di accedere ai dati personali dei cittadini europei**, comprese le comunicazioni, ma **pretende di limitarne l'accesso a quanto "necessario e proporzionato"** per la sicurezza nazionale e di sottoporlo a nuovi meccanismi di controllo e ricorso.

La criticità decisiva non è solo che i servizi americani possano accedere ai dati, ma che i diritti europei in materia di privacy e protezione dei dati non si trasformano automaticamente in pretese direttamente azionabili contro l'intelligence statunitense

Dal 1995 al 2018, le imprese americane hanno operato in Europa senza vincoli effettivi sulla raccolta dei dati personali e sulle conseguenti tecniche di profilazione

davanti a un giudice indipendente negli USA. Questo significa che **manca il momento chiave in cui un soggetto esterno e imparziale verifichi se la raccolta sia davvero necessaria, proporzionata e limitata al minimo indispensabile secondo lo standard europeo.**

Per quasi vent'anni — dalla nascita del web commerciale nel 1995 fino al 2018 — le imprese americane hanno quindi operato in Europa senza vincoli effettivi sulla raccolta dei dati personali e sulle conseguenti tecniche di profilazione. Le piattaforme hanno utilizzato le proprie condizioni d'uso come base contrattuale, sostenendo che l'utente accettando i termini di servizio acconsentisse implicitamente alla raccolta e al trattamento dei propri dati.

Il **Regolamento Generale sulla Protezione dei Dati** entrato in applicazione il 25 maggio 2018 **ha introdotto un cambio di paradigma ma oramai la situazione era compromessa**. Il risultato netto di questo percorso è che **le**

piattaforme americane hanno costruito il proprio vantaggio competitivo globale — database di profilazione con miliardi di profili, algoritmi di targeting addestrati su decenni di dati comportamentali, infrastrutture pubblicitarie integrate verticalmente in un periodo in cui non esistevano regole efficaci.

Il problema non è però solo il vantaggio competitivo derivante dall'accesso ai dati personali degli utenti ma anche il fatto che **alle piattaforme è stato consentito di utilizzare tecniche manipolatorie per creare dipendenza dai network.**

Per questo bisogna risalire ad un altro provvedimento varato dal congresso americano **La Section 230 del Communications Decency Act**, che è parte integrante del Telecommunications Act del 1996. Per effetto di questo provvedimento **i provider non sarebbero stati considerati "editori" né "distributori" del contenuto altrui**, dunque non soggetti a responsabilità civile o penale per esso. L'effetto fu immediato e trasformativo: le imprese tecnologiche poterono ospitare quantità illimitate di contenuti generati dagli utenti senza il rischio di finire in giudizio per ogni post diffamatorio, contenuto illecito o informazione falsa. I tribunali americani interpretarono la Section 230 in modo sempre più estensivo, esonerando le piattaforme non solo dalla responsabilità per contenuti terzi, ma anche per le scelte algoritmiche che determinavano quali contenuti amplificare. **Le piattaforme scoprirono presto che i contenuti emotivamente intensi** — rabbia, paura, indignazione, contenuti di dipendenza — **generavano il maggiore engagement, e quindi i maggiori ricavi pubblicitari**. Dal momento che nessuna norma le obbligava a moderare tale amplificazione, e che l'autoregolamentazione era esattamente il principio che Magaziner aveva codificato nel Framework del 1997, le imprese non solo tollerarono la tossicità ma la ingegnerizzarono deliberatamente nei propri prodotti.

Quando l'UE costruì il proprio regime di responsabilità delle piattaforme con la **Direttiva sul commercio elettronico 2000/31/CE** — adottata quattro anni dopo la Section 230 — scelse un approccio formalmente diverso ma sostanzialmente compatibile con quello americano. **La Direttiva esonera i provider di hosting dalla responsabilità purché non siano a conoscenza di contenuti illegali** o, una volta venuti a conoscenza, li rimuovano tempestivamente. Non introdusse obblighi proattivi di monitoraggio, non impose trasparenza algoritmica, non riconobbe la distinzione tra contenuto e design della piattaforma.
Il risultato fu che **le imprese americane operarono in Europa** sostanzialmente **alle stesse condizioni che avevano in patria**: protette da responsabilità per contenuti terzi, libere di progettare algoritmi di amplificazione senza obbligo di rendiconto, autorizzate ad autoregolarsi. Questa convergenza non fu casuale: il diritto europeo si sviluppò in parallelo alla Section 230, in un contesto in cui la liberalizzazione del commercio digitale era l'obiettivo condiviso da Washington e Bruxelles, e in cui l'accordo Safe Harbour del 2000 aveva già stabilito il principio che le imprese americane avrebbero operato in Europa secondo i propri standard interni.

L'UE iniziò a prendere consapevolezza del problema a partire dal 2016-2018, sull'onda dello scandalo Cambridge Analytica, delle accuse di manipolazione elettorale e delle pressioni politiche crescenti sulle piattaforme. Dopo anni di soft law e codici di condotta volontari **la Commissione europea cambiò strategia e nel dicembre 2020 presentò il Digital Services Act.** Il DSA, entrato pienamente in vigore per le piattaforme molto grandi nel 2023, introduce per la prima volta un sistema di responsabilità basato non sulla singola illiceità del contenuto ma sul rischio sistemico della piattaforma: le imprese devono valutare se la propria architettura, inclusi gli algoritmi di raccomandazione, produca effetti negativi sul discorso civico, sulla sicurezza pubblica, sui minori.

Questo cambiamento di paradigma ha prodotto una reazione durissima da parte americana. Nel 2024 le imprese tech USA hanno ricevuto dall'UE sanzioni complessive per oltre 3,8 miliardi di euro. La risposta dell'amministrazione Trump è stata sistematica: minacce di tariffe, pressioni diplomatiche, visti negati a funzionari europei coinvolti nell'enforcement del DSA, accuse di censura e attacchi all'ordinamento regolatorio europeo definito "orwelliano" dal Segretario di Stato Rubio.

Solo ora anche negli Stati Uniti, i tribunali stanno iniziando a distinguere tra immunità per il contenuto degli utenti — che rimane protetta dalla Section 230 — **e responsabilità per la condotta della piattaforma**, cioè per le scelte progettuali che amplificano contenuti tossici. I giudici dei casi contro Meta, YouTube, Snap e TikTok hanno riconosciuto che funzionalità come lo scroll infinito, la distribuzione algoritmica e i sistemi di reward rientrano nella sfera della condotta e non sono protette dalla Section 230. **Questa evoluzione giurisprudenziale americana, combinata con il DSA europeo, configura per la prima volta un doppio fronte di accountability sistemica per le piattaforme**, pur muovendo da tradizioni giuridiche profondamente diverse.

Veniamo all'ultimo fattore che ha favorito il sostanziale **monopolio delle piattaforme americane** e che assieme alla insufficiente disponibilità di capitale di rischio in Europa, ha impedito alle imprese tecnologiche europee di crescere fino a rappresentare un rischio sotto il profilo della concorrenza Le **differenze nella dottrina antitrust tra Stati Uniti ed Europa** è uno dei fattori strutturali più importanti nella **spiegazione del perché le grandi imprese tecnologiche siano tutte americane e non europee**. Fino agli anni Settanta, il diritto antitrust americano aveva una vocazione strutturalista: le grandi concentrazioni di potere di mercato erano considerate di per sé sospette, indipendentemente dall'effetto immediato sui prezzi. Il punto di svolta fu la pubblicazione nel 1978 del libro **"The Antitrust Paradox"** del giurista Robert Bork nel quale si sostiene che **l'unico obiettivo legittimo del diritto antitrust è quello di massimizzare il benessere del consumatore**, definito quasi esclusivamente attraverso prezzi, output ed efficienza produttiva. Se un'acquisizione o una pratica di mercato non aumenta i prezzi al consumatore nel breve periodo, essa è per

definizione accettabile, anche se riduce strutturalmente la concorrenza.
L'amministrazione Reagan recepì questa dottrina in modo organico e l'antitrust americano smise di chiedersi se un'impresa dominante stesse soffocando la concorrenza futura, e si limitò a verificare se i prezzi pagati dai consumatori nell'immediato fossero alti.

Il problema esplose nel settore tecnologico perché i servizi delle grandi piattaforme — Google Search, Facebook, Gmail, YouTube — **erano formalmente gratuiti per l'utente finale.** Il consumer welfare standard, misurato sul prezzo pagato dal consumatore, non rilevava alcun danno: il prezzo era zero. Così **Google poté acquisire DoubleClick nel 2008, YouTube nel 2006, Waze nel 2013, Nest nel 2014** — costruendo un sistema verticalmente integrato — senza che nessuna autorità americana bloccasse seriamente una singola operazione. **Facebook poté acquisire Instagram nel 2012 per 1 miliardo di dollari e WhatsApp nel 2014 per 19 miliardi,** eliminando i propri principali concorrenti emergenti senza ricevere opposizione antitrust. Il ragionamento implicito era sempre lo stesso: **i consumatori non pagano di più, dunque non c'è danno.**

Il diritto europeo della concorrenza muove da presupposti radicalmente diversi. Gli articoli 101 e 102 del TFUE proibiscono rispettivamente accordi anticoncorrenziali e abusi di posizione dominante, e quest'ultimo concetto è costruito in modo strutturale: un'impresa dominante ha la responsabilità di non distorcere la concorrenza anche con comportamenti che, se attuati da un'impresa non dominante, sarebbero leciti. La Commissione europea non deve dimostrare che i prezzi al consumatore siano aumentati: è sufficiente dimostrare che la condotta dell'impresa dominante esclude o penalizza i concorrenti e rafforza la posizione di mercato. Questo ha consentito all'Europa di multare Google per 8 miliardi di euro in tre procedimenti tra il 2017 e il 2019, di colpire Apple con 1,84 miliardi per le restrizioni nell'App Store, e di avviare procedimenti contro Amazon, Meta e Microsoft.

La Commissione europea deve dimostrare che la condotta dell'impresa dominante esclude o penalizza i concorrenti e rafforza la posizione di mercato

La combinazione di enforcement antitrust permissivo negli USA e mercato dei capitali europeo frammentato ha prodotto un meccanismo di drenaggio tecnologico dall'Europa verso gli USA. Le imprese tecnologiche americane hanno acquistato sistematicamente le startup europee più promettenti in fasi pre-IPO, usando la loro enorme liquidità generata proprio dalla mancata enforcement antitrust in patria — per operazioni che spesso sfuggivano anche alle soglie di notifica previste dalla normativa UE.

