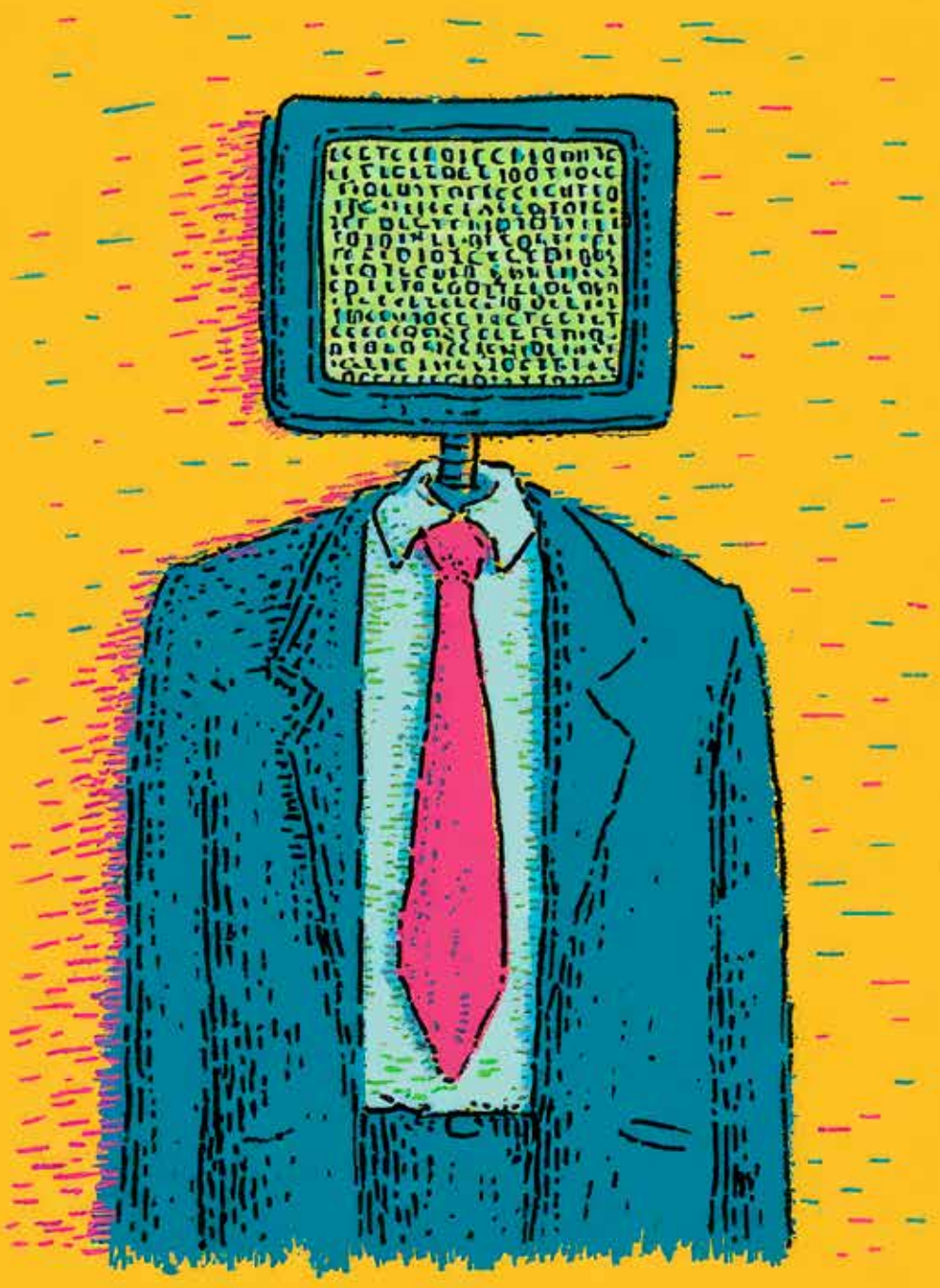
N. 1 - 2026 - YEAR 1 - FOUR-MONTHLY MAGAZINE OF THE REGISTRO .IT

dot.it

DOMAINS • OPINIONS • TRENDS



Registro.it
L'ANAGRAFE DEI DOMINI .IT

EDITORIAL COORDINATION
Chiara Spinelli

EDITORIAL COMMITTEE
Valentina Amenta, Maurizio Martinelli, Chiara Spinelli

GRAPHIC DESIGN
Coesiva

EDITORIAL BOARD
Francesca Nicolini (editorial coordinator), Stefania Fabbri, Chiara Spinelli

PARTICIPANTS
Giorgia Bassi, Arianna Del Soldato, Adriana Lazzaroni, Beatrice Lami, Daniele Sartiano, Gino Silvatici, Chiara Spinelli, Luca Albertario con Sonia Sbrana e Daniele Pancrazi (legal captions)
Michela Serrecchia (tecnichal capitons)
Silvia Giannetti (operational captions)

We would like to thank
Professor Franco Bernabè for his contribution "The paradoxes of regulation"

DATA SOURCE
Systems and Technological Development Unit of the .it Registry

DATA PROCESSING
Lorenzo Luconi Trombacchi, Michela Serrecchia (Systems and Technological Development Unit of the .it Registry)
Luca Albertario, Daniele Pancrazi, Sonia Sbrana (Legal Aspects and Litigation Unit)
Silvia Giannetti (Operations and Registrars Services Unit)

EDITED BY
External Relations, Media, Communication and Marketing Unit

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

HEAD OF 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 **Preview | 4**

- DOT: inside the Web in evolution, from AI and the transformation of the Internet to the growth of .it domains 5

02 **Statistics | 8**

- Annual growth of .it 9
- Four-month growth of .it 10
- Top 10 regions with the most .it domains 11
- The types of .it domain assignees 12
- Reasons for oppositions 13
- Opposition report - reassignments 14
- Annual trend of oppositions - reassignments 15
- Resolution of Oppositions 16
- Domain verification by the Registro 17
- Authinfo requests 18
- Requests by competent Authorities 18
- Names reserved 19

03 **News | 20**

- The first 40 years of the Internet: a revolution that looks to the future between AI and Quantum 21
- Ludoteca of Registro .it - Digital education workshops in schools 25

04 **In-depth dives | 28**

- The paradoxes of regulation 29
- Domain Renewal Analysis: the .it contribution to the CENTR task force 38
- From AI to NIS2: the digital challenges for businesses in the live LinkedIn of Registro .it 46
- Educare alla cybersicurezza: in arrivo “Nel Mezzo dei Maghi”, il nuovo gioco da tavolo della Ludoteca 50
- IOCTA Report 2026: from AI to malicious domains, Europol’s alarm on cybercrime 56
- ICANN and the impact of artificial intelligence on DNS 61

05 **Events | 66**

- International events from the Internet world 67

01

Preview

Statistics

News

In-depth dives

Events

DOT: INSIDE THE WEB IN EVOLUTION, FROM AI AND THE TRANSFORMATION OF THE INTERNET TO THE GROWTH OF .IT DOMAINS

The Italian and global digital sectors are entering a phase in which growth, **infrastructure, artificial intelligence, security and governance can no longer be viewed as separate areas, but as parts of a single system undergoing transformation.** It is no longer just a question of measuring the expansion of online presence or the adoption of new technologies, but of **understanding how these dimensions interconnect, redefining the very functioning of the Web** and its role in economic and social systems.
It is from this realisation that **DOT - Domains, Opinions, Trends** was born: after thirteen years, Quarter of Registro .it evolves into DOT, marking the start of a new phase in its editorial journey. **A new name** which, whilst upholding the mission that has guided the four-monthly publication from the outset – to inform, explore and interpret issues relating to domain names, the evolution of the Internet and the digital world – **reinforces its identity and its ability to understand an increasingly interconnected ecosystem**.

DOT thus builds on Quarter's legacy and continues along the same path, with the aim of supporting its ongoing evolution, including in editorial terms, in line with the changes currently taking place in the digital dimension.

The first four months of 2026 paint a picture of a dynamic ecosystem, **confirming the vitality of the country's digital landscape**. By the end of April, the number of registered domains had reached **3,578,851**, representing **an increase of 1.17% compared to the end of 2025** – **more than double the growth rate observed during the same period the previous year.** This figure confirms that an online presence continues to be a strategic tool for businesses, organisations and citizens in terms of identity, visibility and engagement.

Growth, however, tells only part of the story: in order to be truly understood, **it must also be read in its dimension of stability and continuity**. It is in this context that Registro .it contributed to the **Benchmarking Renewal Indicators Task Force**, promoted by the Council of European National Top-level Domain Registries (CENTR), which analysed about 40 million domains expiring in 2024, comparing ten ccTLD registries. The results show that domain renewal is closely linked to factors such as the age of the domain, the age of the registrant, and the registrant's category, offering an important insight: **digital continuity is not a matter of chance, but is built up over time**. In this perspective, **renewal becomes useful for understanding the value attributed to the online presence**, transforming data into operational tools that will, in perspective, concretely support Registrars in the management of their domain portfolio.

Alongside the data, **the major transformations reshaping the internet are also reflected in the LinkedIn live sessions** organised by Registro .it, and broadcast in early 2026, dedicated to the impact of artificial intelligence on SME websites, the evolution of digital tourism, and the implications of the NIS2 Directive. A clear picture is emerging: **AI is profoundly changing the way content is produced, how information is sought, and how online trust is built, but it does not diminish the central role of the website and the domain name as a bastion of identity and credibility.** At the same time, security is no longer a technical topic for specialists, but a strategic responsibility that involves governance, supply chain management and business organisation.

This look at the present and future of the Internet also coincides with a symbolic anniversary: **the 40th anniversary of Italy's first connection to the Internet**, which took place on 30 April 1986. The event, organised in Pisa by the Institute of Informatics and Telematics of the CNR (CNR-IIT), was not only a celebration of a **key milestone in Italy's digital history, but above all an opportunity for discussion on its future**: a Web that is increasingly integrated with artificial intelligence, distributed, intelligent and geared towards the production of services and knowledge. **Franco Bernabè**'s reflections, set out in his **keynote** address – **published in full in this issue** – on Europe's role in global technological competition and the need to avoid new forms of technological dependence, are part of the same discussion.

Beyond data, infrastructure and technology, **DOT also highlights the**

cultural dimension of the digital transformation: from outreach and training initiatives to the new educational experiences focused on cybersecurity offered by the Ludoteca of Registro .it, **there is a growing recognition of the need to guide the younger generation towards the responsible use of digital tools.** It is against this backdrop that the new board game **"Nel Mezzo dei Maghi"** (Among the Wizards) has been **developed by the Ludoteca of Registro .it, in collaboration with CINI (the National Interuniversity Consortium for Informatics) and the IMT School in Lucca**, with the aim of introducing very young children to the world of cybersecurity through increasingly interactive and experiential methods.

The issue is rounded off with in-depth articles on **cybersecurity, Internet governance and the impact of artificial intelligence on digital ecosystems**, with a particular focus on European and international regulatory frameworks. **These are diverse yet increasingly intertwined themes that paint a picture of a Web undergoing transformation and they confirm the central role that domain names continue to play within it.** In this context, security and governance remain fundamental aspects of the online dimension, against a backdrop characterised by the growing impact of artificial intelligence on models of Internet use.

DOT was created to observe and report on this complex and ever-changing digital landscape: a **"point"** on the Web, but also a prime vantage **"point"** from which to observe the changes that are reshaping the digital world. The aim is to provide the Registrar community, professionals, businesses and all stakeholders in the Internet ecosystem with resources for reading, in-depth analysis and discussion.

Have a good read!

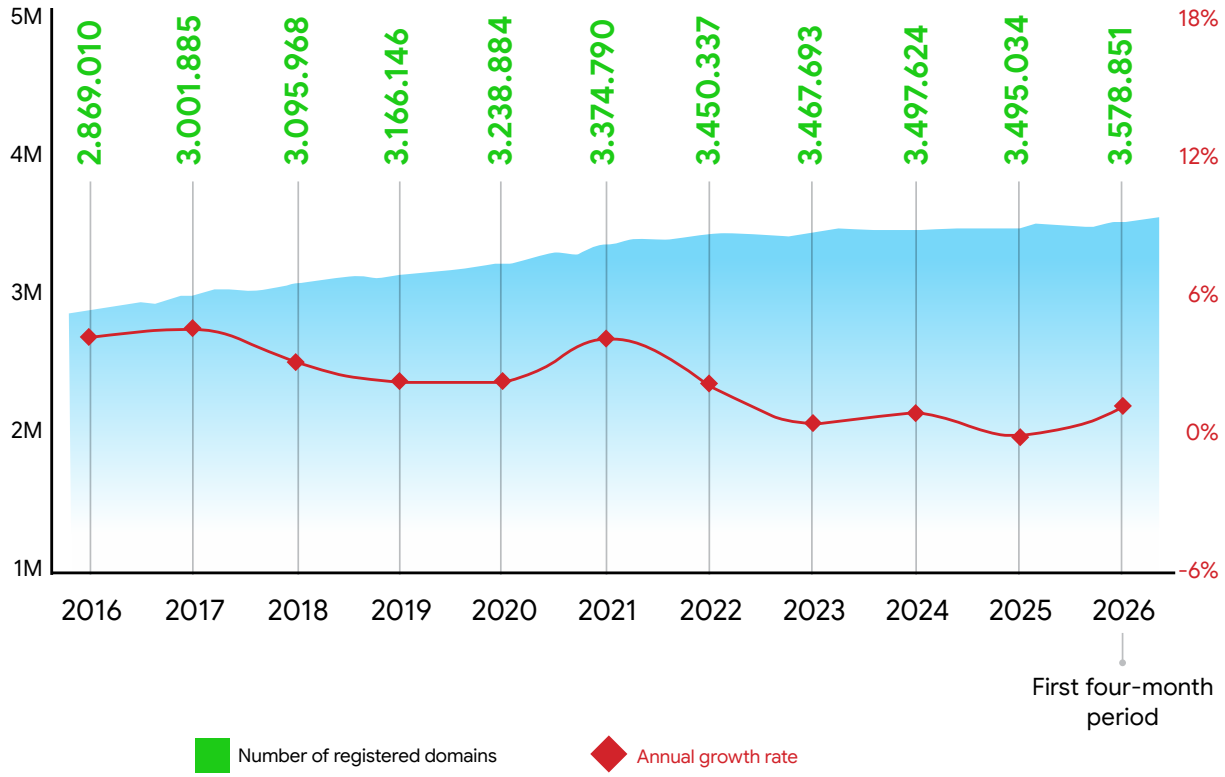
02

Preview
Statistics
News
In-depth dives
Events

ANNUAL GROWTH OF .IT

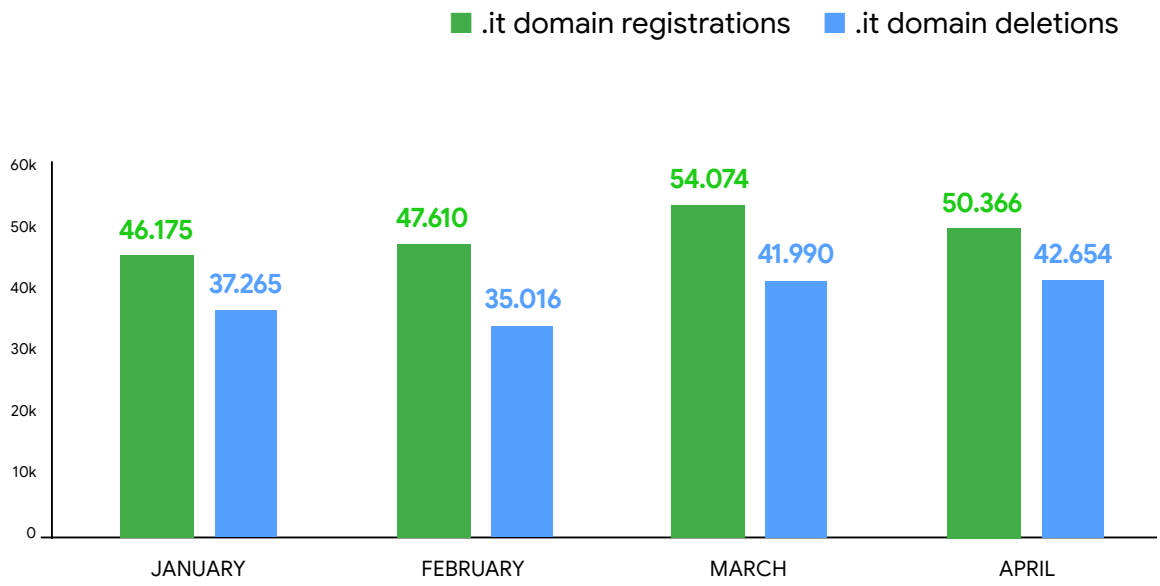
At the end of the first four months of 2026, the **overall number** of .it domains amounted to **3,578,851**, with an **increase of 1.17% (+41,300 domains), compared to the end of 2025**. This result marks a significant acceleration compared to the same period of the previous year, when growth stood at 0.54% (+19,023 domains compared to the end of 2024).

