bilingual edition

ptsoc {news}

16

Regulamento dos Serviços Digitais: um ano de balanço

3 perguntas a Polina Malaja

Entrevista a Eleanora Petridou

Digital Services Act: a year in the making

3 questions to Polina Malaja

Interview to Eleanora Petridou

.pt

Regulamento dos Serviços Digitais: um ano de balanço

Aplicável desde 17 de fevereiro de 2024, o Regulamento dos Serviços Digitais (RSD) visa, em termos genéricos, proteger os consumidores e combater a difusão de conteúdos ilegais online, incluindo os riscos da desinformação e da difusão de outros conteúdos ilegais, e com isto, contribuir também para garantir a eficácia dos direitos fundamentais. É um Regulamento Europeu que define neste âmbito as responsabilidades dos chamados Prestadores de Serviços Intermediários (PSI) e que tem como objetivo criar um espaço digital mais seguro e responsável para os cidadãos e as empresas, como resposta à transformação digital e à utilização crescente destes serviços.

No contexto deste Regulamento, são definidas as obrigações dos PSI (entre eles redes sociais, motores de busca e plataformas e mercados online) enquanto intermediários entre os consumidores e os produtos, serviços e conteúdos. Estas obrigações são determinadas em função da natureza dos serviços prestados e da sua dimensão, distinguindo-se, nomeadamente, obrigações específicas para as plataformas online e os motores de busca com maiores dimensões.

De acordo com a ANACOM, "um número significativo das novas obrigações deste Regulamento diz respeito à forma como os prestadores de serviços intermediários lidam com conteúdos ilegais" uma vez que

Digital Services Act: a year in the making

Applicable since 17 February 2024, the Digital Services Act (DSA) aims, in general terms, to protect consumers and combat the dissemination of illegal content online, including the risks of disinformation and the dissemination of other illegal content, thus helping to guarantee the effectiveness of fundamental rights. This European Regulation defines the responsibilities of the so-called Providers of Intermediary Service (PISs) and aims to create a safer and more responsible digital space for citizens and businesses, in response to the digital transformation and the growing use of these services.

This Regulation defines the obligations of PISs (including social networks, search engines, and online platforms and marketplaces) as intermediaries between consumers and products, services and content. These obligations are determined according to the nature of the services provided and their size, with specific obligations for online platforms and larger search engines.

According to ANACOM, 'a significant number of this Regulation's new obligations concern the way in which providers of intermediary services deal with illegal content' since 'there are certain actions that these providers must take in relation to [this type of content] when they are notified, for example.'

"há certas ações que estes prestadores devem adotar em relação [a este tipo de conteúdos] quando estes lhes são notificados, por exemplo."

A ANACOM foi designada pelo Governo como autoridade competente e Coordenador dos Serviços Digitais em Portugal, na supervisão e execução do RSD. Outras instituições com competências neste âmbito incluem a Entidade Reguladora para a Comunicação Social (ERC) – em matéria de comunicação social e outros conteúdos mediáticos – e a Inspeção-Geral das Atividades Culturais (IGAC), em matéria de direitos de autor e dos direitos conexos.

O RSD, um ano depois

A ANACOM divulgou no início de março um comunicado em que faz um pequeno balanço relativo às reclamações contra os prestadores de serviços intermediários que recebeu em 2024.

No total, ao longo do ano passado, foram recebidas 65 reclamações. Destas, os assuntos mais reclamados foram os "conteúdos considerados ilegais pelos destinatários dos serviços" (45%) bem como a "insatisfação com a suspensão ou desativação de contas consideradas ilegais ou contrárias aos termos e condições pelos PSI" (31%).

Foram mencionadas pelos destinatários dos serviços (cerca de 19% das reclamações

ANACOM was appointed by the government as the competent authority and Coordinator of Digital Services in Portugal, in the supervision and execution of the DSA. Other competent institutions in this area include the ERC - *Entidade Reguladora para a Comunicação Social* (Regulatory Authority for the Media) for media and other media content, and the IGAC - *Inspeção-Geral das Atividades Culturais* (General Inspectorate for Cultural Activities), for copyright and related rights.

The DSA, one year later

At the beginning of March, ANACOM released a statement in which it gave a brief overview of the complaints it received against providers of intermediary services in 2024.

In total, 65 complaints were received last year. Most complaints related to 'content considered illegal by service recipients' (45 %), as well as 'dissatisfaction with the suspension or deactivation of accounts considered illegal or contrary to the terms and conditions by PISs' (31 %).

Service recipients (around 19 % of the complaints received) referred 'difficulties in complaining, namely because it was impossible to contact them to appeal a decision taken by the PIS, including the lack of contact points'. Dissatisfaction with the PIS's decision to remove or not remove content reported as illegal was another of

Foto: Skórzewiak, adobe.stock

recebidas) as "dificuldades para reclamar, nomeadamente, por impossibilidade de contacto para recorrer de uma decisão tomada pelo PSI, incluindo a falta de disponibilização de pontos de contacto". A insatisfação com a decisão dos PSI de remoção ou não remoção de conteúdos denunciados como ilegais foi outro dos assuntos mais reclamados (11% do total), de acordo com o regulador.

Segundo a ANACOM, os maiores alvos de reclamações em termos de redes sociais foram o Facebook e o Instagram, ambas plataformas da Meta, com quase metade (48%) das reclamações recebidas. O Google, que continua a ser, de longe, o motor de busca mais usado em Portugal, the most complained about issues (11 % of the total), according to the regulator.

According to ANACOM, the biggest targets of complaints in terms of social networks were Facebook and Instagram, both Meta platforms, with almost half (48 %) of the complaints received. Google, which remains by far the most used search engine in Portugal, was also the target of a significant number of complaints (12 %) while the WhatsApp messaging service, also from Meta, came in at 8 %.

Complaints were also registered against the Temu online sales platform, X, the Microsoft Onedrive service, Snapchat, Reddit and the Starlink satellite Internet access service.

foi também alvo de um número significativo de reclamações (12%) enquanto o serviço de mensagens WhatsApp, também da Meta, surge com 8%.