Il quadro è aggravato da un secondo fattore strutturale europeo: il mercato dei capitali frammentato e le differenze negli ordinamenti giuridici che comportano costi di compliance cumulativi che un'impresa americana non incontra mai all'interno del proprio mercato domestico. Prendendo atto che le tradizionali procedure antitrust — basate su indagini caso per caso, lunghe anni e con sanzioni irrogate solo ex post erano inadeguate per mercati tecnologici in cui il vantaggio competitivo si costruisce in mesi, **l'UE ha cambiato approccio con il Digital Markets Act del 2022**. Il DMA non aspetta di dimostrare un abuso: designa preventivamente le piattaforme dominanti come "gatekeeper" e impone loro **obblighi proattivi** — divieto di self-preferencing, apertura all'interoperabilità, obbligo di condivisione dei dati con terzi — a prescindere da qualsiasi accertamento di danno concreto.

La reazione americana è stata immediata: la pressione diplomatica dell'amministrazione Trump contro il DSA e il DMA, le accuse di discriminazione verso imprese americane, le minacce di tariffe — tutto ciò configura il conflitto digitale transatlantico non come un'astratta disputa giuridica, ma come uno scontro di sovranità economica in cui il diritto della concorrenza è diventato uno strumento di geopolitica tecnologica.

Il conflitto digitale tra UE e Stati Uniti è ormai uno scontro di sovranità economica in cui il diritto della concorrenza è diventato uno strumento di geopolitica tecnologica

Come negli anni Novanta con Internet, **la rivoluzione dell'IA riproduce oggi lo stesso schema di fondo**: gli Stati Uniti costruiscono la tecnologia e il mercato lasciando che il settore privato corra senza vincoli; l'Europa risponde con la regolazione. **L'AI Act del 2024 è ciò che il GDPR è stato per i dati personali**: un tentativo di fissare standard di sicurezza, trasparenza e accountability prima che il mercato si consolidi in modo irreversibile. Il rischio simmetrico è lo stesso: **la regolazione arriva quando il vantaggio competitivo americano è già strutturalmente consolidato**, e diventa così un ulteriore ostacolo per chi deve recuperare un ritardo.

Qui però il parallelo con Internet si ferma. Negli anni Novanta il confronto era bilaterale: USA da un lato, Europa dall'altro, con Washington che dettava le regole del gioco e Bruxelles che cercava di imporre le proprie. **Oggi il campo è tripolare e la geometria del potere è radicalmente diversa.**
La Cina non è un attore che subisce la regolazione come l'Europa: ha una strategia nazionale di AI che copre l'intero stack tecnologico — ricerca di base, semiconduttori, modelli fondazionali, applicazioni verticali, 6G, quantum. Soprattutto, la Cina ha adottato una strategia open source — con DeepSeek, Qwen, Alibaba e altri — che ha una

funzione geopolitica precisa: abbassare le barriere di accesso alla tecnologia AI per i paesi che vogliono ridurre la dipendenza dagli USA, guadagnare quote di mercato globali e costruire ecosistemi dipendenti dall'infrastruttura cinese. DeepSeek R1 costa 20-30 volte meno dei modelli americani equivalenti, il che lo rende accessibile a startup europee con limitata capacità di spesa.

L'Europa si trova dunque in un dilemma classico: usare la tecnologia cinese per ridurre la dipendenza americana rischia di creare una dipendenza cinese altrettanto o più pericolosa. La risposta più organica e autorevole è contenuta nel **Rapporto Draghi del** settembre **2024**, che ha diagnosticato il problema con una chiarezza: l'Europa rischia di perdere la sovranità tecnologica non per mancanza di talento ma per mancanza di scala, capitali e coordinamento.

Draghi raccomanda di aprire i supercomputer pubblici europei a un modello federato pubblico-privato che metta la potenza di calcolo a disposizione delle PMI e delle startup europee per training e fine-tuning dei modelli, così da colmare il divario di accesso all'infrastruttura rispetto agli operatori americani. Propone inoltre una legge ad hoc per armonizzare i requisiti di architettura cloud, coordinare gli acquisti pubblici e creare un quadro unico europeo per il "computing capital" accessibile alle imprese innovative. Questo fornirebbe alle startup europee un'alternativa reale ai cloud provider americani — AWS, Azure, Google Cloud — che oggi controllano oltre l'80% del mercato europeo del cloud.

Rapporto Draghi 2024: l'Europa rischia di perdere la sovranità tecnologica non per mancanza di talento ma per mancanza di scala, capitali e coordinamento

Nell'era dell'Intelligenza Artificiale l'UE possiede vantaggi competitivi reali in settori come manifattura avanzata, farmaceutica, energia, automotive, agroalimentare e servizi finanziari. per sfruttare questi vantaggi serve un piano che finanzi lo sviluppo di modelli AI specializzati in questi settori, costruiti su dati europei e protetti dall'enforcement antitrust. **Per creare valore europeo nell'AI** non **serve** competere frontalmente sui modelli fondazionali generalisti — dove il vantaggio americano e cinese è strutturale — ma **eccellere nelle applicazioni verticali dove i dati, il know-how industriale e la regolazione europea sono un asset.** Rispetto al mondo di internet, nell'AI la posta in gioco è la competitività industriale diretta, non solo la protezione dei diritti individuali. Se l'Europa non riuscirà a sviluppare il proprio modello di sviluppo della tecnologia AI il rischio è che l'industria europea — manifattura, sanità, energia, finanza — si trovi a usare AI americana o cinese per i propri processi produttivi critici perdendo tutto il vantaggio competitivo che ancora possiede.

ANALISI DEI RINNOVI DEI DOMINI: IL CONTRIBUTO DEL .IT ALLA TASK FORCE CENTR

di **Daniele Sartiano**

Il rinnovo di un nome a dominio non è soltanto un passaggio amministrativo, ma è anche un **segnale di continuità**: ci racconta se un dominio mantiene nel tempo il proprio valore, se resta collegato a un progetto, a un servizio, a un'identità digitale o a una presenza online ancora rilevante.
Per i registri e per i Registrar, leggere questi segnali significa comprendere con precisione l'evoluzione del mercato, interpretare la stabilità dei portafogli domini e individuare, con anticipo, le aree in cui i domini sono più esposti al mancato rinnovo. In questo senso, il rinnovo diventa una chiave di lettura del ciclo di vita dei nomi a dominio e del valore percepito da parte dei registranti.

Da questa esigenza nasce la **Benchmarking Renewal Indicators Task Force promossa da Centr** (Council of European National Top-Level Domain Registries), avviata nel maggio 2025 durante il Centr Jamboree di Lione.
Alla task force hanno partecipato dieci registri ccTLD (.at, .be, .de, .ie, .it, .nl, .no, .nu, .nz, .uk), con l'obiettivo di definire una metodologia condivisa per l'analisi dei rinnovi dei nomi a dominio. Lo studio ha preso in esame circa **40 milioni di domini in scadenza nel 2024**, analizzando gli indicatori un mese prima della data di expiry, così da osservare il dominio nel momento più vicino alla decisione di rinnovo. Ogni registro ha condotto localmente le elaborazioni sui propri dati, condividendo successivamente soltanto risultati aggregati.

Alla task force hanno partecipato dieci registri ccTLD (.at, .be, .de, .ie, .it, .nl, .no, .nu, .nz, .uk), con l'obiettivo di definire una metodologia condivisa per l'analisi dei rinnovi dei nomi a dominio

Per il Registro .it, i segnali risultati maggiormente correlati al rinnovo sono stati l'età del dominio, l'età e la categoria del registrante.

Il Registro .it ha contribuito a questo percorso portando il proprio caso di studio all'interno di un confronto più ampio tra registri. Questo lavoro ha permesso di identificare e **mettere a fattor comune indicatori, codice e scelte di analisi**, mantenendo al tempo stesso un **approccio "privacy-first"**, senza condividere dati sensibili dei registranti.

Il lavoro della task force è sintetizzato nell'articolo disponibile nel blog di CENTR **Analysing domain name renewals across ccTLDs**, che ne ripercorre i principali risultati, concentrandosi sul caso del Registro .it e sui trend più significativi osservati nei dati italiani.

OBIETTIVO: INDICATORI E DINAMICHE DI RINNOVO DEI DOMINI

L'obiettivo principale del lavoro è stato **individuare gli indicatori maggiormente associati al rinnovo di un nome a dominio**, così da comprendere quali segnali consentano di distinguere i domini più stabili da quelli più esposti al rischio di mancato rinnovo.
La task force ha quindi concentrato l'analisi su una domanda centrale: **quali caratteristiche del nome a dominio, e dei dati a esso correlati, risultano associate al rinnovo?** Rispondere a questo quesito ha permesso di identificare gli indicatori più informativi, che potrebbero costituire la base per strumenti in grado di stimare la probabilità di rinnovo e supportare i Registrar nell'analisi del proprio portafoglio domini.

IL WORKFLOW DELL'ANALISI

Il lavoro è partito da una ricognizione degli indicatori già utilizzati o ritenuti utili dai registri partecipanti. Questa prima fase ha permesso di mettere a confronto esperienze e approcci diversi, e di capire quali informazioni fossero disponibili in modo sufficientemente omogeneo nei vari contesti nazionali. Infatti, il processo di rinnovo dei nomi a dominio può variare da un ccTLD all'altro, e proprio per questo armonizzare gli indicatori e arrivare a una loro definizione condivisa non è stato immediato.

È stato definito un set comune di indicatori, pensato non come un elenco astratto di variabili, ma come una base utile al confronto dei risultati tra registri

A partire da questa analisi è stato definito un set comune di indicatori, pensato non come un elenco astratto di variabili, ma come una base utile al confronto dei risultati tra registri. Gli **indicatori individuati** coprono, ad

alto livello, le seguenti aree:

- **caratteristiche del nome a dominio**, come lunghezza e presenza di numeri;
- **storia della registrazione**, inclusi età del dominio, eventuali trasferimenti recenti tra Registrar e casi di registrazione successiva a un rilascio;
- **profilo del registrante**, considerando anzianità, numerosità del portafoglio domini e localizzazione rispetto al Paese del ccTLD;
- **categoria del registrante**, distinguendo, per esempio, persone fisiche, aziende e altre tipologie di soggetti;
- **variabili tecniche e di utilizzo**, come la presenza di record MX, lo stato rilevato tramite crawling, il livello di utilizzo web e la **magnitudine DNS**;
- **contesto del Registrar**, con particolare attenzione al modello di business dichiarato o ricostruito tramite classificazioni condivise.