January–April 2026



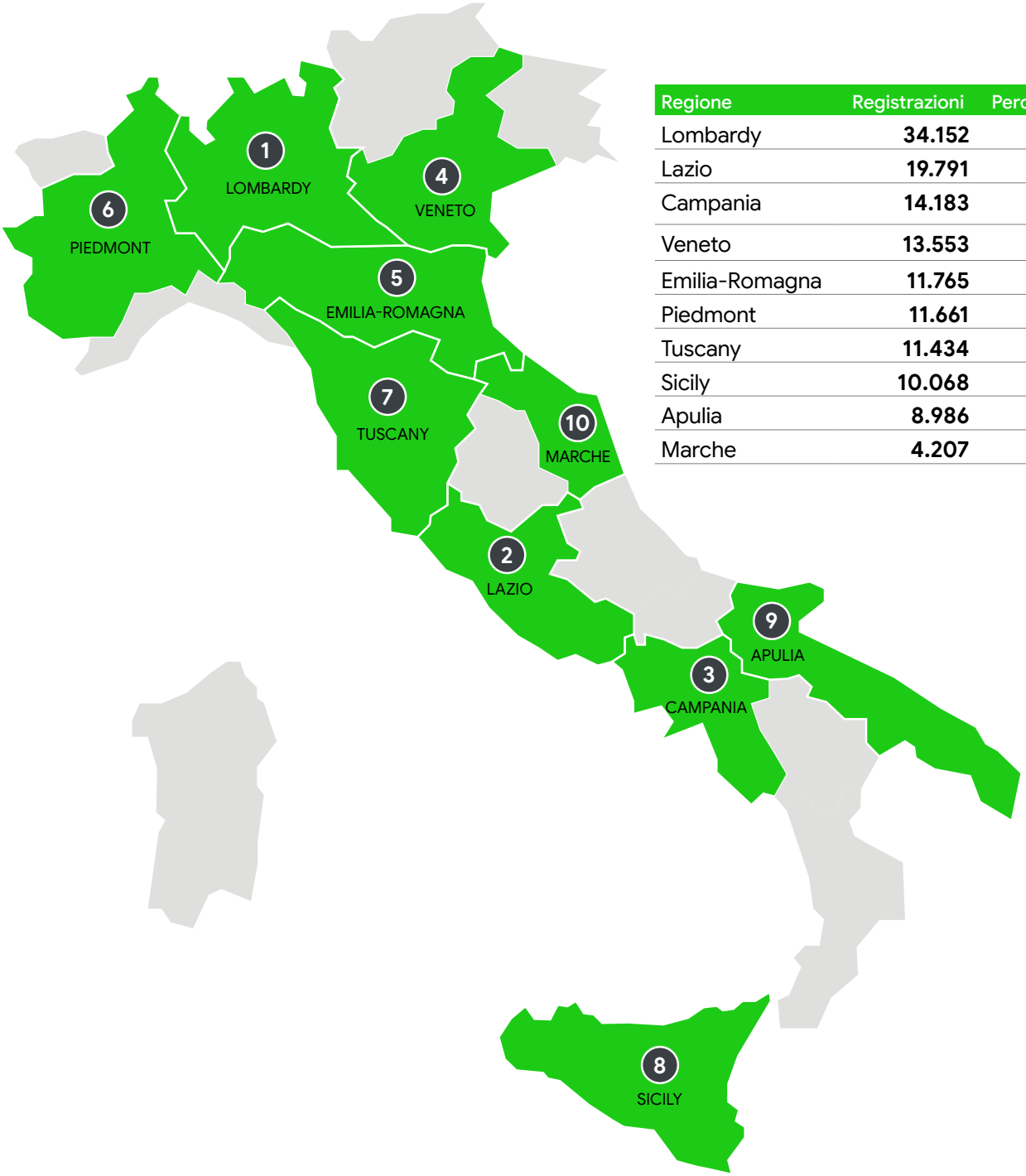
FOUR-MONTH GROWTH OF .IT

The trend in .it domain registrations over the first four months of the year shows a net increase in new domains compared to cancellations, with a significant peak in February. The total balance for the period under review exceeds 41,000 units, a figure that has almost doubled compared to the same four-month period in 2025, when the total stood at just over 19,000 domains. The trend is positive in two respects: an increase in new registrations and a simultaneous decrease in cancellations compared to the previous year.



TOP 10 REGIONS WITH THE MOST .IT DOMAINS

In the first four months of the year, Lombardy remains the undisputed leader of the rank: the percentage of new registrations remains stable at 21%, compared to the same period of the previous year. Lazio remains in second place, also with an unchanged figure of 12%. Campania has performed exceptionally well, climbing to third place with a figure of 9%, at the expense of Veneto, which has dropped one place to fourth. Piedmont is also losing ground, dropping to sixth place with a figure of 7%.

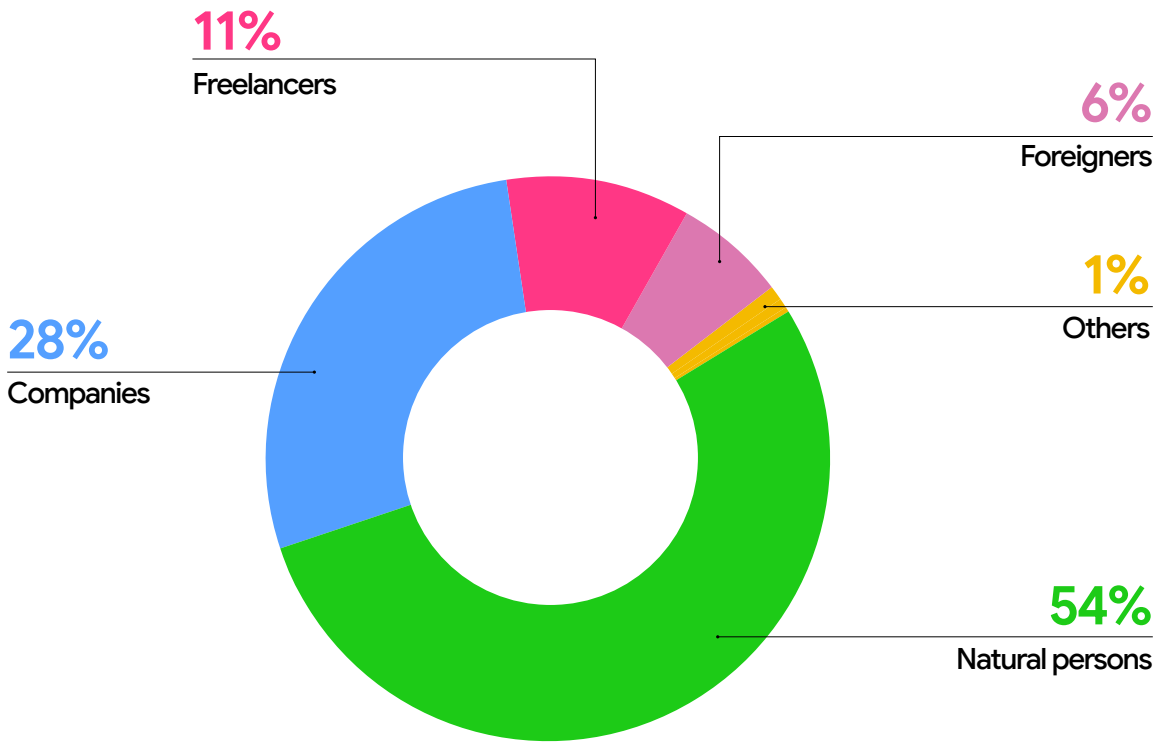


Regione	Registrazioni	Percentuale
Lombardy	**34.152**	20,79%
Lazio	**19.791**	12,05%
Campania	**14.183**	8,63%
Veneto	**13.553**	8,25%
Emilia-Romagna	**11.765**	7,16%
Piedmont	**11.661**	7,10%
Tuscany	**11.434**	6,96%
Sicily	**10.068**	6,13%
Apulia	**8.986**	5,47%
Marche	**4.207**	2,56%

THE TYPES OF .IT DOMAIN ASSIGNEES

Compared to the first four months of 2025, the percentage of new .it domains relating to natural persons increased by four points to 54%. The number of businesses, however, has fallen, dropping by two percentage points to 28%. There has also been a slight decline among the freelancers, whose share has fallen by one percentage point to 11%.

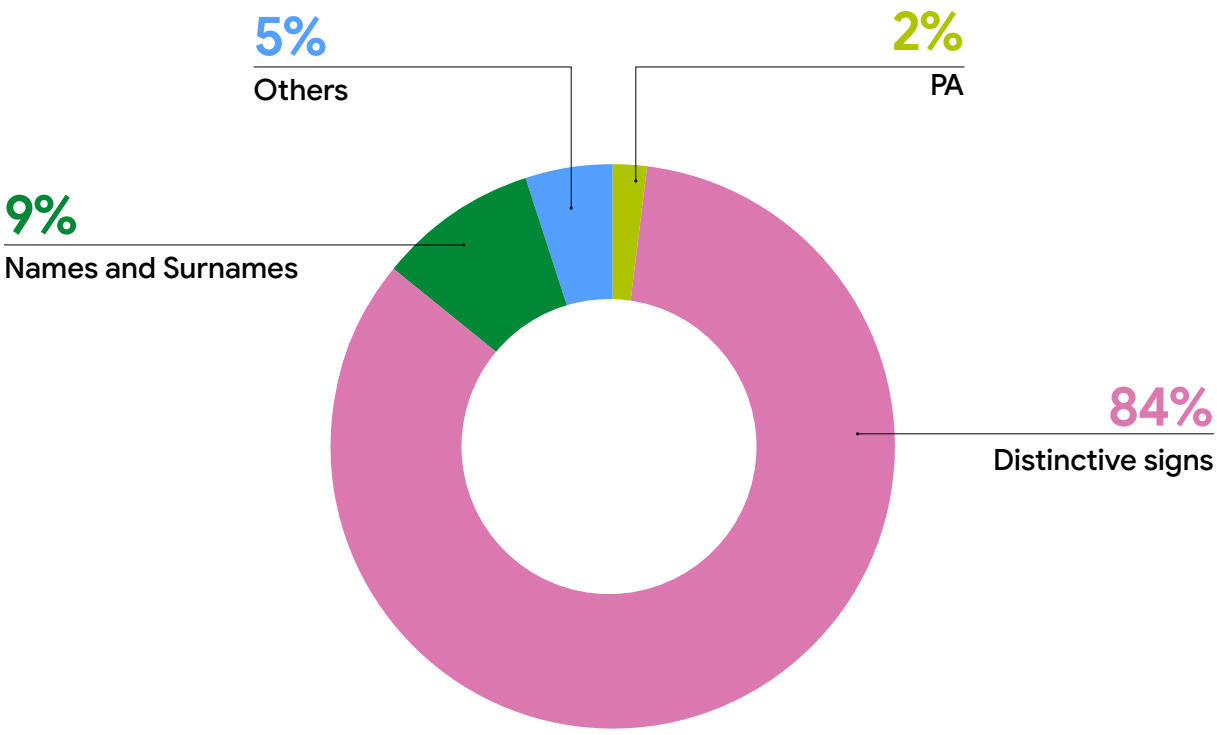
Recording January–April 2026



REASONS FOR OPPOSITIONS

In the first four months of the year, **oppositions for infringement of the distinctive signs remains prevalent**, although slightly down from 2025 (**84%** vs. 89%). **Instead, the requests for first and last names have increased**, rising **from 8% to 9%**, while the oppositions promoted by public administrations have reached 2%, compared to the absence of cases in the previous year.
Finally, requests based on other grounds account for 5%, up from the 3% recorded in 2025.

Distinctive signs January–April 2026

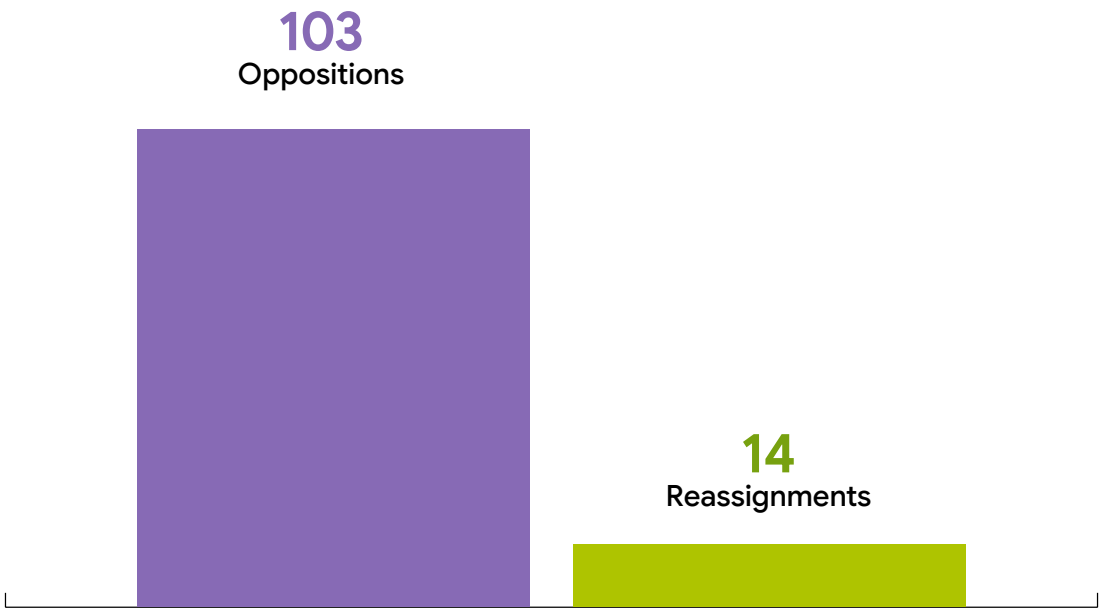


OPPOSITION REPORT - REASSIGNMENTS

In the period examined, **103 oppositions were activated, up from 83** in the same four-month period **of 2025**, with a monthly average rising from 21 to 26 activations. March was the most active month with 34 oppositions, while February had the lowest value (22).