Foram ainda registadas reclamações contra a plataforma de vendas online Temu, o X, o serviço Microsoft Onedrive, o Snapchat, o Reddit e o serviço de acesso à Internet via satélite Starlink.

Entre as reclamações recebidas, a ANACOM indica ter transmitido sete com indícios de infração que se visavam a Meta, a Temu e o Google para o Coordenador dos Serviços Digitais da Irlanda, já que se trata de plataformas se encontram estabelecidas naquele país, em conformidade com o que se encontra previsto no artigo 53.º do Regulamento dos Serviços Digitais.

A falta de exposição de motivos após uma tomada de decisão sobre um conteúdo considerado ilegal por parte dos PSI e a falta de resposta às reclamações dos destinatários do serviço foram os motivos de transmissão de reclamações mais recorrentes.

Conteúdos ilegais

O Regulamento dos Serviços Digitais inclui regras e medidas específicas para o caso dos conteúdos ilegais online. O considerando 9. do preâmbulo do RSD indica, precisamente que "o regulamento harmoniza plenamente as regras aplicáveis

Among the complaints received, ANACOM said it had forwarded seven with indications of infringement against Meta, Temu and Google to Ireland's Digital Services Coordinator, as these platforms are established in that country, in accordance with Article 53 of the Digital Services Act.

The lack of a justification following a decision on content considered illegal by the PISs and the lack of response to complaints from the recipients of the service were the most recurrent reasons for passing along these complaints.

Illegal content

The Digital Services Act includes specific rules and measures for illegal content online. Recital 9 of the preamble to the DSA states precisely that 'this Regulation fully harmonises the rules applicable to intermediary services in the internal market with the objective of ensuring a safe, predictable and trusted online environment, addressing the dissemination of illegal content online and the societal risks that the dissemination of disinformation or other content may generate, and within which fundamental rights enshrined in the Charter are effectively protected and innovation is facilitated.'

For that reason, it is considered that 'Member States should not adopt or maintain additional national requirements relating to

Google e Meta dominam em Portugal

O Google continua a ser o motor de busca mais utilizado no mundo (mais de 90% de quota de mercado) mas, em Portugal, o seu domínio é ainda maior, com quase 93% de quota. Em termos de redes sociais, os ativos da Meta são também os mais populares em Portugal, por uma larga margem quando comparados com outras plataformas. O Facebook é usado por mais de 67% dos internautas (percentagem semelhante à do resto do mundo), a grande distância do Instagram (também da Meta), com cerca de 15% (contra cerca de 11% no resto do mundo).

Google and Meta dominate in Portugal

Google continues to be the most widely used search engine in the world (with more than 90 % market share); in Portugal, its dominance is even greater, with almost 93 % share. In terms of social networks, Meta's assets are also the most popular in Portugal, by a wide margin when compared to other platforms. Facebook is used by more than 67 % of internet users (a similar percentage to the rest of the world), a long way behind Instagram (also owned by Meta), with around 15 % (compared to around 11 % in the rest of the world).

aos serviços intermediários no mercado interno com o objetivo de assegurar um ambiente online seguro, previsível e fiável, combatendo a difusão de conteúdos ilegais online e os riscos sociais que a difusão de desinformação ou de outros conteúdos pode gerar, e no qual os direitos fundamentais consagrados na Carta sejam eficazmente protegidos e a inovação seja facilitada".

Por essa razão, considera-se que "os Estados-Membros não deverão adotar ou manter requisitos nacionais adicionais no que diz respeito às matérias abrangidas pelo âmbito de aplicação do presente regulamento, salvo se explicitamente previsto no presente

the matters falling within the scope of this Regulation, unless explicitly provided for in this Regulation, since this would affect the direct and uniform application of the fully harmonised rules applicable to providers of intermediary services in accordance with the objectives of this Regulation. This should not preclude the possibility of applying other national legislation applicable to providers of intermediary services, in compliance with Union law, including Directive 2000/31/EC, in particular its Article 3, where the provisions of national law pursue other legitimate public interest objectives than those pursued by this Regulation'.

regulamento, uma vez que tal afetaria a aplicação direta e uniforme das regras plenamente harmonizadas aplicáveis aos prestadores de serviços intermediários em conformidade com os objetivos do presente regulamento. Tal não deverá excluir a possibilidade de aplicar outra legislação nacional aplicável aos prestadores de serviços intermediários, que seja conforme com o direito da União, incluindo a Diretiva 2000/31/CE, nomeadamente o artigo 3°, sempre que as disposições do direito nacional visem alcançar objetivos legítimos de interesse público distintos dos visados pelo presente regulamento."

No entanto, há um longo caminho – legal, processual e prático – a percorrer entre a receção e análise das queixas no âmbito do RSD e a aplicação das medidas destinadas à eventual remoção de conteúdos ilegais.

Enquanto responsável pela gestão do domínio .pt, a Associação DNS.PT – a par de outros ccTLDs europeus – é uma das entidades que pode colaborar com as autoridades no combate aos conteúdos ilegais online.

Isto não é feito diretamente, como nos explica o CENTR (Council of European National Top-Level Domain Registries) num vídeo disponível em https://youtu.be/mmw4pWYALQ4.

However, there is a long way to go - legally, procedurally, and practically - between receiving and analysing complaints under the DSA and implementing measures to remove illegal content.

While responsible for managing the .pt domain, Associação DNS.PT - along with other European ccTLDs - is one of the entities that can collaborate with the authorities in the fight against illegal content online.

This is not done directly, as the CENTR (Council of European National Top-Level Domain Registries) explains in an educational video available at https://youtu.be/mmw4pWYALQ4.

A situação em Portugal

A nível nacional, o .PT não é responsável pela utilização que é dada a um nome de domínio, designada mas não exclusivamente, pelos conteúdos que lhe estão associados, independentemente do formato e meios de transmissão (artigo 25.°, n.° 4 das Regras de Registo de .pt).