Ciascun registro ha poi elaborato localmente i propri dati, calcolando gli indicatori secondo le definizioni concordate e **riconducendoli a uno schema comune**. Il confronto è avvenuto esclusivamente sui **risultati aggregati** e non sui dati grezzi: **una scelta che ha reso possibile lavorare insieme senza trasferire informazioni sensibili sui registranti.**
Il percorso di analisi ha previsto tre momenti principali: una **prima lettura** descrittiva dei segnali, un **modello statistico** per valutarli congiuntamente e, infine, un **approfondimento interpretativo** sui risultati emersi.
L'evoluzione naturale di questo lavoro è la possibile trasformazione del processo di analisi in uno strumento operativo, con **score di rinnovo o segnali di rischio messi a disposizione dei Registrar anche tramite API** (Application Programming Interface) così da permettere l'integrazione nei propri sistemi.

Dal benchmarker CENTR al caso .it



DATI, METODO E PRIVACY

L'analisi, in particolare, ha preso in esame i domini la cui scadenza era prevista nel corso del 2024. Gli indicatori sono stati misurati con una finestra temporale di un mese rispetto alla scadenza: così da fotografare lo stato del dominio, e dei dati relativi (ad esempio il registrante) quando l'esito del rinnovo era ormai vicino.

In particolare **il Registro .it ha costruito una pipeline di estrazione e calcolo dei dati** coerente con lo schema condiviso e definito dalla task force. L'obiettivo era **rendere confrontabili i risultati, pur partendo da basi dati e strutture informative differenti.**
Un elemento centrale del progetto è stato l'approccio "privacy-first". Ogni registro ha eseguito le analisi nel proprio perimetro, sui propri dati, condividendo con la task force soltanto risultati aggregati. La comparabilità non deriva quindi dalla centralizzazione dei dataset, ma dall'allineamento delle definizioni, delle trasformazioni e delle misure prodotte.
La disponibilità degli indicatori non è stata identica per tutti i registri. Per questo **il framework è stato pensato in modo flessibile,** così da permettere la partecipazione anche in presenza di variabili mancanti, **mantenendo al tempo stesso una base metodologica comune.**

DAGLI INDICATORI AL MODELLO STATISTICO

Per interpretare i risultati emersi, la task force ha seguito un percorso in più passaggi.
Inizialmente, è stato utilizzato il **Cramer's V**, per osservare un indicatore alla volta e misurare quanto fosse associato al rinnovo. Questa prima fase ha permesso di **individuare rapidamente i segnali più evidenti e di confrontare tra loro indicatori diversi, come l'età del dominio, l'età o la categoria del registrante.**
Successivamente è stata applicata una **regressione logistica**, cioè un modello statistico che consente di **guardare più indicatori insieme**. Questo passaggio è importante perché **alcuni segnali possono essere collegati tra loro**: ad esempio, i domini più longevi spesso appartengono anche a registranti presenti da più tempo nel registro o con un portafoglio di domini più ampio. La regressione aiuta quindi a capire quali indicatori restano rilevanti anche quando vengono considerati insieme agli altri.
Per rendere i risultati del modello più chiari, la regressione è stata poi interpretata attraverso due letture complementari: gli **"odds ratio",** utili per capire la direzione e la forza dell'associazione, e le probabilità marginali, più immediate per leggere il risultato in termini di probabilità di rinnovo.

I domini più longevi spesso appartengono anche a registranti presenti da più tempo nel registro o con un portafoglio di domini più ampio

Il percorso tecnico può quindi essere così riassunto:

- **Cramer's V**: guarda un indicatore alla volta e misura quanto è associato al rinnovo.
- **Regressione logistica**: guarda più indicatori insieme e mostra quali

segnali restano rilevanti anche in presenza degli altri.

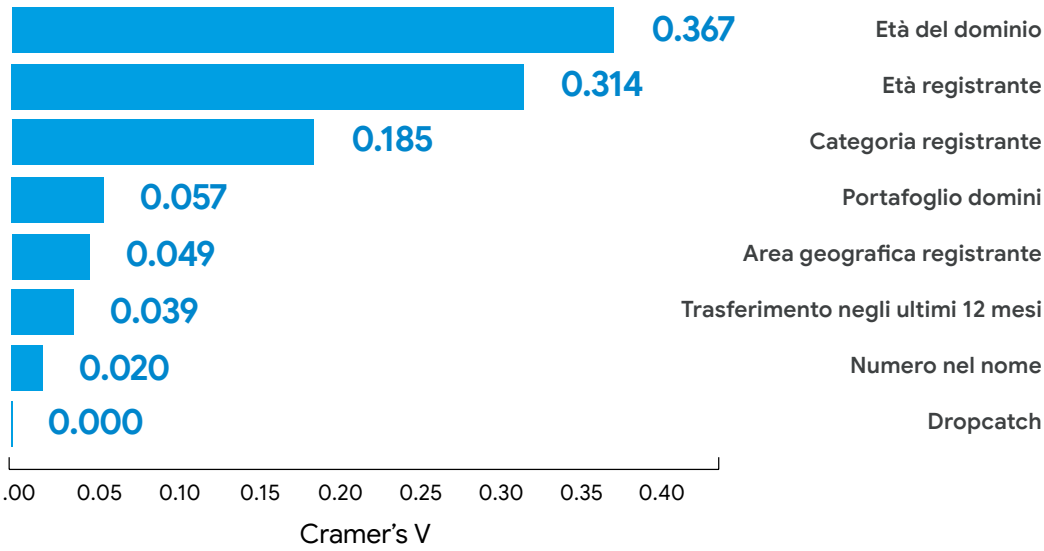
- **Odds ratio**: esprime in modo tecnico l'effetto stimato dalla regressione. Valori superiori a 1 indicano una relazione positiva con il rinnovo, mentre valori inferiori a 1 indicano una relazione negativa.
- **Probabilità marginali**: traducono le predizioni del modello in una forma più leggibile, mostrando come cambia la probabilità attesa di rinnovo al variare di alcuni indicatori chiave.

In questo modo, l'analisi mantiene una base statistica solida, ma resta leggibile anche dal punto di vista operativo: prima individua i segnali più forti, poi verifica come si comportano quando vengono valutati nel loro insieme.

I PRINCIPALI SEGNALI DI RINNOVO NEL .IT

Nel **caso .it**, i risultati mostrano una struttura chiara: **la storia del dominio e la storia del registrante sono i segnali più informativi**. Non tutti gli indicatori contribuiscono allo stesso modo: alcuni descrivono dimensioni utili, ma deboli, altri, invece, emergono con maggiore continuità sia nella lettura descrittiva sia nel modello statistico.

.it: segnali associati al rinnovo

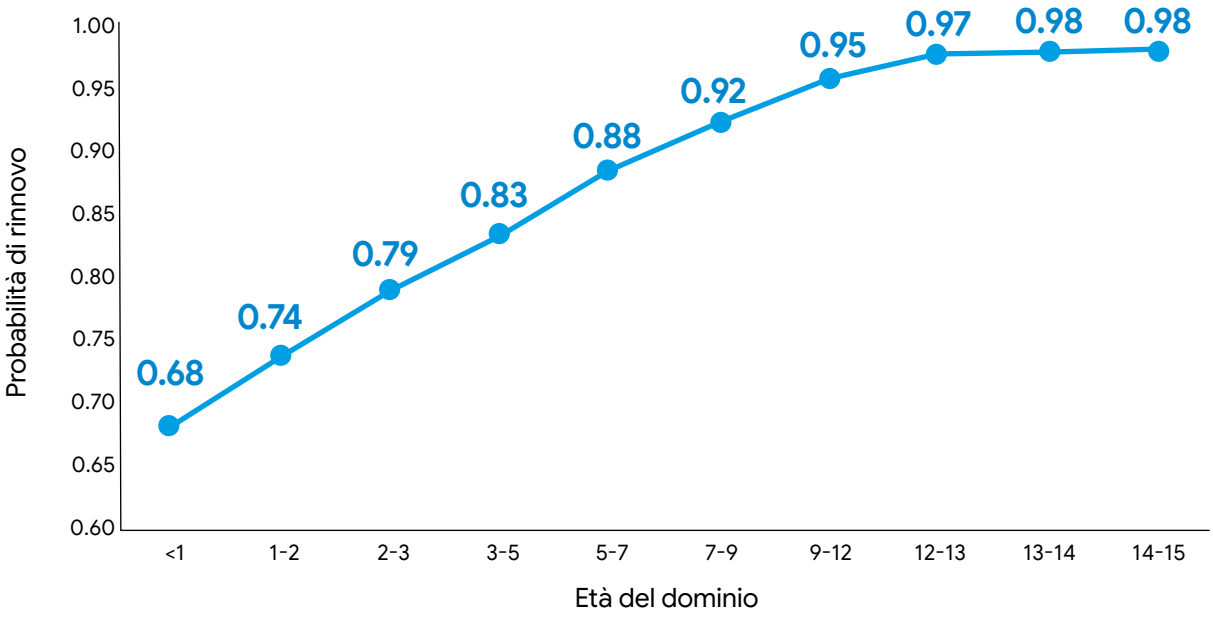


Il primo elemento che emerge è l'**età del dominio**, che nell'analisi descrittiva risulta l'indicatore **maggiormente associato all'esito del rinnovo**. A seguire si collocano l'**età e la categoria del registrante**, mentre gli altri indicatori hanno un peso più contenuto.