From a geographical point of view, **38 procedures involved exclusively Italian subjects**; among the assignees/respondents prevails the North (17), followed by the South (13) and the Centre (8), while among the opponents/complainants the North records 23 subjects, compared with 10 from the Centre and 5 from the South. The picture is completed with **48 cases in which Italian opponents acted against foreign assignees**, 4 oppositions of foreign opponents against Italian assignees and 13 entirely foreign procedures.

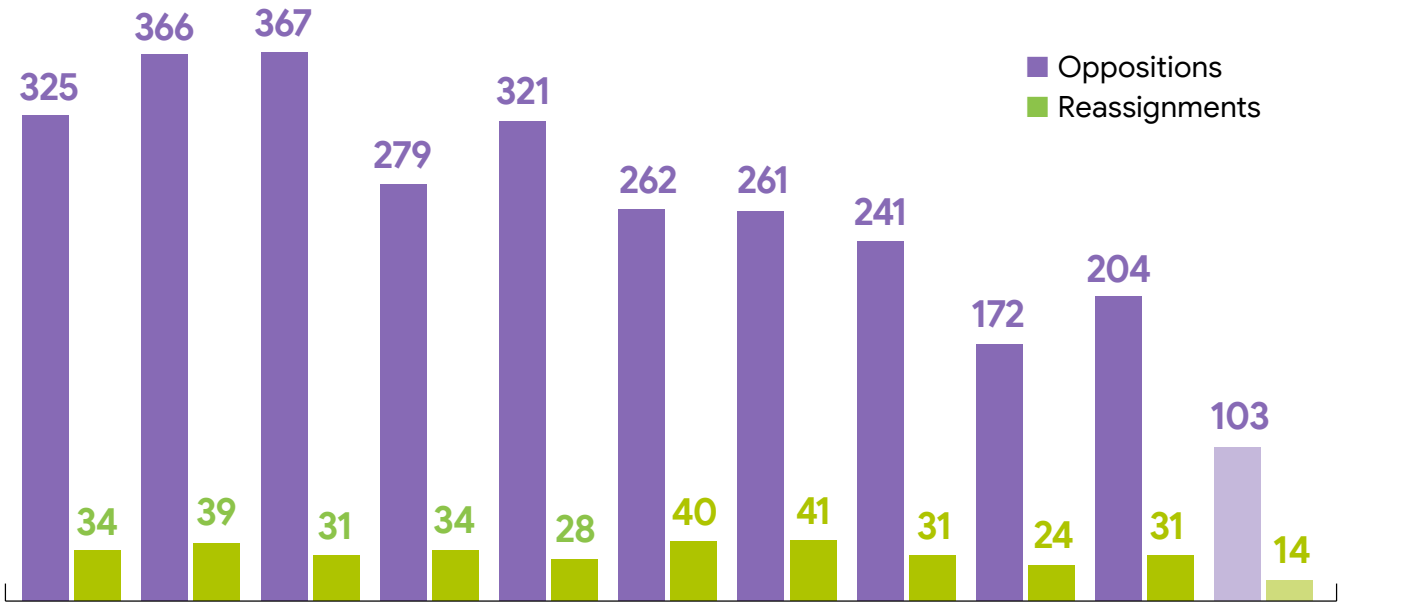
14 reassignment procedures have been introduced at PSRDs: 4 entirely national (Italian assignees/respondents and opponents/complainants), 2 among only foreign subjects, 2 initiated by Italian opponents/complainants against foreign assignees/respondents and 6 with Italian assignees/respondents and foreign opponents/complainants.



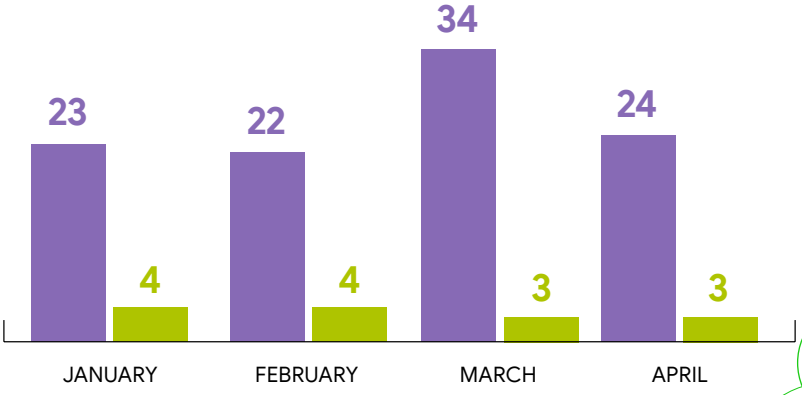
ANNUAL TREND OF OPPOSITIONS - REASSIGNMENTS

In the first four months of the year, there is an **overall increase in opposition compared to 2025**, despite different monthly dynamics. January and April show an increase of +5 oppositions each (from 18 to 23 and from 19 to 24 respectively), March jumps from 23 to 34 with +11 cases, while February shows a slight decline (-1), from 23 to 22 procedures.

The reassignment procedures are increased from 9 to 14. Most of the appeals were upheld (8 transfers of domain to the opponents/complainants), while only one case was dismissed and retains the original allocation. One procedure has been terminated and 4 proceedings are still pending, awaiting a decision by the Board.

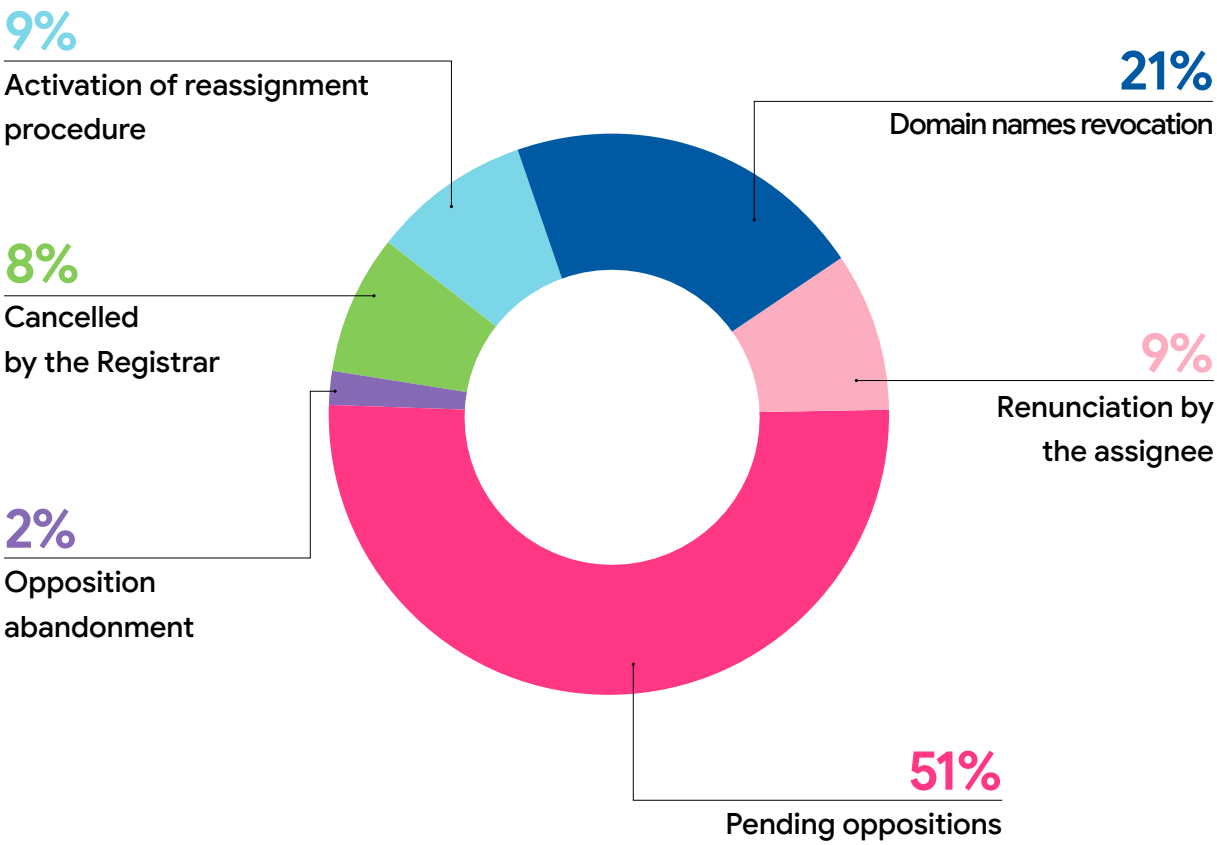


Four-month trend



RESOLUTION OF OPPOSITIONS

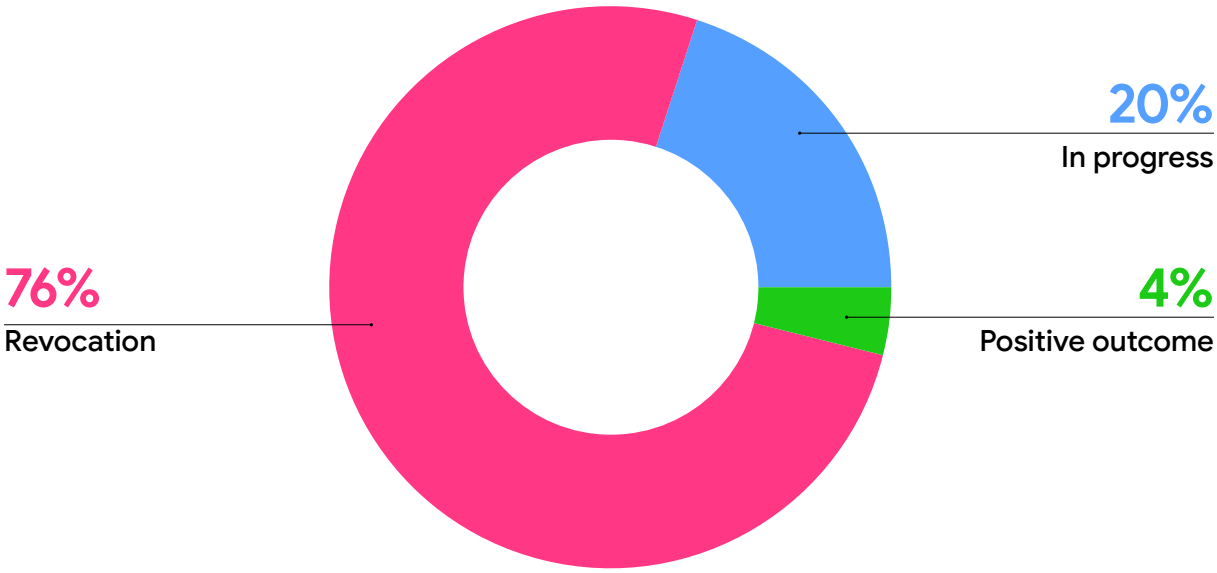
51% of the 103 oppositions are still pending. Among those concluded, the most common case is the revocation of domain names following verification of subjective requirements (21%). Both follow, with 9%, the cancellations at the request of the assignees to the Registro .it and the reassignment procedures initiated by the opponents at a PSRD. In 8% of cases the domain was cancelled by the Registrar, while in the remaining 2% the opponent formally renounced the continuation of the opposition. There is no case of termination due to non-renewal during the period considered, as the opposition remains pending for 180 working days.



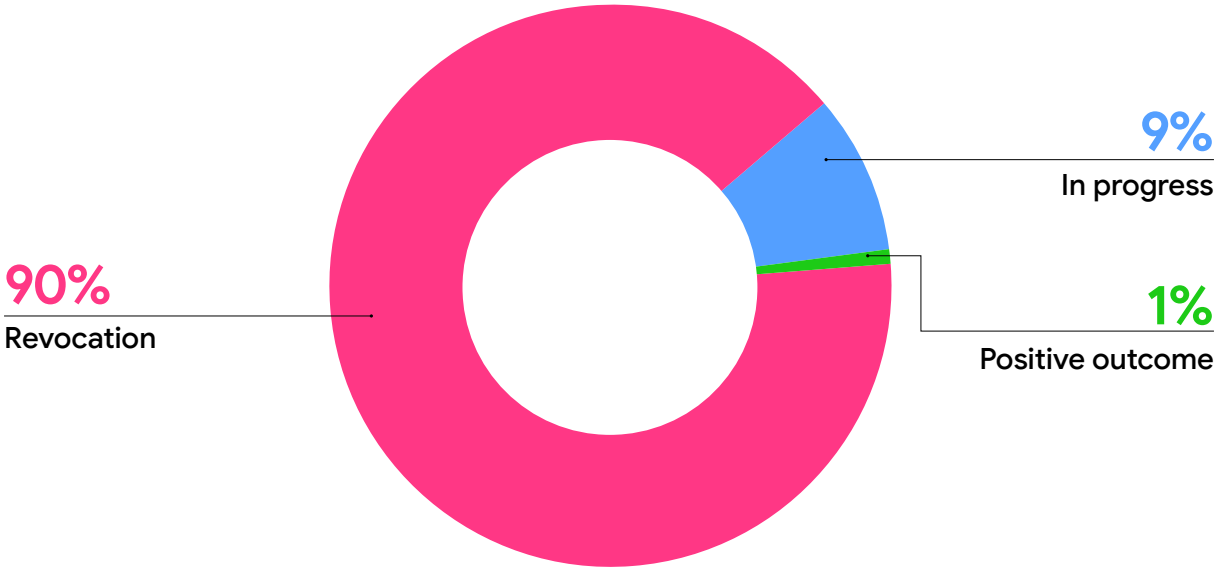
DOMAIN VERIFICATION BY THE REGISTRO

To verify the accuracy of Registrant data in the Whois database, the Registro .it started **109 verification procedures relating to 270 domain names**. Of these, 242 have been revoked, 4 have been approved, whilst 24 are still under review.

Checks January-April 2026



Domains involved January-April 2026



AUTHINFO REQUESTS

In the first four months of the year, the Registro .it issued **45 AuthInfo codes** directly to Registrants, to protect domain owners in cases where the Registrar was no longer active. There were 8 Registrars involved.