Cumpre ao titular de cada nome de domínio registado sob .pt garantir o integral cumprimento das disposições previstas nas Regras de Registo de .pt e na legislação aplicável, abstendo-se de fazer qualquer uso ilícito do mesmo e sendo exclusivamente responsável por quaisquer danos que, direta ou indiretamente, cause pelo seu registo ou utilização indevida (artigo 23.°, n.° 2 das Regras de Registo de .pt).

Não obstante este facto, considerando que o .PT é responsável pela base de dados de suporte ao registo e gestão de nomes de domínio na sua zona, tem sempre em seu poder os dados pessoais, ou relativos a pessoa coletiva, que identificam os titulares e os demais responsáveis por cada registo, sendo esta circunstância muito relevante em material de colaboração e apoio à investigação. Por exemplo, em 2024, o .PT respondeu a 59 pedidos de informação veiculados por entidades com competências legais para o efeito.

The situation in Portugal

In Portugal, .PT is not liable for the use given to a domain name, designated but not exclusively, for the contents associated with it, regardless of the format and means of transmission (article 25(4) of .pt Registration Rules).

The registrant of each domain name registered under .pt is responsible for ensuring full compliance with the provisions of the .pt Registration Rules and applicable legislation, refraining from any unlawful use of it and being solely liable for any damage caused, directly or indirectly, by its registration or misuse (article 23(2) of the .pt Registration Rules).

Notwithstanding, given that .PT is responsible for the database that supports the registration and management of domain names in its area, it always holds the personal data, or data relating to legal persons, that identifies the registrants and others responsible for each registration, a circumstance that is very relevant in terms of collaboration and support for research. For example, in 2024, .PT responded to 59 requests for information from organisations with legal powers to do so.

3

Polina Malaja

Policy Director , CENTR

1. Embora os ccTLD não tenham responsabilidade direta na remoção de conteúdos ilegais online, quais são as suas responsabilidades (caso existam) neste contexto?

Como intervenientes na infraestrutura técnica da Internet, os ccTLD têm uma capacidade limitada para combater os conteúdos ilegais em linha. Os ccTLD exploram a infraestrutura técnica para o seu TLD e organizam o processo de registo de nomes de domínio. Em nenhum momento a infraestrutura gerida por um ccTLD transmite, aloja ou faz cópias acidentais de qualquer conteúdo disponibilizado. Por estas razões, os ccTLD não estão equipados para remover conteúdos ilegais, uma vez que são considerados o agente técnico sem controlo sobre os conteúdos online.

No entanto, todas as aplicações ou websites requerem um nome de domínio para estarem acessíveis online. Consequentemente, embora a ação a nível de TLD não possa remover o conteúdo, pode dificultar a sua acessibilidade. Os ccTLD têm um conjunto

1. Although ccTLDs do not have direct responsibility in taking down illegal online content, what are their responsibilities (if any) in this context?

As technical internet infrastructure actors, ccTLDs have limited capacity in tackling illegal online content. ccTLDs operate the technical infrastructure for their TLD and organize the domain name registration process. At no point in time does the infrastructure managed by a ccTLD transmit, host or make incidental copies of any content made available online. For these reasons, ccTLDs are not equipped to remove illegal online content, as they are considered to be the technical actor with no control over online content.

Nevertheless, every application or a website requires a domain name to be accessible online. As a result, although TLD-level action is unable to remove content, it can hamper its accessibility online. ccTLD registries have a limited set of actions available to take action against a domain name that is associated with any unwanted content. Essentially, there is only one action that ccTLD registries can take, that is disabling the underlying infrastructure - the domain name. By suspending or deleting a domain name, all services connected to it, such as a website, platform, application or an email service become inaccessible, along with all content associated with the domain name.

limitado de ações disponíveis para tomar medidas contra um nome de domínio que esteja associado a qualquer conteúdo indesejado. Essencialmente, só há uma ação que os ccTLD podem tomar, que é desativar as infraestruturas subjacentes – o nome de domínio. Ao suspender ou eliminar um nome de domínio, todos os serviços a ele ligados, como um website, uma plataforma, uma aplicação ou um serviço de email, ficam inacessíveis, juntamente com todo o conteúdo associado a esse nome.

Dado que os ccTLD não podem tomar medidas específicas contra conteúdos ilegais, como desativar um URL específico ou remover um conteúdo concreto (por exemplo, uma imagem ou um comentário ofensivo), a ação a nível do TLD só pode ser considerada em circunstâncias excecionais, quando for adequada e proporcional ao nível de danos causados aos utilizadores finais. Quando se considera uma ação a nível do TLD, é necessário avaliar o nível de interferência com a capacidade dos utilizadores finais para acederem a quaisquer serviços legais ligados a um nome de domínio. A cooperação com as autoridades públicas competentes é fundamental nos casos que envolvem uma ação a nível do TLD, dado que a legalidade de um conteúdo concreto e os critérios de proporcionalidade só podem, na maioria dos casos, ser adequadamente avaliados por uma autoridade pública competente.

Due to ccTLDs being unable to take a targeted action against illegal content, such as disabling a specific URL or removing a concrete piece of content (e.g., an image or an offensive comment), TLD-level action can only be considered in exceptional circumstances when it is appropriate and proportionate with the level of harm posed to end-users. When TLD action is considered, it is necessary to assess the level of interference with end-users' ability to access any legal services connected to a domain name. Cooperation with public competent authorities is the key in the cases involving TLD-level action, as legality of a concrete piece of content and proportionality criteria can in most of the cases be only appropriately assessed by a competent public authority.

2. Which are the current ccTLDs good practices against illegal online content, namely regarding cooperation with law enforcement agencies?

European ccTLDs consider the security and safety of their domain name zones as a matter of priority. European ccTLDs are also consistently being ranked as zones with the lowest abuse rates globally. This means that a combination of existing measures within their technical remit to address illegal and other unwanted behavior online is working well.

2. Quais são as boas práticas dos atuais ccTLD contra os conteúdos ilegais online, nomeadamente no que diz respeito à cooperação com as autoridades policiais?

Os ccTLD europeus consideram a segurança e a proteção das suas zonas de nomes de domínio uma questão prioritária. Os ccTLD europeus também são sistematicamente classificados como zonas com as taxas de abuso mais baixas a nível mundial. Isto significa que a combinação de medidas existentes no âmbito das suas competências técnicas para combater comportamentos ilegais e outros comportamentos indesejados online está a funcionar bem.