Il risultato è coerente anche con una lettura intuitiva del ciclo di vita dei domini: **un dominio registrato da più tempo tende più spesso a essere associato a un'attività, a un'identità digitale, a servizi tecnici o a relazioni**

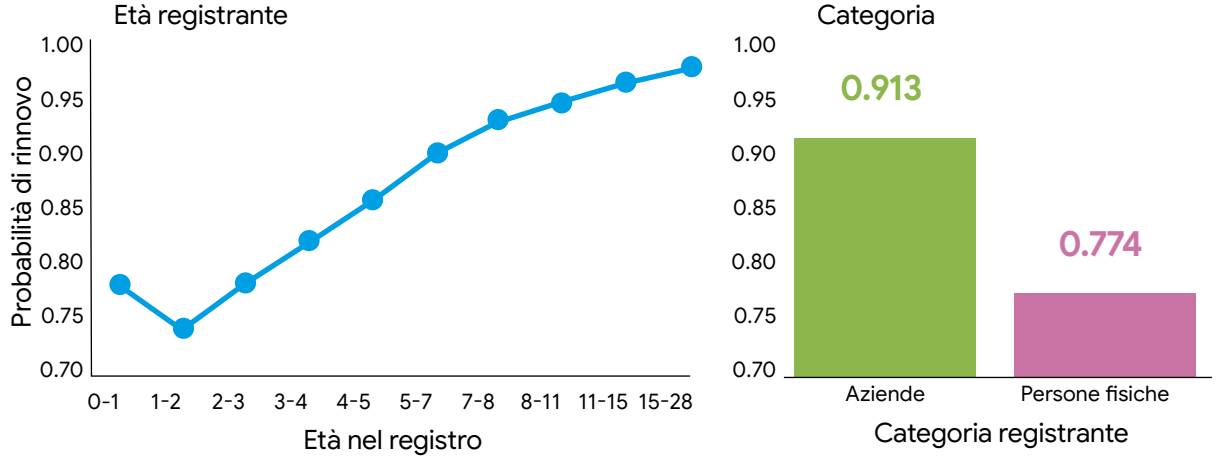
già consolidate. In questi casi, il mancato rinnovo può comportare un costo maggiore, non solo economico ma anche organizzativo e reputazionale. Al contrario, **i domini più giovani possono essere più fragili**, considerato che sperimentazioni, progetti non ancora maturi o registrazioni occasionali hanno una probabilità più alta di non proseguire nel tempo.

.it: rinnovo per età del dominio



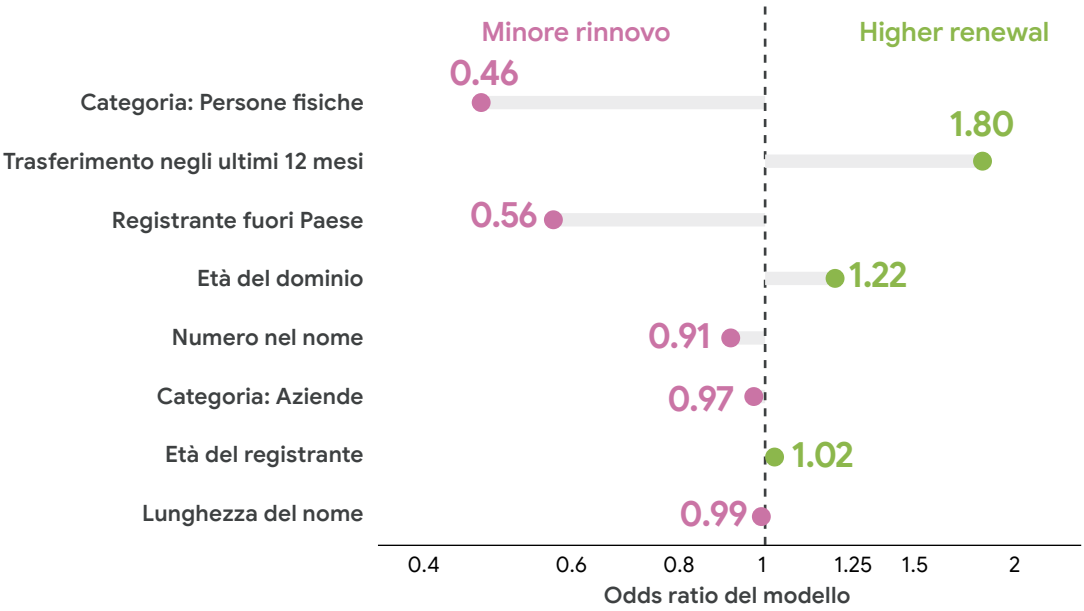
Le probabilità marginali stimate confermano questa dinamica. Il risultato è molto chiaro: **più aumenta l'età del dominio, più cresce la probabilità di rinnovo.**

.it: ruolo del registrante



Anche la storia del registrante ha un ruolo rilevante. **Un registrante presente da più tempo nel registro può indicare un rapporto più stabile con il dominio e**, più in generale, **con la gestione della propria presenza online**. Non significa che l'anzianità determini il rinnovo, ma è un indicatore di continuità nei comportamenti.
Non tutte le tipologie di registrante mostrano lo stesso comportamento. La categoria del registrante aggiunge un'ulteriore dimensione interpretativa: **nel .it, i domini intestati ad aziende presentano una probabilità di rinnovo più alta, rispetto a quelli intestati a persone fisiche.**
Questa differenza può riflettere usi diversi del dominio.
Per un'**impresa**, un nome a dominio è spesso parte integrante dell'identità digitale, della comunicazione, della posta elettronica, dell'e-commerce o delle relazioni con clienti e fornitori. Per una **persona fisica,** invece, il dominio è più spesso collegato a esigenze individuali, temporanee o sperimentali. Anche in questo caso, il dato non va letto in termini causali, ma come un segnale utile a comprendere la diversa stabilità dei profili osservati.

.it: direzione dei segnali del modello



Il grafico mostra alcuni effetti stimati dal modello statistico. I valori sopra 1 indicano segnali associati a una maggiore probabilità di rinnovo, quelli sotto 1 segnali associati a una probabilità minore. La lettura è diversa da Cramer's V: qui gli indicatori sono valutati insieme, non uno alla volta.

I trasferimenti tra Registrar risultano associati positivamente al rinnovo. Questo può indicare che un trasferimento recente è spesso legato a una gestione attiva del dominio, anche se l'effetto può variare tra mercati e politiche commerciali.
Altri indicatori mostrano un'associazione negativa. La presenza di numeri nel nome ha un effetto più contenuto, mentre il fatto che il registrante non risulti localizzato nel Paese di riferimento è associato a

una minore propensione al rinnovo. Quest'ultimo risultato suggerisce che **il radicamento territoriale può avere un ruolo nella continuità del dominio**, pur richiedendo cautela nell'interpretazione.
Nel complesso, il caso .it restituisce un quadro coerente: i domini più maturi e associati a registranti con una storia più lunga nel registro mostrano una maggiore probabilità di rinnovo, mentre i domini più giovani, o caratterizzati da segnali minori di radicamento, sono più soggetti al mancato rinnovo.
I risultati mostrano, inoltre, una buona coerenza tra lettura descrittiva e modello statistico: i segnali che emergono nella prima fase dell'analisi restano rilevanti anche quando vengono valutati insieme agli altri indicatori.
È comunque importante ricordare che gli indicatori descrivono associazioni statistiche e non rapporti di causa-effetto.

DAI DATI AGLI STRUMENTI PER I REGISTRAR

L'evoluzione naturale di questo lavoro è lo **sviluppo di strumenti operativi per l'analisi del rinnovo.** Gli indicatori individuati nello studio costituiscono la base per sviluppare sistemi in grado di **stimare**, in prossimità della scadenza, **la probabilità di rinnovo di un nome a dominio.**
Per i Registrar, strumenti di questo tipo potrebbero offrire un supporto concreto nella gestione del portafoglio domini: individuare domini più fragili, interpretare meglio i pattern di rinnovo, definire azioni mirate e integrare gli indicatori nei propri sistemi interni. L'integrazione tramite API permetterebbe, inoltre, di inserire queste analisi direttamente nei flussi operativi, consentendo ai Registrar di monitorare i domini di propria competenza in prossimità della scadenza.

Per i Registrar, lo sviluppo di strumenti operativi per l'analisi del rinnovo potrebbe offrire un supporto concreto nella gestione del portafoglio domini

Il rinnovo dei nomi a dominio rappresenta una lente preziosa per osservare stabilità, continuità e valore percepito della presenza online. Nel caso .it, l'analisi mostra che alcuni segnali risultano particolarmente informativi, confermando come la **storia del dominio e del registrante** contribuiscano in modo significativo alla **continuità della registrazione nel tempo.**
Il contributo del Registro .it si inserisce in un percorso più ampio di collaborazione tecnica in ambito Centr. La task force ha dimostrato che registri diversi possono affrontare un tema comune condividendo metodi, indicatori e strumenti, senza rinunciare alla protezione dei dati.
Ne emerge un modello di lavoro concreto: partire dai dati, costruire segnali comparabili e trasformare l'analisi in conoscenza utile per registri, Registrar e comunità dei ccTLD.

DALL'AI ALLA NIS2: LE SFIDE DEL DIGITALE PER LE IMPRESE NELLE DIRETTE LINKEDIN DEL REGISTRO .IT

di **Chiara Spinelli**

Uno spazio di confronto con ospiti noti e riconosciuti nel panorama nazionale sui grandi cambiamenti del digitale, dall'intelligenza artificiale alle sfide della cybersecurity: il **ciclo di dirette LinkedIn** organizzate dal Registro .it è entrato nel vivo nei primi mesi dell'anno con i nuovi appuntamenti, sempre condotti dal giornalista Massimo Fellini.

Dopo le puntate di ottobre e dicembre, incentrate rispettivamente sui temi dell'identità online e all'internazionalizzazione, il ciclo di incontri è proseguito affrontando **tre temi che oggi incidono direttamente sulla competitività delle imprese: l'AI per i siti web e il marketing, le sfide del digitale per il turismo e la direttiva NIS2 sulla cybersecurity**.
Come nelle puntate precedenti, il format ha mantenuto un taglio divulgativo ma concreto, alternando riflessioni strategiche ed esempi pratici. Le dirette rimangono ovviamente a disposizione non solo sulla pagina LinkedIn del Registro, ma anche su YouTube, come strumenti che speriamo rimarranno utili per una riflessione informata su questi temi anche nei mesi a venire.



AI PER I SITI DELLE PMI: PRODUTTIVITÀ, CONTENUTI E NUOVI MODELLI DI RICERCA

La terza diretta LinkedIn del ciclo, andata in onda il 21 gennaio con il titolo **"AI per i siti delle PMI: come migliorare produttività e marketing con strumenti smart"**, ha affrontato l'impatto dell'intelligenza artificiale sulle strategie di comunicazione delle imprese. Ospite della puntata è stato **Raffaele Gaito**, *growth coach*, formatore e divulgatore sui temi del marketing e dell'innovazione digitale.

L'AI sta rapidamente cambiando il modo in cui le aziende producono contenuti, organizzano il lavoro e costruiscono la propria presenza online. Ma l'intelligenza artificiale viene oggi percepita da molte PMI come uno strumento ancora da capire, con dubbi legati ai costi, alla formazione interna e alla reale capacità di integrare questo strumento nei processi aziendali.

Gaito ha evidenziato come il vero valore dell'AI risieda nella possibilità di migliorare la qualità del lavoro e accrescere la produttività.