45

Authinfo code requests

45

Domains

8

Registrars involved

REQUESTS BY COMPETENT AUTHORITIES

In the first four months of the year, **the competent Authorities** – in compliance with legal prerogatives – **sent 25 requests for information concerning 28 domain names** registered in the ccTLD .it.

25

Requests

28

Domains involved

NAMES RESERVED

Domain names belonging to this category may be registered exclusively by Italian municipalities (e.g., comune. roma.it, comune.pontedera.pi.it, etc.). During the period under consideration, **13 domain names were registered**. Piedmont was the region with the highest number of registrations (3).

03

Preview
Statistics
News
In-depth dives
Events

THE FIRST 40 YEARS OF THE INTERNET: A REVOLUTION THAT LOOKS TO THE FUTURE BETWEEN AI AND QUANTUM

On 30 April 2026, forty years after the first Italian Internet connection, the National Research Council in Pisa celebrated the anniversary that marked the entry of our country into the global network. It was **30 April 1986**, when the CNR's CNUCE Institute in Pisa **set off the first "ping" toward the United States**, receiving the "ok" response from an Arpanet node in Pennsylvania: a symbolic event that made **Italy the fourth European Internet-connected country**, after the United Kingdom, Norway and Germany.

Above: the auditorium of the CNR Research Area in Pisa, venue of the event held on 30 April 2026.
Top right: **Andrea Passarella**, Director of the Institute of Informatics and Telematics of the CNR and Head of the Registro .it

The celebration took place at the Auditorium of the CNR Research Area in Pisa, on the initiative of the Institute of Informatics and Telematics (CNR-IIT), today a national and international reference point for research on networks. From the ecosystem of that pioneering experience, **one year after that first connection to the Internet**, also in Pisa in 1987, **the Registro .it was established**, the registry of Italian domain names, which is still managed by CNR-IIT.

The event had a high-profile scientific and institutional focus and **brought together representatives from institutions, academia and industry to discuss the evolution of the Internet and its future prospects**. The proceedings were opened by the Director of the CNR-IIT and Head of the Registro .it, **Andrea Passarella**, and were attended, among others, by President of the CNR **Andrea Lenzi**, the Undersecretary to the Presidency of the Council with responsibility for information and publishing, **Alberto Barachini**. From a scientific perspective, internationally renowned researchers and experts in the fields of artificial intelligence and quantum technologies took part in a discussion on the evolution of the Internet and the trajectories that will shape its future.

Franco Bernabè, President of the Board of Directors of the University of Trento and former CEO of Telecom and ENI, was also a guest of the event, and gave a keynote entitled **"The paradoxes of regulation"**. At the centre of the day, not only the historical memory of the first "ping", but above all a **reflection on the future of the Internet and the role that research is called to play in the coming years**. The speeches highlighted how the Internet is evolving from a simple communications infrastructure to a strategic platform for innovation, increasingly integrated with artificial intelligence and quantum technologies. The change taking place is less about

From the top: **Andrea Lenzi**, President of the National Research Council; Senator **Alberto Barachini**, Undersecretary to the Presidency of the Council of Ministers with responsibility for publishing and information

connectivity itself and more about the **ability of the Internet to generate, integrate and process information and services**, through digital infrastructures that combine compute, data and interaction with the physical world, **shaping an intelligent and distributed ecosystem.**

The comparison provided an articulated reading of the ongoing transformations of the Internet, highlighting the implications of **quantum technologies on the security of communications and critical infrastructure**, along with the evolution of AI models and digital architectures. There was also a strong focus on **digital sovereignty** and **technological autonomy**, in a global context marked by strong dynamics of industrial competition, geopolitics and control of strategic infrastructure. At the same time, the importance of **technology transfer and collaboration between public research bodies, universities and businesses** was highlighted as a key driver for transforming scientific findings and cutting-edge technologies into applications capable of generating tangible innovation, growth and sustainable development.

Forty years later, in Pisa, we are once again discussing the **Internet**, not as an object of memory, but as an **open question**

Top left: **Roberto Baldoni**, Senior Advisor for Technology and Cybersecurity Policy at the Embassy of Italy in the United States; **Rita Cucchiara**, Rector of the University of Modena and Reggio Emilia.
Bottom, from left: **Andrea Passarella**, the four protagonists at the time of the first connection (Stefano Trumpy, **Gianfranco Capriz**, **Luciano Lenzini**, **Blasco Bonito**), and journalist **Alessio Jacona**

of research, innovation and responsibility. The anniversary was an opportunity to mark a shift in perspective: from celebrating an infrastructure that has connected the world, to reflecting on new Internet models, the future to come, and how to govern today a technology that affects security, technological autonomy, industrial models and global assets. **A challenge that calls into question the role of public research in guiding the evolution of the Internet in a conscious and sustainable way**.

From left: **Alessandro Zavatta**, President of QTI S.r.l.; **Martina Ottavi**, Head of Quantum Communication Systems Solutions and Technologies at Thales Alenia Space; **Marco Gori**, Professor at the University of Siena; **Rita Cucchiara** and **Alessio Jacona**.

LUDOTECA OF REGISTRO .IT DIGITAL EDUCATION WORKSHOPS IN SCHOOLS

Starting from the first months of the new year, the **educational offer of the Ludoteca of Registro .it** for primary schools has focused, as in previous school years, on the issues of **digital citizenship**, proposing workshops based on the **Internetopoli web app**. A total of 180 primary school pupils participated in the activities.

As for middle schools, the privileged theme of the meetings organised by the Ludoteca was **cybersecurity**, introduced and further explored through workshops based on the **educational video game "Nabbovaldo and blackmail from cyberspace"**. A total of 335 students in Pisa and its province were involved.

From left: **Beatrice Lami**, staff member of the Registro .it Ludoteca; **Giorgia Bassi**, project coordinator of the .it Registry Ludoteca

SCHOOL-WORK TRAINING PROJECTS

As part of the **training** for **high school students**, **two school-work training projects** were activated: "Cybersecurity4Teens" (CS4T) and the "Decision-making education for digital skills" project.

CS4T is a training course, also proposed in previous school years, consisting of 8 hours of in-person lessons, entirely **dedicated to computer security** (6 hours of theoretical introduction and 2 hours of practical exercise), which also includes the participation, as a teacher, of Ilaria Matteucci, researcher at the Trust, Security and Privacy Unit of the Institute of Informatics and Telematics of the CNR (CNR-IIT). This year, two third-year classes of the IIS "Fascetti-Da Vinci" in Pisa took part in the project, with which the three-year agreement for the activities of school-work training was also renewed.

The **"Decision-making education for digital skills"** project represents a new training proposal of the Ludoteca, conceived and realised in collaboration with the benefit company Onoblo srl, specialised in services and consultancy in the training sector, with a **focus on decision-making education tools**. The aim of this proposal, which involved a fourth-year class of the "G. Carducci" High School of Human Sciences, is to promote critical awareness in the use of digital tools (social media, apps, online platforms, online content and information). The project also included a training part for the staff of the Ludoteca, useful for acquiring new skills in teaching methodology and decision-making education, with the aim of making the experience replicable.

Giorgia Bassi

PARTICIPATION IN EVENTS AND INITIATIVES

Also this year, the Ludoteca took part in **Fiera Didacta Italia 2026**, the most important event dedicated to training and innovation in education, which took place in Florence from 11 to 13 March.

On 11 March, at the CNR booth, a talk dedicated to the gender gap in **STEM** disciplines (Science, Technology, Engineering and Mathematics), with a focus on the video column **"Donne&Informatica"** (Women&IT), dedicated to women who were pioneer computer scientists, little known or not valued as they deserved to be.

On 13 March, the immersive workshop **"The SuperCyberKids Platform for cybersecurity education"** was held, with the aim of presenting the **Erasmus Plus project "SuperCyberKids"**, dedicated to training and awareness on cybersecurity. The participants were able to explore

the project's educational web platform, use its tools and educational resources based on a **game-based learning** approach, as well as simulate a "lesson plan" for further insights.

On 24 March, the event entitled **"By playing and reflecting, we learn the value of our personal data"**, organised by the Rights and Privacy Protection Association (Associazione di Promozione Sociale, APS), member - like the Ludoteca - of the **Advisory Board of the Safer Internet Centre-Connected Generations, Italian Ministry of Education and Merit (Ministero Istruzione e Merito, MIM)**. The initiative, designed to encourage dialogue between different generations and compare them, was divided into two sessions, one in the morning and one in the afternoon: In the morning session, reserved for classes (for a total of 120 students) and teachers of the classes of the high school "SMS Teresa Franchini", through games and group activities, the public was able to reflect on the importance of protecting their online data. Instead, the afternoon session was devoted to information security education, interpreted as constructive dialogue between generations. This meeting involved a round table in which experts from the Rights and Privacy Protection Association APS, the Ludoteca of Registro .it and the Polytechnic University of Marche participated.

Finally, on 25 March, **Ludoteca and EURid participated in "All digital weeks"**, one of the leading pan-European awareness campaigns on digital skills for inclusion, empowerment and employment: the joint seminar at the "F. Buonarroti" Scientific High School (Pisa) was an opportunity to introduce students to the world of domain names and the role of TLD registries, proposing a focus on cyber security and ethical hacking.

04

Preview
Statistics
News
In-depth dives
Events

THE PARADOXES OF REGULATION

Why Europe has become a digital colony of the United States and how to prevent it from remaining so in the age of Artificial Intelligence

by **Franco Bernabè**

Keynote Speech delivered by Franco Bernabè at the "40 Years of the Internet in Italy" event, Pisa, 30 April 2026 – CNR Research Area of Pisa

The Internet, whose 40th anniversary of Italy's first connection is commemorated today, has become **the most important infrastructure in the modern world**. Its success since the 1990s is not only the result of a series of important technological innovations. It is the consequence of a visionary and ambitious political design conceived by Al Gore and Bill Clinton and consistently pursued by all subsequent administrations. Compared to the initial promises, today not only the benefits but also the problems that the Internet revolution has produced are evident: in terms of social control, addiction, security and concentration of wealth. However, while the United States has benefited enormously from technology on a geopolitical and commercial level, **for almost forty years, Europe has been subjected to the American initiative and today finds itself without a true autonomous technological stronghold. Europe certainly does not lack the technical, scientific and entrepreneurial skills to hold its own, but the gap that has been created is so wide that it is hard**

Franco Bernabè, Chairman of the Board of Directors of the University of Trento and former CEO of Telecom Italia and Eni

to bridge.
Contrary to a widespread opinion, it was not over-regulation that penalised European growth in the technology sector, but quite the opposite. It was the absence or inefficiency of European regulation prior to the recent passage of the Digital Services Act and the Digital Markets Act that allowed American platforms to conquer the European market by achieving an unprecedented concentration of power in the market.
The **four elements that allowed American dominance in Europe** were **the uncontrolled access to the personal data of Europeans** that favoured the market penetration of Silicon Valley Hyperscalers, **the immunity from civil and criminal liability of the platforms, the proliferation of content** that creates addiction and **the American antitrust doctrine** that has allowed mergers that are inadmissible in Europe.

All these factors have definitely helped American Big Tech companies, but **Europe could have built its own digital champions even in the presence of those American advantages** if it had had an integrated capital market, a single digital market, a culture open to supporting entrepreneurial risk, an advanced technology transfer capacity and innovation-oriented public procurement. In forty years, Europe has done very little on these issues, today's challenge is to learn from the experience and mistakes of the past and prevent Europe from arriving unprepared at the dawn of a new revolution: that of Artificial Intelligence.
It all starts from the **original intuition of Al Gore** in the early 1990s **to make the Internet widespread by promoting its commercial** use, at that time strongly opposed by the National Science Foundation, owner of the Internet backbone.
Gore attributed a civic and international function to the network. In his words, the Global Information Infrastructure was intended to extend knowledge and prosperity, strengthen democratic participation and make it more difficult to suppress freedom of expression. The process of creating the Information Superhighways took shape with the privatisation of the network owned by the NSF in 1995, and the Telecommunications Act of 1996 which dismantled the physical and regulatory structure of the old telecommunications monopolies and paved the way for new broadband platforms that could operate without regulatory constraints.
While the United States built a system based on self-regulation, Europe followed a radically different philosophy. **The European Data Protection Directive**

It was not over-regulation that penalised European growth in the technology sector, but quite the opposite

95/46/EC, adopted in October 1995, and becoming fully applicable on 24 October 1998, in article 25 **prohibited the transfer of personal data from EU Member States to any country that did not offer an "adequate" level of protection**. Since the United States did not meet this standard, **the first thing the Americans were concerned with was to get Europe to accept the principles that had been established in the United States**. This led to the signing of the **Safe Harbour Agreement** in 2000, which allowed American companies to declare their compliance with privacy principles derived from the European Directive, and thus obtain the right to receive data from the EU. Companies that self-certified were included in a public register kept by the United States' Department of Commerce, and EU Member States were obliged to recognise them as "adequate" under European regulation.

At the time, the coordination of European national privacy authorities had repeatedly warned that **the principles were too weak, the exceptions too broad and the enforcement too dependent on self-regulation**. The most serious flaw, however, was structural in nature: **the American national security laws** - in particular those authorising mass surveillance by the NSA - **prevailed over any Safe Harbour commitments, making European citizens' data accessible to American intelligence services** without any legal remedy.

The agreement survived until 6 October **2015, when the Court of Justice of the EU invalidated it in the Schrems vs. Facebook Ireland ruling**, in that the

While the United States built a system based on self-regulation, Europe followed a radically different philosophy

American mass surveillance practices of which there had been numerous examples were incompatible with European fundamental rights, and **EU citizens had no legal and effective remedy.**

After the invalidation of the Safe Harbour, the European Commission and the United States announced on 2 February 2016 a new framework for transatlantic transfers, the **Privacy Shield**, presented as a response to the Court's findings. But in reality, **even this did not solve the problems raised by Schrems**, who in fact reformulated the complaint against Facebook Ireland arguing that, even after the Safe Harbour was no longer valid, **transfers to the United States remained incompatible with EU law** because US law and practices did not guarantee adequate protection against access by public authorities.

Once again, the Court agreed with Schrems by invalidating Privacy Shield with the judgement of 16 July 2020.

The EU's further policy response was the 2023 **Data Privacy Framework**: on 10

July 2023, the Commission adopted a new adequacy decision stating that the United States had introduced binding safeguards to limit intelligence access to what was "necessary and proportionate" and a new redress mechanism for European data subjects. In essence, **Brussels attempted a third legal architecture to preserve data flows**, maintaining the adequacy model but trying to respond to the two flaws that had brought down the Safe Harbour and Privacy Shield, i.e., surveillance and judicial protection.

In reality, **the Data Privacy Framework does not prevent American intelligence from accessing the personal data of European citizens**, including communications, but **claims to limit access to what is "necessary and proportionate"** for national security and to subject it to new control and redress mechanisms.