Como abordagem aos conteúdos ilegais, os ccTLD, entre outros, centram-se no seguinte:

Proporcionar formação e sensibilização a toda a comunidade local sobre como se manter seguro online. Por exemplo, o .PT" aloja um portal que permite o acesso rápido e fácil a conteúdos digitais, respeitando os direitos de propriedade intelectual dos autores e criadores. O .PT publica também uma revista trimestral dedicada exclusivamente à cibersegurança, com o objetivo de sensibilizar para as ameaças online.

Colaboração estreita com as autoridades competentes, incluindo as responsáveis pela aplicação da lei. Por exemplo, a CZ.NIC (.cz) assinou um memorando de cooperação

Foto: alexlmx_adobe stock

As an approach to illegal content, ccTLD registries, amongst others, focus on:

Providing local community-wide education and awareness-raising on how to stay safe online. For example, .PT hosts a portal that provides fast and easy access to digital content, which respects the intellectual property rights of authors and creators. .PT also publishes a quarterly magazine dedicated exclusively to cybersecurity in order to raise awareness on online threats.

Close collaboration with competent authorities, including law enforcement. For example, CZ.NIC (.cz) has signed Memorandum of Cooperation with Czech law enforcement authorities to increase collaboration on the prevention and tracing of criminal activities and the prosecution of crimes online, including increased child protection and detection of risky webshops.

com as autoridades policiais checas para aumentar a colaboração na prevenção e localização de atividades criminosas e na repressão de crimes online, incluindo uma maior proteção das crianças e a deteção de lojas virtuais de risco.

Melhorar a qualidade e a exatidão dos dados de registo. Manter a exatidão dos dados de registo oferece uma ferramenta para os registos tomarem medidas em relação a um nome de domínio, sem fazerem um julgamento sobre o conteúdo associado ao mesmo. É improvável que pessoas com más intenções registem um nome de domínio utilizando informações pessoais corretas. Por exemplo, a SIDN (.nl) implementou um sistema de deteção precoce de domínios utilizados para lojas virtuais falsas e analisa as denúncias de vítimas de burlas e as informações recebidas do National Internet Fraud Report Desk. Se os dados de registo dos nomes de domínio envolvidos forem falsos, o registry pode desativá-los.

Desenvolver processos e procedimentos para responder a denúncias de conteúdos suspeitos. Alguns registos estabeleceram procedimentos para responder a denúncias de conteúdos suspeitos através do bloqueio ou suspensão de um nome de domínio em casos específicos. Estes procedimentos são normalmente aplicáveis a casos limitados e bem definidos, com um perito externo a avaliar o tipo de conteúdo em causa. Por exemplo, a DNS Belgium (.be) pôs em prática

Improving the quality and accuracy of the registration data. Keeping registration data accurate offers a tool for registries to take action regarding a domain name, without making a judgment over the content associated with it. It is unlikely that those with bad intentions would register a domain name using correct personal information. For example, SIDN (.nl) has deployed an early detection system of domains used for fake webshops and looks into reports from victims of scams and information received from the National internet Fraud Report Desk. If the registration data of the domain names involved is fake, the registry is able to deactivate them.

Developing processes and procedures to respond to reports of suspicious content. Some registries have established procedures to respond to reports of suspicious content by blocking or suspending a domain name in specific cases. These procedures are usually applicable to limited and well-defined cases, with an external expert party assessing what type of content is involved. For example, DNS Belgium (.be) has put in place a Notice and Action procedure in collaboration with the FPS Economy. Following reports of serious infringements from the FPS Economy, DNS Belgium makes the relevant .be domains inaccessible by overriding nameservers and redirecting users to a warning page. If the domain name holders cannot prove that they are bona fide, the domain names are removed.

um procedimento de notificação e ação em colaboração com a FPS Economy. Na sequência de relatórios de infrações graves da FPS Economy, o DNS Belgium torna inacessíveis os domínios .be relevantes, anulando os servidores de nomes e redirecionando os utilizadores para uma página de aviso. Se os detentores dos nomes de domínio não puderem provar que estão de boa-fé, os nomes de domínio são removidos.

Para mais informações sobre a variedade de boas práticas em vigor nos ccTLD europeus, consulte o documento do CENTR sobre registos de nomes de domínio e conteúdos online.

3. Como é que as iniciativas legislativas europeias influenciaram o papel e a ação dos ccTLD na Europa relativamente aos conteúdos ilegais online?

Nos últimos anos, assistimos a uma proliferação de legislação da UE relativa ao sistema de nomes de domínio (DNS) e às responsabilidades dos registries ccTLD:

- O Regulamento dos Serviços Digitais da UE (RSD) esclarece que os registries ccTLD podem ser considerados intermediários para efeitos de disponibilização de conteúdos online e, em determinadas circunstâncias, os ccTLD podem também beneficiar de uma exceção de responsabilidade por conteúdos ilegais ao abrigo do RSD. O RSD introduz também um conjunto mínimo de obrigações de "due diligence" que todos os

See more information on the variety of good practices in place across European ccTLDs in CENTR paper on domain name registries and online content.

3. How have European legislative initiatives impacted the role and action of ccTLDs in Europe regarding illegal online content?

In the past years, we have seen a proliferation of EU legislation concerning the Domain Name System (DNS) and responsibilities of ccTLD registries:

- The EU Digital Services Act (DSA) clarifies that ccTLD registries can be considered intermediaries for the purposes of making content available online, and in certain circumstances ccTLDs can also benefit from a liability exception for illegal content under the EU DSA. The EU DSA also introduces a minimum set of due diligence obligations that all intermediaries have to follow, including ccTLDs. The obligations under the EU DSA include acting upon judicial and administrative orders to act against illegal content or/and to provide information about specific "recipients of the service".