Secondo Gaito, l'AI non può sostituire completamente competenze, visione strategica e autenticità, ma grazie ai suoi strumenti (dalla scrittura di testi per il web all'analisi dei dati, passando per la generazione di idee creative e la gestione dei flussi di lavoro) può aiutare le imprese a velocizzare attività ripetitive e a concentrarsi maggiormente sugli aspetti strategici del business. E se in passato il sito web di un'azienda era pensato principalmente per essere trovato dai motori di ricerca tradizionali, oggi deve essere progettato anche per dialogare con gli assistenti AI e con i nuovi sistemi di ricerca conversazionale. Il mondo della GEO (Generative Engine Optimization) è ancora tutto da esplorare, ma quello di cui siamo certi, secondo Gaito, è che **la centralità di un sito web non si perderà.** Contenuti chiari, strutturati, autorevoli e aggiornati restano elementi centrali, non solo per la SEO classica, ma anche per la visibilità all'interno delle risposte generate da piattaforme come ChatGPT o Gemini.

L'AI non può sostituire completamente competenze, visione strategica e autenticità, ma - grazie ai suoi strumenti - può aiutare le imprese a velocizzare attività ripetitive e a concentrarsi sugli aspetti strategici del business



TURISMO DIGITALE: QUANDO L'ALGORITMO DIVENTA IL NUOVO AGENTE DI VIAGGIO

La diretta del 17 febbraio, dal titolo **"Il nuovo agente di viaggio è un algoritmo: ma il biglietto per la fiducia resta .it"**, ha spostato l'attenzione sul settore turistico, uno dei comparti maggiormente trasformati dall'uso dei dati e dell'intelligenza artificiale. Ospite dell'incontro è stato **Mirko Lalli,** Founder e CEO di The Data Appeal Company, azienda specializzata nell'analisi dei dati turistici e della reputazione online.

Mirko Lalli ha ricordato come **gli algoritmi condizionano da anni il turismo,**

influenzando ogni fase dell'esperienza di viaggio, dalla scelta della destinazione alla prenotazione, fino ai suggerimenti personalizzati durante il soggiorno. Ma **l'AI generativa porta una rivoluzione ancora più disruptive: cambia il modo in cui le persone cercano informazioni e costruiscono fiducia online**. Sempre più utenti si affidano alla conversazione con i chatbot per decidere dove andare, cosa prenotare e quali esperienze vivere. Come Gaito, anche Lalli ha sottolineato che in questo scenario di cambiamenti **il sito web proprietario continua comunque ad avere un ruolo centrale**: rappresenta il luogo in cui aziende, strutture ricettive e destinazioni possono consolidare al meglio la propria reputazione digitale, farsi trovare e farsi scegliere.
Il valore percepito di una struttura turistica si costruisce attraverso dati, recensioni, commenti e conversazioni online, elementi che gli algoritmi elaborano continuamente per determinare visibilità e posizionamento. Per questo motivo, anche nell'era dei chatbot, per Lalli **presidiare la propria presenza digitale non significa soltanto "esserci", ma governare in modo coerente contenuti, comunicazione e credibilità**. L'AI non cancella il bisogno di fiducia, ma anzi rende ancora più importante avere una presenza digitale riconoscibile e autorevole, e il dominio .it è un segnale di autenticità, prossimità territoriale e affidabilità.



Sempre più utenti si affidano alla conversazione con i chatbot per decidere dove andare, cosa prenotare e quali esperienze vivere

NIS2 E CYBERSECURITY: LA SICUREZZA DIVENTA UNA RESPONSABILITÀ STRATEGICA

La quinta e ultima diretta del ciclo, andata in onda il 25 marzo con il titolo **"Cybersecurity, con la NIS2 cambia tutto: maggiori responsabilità, a partire dai CDA"**, ha affrontato uno dei temi più urgenti per imprese e organizzazioni digitali: **la sicurezza informatica e l'applicazione della direttiva NIS2.** L'incontro ha visto la partecipazione di **Ernesto Belisario**, avvocato ed esperto di diritto dell'innovazione e AI, **Donato Molino**, presidente del Comitato di Indirizzo del Registro .it (CIR) e di AssoTLD, e **Valentina Amenta**, responsabile dell'Unità aspetti legali e contenzioso del Registro .it.

Come ha evidenziato Ernesto Belisario, **la direttiva europea NIS2 rappresenta un cambio di paradigma nella gestione della cybersecurity**, una evoluzione necessaria alla luce dell'aumento degli attacchi informatici e dei costi legati ai "data breach". **Serve un approccio più strutturato alla sicurezza che coinvolga direttamente anche gli organi amministrativi delle aziende**, perché la direttiva introduce obblighi precisi non solo sul piano tecnico, ma anche su quello della governance: i CdA saranno chiamati ad approvare le misure di sicurezza, supervisionarne l'attuazione e promuovere percorsi di formazione interna.

Tra gli aspetti più innovativi della normativa (anche rispetto alla NIS1) c'è anche il tema della **supply chain security**, sottolineato da Valentina Amenta. La sicurezza non riguarda più soltanto la singola organizzazione, ma l'intero ecosistema digitale in cui opera: fornitori, partner e infrastrutture diventano parte integrante della gestione del rischio. Le aziende devono quindi introdurre controlli, verifiche e requisiti di sicurezza lungo tutta la catena del valore, adottando un approccio più consapevole e proattivo. Una presa di coscienza mai immaginata prima in modo così capillare.

La direttiva impone inoltre **tempi molto rapidi per la notifica degli incidenti informatici** e introduce **un sistema sanzionatorio significativo**, elementi che richiedono strutture organizzative più mature e processi ben definiti. In questo contesto, come ha spiegato Donato Molino, molte imprese stanno passando da una prima fase di adempimenti formali a un lavoro più operativo, fatto di analisi dei rischi, definizione di procedure e implementazione di misure concrete di continuità operativa e "disaster recovery". Se per le grandi aziende integrare le procedure della NIS2 è meno problematico e può garantire anche un maggior consolidamento sul mercato, **per le PMI non è semplice confrontarsi con la carenza di competenze e le risorse limitate** e la scadenza di ottobre rischia di essere vissuta come molto problematica. Proprio per questo, Molino ha sottolineato **l'importanza della collaborazione tra istituzioni, associazioni di categoria e operatori del settore per accompagnare le aziende nel percorso di adeguamento**, ricordando anche il ruolo sempre più centrale dei Registrar, oggi considerati soggetti essenziali per la sicurezza delle infrastrutture digitali e per la corretta gestione dei dati associati ai nomi a dominio.

La sicurezza non riguarda più soltanto la singola organizzazione, ma l'intero ecosistema digitale in cui opera

Il messaggio conclusivo emerso dal confronto è chiaro: la NIS2 non può essere interpretata come un semplice obbligo burocratico, ma come un investimento strategico destinato a rafforzare resilienza, affidabilità e competitività del sistema digitale italiano.

EDUCARE ALLA CYBERSICUREZZA: IN ARRIVO "NEL MEZZO DEI MAGHI", IL NUOVO GIOCO DELLA LUDOTECA

di **Giorgia Bassi**

L'obiettivo della Ludoteca del Registro .it è quello di diffondere la "cultura digitale" tra le giovani generazioni.

Ciò comporta la ricerca costante di metodologie e strumenti didattici innovativi, capaci di mantenere viva l'attenzione di bambini e bambine. Per loro, infatti, **la dimensione online rappresenta un'estensione naturale della quotidianità** e, proprio per questo, non è percepita come qualcosa che richieda spiegazioni o interventi educativi.

Da qui la necessità di **ideare strumenti basati sul gioco** che attivino modalità di apprendimento attivo ed esperienziale, in grado di veicolare competenze specifiche ma anche





trasversali, come - ad esempio - il pensiero critico e la capacità di lavorare in gruppo.

"NEL MEZZO DEI MAGHI"

Su queste basi è nata l'idea di creare un nuovo gioco didattico, intitolato "Nel Mezzo dei Maghi", dedicato ai protocolli di sicurezza, un ambito specifico della cybersecurity, destinato alla fascia d'età 10-14 anni.

"Nel Mezzo dei Maghi" è il nuovo nuovo strumento didattico della Ludoteca, dedicato ai protocolli di sicurezza, un ambito specifico della cybersecurity, destinato alla fascia d'età 10-14 anni

Il progetto nasce dalla collaborazione di Ludoteca con CINI (Consorzio Interuniversitario Nazionale per l'Informatica) e, in particolare, con **Cybersecurity National Lab** che opera al suo interno **e Scuola IMT Alti Studi di Lucca**. Entrambi questi poli di ricerca accademica propongono attività di terza missione, con iniziative rivolte al mondo della scuola e in generale al "public engagement".

In particolare, il Cybersecurity National Lab porta avanti da anni una filiera di addestramento e formazione con l'iniziativa "The Big Game", che - tramite i programmi "CyberTrials", "OliCyber" e "CyberChallenge" - coinvolge studenti e studentesse sia delle scuole superiori di secondo grado sia dell'Università, inserendosi all'interno della Misura #65 del Piano di Implementazione della Strategia Nazionale di Cybersicurezza 2022-2026. La collaborazione con la Ludoteca ha lo scopo, dunque, di estendere le iniziative di "awareness" al target delle scuole secondarie di primo grado, particolarmente esposto ai rischi di un uso non responsabile delle risorse digitali.

La collaborazione tra CINI, IMT e Ludoteca ha lo scopo di estendere le iniziative di "awareness" al target delle scuole secondarie di primo grado, particolarmente esposto ai rischi delle risorse digitali

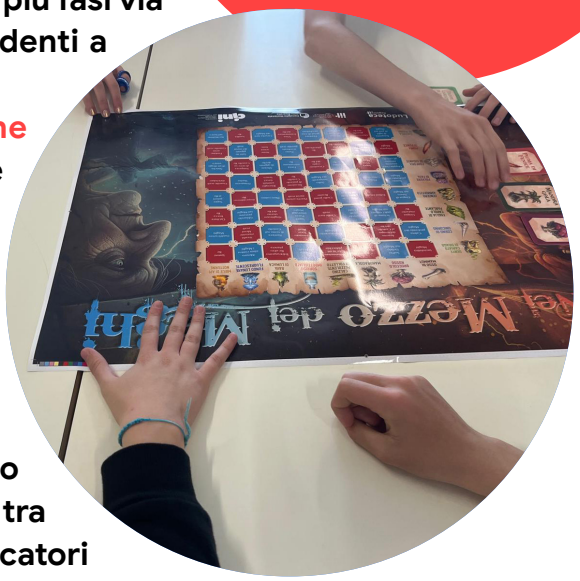
A partire dal **nuovo anno scolastico 2026/27,** la sezione dedicata alla cyber sicurezza della Ludoteca si arricchirà dunque del nuovo gioco da tavolo "Nel mezzo dei Maghi".