The decisive issue is not only that American services can access data, but that European privacy and data protection rights are not automatically transformed into directly actionable claims against US intelligence before an independent judge in the US. This means that **there is no key moment in which an external and impartial party verifies whether the collection is really necessary, proportionate and limited to the minimum necessary according to the European standard.**

For almost twenty years - from the birth of the commercial web in 1995 until 2018 - American companies have therefore operated in Europe without constraints and effects on the collection of personal data and the consequent profiling techniques. The platforms used

From 1995 to 2018, American companies have therefore operated in Europe without constraints and effects on the collection of personal data and the consequent profiling techniques

their terms of use as a contractual basis, arguing that by accepting the terms of service, the user implicitly consented to the collection and processing of their data.

The General Data Protection Regulation, which came into force on 25 May 2018, **introduced a paradigm shift, but by then, the situation was compromised. The net result of this journey is that American platforms have built their own global competitive advantage** - profiling databases with billions of profiles, targeting algorithms trained on decades of behavioural data, vertically integrated advertising infrastructures at a time when there were no rules and no regulations.

The problem, however, is not only the competitive advantage deriving from access to users' personal data, but also the fact that **platforms have been allowed to use manipulative techniques to create addiction to networks**.

For this reason, it is necessary to go back to another measure passed by the United States Congress, **Section 230 of the Communications Decency Act**, which is an integral part of the

Telecommunications Act of 1996. As a result of this measure, **providers would not have been considered "publishers" or "distributors" of other people's content**, therefore not subject to civil or criminal liability for it.

The effect was immediate and transformative: technology companies could host unlimited amounts of user-generated content without the risk of going to court for any amateur post, illegal content or false information. American courts interpreted Section 230 more and more broadly, exempting platforms not only from liability for third-party content, but also for the algorithmic choices that determined what content to amplify. **Platforms soon discovered that emotionally intense content** - anger, fear, outrage, addictive content - **generated the most engagement, and therefore the highest advertising revenue**. Since no regulation required them to moderate such amplification, and since self-regulation was exactly the principle that Magaziner codified in the 1997 Framework, companies not only tolerated toxicity, but deliberately engineered it into their products.

When the EU built its platform liability regime with the **E-Commerce Directive 2000/31/EC** - adopted four years after Section 230 - it chose a formally different but substantially compatible approach with the American one. **The Directive exempts hosting providers from liability as long as they are not aware of illegal content** or, once they become aware, remove it promptly. It did not introduce proactive monitoring obligations, did not impose algorithmic transparency, did not recognise the distinction between content and platform design.

The result was that **American companies operated in Europe under essentially the same conditions as they had at home**: protected from liability for third-party content, free to design amplification algorithms without accountability, authorised to self-regulate. This convergence was not accidental: European law developed in parallel with Section 230, in a context in which the liberalisation of digital trade was the goal shared by Washington and Brussels, and in which the Safe Harbour agreement of 2000 had already established the principle that American companies would operate in Europe according to their own internal standards.

The EU started to become aware of the problem in 2016-2018, in the wake of the Cambridge Analytica scandal, where there were allegations of electoral manipulation and growing political pressure on platforms.

After years of soft law and voluntary codes of conduct, **the European Commission changed its strategy and in December 2020 presented the Digital Services Act**.

The DSA, which came into full force for very large platforms in 2023, introduces for the first time a liability system based not on the individual illegality of the content but on the systemic risk of the platform: companies must assess whether their architecture, including recommendation algorithms, produces negative effects on civic discourse, public safety and minors. **This paradigm shift has generated a very harsh reaction from the American side**. In 2024, US tech companies received total fines of more than €3.8 billion

from the EU. The Trump administration's response has been systematic: threats of tariffs, diplomatic pressure, denied visas to European officials involved in the enforcement of the DSA, accusations of censorship and attacks on the European regulatory system defined as "Orwellian" by US Secretary of State Rubio.

Only now, also in the United States, courts are beginning to distinguish between immunity for user content - which remains protected by Section 230 - **and liability for the conduct of the platform**, i.e., for design choices that amplify toxic content. The judges in the cases against Meta, YouTube, Snap, and TikTok recognised that features such as infinite scrolling, algorithmic distribution and reward systems fall within the scope of conduct and are not protected by Section 230. **This evolution of American jurisprudence, combined with the European DSA, configures for the first time a double front of systemic accountability for platforms**, although operating from profoundly different legal traditions.

We come to the last factor that has favoured the substantial **monopoly of American platforms** and which, together with the insufficient availability of risk capital in Europe, has prevented European technology companies from growing to the point of being a risk from the point of view of competition. **The differences in the antitrust doctrine between the United States and Europe** is one of the most important structural factors in **explaining why the big tech companies are all American and not European.** Until the 1970s, American antitrust law had a structuralist vocation: large concentrations of market power were considered suspect in themselves, regardless of their immediate effect on prices. The turning point was the publication in 1978 of the book **"The Antitrust Paradox"** by jurist Robert Bork in which he argues that **the only legitimate objective of antitrust law is to maximise the welfare of the consumer**, defined as almost exclusively through prices, outputs and production efficiency.

If an acquisition or market practice does not increase prices to the consumer in the short term, it is by definition acceptable, even if it structurally reduces competition. The Reagan administration accepted this doctrine in an organic way and the American antitrust stopped asking whether a dominant company was supporting future competition, and limited itself to verifying whether the prices paid by consumers at the time were high.

The problem exploded in the technology sector because the services of the biggest platforms - Google Search, Facebook, Gmail, YouTube - were formally free for the end user. The consumer welfare standard, measured by the price paid by the consumer, did not detect any harm: the price was zero. So **Google was able to acquire DoubleClick in 2008, YouTube in 2006, Waze in 2013, Nest in 2014** - building a vertically integrated system - without any American authority seriously blocking a single transaction. **Facebook was able to acquire Instagram in 2012 for 1 billion of dollars and WhatsApp in 2014 for 19 billion of dollars**, eliminating its main emerging competitors without receiving antitrust opposition. The implicit reasoning was always the same: **consumers do not pay more, therefore,**

there is no harm to them.

European competition law is based on radically different assumptions. Articles 101 and 102 of the TFEU (Treaty on the Functioning of the European Union), respectively, prohibit anti-competitive agreements and abuses of dominant positions, and the latter concept is built in a structural way: a dominant undertaking has a responsibility not to distort competition even by conduct which, if implemented by a non-dominant undertaking, would be lawful. The European Commission does not have to prove that prices to consumers have increased: it is sufficient to demonstrate that the conduct of the dominant undertaking excludes or penalises competitors and strengthens the market position. This allowed Europe to fine Google 8 billion of euros in three proceedings between 2017 and 2019, hit Apple with 1.84 billion of euros for restrictions in the App Store, and initiate proceedings against Amazon, Meta and Microsoft.

The combination of permissive antitrust enforcement in the US and a fragmented European capital market has resulted in a technological drain from Europe to the US. American tech companies have systematically bought the most promising European startups in pre-IPO stages, using their huge liquidity generated precisely by the lack of antitrust enforcement at home - for transactions that often escaped even the notification thresholds provided for by EU legislation.

The situation is further exacerbated by a second structural factor in Europe: the fragmented capital market and the differences in the legal systems that entail cumulative compliance costs that

The European Commission must demonstrate that the conduct of the dominant undertaking excludes or penalises competitors and strengthens the market position

an American company never encounters within its home market. Acknowledging that traditional antitrust procedures - based on case-by-case, years-long investigations and with sanctions imposed only ex post were inadequate for technology markets where competitive advantage is built in months, **the EU changed its approach with the Digital Markets Act of 2022**.

— The DMA does not wait to prove abuse: it designates dominant platforms as “gatekeepers” in advance and imposes proactive obligations on them - prohibition of self-preferencing, openness to interoperability, obligation to share data with third parties - regardless of any finding of concrete harm.

The American reaction was immediate: the diplomatic pressure of the Trump administration against the DSA and the DMA, the accusations of discrimination against American companies, the threats of tariffs - all this configures the transatlantic digital conflict not as an abstract legal dispute, but as a clash of economic sovereignty in which competition law has become an

instrument of technological geopolitics.
As in the 1990s with the Internet, **the AI revolution today reproduces the same basic pattern**: the United States builds the technology and the market by letting the private sector run without constraints; Europe responds with regulation. The **AI Act of 2024 is what the GDPR was for personal data**: an attempt to set standards for security, transparency, and accountability before the market irreversibly consolidates. The symmetrical risk is the same: **regulation comes when the American competitive advantage is already structurally consolidated**, and thus becomes a further obstacle for those who have to catch up.
Here, however, the parallel with the Internet stops. In the 1990s the confrontation was bilateral: USA on one side, Europe on the other, with Washington dictating the rules of the game and Brussels trying to impose their own.

Today the field is tripolar, and the geometry of power is radically different. **China is not a regulated player like Europe**: it has a national AI strategy that covers the entire technology stack - basic research, semiconductors, foundational models, vertical applications, 6G, quantum. Above all, China has adopted an open-source strategy - with DeepSeek, Qwen, Alibaba and others - that has a precise geopolitical function: to lower the barriers to entry to AI technology for countries that want to reduce dependence on the US, gain global market share and build ecosystems dependent on Chinese infrastructure. DeepSeek R1 costs 20-30 times less than equivalent American models, making it accessible to European startups with limited spending power.
Europe is therefore in a classic dilemma: **using Chinese technology to reduce American dependence risks creating an equally or more dangerous Chinese dependency**. The most organic and authoritative answer is contained in the **Draghi Report of September 2024**, which diagnosed the problem with clarity: Europe risks losing technological sovereignty not due to a lack of talent, but due to a lack of scale, capital and coordination.
Draghi recommends opening up European public supercomputers to a federated public-private model that makes computing power available to European SMEs and startups for training and fine-tuning models, so as to bridge the gap in access to infrastructure compared to American operators. It also proposes an ad hoc law to harmonise cloud architecture requirements, coordinate public procurement and create a single European framework for the “computing capital” accessible to innovative companies. This would provide European startups with a real alternative to the American cloud providers - AWS,

The digital conflict between the EU and the United States has now become a struggle over economic sovereignty, in which competition law has become an instrument of technological geopolitics

Azure, Google Cloud - which now control more than 80% of the European cloud market.

In the age of Artificial Intelligence, the EU has real competitive advantages in sectors such as advanced manufacturing, pharmaceuticals, energy, automotive, agri-food and financial services. To exploit these advantages to the fullest, a plan is needed that finances the development of AI models specialised in these sectors, built on European data and protected by antitrust enforcement. **To create European value in AI, it is not necessary** to compete head-on on generalist foundational models - where the American and Chinese advantage is structural - but **to excel in the vertical applications where data, industrial know-how and European regulation are an asset**.

Compared to the world of the Internet, in AI the stake is direct industrial competitiveness, not just the protection of individual rights. If Europe fails to develop its own AI technology development model, the risk is that European industry - manufacturing, health, energy, finance - will find itself using American or Chinese AI for its critical production processes, losing all the competitive advantage it still possesses.

Draghi Report (2024): Europe risks losing technological sovereignty not due to a lack of talent, but due to a lack of scale, capital and coordination

DOMAIN RENEWAL ANALYSIS: THE .IT CONTRIBUTION TO THE CENTR TASK FORCE

by **Daniele Sartiano**

Renewing a domain name is not only an administrative step, it's also a **sign of continuity**: it tells us whether a domain maintains its value over time, whether it remains connected to a project, service, digital identity or still-relevant online presence.
For registries and Registrars, reading these signals means having a precise understanding of market developments, being able to interpret portfolio stability, and identifying, in advance, areas where domains are most susceptible to non-renewal. In this sense, renewal becomes a key to understanding the domain name life cycle and its perceived value by registrants.

From this need comes the **Benchmarking Renewal Indicators Task Force promoted by the Council of European National Top-level Domain registries (CENTR)**, which was launched in May 2025 during the CENTR Jamboree in Lyon.
Ten ccTLD registries (.at, .be, .de, .ie, .it, .nl, .no, .nu, .nz, .uk) participated in the task force, with the aim of establishing a shared methodology for analysing domain name renewals. The study examined around **40 million domains expiring in 2024**, analysing the indicators one month before the expiry date, so as to observe the domain at the time closest to the renewal decision. Each registry conducted local processing on its own data, subsequently sharing only aggregated results.
For Registro .it, the signals most related to renewal were the domain age and the age and category of the registrant.

Ten ccTLD registries (.at, .be, .de, .ie, .it, .nl, .no, .nu, .nz, .uk) participated in the task force, with the aim of establishing a shared methodology for analysing domain name renewals

Registro .it has contributed to this project by taking its case study into a broader comparison between registries. This work has allowed us to identify and **share indicators, code and analysis choices**, while maintaining a **"privacy-first" approach**, without sharing sensitive registrant data.

The work of the task force is summarised in the article available in the CENTR blog **Analysing domain name renewals across ccTLDs**, which traces the main results, focusing on the case of Registro .it and on the most significant trends observed in the Italian data.

OBJECTIVE: DOMAIN RENEWAL INDICATORS AND DYNAMICS

The main objective of the work was **to identify the indicators most associated with domain name renewal**, so as to understand which signals distinguish the most stable domains from those most at risk of non-renewal.
The task force therefore focused its analysis on a central question: **which characteristics of the domain name and related data are associated with the renewal?** Answering this question helped identify the most precise indicators, ones that could constitute the basis for tools that can estimate the likelihood of renewal and help Registrars analyse their domain portfolio.

THE WORKFLOW OF THE ANALYSIS

The work started with a review of the indicators already used or deemed useful by the participating registries. This first phase made it possible to compare different experiences and approaches and to understand what information was available in a sufficiently homogeneous way in the various national contexts. In fact, the process of renewing domain names can vary from one ccTLD to another, so harmonising the indicators and arriving at a shared definition of the indicators was not a straightforward task.

A common set of indicators has been defined from this analysis, not as an abstract list of variables, but as a useful basis for comparing results between registries

A common set of indicators has been defined from this analysis, not as an abstract list of variables, but as a useful basis for comparing results between registries. The **indicators identified** cover, at high level, the

following areas:

- **characteristics of the domain name**, such as length and presence of numbers;
- **registration history**, including domain age, any recent transfers between Registrars and post-issue registration cases;
- **registrant profile**, considering domain age, domain portfolio number and location relative to the ccTLD country;
- **category of the registrant**, distinguishing, for example, natural persons, companies and other types of entities;
- **technical and usage variables**, such as the presence of MX records, crawling status, web usage level, and **DNS magnitude**;
- **context of the Registrar**, with particular attention to the business model declared or reconstructed through shared classifications.

Each registry then compiled its own data locally, calculating the indicators according to the agreed definitions and **linking them to a common scheme**. The comparison was made only on the **aggregated results and not on the raw data, which made it possible to work together without transferring sensitive information on the registrants**. The analysis process included three main moments: **a first descriptive reading** of the signals, a **statistical model** to evaluate them jointly and, finally, an **interpretative analysis** of the results.
The natural evolution of this work is the possible transformation of the analysis process into an operational tool, with **renewal scores or risk signals made available to Registrars also via API (Application Programming Interface)** so as to allow integration into their systems.

Dal benchmarker CENTR al caso .it

DATA, METHOD AND PRIVACY

The analysis, in particular, examined the domains that were expected to expire in 2024. The indicators were measured with a one-month window of time to the expiry: making it possible to photograph the status of the domain and related data (such as the registrant) when the renewal outcome was near.

