CONSELHO DIGITAL
contato@conselhodigital.org.br

A falsa sensação de anonimato na internet: entenda o que é guarda de registro, IP e como requisitar dados de acesso

A sensação de anonimato na internet, muitas vezes alimentada pelo uso de pseudônimos e identidades fictícias, é na verdade uma ilusão. **A Constituição Federal brasileira proíbe o anonimato, e essa regra se aplica também ao ambiente digital.** Diferente de um bilhete deixado anonimamente em um local físico, onde a autoria pode ser difícil de rastrear, as ações realizadas na internet deixam rastros digitais. **Esses rastros, ou registros, são armazenados** por provedores de conexão de internet e plataformas online, conforme determina o Marco Civil da Internet.

O Marco Civil da Internet (MCI), Lei nº 12.965/14, estabelece normas sobre a guarda de registros de conexão e de acesso a aplicações de internet, visando assegurar a proteção de dados pessoais e a privacidade dos usuários, além de permitir a identificação de responsáveis por atos ilícitos online. Adiante explicaremos alguns conceitos básicos para compreender a guarda de registros e também como requisitar estes dados.

Mas o que é Guarda de Registro?

A **guarda de registros** é a prática de armazenar informações sobre as atividades realizadas pelos usuários na internet. No contexto do Marco Civil da Internet, isso se refere

especificamente à **obrigação dos provedores de conexão e de aplicação de internet de manterem registros detalhados das conexões e acessos realizados pelos usuários**. Esses registros são utilizados para fins de segurança, investigação e identificação de autores de atos ilícitos online.

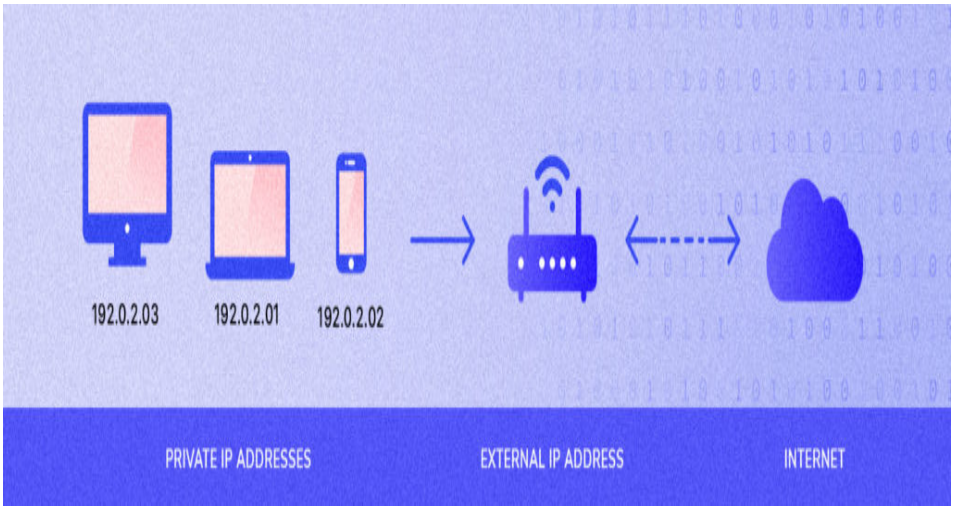
É importante, contudo, **distinguir a guarda de registros da guarda de conteúdos**. Enquanto a **guarda de conteúdo se refere à retenção de informações relacionadas ao conteúdo das comunicações** – como mensagens, fotos, vídeos e outros materiais publicados ou transmitidos pelos usuários – a **guarda de registro trata dos dados de conexão e acesso a aplicações de internet**.

Embora o **Marco Civil da Internet não exija que os provedores de conexão ou de aplicação guardem o conteúdo das comunicações dos usuários**, ele prevê em seu **artigo 10** que, **mediante ordem judicial, os provedores podem ser obrigados a fazê-lo para um usuário específico**. Essa obrigação de guardar o conteúdo das comunicações só é válida a partir do momento da intimação judicial, e os provedores não podem ser responsabilizados por não terem armazenado esses dados antes da ordem judicial.

Por outro lado, o Marco Civil da Internet prevê obrigações de guarda de registro. De acordo com o **artigo 13**, os **provedores de conexão à internet** – como Net, Vivo, GVT etc – devem manter os **registros de conexão** sob sigilo, em ambiente controlado e de segurança, pelo **prazo de um ano**. Esses registros incluem a **data e a hora de início e término de uma conexão, sua duração e o endereço IP utilizado**.

Já os **provedores de aplicações de internet** – como Instagram, Youtube, Google ou TikTok, por exemplo – nos termos do **artigo 15**, devem manter os **registros de acesso** a essas aplicações, também sob sigilo e em ambiente seguro, pelo **prazo de seis meses**, salvo disposição em contrário. Esses registros abrangem a **data e a hora de uso de uma aplicação de internet a partir de um determinado endereço IP**.

Em todos os casos, a autoridade policial ou administrativa ou o Ministério Público poderá **requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto inicialmente pela lei**.