I **giochi da tavolo scientifici**, oggi molto diffusi e apprezzati anche tra giocatori adulti, hanno il **vantaggio di unire l'intrattenimento alla stimolazione cognitiva e alla sensibilizzazione su temi complessi**, attraverso una modalità immersiva che non presenta lo stress dell'apprendimento tradizionale.
Dal punto di vista educativo, presentano le seguenti peculiarità:

- favoriscono un apprendimento esperienziale con cui è possibile "toccare con mano" concetti complessi, rendendo le nozioni astratte concrete e facili da memorizzare;
- nella maggior parte dei casi sono sviluppati con il supporto di esperti per garantire la rigorosità e accuratezza dei contenuti scientifici;
- incentivano la cooperazione e la discussione tra i giocatori, promuovendo l'apprendimento collettivo.

Nel gioco si utilizzano strategie e strumenti che richiamano le tecniche di "hacking etico"

"Nel Mezzo dei Maghi" è un **gioco immersivo, di ambientazione fantasy**, che prevede l'uso di un kit composto da tabellone, carte, casseforti, lucchetti, buste da lettere e **articolato in più fasi via via sempre più complesse, corrispondenti a diversi protocolli di sicurezza.**
Il titolo richiama all'attacco **"man in the middle"** (in italiano "uomo nel mezzo") che in crittografia e sicurezza informatica sta a indicare un **attacco informatico** in cui qualcuno segretamente ritrasmette o altera la comunicazione tra due parti che credono di comunicare direttamente tra di loro.



Non manca l'elemento narrativo: **nell'intro si racconta l'origine e lo stato della lotta tra l'Allenza di Maghi, Streghe e il Re. I giocatori impersonano il servizio postale reale**, il cui compito è impedire all'Alleanza di comunicare per perseguire obiettivi malevoli, attraverso il compimento di incantesimi. Per riuscirci, **i postini reali devono compiere specifiche azioni di interferenza**, via via sempre più complesse, sui messaggi inviati dall'Alleanza, utilizzando strategie e strumenti che richiamano le tecniche di "hacking etico" (il fine non è infatti malevolo ma ne va della salvezza del Re!).

Nel mese di aprile il gioco è stato testato in otto classi della scuola secondaria di primo grado "D. Settesoldi" (Vecchiano, Pi), coinvolgendo un totale di 174 alunni e alunne. Lo staff della Ludoteca e l'esperto dell'IMT hanno condotto i laboratori, con il supporto dei docenti, dividendo la classe in gruppi e curando la fase di "briefing" e "debriefing", in modo da introdurre le tematiche presenti nel gioco e fissare le nozioni acquisite a fine partita.
Il **gioco sarà proposto nella versione definitiva per il prossimo anno scolastico** e sarà protagonista di eventi e iniziative dedicate alla formazione e divulgazione scientifica.



MINORI E DIMENSIONE DIGITALE: TRA ABITUDINI ONLINE ED EDUCAZIONE ALLA CYBERSICUREZZA

La scelta della Ludoteca di realizzare un nuovo gioco dedicato alla cybersicurezza nasce dalla crescente necessità di **accompagnare i più giovani verso un uso consapevole delle tecnologie digitali,** come confermano anche i dati sulle loro abitudini online.
Come evidenzia l'**indagine di Save The Children 2025** sul rapporto infanzia e digitale, l'**età di utilizzo dello smartphone è sempre più precoce**. In Italia circa un bambino su tre tra i 6 e i 10 anni (il 32,6%) usa lo smartphone tutti i giorni, una tendenza in costante aumento negli ultimi anni (nel 2018-2019 erano il 18,4%).
Inoltre, il 62,3% dei preadolescenti tra gli 11 e i 13 anni - oltre tre su cinque - possiede almeno un account social: il 35,5% ne ha uno su più social e un ulteriore 26,8% soltanto uno. Questo nonostante la normativa vigente (GDPR - General Data Protection Regulation) stabilisca che, per aprire un account e fornire il consenso al trattamento dei dati personali online, sia necessario aver compiuto 14 anni, oppure 13 anni con l'autorizzazione dei genitori.
Il 31,3% dei ragazzi e delle ragazze di questa fascia d'età è connesso online con gli amici - tramite chat, chiamate e videochiamate - più volte al giorno, il 5% lo è in modo continuativo. L'82,2% dei preadolescenti usa Internet per scambiare messaggi, poco meno del 40% per inviare e ricevere mail, quasi 1 su 5 (18,5%) per leggere giornali o siti di

In Italia circa un bambino su tre tra i 6 e i 10 anni (il 32,6%) usa lo smartphone tutti i giorni, una tendenza in costante aumento negli ultimi anni (nel 2018-2019 erano il 18,4%)

informazione, l'11,3% per esprimere opinioni su temi politico-sociali, il 9,6% per seguire corsi online.
Anche la popolazione dei minori vive dunque immersa nella dimensione dell'"onlife", secondo la definizione del filosofo **Luciano Floridi** (The Onlife Manifesto, 2014), **un mondo ibrido in cui le scelte individuali sono continuamente plasmate dalle interazioni digitali** e da tutto ciò che comportano, sia in termini di opportunità che di rischi.



Educare i più piccoli all'uso responsabile delle risorse digitali, anche attraverso la conoscenza dei meccanismi che ne regolano il funzionamento, diventa quindi un'azione strategica per crescere futuri cittadini (digitali) consapevoli. **La consapevolezza è anche la base per educare i più piccoli e le più piccole a un uso sicuro degli ambienti digitali**, considerando anche che quelli più frequentati - social network, piattaforme di messaggistica e di gioco - sono sempre più esposti alle attività della cybercriminalità e presentano, di conseguenza, alti livelli di rischio.

Educare i più piccoli all'uso responsabile delle risorse digitali, anche attraverso la conoscenza dei meccanismi che ne regolano il funzionamento, diventa un'azione strategica per crescere futuri cittadini (digitali) consapevoli

Per andare incontro alle frequenti richieste di formazione nel campo della cybersicurezza da parte delle istituzioni scolastiche, **la Ludoteca ha già attivato una sezione didattica interamente dedicata**, composta da **diverse proposte** tutte basate sul gioco e profilate in base alle diverse fasce di età.



Nel mezzo dei Maghi" rappresenta solo l'ultima risorsa didattica della Ludoteca in tema di cybersecurity. Tra gli strumenti cardine, c'è il **videogioco "Nabbovaldo e il ricatto dal cyberspazio"**, pensato per le scuole secondarie di primo grado e sviluppato in un'ottica di gamification, che **permette di introdurre, in modo interattivo e coinvolgente, alcune tra le principali tematiche della cybersecurity: attacchi informatici, truffe online, malware, contromisure tecniche.** I giocatori vivono un'avventura articolata in quattro capitoli, con epilogo finale, attraverso uno storytelling

divertente che segue le vicende del protagonista Nabbovaldo, ingenuo abitante di Internetopoli, sconfinata città della Rete. Nel corso del gioco, Nabbovaldo incontra diversi personaggi che rappresentano, già a partire dal nome, opportunità e rischi del mondo online: Mr D, Super Virus Block, Troll, Dark Fred.

A integrazione del laboratorio incentrato sul videogioco, a seconda delle esigenze specifiche delle classi, **vengono proposte anche le seguenti risorse e attività:**

- **Gioco Cifrario di Cesare:** ispirato al metodo di cifratura utilizzato dal celebre condottiero romano, rappresenta un valido strumento per introdurre il concetto di "confidenzialità" dei dati e dei messaggi e al tempo stesso per spiegare le tecniche di crittografia.
- **Gioco Carte Memory:** i partecipanti devono memorizzare delle password cercando di accoppiare le carte identiche. Questo gioco stimola la riflessione sull'importanza di gestire le password con attenzione, evidenziando il diverso livello di robustezza.
- **Gioco acronimo:** partendo dal testo di una canzone famosa, i gruppi considerano solo le prime lettere delle varie parole che compongono la frase e creano così una password robusta ma facilmente memorizzabile.
- **Gioco Cyber Quiz:** gioco di gruppo basato su tavole a fumetti in cui viene presentata una possibile situazione di rischio online e tre possibili finali: soltanto uno di questi rappresenta il comportamento corretto in un'ottica di igiene informatica.
- **Gioco Prima pensa poi condividi:** prevede l'utilizzo di carte che riportano su un lato varie tipologie di informazioni personali, sull'altro le argomentazioni per cui è opportuno o meno non condividerle online.
- **Manifesto per la sicurezza online:** un decalogo sulla sicurezza digitale con raccomandazioni per prevenire e contrastare le principali cyber minacce.

Nel loro insieme, **le attività della Ludoteca del Registro .it delineano un percorso educativo integrato** che, attraverso il gioco e la sperimentazione, mira a rafforzare nei più giovani la capacità di orientarsi tra rischi e opportunità della dimensione online, **contribuendo alla formazione di cittadini digitali più consapevoli e responsabili.**

RAPPORTO IOCTA 2026: DALL'AI AI DOMINI MALEVOLI, L'ALLARME DI EUROPOL SUL CYBERCRIME

di **Gino Silvatici**

Il 28 aprile, **Europol ha pubblicato l'edizione 2026 dell'Internet Organised Crime Threat Assessment (Iocta), il report annuale che analizza l'evoluzione delle principali minacce legate alla criminalità organizzata online nell'Unione europea.** Il documento rappresenta uno dei riferimenti più importanti per comprendere le tendenze del cybercrime in Europa e le sfide che le autorità di contrasto dovranno affrontare nei prossimi anni.

L'AI sta diventando un moltiplicatore di capacità per le organizzazioni illegali online

IL CYBERCRIME NELL'ERA DELL'AI: NUOVE MINACCE E CRITICITÀ PER LE AUTORITÀ EUROPEE

Lo Iocta 2026 dedica particolare attenzione agli **strumenti che facilitano il cybercrime, alle infrastrutture digitali utilizzate dalle reti criminali, agli attacchi informatici, alle frodi online e allo sfruttamento sessuale minorile su Internet.** Uno degli elementi più rilevanti dello studio riguarda il ruolo crescente dell'intelligenza artificiale, considerata da Europol un fattore destinato a trasformare profondamente il panorama delle minacce digitali.

Secondo il rapporto, **la crescente accessibilità degli strumenti basati sull'AI sta abbassando significativamente le barriere di ingresso per i criminali informatici.** In pratica, attività che in passato richiedevano elevate competenze tecniche possono oggi essere realizzate anche da soggetti con conoscenze limitate, grazie all'automazione e alla disponibilità di strumenti sempre più sofisticati.