In particular, **Registro .it built a data extraction and calculation pipeline** that was consistent with the shared scheme defined by the task force. The aim was **to make the results comparable, while starting from different databases and information structures**.
A central element of the project was the "privacy-first" approach. Each registry performed the analysis on its own perimeter, on its own data, sharing only aggregated results with the task force. Comparability therefore does not result from centralisation of the datasets, but from the alignment of the definitions, transformations and measures produced.
The availability of indicators was not identical for all registries. For this reason, **the framework has been designed in a flexible way**, so that participation is possible even in the presence of missing variables, while maintaining a common methodological basis.

From the indicators to the statistical model
To interpret the findings, the task force followed a multi-step approach. Initially, **Cramer's V** was used to observe one indicator at a time and measure how associated it was with renewal. This first step allowed us to quickly **identify the most obvious signs and compare different indicators, such as domain age and the age or category of the registrant**.
A **logistical regression**, i.e., a statistical model that allows **looking at several indicators together**, was subsequently applied. This step is important because **some signals can be linked together**: for example, longer-lived domains often belong to registrants with a longer history in the registry or with a larger domain portfolio. Regression therefore helps us understand which indicators remain relevant even when considered together with others.
To make the results of the model clearer, the regression was then interpreted through two complementary readings: the "**odds ratios**", useful for understanding the direction and strength of the association, and the marginal probabilities, more immediate for reading the result in terms of renewal probability.

Longer-lived domains often belong to registrants with a longer history in the registry or with a larger domain portfolio

The technical path can then be summarised as follows:
- **Cramer's V**: looks at one indicator at a time and measures how much it is associated with renewal.
- **Logistical regression**: looks at several indicators together and shows which signals remain relevant even in the presence of the others.
- **Odds ratio**: technically expresses the estimated effect of the regression.

Values above 1 indicate a positive relationship with renewal, while values below 1 indicate a negative relationship.

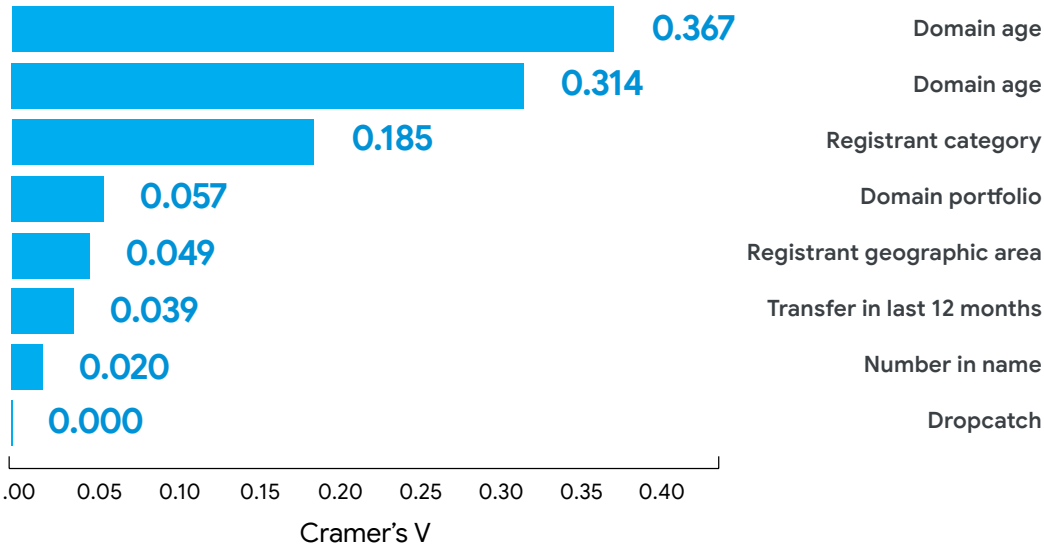
- **Marginal probabilities**: they translate the model's predictions into a more readable form, showing how the expected renewal probability changes as some key indicators change.

In this way, the analysis maintains a solid statistical basis, but also remains readable from the operational viewpoint: first it detects the strongest signals, then it tests how they behave when evaluated as a whole.

THE MAIN SIGNS OF RENEWAL IN .IT

In **the .it case**, the results show a clear structure: **the history of the domain and the history of the registrant are the most explanatory signals**. Not all indicators contribute in the same way: some describe useful but weak dimensions, while others emerge more continuously in both the descriptive reading and the statistical model.

.it: signals associated with renewal

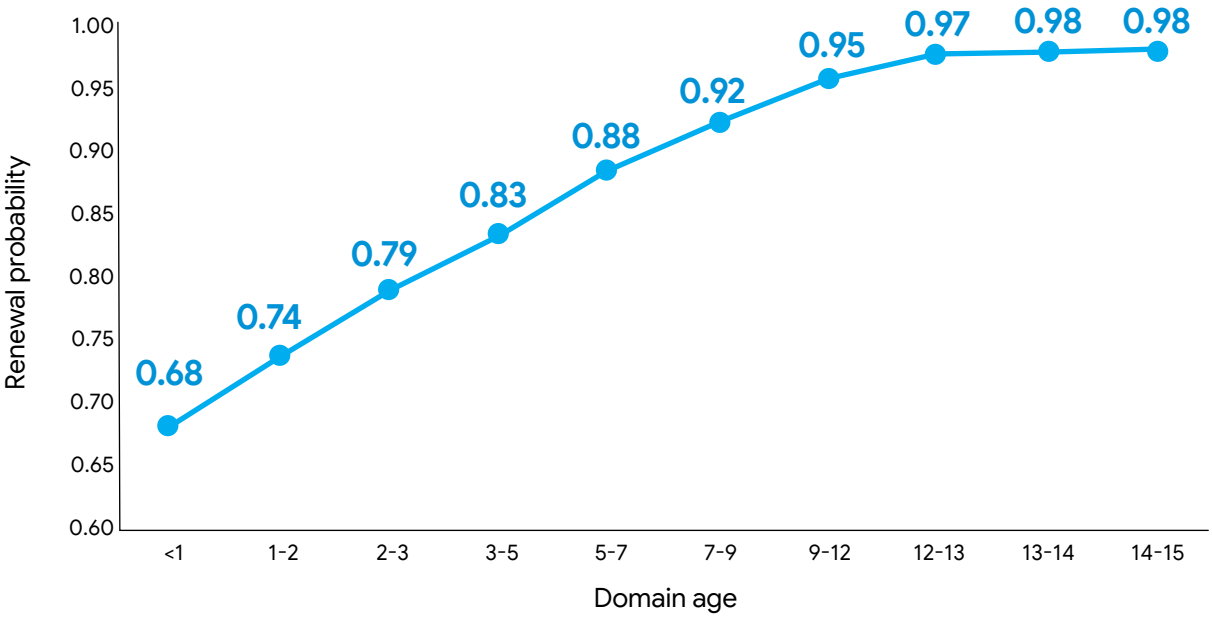


The first element that emerges is the **age of the domain**, which in the descriptive analysis is the indicator that is **most closely associated with the outcome of the renewal. The age and category of the registrant** then follow, while the other indicators have a lower weight.

The result is also consistent with an intuitive reading of the domain life cycle: **a longer-registered domain more often tends to be associated with a business, digital identity, technical services or established**

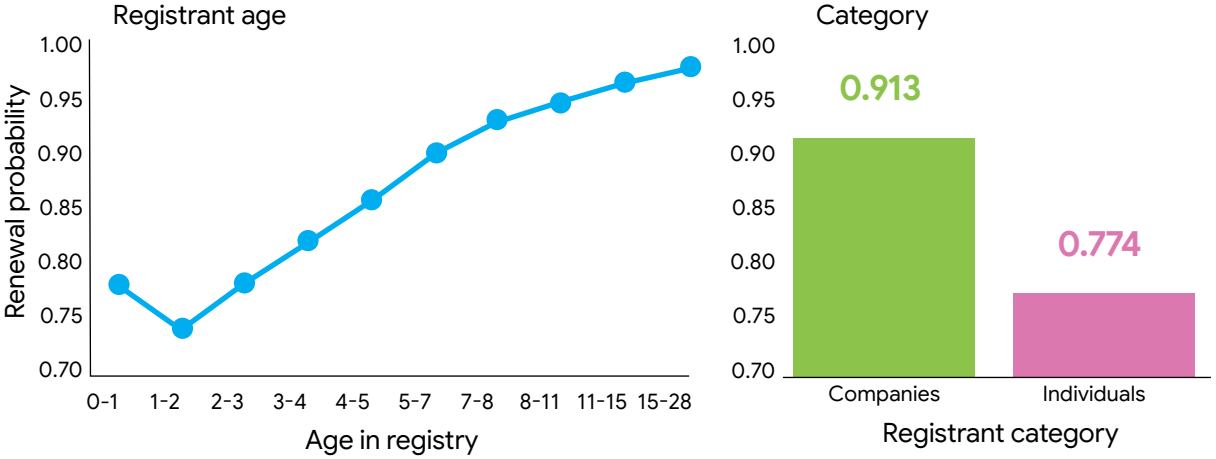
relationships. In these cases, non-renewal can result in a higher cost, not only economic, but an organisational and reputational cost as well. By contrast, **younger domains may be more fragile**, given that experiments, projects that are not yet mature or occasional registrations are more likely to not continue in time.

.it: renewal by domain age



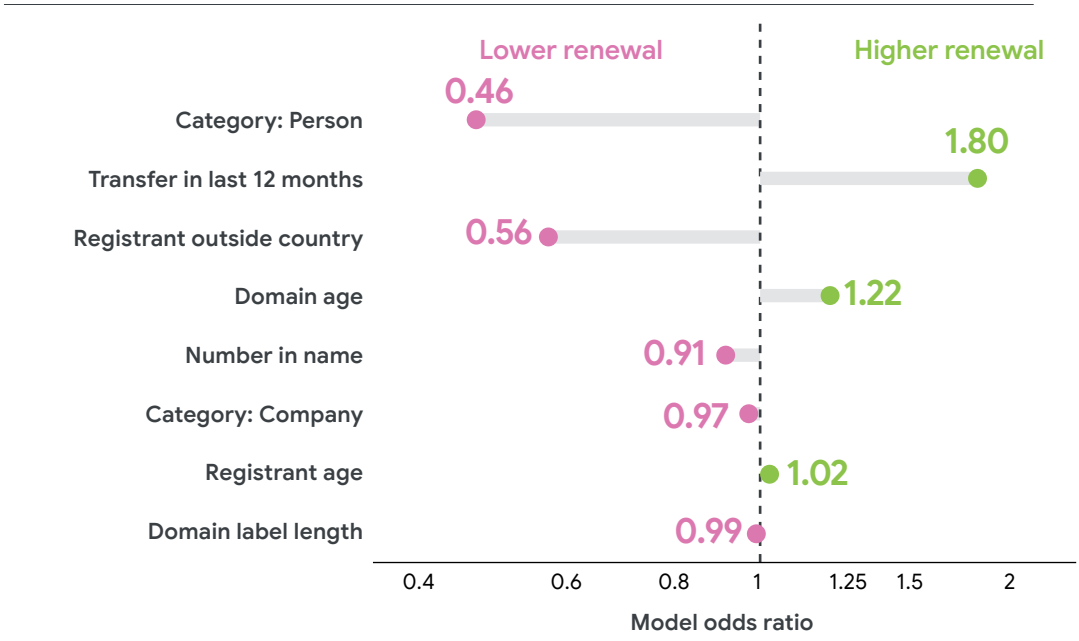
The estimated marginal probabilities confirm this dynamic. The result is very clear: **the older the domain, the more likely it is to renew**.

.it: ruolo del registrante



The history of the registrant also plays an important role. **A longer registrant in the registry may indicate a more stable relationship with the domain and**, more generally, indicate management of their online presence. This does not mean that the age of a domain determines its renewal, but it is an indicator of continuity in behaviour.
Not all registrant types show the same behaviour. The registrant category adds an additional interpretative dimension: **in the .it domain, domain names registered to companies show a higher renewal probability than those registered to individuals**.
This difference may reflect different uses of the domain. For an enterprise, a domain name is often an integral part of the digital identity, involving communication, e-mail, e-commerce, or customer and supplier relationships. For a natural person, the domain is more often linked to individual, temporary or experimental needs. Again, this should not be read in causal terms, but as a signal that helps us understand the different stability of the profiles observed.

.it: direction of model signals



The chart shows some effects estimated from the statistical model. Values above 1 indicate signals associated with a higher probability of renewal, and those below 1 indicate signals associated with a lower probability. The reading is different from Cramer's V: here the indicators are evaluated together, not individually

Transfers between Registrars are positively associated with renewal. This may indicate that a recent transfer is often linked to active domain management, although the effect may vary between markets and trade policies.
Other indicators show a negative association. The presence of numbers in the name has a limited effect, while the fact that the registrant is not located in the country of reference is associated with a lower tendency to

renew. The latter result suggests that **territorial rooting may play a role in domain continuity**, while requiring caution in interpretation.
Overall, the .it case returns a consistent picture: older domains associated with registrants with a longer history in the registry show a higher probability of renewal, while younger domains, or those with less rooted signals, are more susceptible to non-renewal.
The results also show good consistency between descriptive reading and the statistical model: the signals that emerge in the first phase of the analysis remain relevant even when evaluated together with the other indicators. **However, it is important to remember that the indicators describe statistical associations and not cause and effect relationships**.

FROM DATA TO TOOLS FOR REGISTRARS

The natural evolution of this work is the **development of operational tools for renewal analysis**. The indicators identified in the study form the basis for developing systems that can **estimate** the probability of renewal of a domain name as it approaches its expiry.
For Registrars, tools of this kind could offer concrete support in the management of the domain portfolio: identifying weaker domains, better interpreting renewal patterns, defining targeted actions, and integrating indicators into their internal systems.
API integration would also allow these analytics to be embedded directly into operational flows, allowing Registrars to monitor their domains as they near expiry.

For Registrars, tools of this kind could offer concrete support in the management of the domain portfolio

Domain name renewal is a valuable lens for observing the stability, continuity and perceived value of one's online presence. In the .it case, the analysis shows that some signals are particularly explanatory, confirming how the **history of the domain and registrant** contribute significantly to the **continuity of registration over time**.
The contribution of the Registro .it is part of a broader framework of technical collaboration within CENTR. The task force has shown that different registries can address a common issue by sharing methods, indicators and tools, without sacrificing data protection.
The result is a concrete working model: **starting with data, building comparable signals, and turning analytics into useful knowledge for registries, Registrars, and ccTLD communities.**

FROM AI TO NIS2: THE DIGITAL CHALLENGES FOR BUSINESSES IN THE LIVE LINKEDIN OF REGISTRO .IT

by **Chiara Spinelli**

A space for discussion with well-known and acclaimed guests in the national panorama on the great changes in digital, from artificial intelligence to the challenges of cybersecurity: the **cycle of live LinkedIn** organised by Registro .it got underway in the first months of the year with new appointments, all of them conducted by the journalist Massimo Fellini.