- The NIS2 Directive introduces an unprecedented data accuracy obligation for ccTLD registries and registrars when collecting and maintaining domain name registration data which includes identity verification checks for domain name holders.

intermediários têm de cumprir, incluindo os ccTLD. As obrigações previstas no RSD da UE incluem a atuação mediante ordens judiciais e administrativas para agir contra conteúdos ilegais e/ou fornecer informações sobre "destinatários do serviço" específicos.

• A Diretiva NIS2 introduz uma obrigação de rigor de dados sem precedentes para os registos e agentes de registo de ccTLD na recolha e manutenção de dados de registo de nomes de domínio, que inclui verificações da identidade dos titulares de nomes de domínio. A obrigação de rigor é introduzida com o objetivo de combater o "abuso do DNS" e pode também ajudar a combater indiretamente outras formas de abuso, como os conteúdos ilegais. No entanto, é importante ter em conta que as práticas de rigor dos dados não são uma panaceia e que os agentes maliciosos estão continuamente a adaptar o seu modus operandi, incluindo o modo de passar nos controlos de verificação da identidade.

• O regulamento europeu relativo à cooperação no domínio da proteção dos consumidores (CPC) codificou os critérios de proporcionalidade para as ações a nível dos TLD destinadas a combater as infrações graves à defesa dos consumidores online. De acordo com o CPC, as ações a nível do TLD, como a supressão de nomes de domínio, só podem ser consideradas como medida de último recurso e em caso de infrações graves à defesa do consumidor. As autoridades competentes devem aplicar os critérios de

The accuracy obligation is introduced for the purposes of tackling "DNS abuse" and can also help in tackling indirectly other forms of abuse, such as illegal content. It is, however, important to keep in mind that data accuracy practices are not panacea and that malicious actors are continuously adapting their modus operandi, including on how to pass identity verification checks.

• The EU Consumer Protection Cooperation (CPC) Regulation has codified the proportionality criteria for TLD-level action for tackling serious consumer protecting infringements online. According to the CPC Regulation, TLD-level action, such as deletion of domain names can only be considered as a measure of last resort and in case of serious consumer protection infringements. Competent authorities must apply the proportionality criteria when ordering TLD registries to delete domain names of an infringing service. The CPC Regulation approach of considering TLD-action as a measure of last resort has also inspired EU policymakers to introduce a similar enforcement action in the financial sector, as evident from the recently adopted regulation on markets in crypto-assets, and the on-going discussions on the framework for financial data access in the EU. Both legislative instruments give financial supervisory authorities the power to order the deletion of domain names.

proporcionalidade quando ordenam aos TLD registries que eliminem os nomes de domínio de um serviço infrator. A abordagem do CPC de considerar a ação TLD como uma medida de último recurso também inspirou os decisores políticos da UE a introduzirem uma ação de execução semelhante no sector financeiro, como é evidente no regulamento recentemente adotado sobre os mercados de criptoativos e nas discussões em curso sobre o quadro de acesso aos dados financeiros na UE. Ambos os instrumentos legislativos conferem às autoridades de supervisão financeira o poder de ordenar a supressão de nomes de domínio.

Todas as leis acima mencionadas consideram o DNS como um vetor de intervenção quando se trata de comportamentos ilegais e indesejados online. Infelizmente, os decisores políticos ainda não estão suficientemente sensibilizados para as implicações mais vastas de tratar o DNS como uma ferramenta de intervenção na tentativa de resolver problemas sociais mais vastos e complexos e para o que isso significa em termos de acessibilidade das infraestruturas essenciais da Internet – como é o caso dos nomes de domínio – para todos os cidadãos e empresas online.

As implicações preocupantes da introdução de encargos e obstáculos adicionais ao registo de nomes de domínio incluem a deslocação de mais utilizadores finais europeus para operadores históricos não comunitários e ambientes menos seguros.

All of the abovementioned laws consider the DNS as a vector of intervention when it comes to illegal and unwanted behavior online. Unfortunately, there is still not enough awareness amongst policymakers over the broader implications of treating DNS as an intervention tool in an attempt to solve broader and complex societal problems. and what it means for accessibility of essential internet infrastructure, such as domain names for all citizens and businesses online.

The worrisome implications of introducing additional burdens and obstacles for domain name registration include pushing more European end-users to non-EU incumbents and less secure environments.

Eleanora Petridou

Diretora de Segurança da Informação no RIPE NCC *
Chief Information Security Officer at RIPE NCC *

Enquanto Registry Regional da Internet, que serve mais de 20.000 membros em 76 países, quais são as suas principais funções e responsabilidades em termos de cibersegurança?

Como Registry Regional da Internet, operamos uma série de serviços críticos para os nossos membros e para a comunidade Internet em geral. Estes serviços devem ser protegidos não só contra intrusões, mas também contra a sua utilização abusiva para lançar ataques contra terceiros. Temos a clara responsabilidade de salvaguardar os dados dos nossos membros e garantir o seu acesso seguro aos sistemas do RIPE NCC.

Para proteger a confidencialidade, disponibilidade e integridade dos nossos serviços, estamos empenhados em cumprir as mais recentes normas e melhores práticas de segurança da informação. Concentramo-nos em proteger as nossas infraestruturas e dados, assegurando ao mesmo tempo que os nossos processos permanecem totalmente em conformidade com os requisitos regulamentares e as expectativas da indústria.

As the Regional Internet Registry, which serves over 20,000 members in 76 countries, what are your main roles and responsibilities in terms of cybersecurity?

As a Regional Internet Registry, we operate a range of critical services for our members and the broader Internet community. These services must be protected not only against intrusion but also from being misused to launch attacks against others. We have a clear responsibility to safeguard our members' data and ensure their secure access to RIPE NCC systems.

To protect the confidentiality, availability, and integrity of our services, we are committed to meeting the latest information security standards and best practices. Our focus is on securing our infrastructure and data, while ensuring our processes remain fully compliant with both regulatory requirements and industry expectations.

The Registry and RIPE Database contain member information essential for running their network, making their protection - and compliance with personal data privacy regulations - a top priority.

O Registry e a Base de Dados do RIPE contêm informações dos membros essenciais para o funcionamento da sua rede, tornando a sua proteção – e o cumprimento dos regulamentos de privacidade de dados pessoais – uma prioridade máxima.