Europol evidenzia come l'AI stia diventando un moltiplicatore di capacità per le organizzazioni illegali online. I sistemi generativi e gli strumenti automatizzati consentono infatti di creare campagne fraudolente più credibili, automatizzare attacchi informatici e migliorare le tecniche

di ingegneria sociale.
Uno dei settori più colpiti è quello del phishing. Grazie all'intelligenza artificiale, i criminali possono produrre email, messaggi e siti web contraffatti sempre più convincenti, riducendo errori grammaticali o segnali tipici delle frodi tradizionali. Inoltre, l'AI può essere utilizzata per automatizzare l'analisi delle vulnerabilità informatiche, personalizzare gli attacchi contro specifici bersagli e generare contenuti audio o video manipolati attraverso tecnologie deepfake.
Questa evoluzione rappresenta una sfida importante per le autorità europee. Se da un lato l'intelligenza artificiale può diventare uno strumento di supporto per la cybersecurity e per le attività investigative, dall'altro rischia di aumentare la velocità, la scala e la sofisticazione delle attività illecite online.
Europol sottolinea che **il cybercrime sta diventando sempre più industrializzato e accessibile. Il modello "crime-as-a-service"**, già diffuso nel dark web, permette infatti a gruppi criminali di vendere strumenti di attacco, malware e servizi illegali anche a soggetti privi di competenze tecniche avanzate.
Lo studio rileva anche le crescenti difficoltà incontrate dalle forze di polizia europee nel contrastare il cybercrime. Tra i principali ostacoli viene indicata la **diffusione delle piattaforme con crittografia end-to-end.** Sebbene questi sistemi siano fondamentali per la protezione della privacy e della sicurezza delle comunicazioni, **Europol sostiene che essi rendano più complesso il monitoraggio delle operazioni illecite online e l'identificazione dei sospetti.**
Il report evidenzia come le autorità investigative siano spesso impossibilitate ad accedere alle comunicazioni utilizzate dalle reti criminali, anche in presenza di indagini formalmente autorizzate.
Un altro problema segnalato riguarda le **politiche di conservazione dei dati** ("data retention") adottate nei diversi Stati membri dell'Ue. Europol definisce alcune di queste politiche **"restrittive o inadeguate"**, sostenendo che limitino la capacità delle autorità di ricostruire attività illecite e individuare responsabili.
La frammentazione normativa europea sul tema della conservazione dei dati continua infatti a rappresentare un nodo delicato. Negli ultimi anni il tema è stato oggetto di numerose controversie giuridiche, soprattutto dopo diverse decisioni della Corte di giustizia dell'Unione europea che hanno imposto limiti significativi alla conservazione generalizzata dei dati di traffico.

La frammentazione normativa europea sul tema della conservazione dei dati continua a rappresentare un nodo delicato

L'ECOSISTEMA DEI DOMINI NEL CYBERCRIME: TRA DNS ABUSE E FRODI ONLINE

Uno degli aspetti più interessanti dell'locta

2026 riguarda l'attenzione dedicata agli **abusi del DNS e dell'ecosistema dei nomi a dominio:** "technical DNS abuse" e "website content abuse" sono strettamente collegati nella dinamica criminale. In pratica, **le organizzazioni illegali utilizzano i nomi a dominio e le infrastrutture DNS come componenti essenziali delle loro operazioni online.** Secondo il rapporto, i criminali registrano domini Internet per imitare siti legittimi (ad esempio istituti finanziari, piattaforme di pagamento o servizi online), con l'obiettivo di rubare credenziali, dati personali e informazioni bancarie agli utenti. I domini fraudolenti vengono inoltre utilizzati per distribuire malware, gestire botnet e coordinare campagne di attacco automatizzate.

Europol sottolinea che **il periodo compreso tra la registrazione di un dominio malevolo e l'intervento delle autorità rappresenta una finestra temporale particolarmente sfruttata dalle reti criminali.** In molti casi, infatti, bastano poche ore o pochi giorni per avviare campagne di phishing o distribuzione malware in grado di colpire migliaia di utenti prima che il dominio venga bloccato o rimosso.

I criminali registrano domini Internet per imitare servizi online e rubare credenziali, dati personali e informazioni bancarie. Questi domini fraudolenti sono utilizzati anche per distribuire malware, gestire botnet e coordinare attacchi automatizzati

Questo aspetto è particolarmente rilevante anche per i registri ccTLD (country code Top-Level Domain) e per gli operatori del settore dei nomi a dominio. **Il report critica**, inoltre, **la lentezza delle procedure di cooperazione internazionale utilizzate per contrastare le attività illegali online** e questo potrebbe avere degli impatti sulle procedure di enforcement che dovranno essere sempre più rapide per combattere questo tipo di abusi. Secondo Europol, "l'assenza di interfacce automatizzate di segnalazione" e la dipendenza da procedure giudiziarie transfrontaliere lente impediscono interventi rapidi contro i domini malevoli. Questo problema è particolarmente evidente nel contesto del cybercrime globale, dove infrastrutture, server, registranti e vittime possono trovarsi in giurisdizioni diverse. Le autorità di contrasto spesso devono seguire procedure legali internazionali complesse e lente per ottenere informazioni sui registranti, bloccare domini o richiedere la rimozione di contenuti illegali. Europol suggerisce quindi la necessità di strumenti più rapidi ed efficienti per il contrasto operativo alle minacce online, soprattutto nei casi di frodi automatizzate e distribuzione di malware.

Lo studio non propone misure legislative specifiche nei confronti dei registri ccTLD o degli operatori DNS europei. Tuttavia, **il documento attribuisce chiaramente un ruolo centrale alle infrastrutture Internet nella catena operativa del cybercrime.**



Europol, The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026, Publications Office of the European Union, Luxembourg, 2026.

Lo locta potrebbe diventare un ulteriore riferimento politico nel dibattito europeo sulla responsabilità degli intermediari tecnici e sulla governance delle infrastrutture digitali

Per questo motivo, l'analisi dell'locta 2026 potrebbe influenzare future iniziative della Commissione europea o degli Stati membri in materia di contrasto agli abusi online. Il settore dei nomi a dominio si trova, infatti, sempre più spesso al centro delle discussioni politiche e regolatorie legate alla cybersecurity.

Negli ultimi anni **le istituzioni europee hanno aumentato l'attenzione verso temi come la verifica dell'identità dei registranti, la rapidità delle procedure di take-down, la cooperazione tra registri e forze dell'ordine e il monitoraggio degli abusi DNS**.

L'locta potrebbe quindi diventare un ulteriore riferimento politico nel dibattito europeo sulla responsabilità degli intermediari tecnici e sulla governance delle infrastrutture digitali.

SCENARIO E PROSPETTIVE

Il rapporto di Europol si inserisce in un contesto in cui **la cybersicurezza è diventata una componente centrale della sicurezza economica e geopolitica europea.**

Le infrastrutture digitali sono ormai essenziali per il funzionamento delle economie moderne, dei servizi pubblici

e delle comunicazioni. Di conseguenza, attacchi informatici, campagne di ransomware e frodi online possono avere impatti sistemici molto rilevanti.

L'Ue sta cercando di rafforzare progressivamente il proprio ecosistema di cybersecurity attraverso regolamenti come **NIS2**, il **Cyber Resilience Act** e altre **iniziative dedicate alla sicurezza digitale.**

Tuttavia, **l'Iocta 2026 mostra come l'evoluzione tecnologica stia aumentando rapidamente la complessità delle minacce.**

L'accessibilità dell'intelligenza artificiale, la rapidità delle infrastrutture criminali online e la dimensione globale delle operazioni cyber rendono sempre più difficile il lavoro delle autorità di contrasto. Il rapporto conferma che il cybercrime continua a evolversi con estrema velocità e che le infrastrutture digitali stanno assumendo un ruolo sempre più centrale nelle attività illecite. Nel documento emergono sia la crescente sofisticazione tecnologica delle reti illegali, sia le difficoltà strutturali che le autorità europee incontrano nel contrastarle in modo efficace.

L'intelligenza artificiale, le piattaforme cifrate, gli abusi DNS e la lentezza della cooperazione internazionale rappresentano elementi destinati a influenzare il dibattito politico e regolatorio europeo nei prossimi anni.

Per il settore digitale europeo, inclusi registri ccTLD, provider e operatori infrastrutturali, **il report costituisce un segnale importante:** la pressione normativa e politica sul tema degli abusi online potrebbe aumentare ulteriormente. La sfida per l'Europa sarà trovare un equilibrio tra sicurezza, tutela dei diritti fondamentali, innovazione tecnologica e rapidità operativa nel contrasto al cybercrime globale.

La sfida per l'Europa sarà trovare un equilibrio tra sicurezza, tutela dei diritti fondamentali, innovazione tecnologica e rapidità operativa nel contrasto al cybercrime globale

ICANN E L'IMPATTO DELL'INTELLIGENZA ARTIFICIALE SUL DNS

di **Arianna Del Soldato** e **Adriana Lazzaroni**

All'interno dell'ecosistema di **Icann** (Internet Corporation for Assigned Names and Numbers), **l'intelligenza artificiale è diventata uno dei temi chiave di discussione**, non perché modifichi l'architettura del DNS, ma perché **sta incidendo in modo crescente sui suoi modelli di utilizzo**. In particolare, **l'attenzione si concentra sui possibili impatti dell'IA, soprattutto dei modelli linguistici di grandi dimensioni (LLM) come ChatGPT e i suoi omologhi, sul Domain Name System (DNS), sull'ecosistema degli identificatori e sulla missione stessa di Icann.**

L'IA non modifica l'architettura fondamentale del DNS né la missione principale di Icann di contribuire a garantire una rete stabile, sicura, globale e unificata. Tuttavia, ogni cambiamento tecnologico significativo ha delle implicazioni per l'ecosistema in cui opera

Sebbene l'IA rappresenti attualmente la narrativa tecnologica dominante - ereditando il clamore che un tempo circondava "blockchain" e "big data" - è fondamentale distinguere l'entusiasmo mediatico dalle reali implicazioni strutturali. Come sottolineato da Matt Larson, Icann VP of Research, l'IA non modifica l'architettura fondamentale del DNS né la missione principale di Icann di contribuire a garantire una rete stabile, sicura, globale e unificata, coordinando gli identificatori univoci di Internet inclusi i nomi a dominio, gli indirizzi IP e i parametri di protocollo. Il livello degli identificatori appartiene all'infrastruttura, non genera contenuti, non prende decisioni né interagisce con gli utenti come fanno i modelli LLM. Tuttavia, ogni cambiamento tecnologico significativo ha delle implicazioni per l'ecosistema in cui opera e alcune di queste meritano senza dubbio un'attenzione particolare.