After the episodes of October and December, which focused respectively on the themes of online identity and internationalisation, the cycle of meetings continued by addressing **three issues that currently directly affect the competitiveness of companies: AI for websites and marketing, digital challenges for tourism and the NIS2 Directive on cybersecurity**.
As in the previous episodes, the format has maintained an informative but concrete style, alternating strategic reflections with practical examples. The live streams will of course remain available not only on the LinkedIn page of the Registro, but also on YouTube, as tools that we hope will remain useful for an informed reflection on these issues in the months to come.

AI FOR SME WEBSITES: PRODUCTIVITY, CONTENT, AND NEW SEARCH MODELS

The cycle's third live LinkedIn, airing on 21 January, entitled **"AI for SME websites: how to improve productivity and marketing with smart tools"**, addressed the impact of AI on the communication strategies of enterprises. Guest of the episode was **Raffaele Gaito**, *growth coach*, trainer and populariser on the themes of marketing and digital innovation.
AI is rapidly changing the way

companies produce content, organise work, and build their online presence. But AI is now perceived by many SMEs as a tool yet to be understood, with doubts about costs, in-house training, and the actual ability to integrate AI into business processes.

Gaito pointed out that the true value of AI lies in the possibility of improving the quality of work and increasing productivity. According to Gaito, AI cannot completely replace skills, strategic vision and authenticity, but thanks to its tools (from the writing of texts for the web to data analysis, generation of creative ideas and management of workflows) it can help businesses speed up repetitive tasks and focus more on the strategic aspects of their business. And while a company's website was once intended primarily to be found by traditional search engines, it must now also be designed to engage with AI assistants and new conversational search systems. The world of GEO (Generative Engine Optimisation) is still unexplored, but what we are certain of, according to Gaito, is that **the centrality of a website will not be lost**. Clear, structured, authoritative and up-to-date content remains central not only to the classic SEO, but also to the visibility within responses generated by platforms such as ChatGPT or Gemini.

AI cannot completely replace skills, strategic vision and authenticity, but - thanks to its tools - it can help businesses speed up repetitive tasks and focus more on the strategic aspects of their business

DIGITAL TOURISM: WHEN THE ALGORITHM BECOMES THE NEW TRAVEL AGENT

The live broadcast of 17 February, entitled **"The new travel agent is an algorithm: but the ticket to trust remains .it"**, shifted attention to the tourism sector, one of the sectors most transformed by the use of data and artificial intelligence. Guest of the meeting was **Mirko Lalli**, Founder and CEO of The Data Appeal Company, a company specialising in the analysis of tourism data and online reputation.

Mirko Lalli recalled how **algorithms have been influencing tourism for years, influencing every stage of the travel experience**, from the choice of destination to booking, up to personalised suggestions during the stay. But **generative AI brings an even more disruptive revolution: it changes the**

way people search for information and build trust online. More and more users are relying on chatbot conversations to decide where to go, what to book, and what experiences to try. Like Gaito, Lalli also pointed out that in this changing landscape, **the proprietary website continues to play a central role**: it is the place where companies, accommodation facilities and destinations can best consolidate their digital reputation, be found and be chosen.

The perceived value of a tourist facility is built through data, reviews, comments and online conversations, which algorithms continuously process to determine visibility and positioning. For this reason, even in the age of chatbots, for Lalli to maintain his **digital presence is not just "to be there", but to govern content, communication and credibility consistently**. AI does not erase the need for trust, but rather, makes it even more important to have a recognisable and authoritative digital presence, and the .it domain is a sign of authenticity, territorial proximity and reliability.

More and more users are relying on chatbot conversations to decide where to go, what to book, and what experiences to try

NIS2 AND CYBERSECURITY: SECURITY BECOMES A STRATEGIC RESPONSIBILITY

The fifth and final live broadcast of the cycle, aired on 25 March with the title **"Cybersecurity, with NIS2 everything changes: greater responsibilities, starting with the Boards of Directors"**, addressed one of the most urgent issues for digital businesses and organisations: **Cybersecurity and the application of the NIS2 Directive**. The meeting involved the participation of **Ernesto Belisario** (lawyer and expert in innovation and AI law), **Donato Molino** (Chairman of the Steering Committee of Registro .it – CIR and AssoTLD) and **Valentina Amenta** (Head of the Legal and litigation Unit of Registro .it).

As Ernesto Belisario has pointed out, **the European NIS2 Directive represents a paradigm shift in cybersecurity management**, a necessary evolution in light of the rise in cyberattacks and "data breach" costs. **We need a more structured approach to security that also directly involves the administrative bodies of companies**, because the

directive introduces clear obligations not only on the technical level, but also on that of governance: the Boards of Directors will be called upon to approve security measures, supervise their implementation and promote internal training pathways.
Among the most innovative aspects of the legislation (also with respect to NIS1) there is also the theme of **supply chain security**, emphasised by Valentina Amenta. Security is no longer just about the individual organisation, but about the entire digital ecosystem in which it operates: suppliers, partners and infrastructure become an integral part of risk management. Companies must therefore introduce controls, audits and security requirements across the entire value chain, adopting a more informed and proactive approach. An awareness never imagined before in such a capillary way.
The directive also imposes a **very rapid time-frame for reporting cyber incidents** and introduces a **significant penalty system**, which requires more mature organisational structures and well-defined processes. In this context, as Donato Molino explained, many companies are moving from a first phase of formal fulfilment to more operational work, consisting of risk analysis, definition of procedures and implementation of concrete measures of business continuity and "disaster recovery". While integrating NIS2 procedures is less problematic for large companies and can also ensure

Security is no longer just about the individual organisation, but about the entire digital ecosystem in which it operates

greater consolidation in the market, **SMEs face a shortage of skills and limited resources**, and the October deadline is likely to be seen as very problematic. Precisely for this reason, Molino stressed the **importance of collaboration between institutions, trade associations and operators in the sector to accompany companies on the path of adaptation**, also recalling the increasingly central role of Registrars. Today, they are considered essential to the security of digital infrastructure and the proper management of domain name data.
The final message that emerged from the discussion is clear: NIS2 cannot be interpreted as a mere bureaucratic obligation, but as a strategic investment aimed at strengthening the resilience, reliability and competitiveness of the Italian digital system.

TEACHING CYBERSECURITY: “NEL MEZZO DEI MAGHI”, THE NEW BOARD GAME FROM LUDOTECA, IS ON ITS WAY

By **Giorgia Bassi**

The aim of the Ludoteca of Registro .it is to spread the “digital culture” among the young generations. This involves the constant search for innovative methodologies and educational tools capable of holding children’s attention. For them, in fact, **the online dimension is a natural extension of everyday life** and, precisely for this reason, it’s not perceived as something requiring explanations or educational interventions.

Hence the need **to devise game-based tools** that trigger active and experiential learning modes, capable of conveying specific but also transversal skills, such as critical thinking and the ability to work in groups.

"NEL MEZZO DEI MAGHI" (AMONG THE WIZARDS)

On this basis, the idea was born to create a new educational game, entitled "Nel Mezzo dei Maghi" (Among the Wizards), dedicated to security protocols, a specific area of cybersecurity, intended for children aged 10-14 years.

The project was born from the collaboration of Ludoteca with CINI (the National Interuniversity Consortium for Informatics) and, in particular, with **Cybersecurity National Lab** that operates within it and the **IMT School of Advanced Studies of Lucca**. Both of these academic research poles propose third-mission activities, with initiatives aimed at the world of schools and "public engagement" in general.

"Nel Mezzo dei Maghi" is the new educational tool developed by the Ludoteca, dedicated to security protocols, a specific area of cybersecurity, designed for the 10–14 age group

In particular, the Cybersecurity National Lab has been working for years on a training and education chain with "The Big Game" initiative, which – through the "CyberTrials", "OliCyber", and "CyberChallenge" programmes – involves students from high schools and Universities, as part of measure #65 of the Implementation Plan of the National Cybersecurity Strategy 2022-2026. The collaboration with the Ludoteca aims, therefore, at extending awareness initiatives to the target of middle schools, which are particularly exposed to the risks of irresponsible use of digital resources.

The collaboration between CINI, IMT and the Ludoteca aims to extend awareness initiatives to lower secondary school students, who are particularly exposed to the risks of digital resources

Starting from the **new school year 2026/27**, the section dedicated to cybersecurity of the Ludoteca will be enriched with the new board game "Nel Mezzo dei Maghi" (Among the Wizards).

Scientific board games, which are now popular and appreciated even among adult gamers, have the **advantage of**

combining entertainment with cognitive stimulation and awareness of complex themes, through an immersive mode without the stress of traditional learning.

- From an educational point of view, they have the following characteristics:
  they foster experiential learning with which complex concepts can be "experienced firsthand", making abstract notions concrete and easy to memorise;
- in most cases, they are developed with expert support to ensure the rigour and accuracy of scientific content;
- they encourage cooperation and discussion among players, promoting collective learning.

"Nel Mezzo dei Maghi" (Among the Wizards) is an **immersive game, with a fantasy setting**, which involves the use of a kit consisting of a board, cards, safes, locks and envelopes. Everything is **articulated in more and more complex phases, corresponding to different security protocols**. The title recalls the **"Man-in-the-Middle"** attack that in encryption and computer security means a **cyberattack** in which someone secretly retransmits or alters communication between two parties who believe they are communicating directly with each other. The narrative element is not lacking: **the intro tells the origin and state of the struggle between the Alliance of Wizards, Witches and the King. Players impersonate the royal postal service**, whose task is to prevent the Alliance from communicating in pursuit of malicious goals, through the casting of spells. In order to accomplish this, **the royal postmen must perform specific, increasingly complex interference actions** on the messages sent by the Alliance, using strategies and tools that recall the techniques of "ethical hacking" (the end is not malicious, indeed the King's salvation depends on it!).

The game uses strategies and tools that draw on techniques from "ethical hacking"

In April the game was tested in eight classes of the middle school "D. Settesoldi" (Vecchiano, Pisa), involving a total of 174 pupils. The Ludoteca staff and the IMT expert conducted

the workshops, with the support of the teachers, dividing the class into groups and taking care of the "briefing" and "debriefing" phase, so as to introduce the themes present in the game and fix the notions acquired at the end of the game.
The **game will be presented in the final version for the upcoming school year** and will feature events and initiatives dedicated to education and scientific dissemination.

Children and the digital dimension: between online habits and cybersecurity education
The choice of the Ludoteca to create a new game dedicated to cybersecurity stems from the growing need **to accompany young people toward a conscious use of digital technologies**, as confirmed by the data on their online habits. As **Save the Children 2025's survey** on the childhood and digital relationship highlights, **smartphone use happens at a progressively younger age**. In Italy, about one in three children between the ages of 6 and 10 (32.6%) use smartphones every day, a trend that has been steadily increasing in recent years (in 2018-2019 it was 18.4%).
In addition, 62.3% of pre-adolescents between 11 and 13 - over three in five - have at least one social network account: 35.5% have more than one account and 26.8% have only one. This is despite the fact that the GDPR (General Data Protection Regulation) states that you must be 14 years of age or 13 years of age with parental consent to open an account and consent to the processing of personal data online.
31.3% of boys and girls in this age group are connected online with friends – via chat, voice and video calls – several times a day, 5% are continuously connected. 82.2% of pre-teens use the Internet to exchange messages, just under 40% to send and receive emails, nearly 1 in 5 (18.5%) to read newspapers or news sites, 11.3% to express opinions on social-political issues, and 9.6% to take online courses.
Even the population of minors lives therefore immersed in the "onlife" dimension, according to the definition of the philosopher **Luciano Floridi** (the Onlife Manifesto, 2014), **a hybrid world in which individual choices are continuou-**

In Italy, about one in three children aged 6 to 10 (32.6%) uses a smartphone every day, a trend that has been steadily increasing in recent years (18.4% in 2018–2019)

sly shaped by digital interactions and everything they entail, both in terms of opportunities and risks.

Educating children on the responsible use of digital resources, including through knowledge of the mechanisms that govern how they work, thus becomes a strategic action for growing future conscious (digital) citizens. **Awareness is also the basis for educating the youngest in how to use digital environments safely**, considering that the most popular ones - social networks, messaging and gaming platforms - are increasingly exposed to the activities of cybercrime and therefore present high levels of risk.

To meet the frequent requests by educational institutions for training in the field of cybersecurity, **the Ludoteca has already activated a dedicated didactic section**, composed of **several proposals** all based on play and profiled according to different age groups.

Educating children on the responsible use of digital resources, including through knowledge of the mechanisms that govern how they work, thus becomes a strategic action for growing future conscious (digital) citizens

"Nel Mezzo dei Maghi" represents only the latest educational resource developed by the Ludoteca in the field of cybersecurity. Among its key tools, there is the **video game "Nabbovaldo and blackmail from cyberspace"** ("Nabbovaldo e il ricatto dal cyberspazio"), designed for middle schools and developed with a gamification perspective, which **makes it possible to introduce, in an interactive and engaging way, some of the main issues of cybersecurity: cyberattacks, online scams, malware and technical countermeasures**. Players are on a four-part adventure, with a final epilogue, through fun storytelling that follows the protagonist Nabbovaldo, a naive inhabitant of Internetopoli, a vast city of the Web. Throughout the game, Nabbovaldo encounters various characters whose very names represent the opportunities and risks of the online world: Mr. D, Super Virus Block, Troll and Dark Fred.

To complement the game-focused lab, depending on the specific needs of the classes, **the following resources and**

activities are also proposed:

- **Caesar** cipher game: inspired by the method of encryption used by the famous Roman leader, it represents a valid tool for introducing the concept of "confidentiality" of data and messages and at the same time, explaining encryption techniques.
- **Memory Card Game**: participants must memorise passwords by trying to match identical cards. This game stimulates reflection on the importance of managing passwords carefully, highlighting the different level of robustness.
- **Acronym Game**: starting from the lyrics of a famous song, groups consider only the first letters of the various words that make up the phrase and thus create a strong but easily memorisable password.
- **Cyber Quiz Game**: a group game based on comic strip boards in which a possible online risk situation and three possible endings are presented: only one of these is the correct behaviour from a point of view of cyber hygiene.
- **Think first then share Game**: involves the use of cards that show on one side various types of personal information, on the other the arguments on why it may or may not be appropriate share them online.
- **Online Security Manifesto**: a digital security decalogue with recommendations to prevent and counter major cyber threats.

Together, **the activities of the Ludoteca of Registro .it outline an integrated educational path** that, through play and experimentation, aims at strengthening the ability of young people to orient themselves among risks and opportunities of the online dimension, **contributing to the training of more conscious and responsible digital citizens**.

IOCTA REPORT 2026: FROM AI TO MALICIOUS DOMAINS, EUROPOL'S ALARM ON CYBERCRIME

by **Gino Silvatici**

On 28 April, **Europol published the 2026 edition of the Internet Organised Crime Threat Assessment (IOCTA)**, **the annual report that analyses the evolution of the main threats related to online organised crime in the European Union**. The document represents one of the most important references for understanding cybercrime trends in Europe and the challenges that law enforcement authorities will have to face in the coming years.