Também reconhecemos a importância de proporcionar aos nossos funcionários um ambiente de trabalho seguro e flexível, quer estejam no escritório, a trabalhar a partir de casa ou em viagem. Em última análise, o nosso objetivo é garantir a resiliência e a segurança das nossas redes, sistemas e informações a todos os níveis.

Qual é o panorama da cibersegurança nas regiões da Europa, Médio Oriente e Ásia Central, especialmente no que diz respeito às recentes questões geopolíticas? Que ameaças são mais comuns? Se possível, indique-nos alguns números.

Nos últimos anos, o panorama global da cibersegurança tem sido fortemente moldado por tensões geopolíticas. Os conflitos nalgumas áreas conduziram a um aumento dos ciberataques.

As ameaças mais comuns incluem ataques de negação de serviço distribuído (DDoS) de grande volume, violações de dados em grande escala, campanhas de ransomware e espionagem sofisticada patrocinada pelo Estado. No geral, as tendências de ataques DDoS em 2024 destacam uma realidade

We also recognise the importance of providing our staff with a secure and flexible working environment, whether they are in the office, working from home, or traveling. Ultimately, our goal is to ensure the resilience and security of our networks, systems, and information at every level.

What is the cybersecurity landscape in Europe, Middle East and Central Asia regions, especially regarding the recent geopolitical issues? What threats are most common? If possible, give us some figures.

Over the past few years, the global cybersecurity landscape has been heavily shaped by geopolitical tensions. Conflicts in some areas have driven a surge in cyberattacks.

The most common threats include high volume Distributed Denial of Service (DDoS) attacks, large-scale data breaches, ransomware campaigns and sophisticated state-sponsored espionage. Overall, DDoS attack trends in 2024 highlight a concerning reality: threat actors are capable of generating unprecedented volumes of traffic to disrupt critical services. Ransomware continues to pose a widespread threat, with rising average extortion demands and known vulnerabilities frequently exploited as entry points. State-sponsored attacks have grown in impact over the past year, as nation-states increasingly target critical infrastructure, such as energy grids and

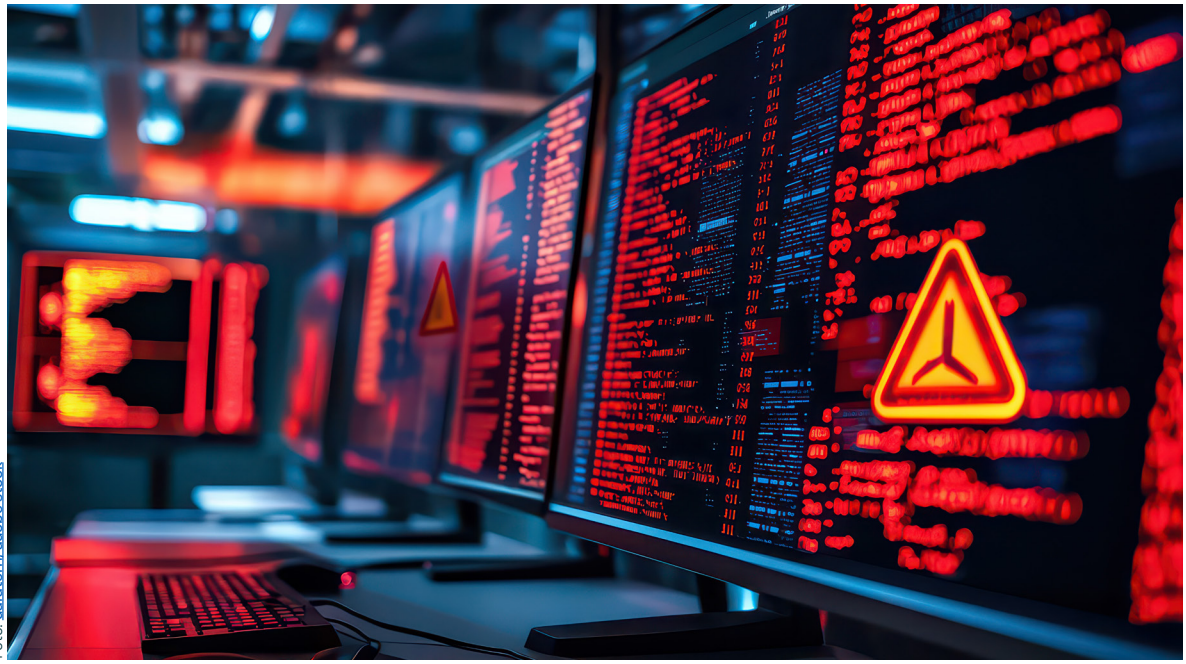

Foto: daratorn_adobe.stock

preocupante: os agentes de ameaças são capazes de gerar volumes de tráfego sem precedentes para perturbar serviços críticos.

O ransomware continua a representar uma ameaça generalizada, com uma média crescente de procura de extorsão e vulnerabilidades conhecidas frequentemente exploradas como pontos de entrada. O impacto dos ataques patrocinados pelo Estado aumentou no último ano, uma vez que os Estados-nação visam cada vez mais infraestruturas críticas, como redes de energia e fornecedores de telecomunicações, para recolher informações, influenciar eventos ou perturbar operações.

telecom providers, to gather intelligence, influence events or disrupt operations.

As a response, the authorities have focused on takedown operations to disrupt the infrastructure of the attackers, e.g. dismantling botnets for ransomware distribution and DDoS campaigns.

On the regulatory front, governments are tightening cybersecurity rules in response to the growing threat landscape. In Europe, the NIS2 Directive and EU Cyber Resilience Act are pushing operators of critical services to adopt stricter security controls, mature their incident reporting and exercise risk management on their supply chain.

Como resposta, as autoridades concentraram-se em operações de remoção para perturbar as infraestruturas dos atacantes, por exemplo, desmantelando botnets para distribuição de ransomware e campanhas DDoS.