IA E DNS: NUOVE DINAMICHE DI TRAFFICO E SICUREZZA DELLE INFRASTRUTTURE

Negli ultimi anni il DNS ha già attraversato profonde trasformazioni: cloud, CDN, mobile internet, DNS cifrato. Oggi, però, **l'IA sta iniziando a cambiare il modo in cui nomi a dominio e le infrastrutture DNS vengono utilizzati.** L'impatto non riguarda soltanto i grandi modelli linguistici o i servizi di AI generativa. Sempre più sistemi automatizzati - chatbot, agenti autonomi, piattaforme di analisi, AI crawler e strumenti di retrieval - utilizzano il DNS in modo intensivo e diverso rispetto alla tradizionale navigazione web degli utenti.

Il traffico generato da sistemi automatizzati può differire sensibilmente dalla normale attività online degli utenti per volume, frequenza e distribuzione delle richieste

Ogni volta che un chatbot consulta il web per elaborare una risposta o un agente di IA esegue attività automatizzate su più siti, vengono generate query DNS. Questo traffico, prodotto da sistemi automatizzati, può differire significativamente dalla normale attività online degli utenti in termini di volume, frequenza e distribuzione delle richieste. **Per i Registrar e i registri questo cambiamento potrebbe tradursi in nuove dinamiche di traffico**, in differenti modelli di registrazione dei domini e in una crescente attenzione ai temi della sicurezza e dell'affidabilità. Sebbene il DNS sia stato progettato per gestire la crescita e i modelli di utilizzo in evoluzione, l'emergere dell'IA come fonte significativa di traffico Internet è uno sviluppo che merita di essere monitorato. Per gli operatori del settore ciò significa, infatti, porre maggiore attenzione alla resilienza delle infrastrutture DNS, così come alla capacità di mitigazione del traffico anomalo, al monitoraggio dei pattern automatizzati, nonché alla gestione della sicurezza a livello resolver e authoritative DNS.

Una delle principali preoccupazioni riguarda il potenziale dell'IA di ampliare, accelerare e automatizzare attività malevole legate ai nomi a dominio, modificando in modo significativo il panorama delle minacce. I modelli di LLM possono rendere significativamente più facile generare contenuti di phishing convincenti, creare siti di impersonificazione o elaborare campagne mirate di ingegneria sociale. Molte di queste attività sono basate sui nomi a dominio. Gli strumenti di IA possono anche essere utilizzati per registrare domini per campagne di abuso su vasta scala, e per farlo in modi più difficili da rilevare utilizzando metodi tradizionali.

In tale contesto vi è comunque un risvolto positivo che risiede nella possibilità di impiegare le tecnologie di IA anche nel contrasto agli

abusi del DNS. I team di ricerca di Icann, e dei principali ccTLD, impiegano già tecniche di machine learning per identificare nomi a dominio malevoli, analizzare pattern di abusi su vasta scala, rilevare i DGA (Domain Generation Algorithms) e monitorare le anomalie nel traffico DNS.
L'evoluzione del contesto attuale richiederà una focalizzazione su soluzioni d'avanguardia, a partire dai **sistemi di "threat intelligence"** fino al monitoraggio comportamentale delle registrazioni. **Il successo di queste strategie dipenderà** non solo dall'impiego di strumenti automatizzati per il rilevamento degli abusi, ma **soprattutto dalla capacità di creare una rete di cooperazione solida tra Registri, registrar e professionisti della sicurezza.**

IA, CLOUD E DNS: VERSO UN'INFRASTRUTTURA INTERNET SEMPRE PIÙ CENTRALIZZATA

La convergenza tra IA, infrastrutture cloud e protocolli di cifratura come il DoH (DNS over HTTPS) e il DoT (DNS over TLS) **sta delineando un ecosistema digitale caratterizzato da una marcata centralizzazione.** Poiché lo sviluppo dei sistemi di IA richiede capacità computazionali e volumi di dati sostenibili quasi esclusivamente dai grandi "hyperscaler", si assiste a un progressivo spostamento della risoluzione del DNS dai "resolver" locali verso piattaforme pubbliche gestite da pochi operatori.
In questo scenario, una quota crescente di traffico viene instradata attraverso provider che controllano simultaneamente l'intera filiera tecnologica: dalle infrastrutture cloud ai servizi di IA, passando per le reti di distribuzione dei contenuti (CDN), ai resolver DNS, fino ai browser e ai sistemi operativi. Tale concentrazione verticale produce effetti critici che vanno ben oltre l'aspetto tecnico, determinando un **accumulo senza precedenti di metadati e informazioni comportamentali nelle mani di pochi soggetti.** Ciò non solo riduce drasticamente la visibilità operativa dei fornitori di servizi internet (ISP) e degli operatori locali, ma accresce la dipendenza infrastrutturale globale, conferendo al controllo delle reti digitali una **rilevanza geopolitica sempre più marcata.** Dinanzi a queste sfide, il tema della sovranità digitale e della resilienza della rete è divenuto centrale nell'agenda degli organismi tecnici e regolatori internazionali, tra i quali anche Icann, chiamati a definire nuovi modelli di governance che bilancino

Il tema della sovranità digitale e della resilienza della rete è ormai centrale nell'agenda degli organismi tecnici e regolatori internazionali, chiamati a bilanciare innovazione tecnologica, protezione dei dati e autonomia delle infrastrutture nazionali

l'innovazione tecnologica con la protezione dei dati e l'autonomia delle infrastrutture nazionali.

L'IA RIDEFINISCE IL VALORE DEI NOMI A DOMINIO

L'avvento dell'IA sta ridefinendo profondamente il valore dei nomi a dominio, trasformando il modo in cui gli utenti interagiscono con il web. Sebbene l'evoluzione della "AI search" tenda a fornire risposte dirette riducendo la visibilità immediata degli URL, **il dominio non perde affatto la sua centralità.** Al contrario, ne emerge rafforzata la funzione reputazionale come garanzia di affidabilità della fonte.

In un ecosistema dove gli assistenti virtuali filtrano e selezionano i contenuti, l'autorevolezza e la riconoscibilità di un nome a dominio diventano asset strategici per distinguersi

In un ecosistema dove gli assistenti virtuali filtrano e selezionano i contenuti, l'autorevolezza e la riconoscibilità di un nome a dominio diventano asset strategici per distinguersi. Questa metamorfosi del mercato è già testimoniata da una crescita esponenziale delle registrazioni di keyword legate all'IA e dall'adozione di nuove strategie di branding, sebbene ciò porti con sé sfide critiche, come l'aumento di fenomeni speculativi e di cybersquatting mirati ai nuovi servizi di IA.

IA E PROCESSI MULTISTAKEHOLDER

Esiste tuttavia un'altra dimensione che va oltre quella dell'infrastruttura tecnica: **la legittimità di Icann si basa in gran parte sull'integrità del suo riconfermato modello *multistakeholder* e sull'autenticità della partecipazione umana allo sviluppo di *policies*** e alla realizzazione del consenso. L'impiego dell'IA per generare commenti pubblici, redigere testi normativi, rispondere alle mailing list e partecipare ai processi comunitari avviene con una rapidità e una portata tali da poter influire sui processi decisionali. **Icann ha quindi il compito**, nello svolgimento delle sue specifiche attività, **di tutelare l'affidabilità delle informazioni generate dall'intelligenza artificiale** poiché parte della sua missione consiste nel fungere da fonte autorevole delle informazioni fornite.

Attraverso le funzioni di Iana, Icann gestisce registri autorevoli relativi ai parametri di protocollo, alle risorse numeriche e ai domini di primo livello, ambiti nei quali la precisione è fondamentale e non permette le approssimazioni tipiche dei modelli linguistici. Quando l'IA funge da intermediario per l'accesso a queste risorse, il rischio di informazioni inesatte, distorte o di cosidette "allucinazioni" può compromettere l'affidabilità delle informazioni fornite e, di conseguenza, il ruolo di Icann

come riferimento autorevole. La questione di come identificare e valutare i contributi generati dall'IA rappresenta quindi una sfida di governance che Icann, insieme a molte altre organizzazioni, sarà chiamata ad affrontare.

La questione di come identificare e valutare i contributi generati dall'IA rappresenta quindi una sfida di governance che Icann, insieme a molte altre organizzazioni, sarà chiamata ad affrontare

CONCLUSIONI

Quando emerge una nuova tecnologia significativa, Icann è chiamata a comprenderne gli effetti sull'ecosistema in cui opera. Nello specifico, nel caso dell'IA, **la tecnologia non modifica la missione di Icann, ma incide profondamente sull'ambiente in cui essa si sviluppa.** L'IA può influenzare i modelli di traffico DNS, modificare il panorama degli abusi e delle relative strategie di mitigazione, e porre nuove questioni in merito all'integrità della partecipazione e all'autorevolezza delle informazioni. Per questo motivo, **pur non rappresentando un fattore di discontinuità strutturale, l'evoluzione dell'IA richede un monitoraggio costante e attento da parte di Icann.**

05

Anteprima
Statistiche
News
Approfondimenti
Eventi

GLI APPUNTAMENTI INTERNAZIONALI DAL MONDO DELLA RETE

3-4 GIUGNO
RIPE NCC |
Riga, Lettonia

4 GIUGNO
* **CENTR 13th Academy** |
Online

8-11 GIUGNO
ICANN 86 **(Policy Forum)** |
Siviglia, Spagna

23 GIUGNO
* **CENTR Legal & Regulatory WG Tour de Table Meeting** | Online

24-26 GIUGNO
WMF - We Make Future |
Bologna, Italia

Il Registro c'è con uno stand e due eventi!

18-24 LUGLIO
IETF 126 | Vienna, Austria

10-11 SETTEMBRE
* **CENTR 2nd CSR workshop** |
Parigi (da confermare), Francia

24-25 SETTEMBRE
* **CENTR 3rd Joint BOP & Marketing workshop** | Ljubljana - Slovenia

14 SETTEMBRE
APTLD 90 |
Ulaanbaatar, Mongolia

* *Eventi riservati ai membri di Centr*




Registro.it
L'ANAGRAFE DEI DOMINI .IT

è gestito da


ISTITUTO
DI INFORMATICA
E TELEMATICA
CNR


Consiglio Nazionale
delle Ricerche