AI is becoming a capacity multiplier for illegal online organisations

CYBERCRIME IN THE AGE OF AI: NEW THREATS AND CRITICAL ISSUES FOR EUROPEAN AUTHORITIES

The 2026 IOCTA pays particular attention to the **tools that are facilitating cybercrime, digital infrastructures used by criminal networks, cyberattacks, online fraud and child sexual exploitation on the Internet**. One of the most relevant elements of the study concerns the growing role of artificial intelligence, considered by Europol to be a factor destined to profoundly transform the digital threat landscape.

According to the report, **the increasing accessibility of AI-powered tools is significantly lowering the barriers to entry for cybercriminals**. In practice, activities that in the past required high technical skills can now also be carried out by subjects with limited knowledge, thanks to automation and the availability of increasingly sophisticated tools.

Europol highlights how AI is becoming a capacity multiplier for illegal online organisations. Generative systems and automated tools make it possible to create more credible fraudulent campaigns, automate cyberattacks and improve social engineering techniques.

One of the most affected sectors is phishing. Thanks to artificial intelligence, criminals can produce fake emails,

messages and websites that are ever more convincing, reducing grammatical errors or signals typical of traditional fraud. In addition, AI can be used to automate the analysis of cyber vulnerabilities, customise attacks against specific targets and generate manipulated audio or video content through deepfake technologies.

This development represents a major challenge for the European authorities. While AI can become a support tool for cybersecurity and investigative activities, it risks increasing the speed, scale, and sophistication of illicit activities online. Europol points out that **cybercrime is becoming increasingly industrialised and accessible. The "crime-as-a-service" model**, already widespread on the dark web, allows criminal groups to sell attack tools, malware and illegal services even to individuals without advanced technical skills.

The study also notes the growing difficulties faced by European police forces in countering cybercrime. Among the main obstacles is the **spread of platforms with end-to-end encryption**. While these systems are critical to protecting privacy and communications security, **Europol argues that they make it more complex to monitor unlawful transactions online and identify suspects**. The report highlights how investigative authorities are often unable to access the communications used by criminal networks, even in the presence of formally authorised investigations.

Another problem reported concerns the **data retention policies** adopted in the different EU Member States. Europol calls some of these policies "**restrictive or inadequate**", arguing that they limit the ability of authorities to reconstruct illegal activities and identify perpetrators. The fragmentation of European regulations on the issue of data retention continues to be a delicate issue. In recent years, it has been the subject of numerous legal controversies, especially after several decisions of the Court of Justice of the European Union that imposed significant limits on the generalised retention of traffic data.

The fragmentation of European regulations on the issue of data retention continues to be a delicate issue

THE DOMAIN ECOSYSTEM IN CYBERCRIME: BETWEEN DNS ABUSE AND ONLINE FRAUD

One of the most interesting aspects of IOCTA 2026 concerns the attention paid to the **abuses of DNS and the domain name ecosystem**: "technical DNS abuse" and "website content abuse" are closely linked in the criminal dynamic. In practice, **illegal organisations use domain names and DNS infrastructure as essential components of their online operations**. According to the report, criminals register Internet domains to mimic legitimate sites (e.g. financial institutions, payment

platforms or online services), with the aim of stealing credentials, personal data and banking information from users. Fraudulent domains are also used to distribute malware, operate botnets, and coordinate automated attack campaigns. Europol points out that **the period between the registration of a malicious domain and the intervention of the authorities is a time window that is particularly exploited by criminal networks**. In many cases, in fact, it only takes a few hours or a few days to start phishing campaigns or malware distribution capable of affecting thousands of users before the domain is blocked or removed.

This aspect is also particularly relevant for ccTLD (Country Code Top-Level Domain) registries and for operators in the domain name sector. **The report also criticises the slowness of the international cooperation procedures used to counter illegal online activities** and this could have an impact on enforcement procedures that will have to be increasingly rapid to combat this type of abuse.

According to Europol, "the absence of automated reporting interfaces" and the reliance on slow cross-border judicial procedures prevent rapid action being taken against malicious domains. This problem is particularly evident in the context of global cybercrime, where infrastructure, servers, registrants, and victims may be located in different jurisdictions. Law enforcement authorities often have to follow complex and slow international legal procedures to obtain registrant information, block domains or request the removal of illegal content. Europol therefore suggests the need for faster and more efficient tools for the operational countering of online threats, especially in cases of automated fraud and malware distribution.

The study does not propose specific legislative measures against ccTLD registries or European DNS operators. However, **the document clearly attributes a central role to Internet infrastructures in the cybercrime chain of operations**.

For this reason, the 2026 IOCTA analysis could influence future initiatives by the European Commission or Member States on combating online abuse. The domain name sector is, in fact, increasingly at the centre of political and regulatory discussions related to cybersecurity.

In recent years, **the European institutions have increased their attention to issues such as verifying the identity of registrants, speeding up take-down procedures, cooperation between registries and law enforcement agencies, and monitoring DNS abuse**.

Criminals register Internet domains to mimic online services and steal credentials, personal data and banking information. These domains are also used to distribute malware, operate botnets, and coordinate automated attack campaigns

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.

The IOCTA could become a further political reference in the European debate on the responsibility of technical intermediaries and the governance of digital infrastructures

The IOCTA could therefore become a further political reference in the European debate on the responsibility of technical intermediaries and the governance of digital infrastructures.

SCENARIO AND PROSPECTS

Europol's report is part of a broader context in which **cybersecurity has become a central component of European economic and geopolitical security**.

Digital infrastructures are now essential for the functioning of modern economies, public services and communications. As a result, cyberattacks, ransomware campaigns and online fraud can have very significant systemic impacts.

The European Union is looking to progressively strengthen its cybersecurity ecosystem through regulations such as NIS2, the **Cyber Resilience Act**, and other **initiatives dedicated to digital security**.

However, **the 2026 IOCTA shows how technological evolution is rapidly increasing the complexity of threats**. The accessibility of artificial intelligence, the speed of online criminal infrastructures

and the global scale of cyber operations make the work of law enforcement authorities increasingly difficult. The report confirms that cybercrime continues to evolve at extreme speed and that digital infrastructures are taking on an increasingly central role in illicit activities. The document highlights both the growing technological sophistication of illegal networks and the structural difficulties that European authorities encounter in effectively combating them. Artificial intelligence, encrypted platforms, DNS abuses and the slowness of international cooperation are all set to influence the European political and regulatory debate in the coming years.

For the European digital sector, including ccTLD registries, providers and infrastructure operators, **the report is an important signal**: regulatory and political pressure on the issue of online abuse could increase further. The challenge for Europe will be to find a balance between security, protection of fundamental rights, technological innovation and operational speed in the fight against global cybercrime.

The challenge for Europe will be to find a balance between security, protection of fundamental rights, technological innovation and operational speed in the fight against global cybercrime

ICANN AND THE IMPACT OF ARTIFICIAL INTELLIGENCE ON DNS

by **Arianna Del Soldato** and **Adriana Lazzaroni**

Within the ecosystem of the **Internet Corporation for Assigned Names and Numbers (ICANN)**, **artificial intelligence has become one of the key topics of discussion**, not because it changes the architecture of the DNS, but because **it is increasingly impacting its usage patterns**.
In particular, **the focus is on the possible impacts of AI, especially large language models (LLMs) such as ChatGPT and its counterparts, on the Domain Name System (DNS), on the identifier ecosystem and on ICANN's mission itself**.
While AI currently represents the dominant technology narrative - inheriting the hype that once surrounded *blockchain* and *big data* - it is crucial to distinguish media hype from the true structural implications.
As pointed out by Matt Larson, ICANN VP of Research, AI does not change the fundamental architecture of DNS nor ICANN's core mission to help ensure a stable, secure, global and unified network by coordinating the Internet's unique identifiers including domain names, IP addresses and protocol parameters. The identifier layer belongs to the infrastructure, it does not generate content, make decisions, or interact with users as LLM models do. However, every significant technological change has implications for the ecosystem in which it operates, and some of these undoubtedly deserve special attention.

AI does not change the fundamental architecture of DNS nor ICANN's core mission to help ensure a stable, secure, global and unified network. However, every significant technological change has implications for the ecosystem in which it operates

AI AND DNS: NEW TRAFFIC DYNAMICS AND INFRASTRUCTURE SECURITY

In recent years, DNS has already gone through profound transformations: cloud, CDN, mobile internet, encrypted DNS, but today **AI is starting to change the way domain names and DNS infrastructures are used**. The impact is not just about large language models or generative AI services. More and more automated systems - chatbots, autonomous agents, analytics platforms, AI crawlers, and retrieval tools - are using DNS intensively and differently than traditional user web browsing.

The traffic, produced by automated systems, can differ significantly from users' normal online activity in terms of the volume, frequency and distribution of requests

Whenever a chatbot searches the web to process a response or an AI agent performs automated tasks across multiple sites, DNS queries are generated. This traffic, produced by automated systems, can differ significantly from users' normal online activity in terms of the volume, frequency and distribution of requests.

For Registrars and registries, this change could translate into new traffic dynamics, different domain registration models and a growing focus on security and reliability. While DNS was designed to handle growth and evolving usage patterns, the emergence of AI as a significant source of Internet traffic is a development that deserves to be monitored. For operators in the sector, this means, in fact, paying greater attention to the resilience of DNS infrastructures, as well as the ability to mitigate anomalous traffic, the monitoring of automated patterns, as well as the management of security at the DNS resolver and authoritative DNS level.

One of the main concerns is the potential of AI to extend, accelerate and automate malicious domain name activities, significantly changing the threat landscape. LLM models can make it significantly easier to generate convincing phishing content, create impersonation sites or devise targeted social engineering campaigns. Many of these activities are based on domain names. AI tools can also be used to register domains for large-scale abuse campaigns, and to do so in ways that are harder to detect using traditional methods.

In this context, however, there is a positive aspect that lies in the possibility of using AI technologies also in the fight against DNS abuse. The research teams at ICANN, and the main ccTLDs, already use machine learning techniques to identify malicious domain names, analyse

large-scale abuse patterns, detect DGAs (Domain Generation Algorithms) and monitor anomalies in DNS traffic.
The evolution of the current context will require a focus on cutting-edge solutions, starting from **"threat intelligence" systems** to behavioural monitoring of registrations. **The success of these strategies will depend** not only on the use of automated tools for the detection of abuse, but **above all, on the ability to create a solid network of cooperation between Registries, registrars and security professionals**.

AI, CLOUD AND DNS: TOWARDS AN INCREASINGLY CENTRALISED INTERNET INFRASTRUCTURE

The convergence of AI, cloud infrastructures and encryption protocols such as DoH (DNS over HTTPS) and DoT (DNS over TLS) **is shaping a digital ecosystem characterised by marked centralisation**. As the development of AI systems requires computational capabilities and data volumes that are almost exclusively sustainable by large *hyperscalers*, there is a progressive shift in DNS resolution from local *resolvers* to public platforms managed by a few operators. **In this scenario, an increasing share of traffic is routed through providers that simultaneously control the entire technology chain: from cloud infrastructures to AI services**, through content delivery networks (CDNs), DNS resolvers, browsers and operating systems.
This vertical concentration produces critical effects that go far beyond the technical aspect, resulting in an **unprecedented accumulation of metadata and behavioural information in the hands of a few subjects**. Not only does this dramatically reduce the operational visibility of Internet service providers (ISPs) and local operators, but it also increases global infrastructure dependence, giving control of digital networks an **increasingly geopolitical relevance**.
Faced with these challenges, the issue of digital sovereignty and network resilience has become central to the agenda of international technical and regulatory bodies, including ICANN, called upon to define new governance models that balance technological innovation with data protection and the autonomy of national infrastructures.

The issue of digital sovereignty and network resilience has become central to the agenda of international technical and regulatory bodies, called upon to define technological innovation with data protection and the autonomy of national infrastructures

AI REDEFINES THE VALUE OF DOMAIN NAMES

The advent of AI is profoundly redefining the value of domain names, transforming the way users interact with the web. Although the evolution of *AI search* tends to provide direct answers by reducing the immediate visibility of URLs, **the domain does not lose its centrality at all**. On the contrary, the reputational function emerges as a guarantee of the reliability of the source.

In an ecosystem where virtual assistants filter and select content, the authority and recognisability of a domain name become strategic assets making it possible to stand out from the crowd

In an ecosystem where virtual assistants filter and select content, the authority and recognisability of a domain name become strategic assets making it possible to stand out from the crowd. This market metamorphosis is already evidenced by an exponential growth in AI-related keyword registrations and the adoption of new branding strategies, although this brings with it critical challenges, such as the increase in speculative phenomena and cybersquatting targeting the new AI services.

AI AND MULTI-STAKEHOLDER PROCESSES

However, there is another dimension that goes beyond that of technical infrastructure: **ICANN's legitimacy is largely based on the integrity of its reconfirmed "multi-stakeholder" model and the authenticity of human participation in the development of "policies"** and the realisation of consensus. The use of AI to generate public comments, draft regulatory texts, respond to mailing lists and participate in community processes is done with a speed and scale that can influence decision-making processes. **ICANN therefore has the task, in carrying out its specific activities, of protecting the reliability of the information generated by artificial intelligence** since part of its mission is to act as an authoritative source of the information provided.

Through the functions of IANA, ICANN manages authoritative registers relating to protocol parameters, numerical resources and top-level domains, areas in which precision is fundamental and where the approximations typical of language models is not allowed. When AI acts as an intermediary for access to these resources, the risk of inaccurate, biased information or so-called "hallucinations" can compromise the reliability of the information provided and, consequently, ICANN's role as an authoritative reference. The question of how to identify and evaluate AI-generated contributions is therefore a governance challenge that ICANN, along with many other organisations, will be called upon to address.

CONCLUSIONS

When a significant new technology emerges, ICANN is called upon to understand its effects on the ecosystem in which it operates. Specifically, in the case of AI, **the technology does not change ICANN's mission, but profoundly affects the environment in which it develops**. AI can influence DNS traffic patterns, change the landscape of abuse and related mitigation strategies, and pose new questions about the integrity of participation and the authoritativeness of information. For this reason, **while not representing a factor of structural discontinuity, the evolution of AI requires constant and careful monitoring by ICANN**.

The question of how to identify and evaluate AI-generated contributions is a governance challenge that ICANN, along with many other organisations, will be called upon to address

05

Preview
Statistics
News
In-depth dives
Events

INTERNATIONAL EVENTS FROM THE INTERNET WORLD

3-4 JUNE
RIPE NCC | Riga, Latvia

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

8-11 JUNE
ICANN 86 **(Policy Forum)** | Seville, Spain

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

24-26 JUNE
WMF - We Make Future | Bologna, Italy

The .Registro .it will be there with a booth and two events!

18-24 JULY
IETF 126 | Vienna, Austria

10-11 SEPTEMBER
* **CENTR 2nd CSR workshop** | Paris (to be confirmed), France

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

14 SEPTEMBER
APTLD 90 | Ulaanbaatar, Mongolia

* *Events reserved for CENTR members*


Registro.it
L'ANAGRAFE DEI DOMINI .IT

è gestito da


ISTITUTO
DI INFORMATICA
E TELEMATICA
CNR


Consiglio Nazionale
delle Ricerche