No plano regulamentar, os governos estão a tornar mais rigorosas as regras de cibersegurança em resposta ao crescente cenário de ameaças. Na Europa, a Diretiva NIS2 e a Lei da Ciber-resiliência da UE estão a pressionar os operadores de serviços críticos a adotarem controlos de segurança mais rigorosos, a amadurecerem a comunicação de incidentes e a exercerem a gestão de riscos na sua cadeia de abastecimento.

Que projetos ou iniciativas está a RIPE NCC a implementar para se tornar ainda mais segura e resiliente?

Em 2024, alcançámos um importante marco de conformidade ao obter o relatório de garantia ISAE 3000/SOC 2 Tipo 1 para o serviço RPKI (Resource Public Key Infrastructure) do RIPE NCC. Em 2025, estamos empenhados em desenvolver esta base, obtendo o relatório de garantia ISAE 3000/SOC 2 Tipo 2, refletindo a nossa dedicação a práticas de segurança sustentadas e mensuráveis.

Paralelamente, estamos a tentar obter, em 2026, uma certificação ISO 27001 para os serviços de Registry do RIPE NCC e para a Base de Dados RIPE, com

What projects or initiatives are RIPE NCC implementing to become even more secure and resilient?

In 2024, we achieved an important compliance milestone by obtaining the ISAE 3000/SOC 2 Type 1 assurance report for the RIPE NCC Resource Public Key Infrastructure (RPKI) service. In 2025, we are committed to building on this foundation by pursuing the ISAE 3000/SOC 2 Type 2 assurance report, reflecting our dedication to sustained and measurable security practices.

Alongside, we are pursuing in 2026 an ISO 27001 certification for the RIPE NCC Registry services and the RIPE Database, with a focus on further developing our security capabilities, such as structured security risk management, business continuity, data governance, access management, and incident response processes, as part of strengthening our Information Security Management System (ISMS).

We are advancing application security by embedding security practices throughout the software development lifecycle. This includes the integration of comprehensive assessments and best practices that support a “security by design” approach. Our aim is to ensure that security is not only a checkpoint but a continuous and integrated part of our development process.

o objetivo de continuar a desenvolver as nossas capacidades de segurança, tais como a gestão estruturada dos riscos de segurança, a continuidade das atividades, a governação dos dados, a gestão do acesso e os processos de resposta a incidentes, como parte do reforço do nosso Sistema de Gestão da Segurança da Informação (ISMS).

Estamos a fazer avançar a segurança das aplicações, integrando práticas de segurança em todo o ciclo de vida do desenvolvimento de software. Isto inclui a integração de avaliações abrangentes e melhores práticas que suportam uma abordagem de "segurança desde a conceção". O nosso objetivo é garantir que a segurança não é apenas um ponto de controlo, mas uma parte contínua e integrada do nosso processo de desenvolvimento.

Estamos também a concentrar-nos no reforço da nossa segurança operacional em todas as áreas. Isto inclui um enfoque renovado na gestão de vulnerabilidades e na deteção de ameaças, garantindo que nos mantenhamos à frente dos riscos emergentes num cenário de ameaças cada vez mais complexo. Estamos a melhorar as nossas capacidades de gestão de vulnerabilidades através da introdução de ferramentas de rastreio e de comunicação mais granulares. Estas proporcionarão uma visibilidade em tempo real das exposições críticas e de alto risco, ajudando-nos a dar prioridade aos esforços de correção e a manter o alinhamento com as políticas de segurança internas.

We are also focusing on strengthening our operational security across the board. This includes a renewed focus on both vulnerability management and threat detection, ensuring we stay ahead of emerging risks in an increasingly complex threat landscape. We are enhancing our vulnerability management capabilities by introducing more granular tracking and reporting tools. These will provide real-time visibility into critical and high-risk exposures, helping us prioritise remediation efforts and maintain alignment with internal security policies.

This year Lisbon is hosting RIPE 90, from May 12 to 16. What does this edition of RIPE meeting will bring? What outcomes do you expect?

This May, Lisbon will host the 90th edition of the RIPE Meeting – a key gathering of the RIPE community, which has been shaping the technical coordination of the Internet since 1989. We expect over 500 participants to join us to discuss policies and best practices about Internet number resources, DNS, IPv6, routing, security, network measurements, and IoT to name a few.

The meeting will continue the community's long-standing tradition of open, collaborative discussions in Working Groups and Plenary Sessions that help strengthen and secure the Internet's infrastructure. For those interested in security, you can join the

Este ano, Lisboa acolhe a RIPE 90, de 12 a 16 de maio. O que é que esta edição da RIPE nos vai trazer? Que resultados podemos esperar obter?

No próximo mês de maio, Lisboa acolherá a 90.ª edição do RIPE Meeting – um encontro fundamental da comunidade RIPE, que tem vindo a moldar a coordenação técnica da Internet desde 1989. Esperamos que mais de 500 participantes se juntem a nós para discutir políticas e melhores práticas sobre recursos de números da Internet, DNS, IPv6, routing, segurança, medições de rede e IoT, só para citar alguns.

A reunião continuará a tradição de longa data da comunidade de discussões abertas e colaborativas em Grupos de Trabalho e Sessões Plenárias que ajudam a fortalecer e proteger as infraestruturas da Internet. Para os interessados em segurança, pode juntar-se à sessão do Grupo de Trabalho sobre Segurança. Esta sessão reúne a comunidade para abordar desafios como o abuso de recursos da Internet e para trocar melhores práticas destinadas a melhorar a segurança, a resiliência e a estabilidade das infraestruturas da Internet em toda a região. Gostaríamos de aproveitar esta oportunidade para convidar a comunidade Internet de Portugal a juntar-se a nós neste importante evento para trabalharmos juntos em prol de uma Internet mais segura e resiliente.

** Eleonora é responsável por garantir que o RIPE NCC mantenha os níveis necessários de segurança da informação e a conformidade com as melhores práticas e os regulamentos aplicáveis.*

session of the Security Working Group. This session brings the community together to address challenges like the abuse of Internet resources and to exchange best practices aimed at improving the security, resilience, and stability of Internet infrastructure across the region. We would like to take this opportunity to invite the Internet community of Portugal to join us in this important event to work together towards a more secure and resilient Internet.

Eleonora is responsible for ensuring that the RIPE NCC maintains necessary levels of Information security and compliance with best practices and applicable regulations.

TLD MARKET REPORT | 2024/2

GLOBAL ESTIMATE IN TOTAL DOMAINS BY TLD GROUP AND REGION

		Domains	% All
ccTLDs	ccTLDs (Europe)	77M	21%
	ccTLDs (Other regions)	64M	17%
gTLDs	.com	161M	43%
	.org	11M	3%
	Other gTLDs	59M	16%

Total market size over 1,413 TLDs is estimated at a combined 372M domains.

Note that data on some TLDs is not always available or reliable. In these cases, they are either excluded or the data based on previously known values. Data updated July 2024. Sources: Figures based on available data sourced from CENTR, ICANN, APTLD, ZookNic and other external research.

About this chart: Line show median 1 year growth in total domains across the top 300 largest TLDs globally.

Source: CENTR. Dashboard by CENTR (www.centr.org) 2024

De acordo com o mais recente relatório do CENTR, a taxa de crescimento mediana (CENTR30) dos registos em TLDs europeus mostra um declínio a longo prazo, com um pico durante a pandemia no início de 2021 e uma queda constante para 0,35% em outubro de 2024, refletindo a saturação do mercado e o abrandamento pós-pandemia.

A nível mundial, o crescimento médio de 12 meses (os 300 principais TLDs) nos últimos anos atingiu um pico de 7,5% no final de 2021, seguido de um declínio constante para 1,3% em maio de 2024. Os últimos dois meses analisados no ano passado mostram sinais iniciais de uma recuperação com 2,0% em julho de 2024.

According to CENTR's latest report, the median growth rate (CENTR30) of registrations in European TLDs shows a long-term decline, peaking during the pandemic in early 2021 and a steadily falling to 0.35 % by October 2024, reflecting market saturation and post-pandemic slowdown.

Globally, in recent years, median 12-month growth (the top 300 TLDs) peaked at 7.5 % in late 2021, followed by a steady decline to 1.3 % by May 2024. The last two months of 2024 show early signs of a rebound with 2.0 % in July 2024.

ENISA NIS360 2024 report

O primeiro relatório NIS360 da Agência da União Europeia para a Cibersegurança, publicado em março de 2025, identifica áreas para melhoria e acompanhamento dos progressos nos setores da Diretiva NIS2.

De acordo com o estudo, seis setores da NIS estão na zona de risco NIS360, o que sugere que há margem para melhorar a sua maturidade em relação à sua criticidade. Os setores identificados como estando na zona de risco são: Gestão de Serviços de TIC; Aerospaço; Administrações Públicas; Marítimo; Saúde; e Gás.

The European Union Agency for Cybersecurity's first NIS360 report, published in March 2025, highlights areas for improvement and tracking progress in the sectors of the NIS2 Directive.

According to the study, six NIS sectors are in the NIS360 risk zone, suggesting there is room to improve their maturity in relation to their criticality. The sectors identified in the risk zone are: ICT Service Management, Space, Public Administration, Maritime, Health, and Gas.

Habits of excellence: Why are European ccTLD abuse rates so low?

Um estudo recente da DNS Research Federation tentou encontrar resposta à pergunta "porque é que o abuso dos ccTLDs europeus é tão baixo?" As conclusões apontam para o facto de que "existe uma correlação entre as baixas taxas de abuso dos ccTLDs da UE e os [seus] esforços de verificação dos dados de registo."

Avaliando o impacto nas taxas de abuso das práticas de dados adotadas pelos ccTLDs da UE, a validação automática da sintaxe e as verificações de dados 'ad hoc' e proporcionais feitas em resposta a suspeitas razoáveis de que um nome de domínio é malicioso, são as práticas mais amplamente adotadas no grupo de ccTLD da União Europeia", conclui o relatório.

A recent study by the DNS Research Federation attempted to find an answer to the question of 'Why are European ccTLD abuse rates so low?' The conclusions point to 'a correlation between the low abuse rates of EU ccTLDs and [their] efforts to verify registration data.'

'Evaluating the impact on abuse rates of the data practices undertaken by EU ccTLDs, the automated syntax validation and ad hoc, proportionate data checks done in response to reasonable suspicion that a domain name is malicious are the most widely adopted practices across the EU ccTLD group,' concludes the report.

Nova edição

Organização

.pt

CURSO

Cód. CNCIS

Gestão da Continuidade de Negócio

O que deve uma organização fazer quando um evento interrompe a normal entrega de bens ou serviços?

Descrição

Atualmente, os ciberataques são uma ameaça constante, tanto a pessoas individuais como a organizações. As organizações devem identificar as potenciais ameaças às operações críticas, bem como os impactos que poderão surgir caso estas ameaças se materializem.

As organizações necessitam de proteger as atividades vitais, definindo uma estratégias e elaborando o Plano de Continuidade de Negócio. Os procedimentos que a organização venha a definir devem ser testados e revistos. Neste curso terá a oportunidade de aprender os conceitos básicos de gestão da continuidade de negócio bem como de aplicar os conhecimentos desenvolvidos através de um caso prático.

Formato

- Duração: 10 horas
- Esforço: 10 horas
- Ritmo: Ao ritmo do estudante
- Idiomas: Português

O curso é constituído por um módulo de boas-vindas, quatro módulos teóricos com avaliação formativa e sumativa, e um módulo marcadamente prático.

Inscrições

De 24/03/2025 até 26/03/2026

Curso

De 31/03/2025 até 02/04/2026

Curso através da plataforma nau SEMPRE A APRENDER

Mais informações em www.nau.edu.pt

Esta publicação é produzida pelo .PT
This publication is produced by .PT

Editor | Editor
António Eduardo Marques

Design Gráfico | Graphic Design
Sara Dias
Maria Cristóvão

Tradução | Translation
Sara Pereira

Fotografia | Photography
Capa/Cover: AmazingArt, Adobe Stock
Índice/Table of contents: kribbox, Adobe Stock

Publicação trimestral | Quarterly publication
Abril 2025 | April 2025


.pt
www.pt.pt