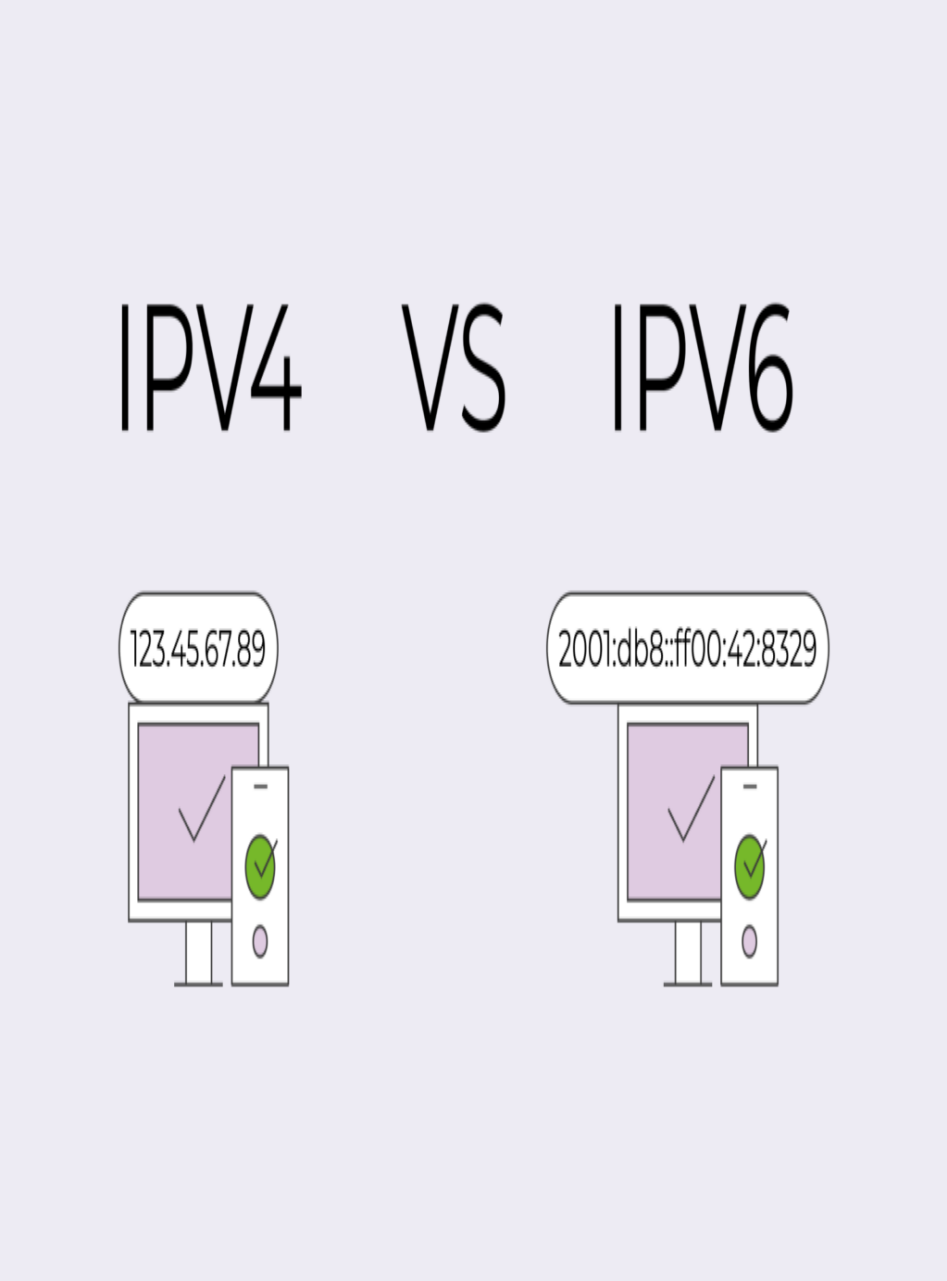


Mas o que é IP?

Um IP (Internet Protocol) nada mais é que um **identificador atribuído a cada dispositivo conectado à internet.** Assim como uma placa de veículo, ele permite que computadores, smartphones e outros dispositivos se comuniquem entre si na rede.

Assim, se uma pessoa comete um ilícito online, como espalhar informações caluniosas ou difamar alguém, **as autoridades podem rastrear a atividade até um endereço IP específico**. Com a devida autorização judicial, elas podem solicitar os registros ao provedor de aplicação (por exemplo, uma rede social), descobrir o endereço IP utilizado e, em seguida, pedir ao provedor de conexão os dados do usuário que estava usando aquele endereço IP na data e hora em questão. Dessa forma, conseguem identificar o responsável pelo ato ilícito.

Assim, o endereço IP é uma ferramenta essencial para a investigação e resolução de crimes cibernéticos, permitindo que as autoridades conectem atividades online a usuários específicos, garantindo que os infratores possam ser responsabilizados.



Existem duas versões de IP. O IPv4, mais antigo, usa endereços de 32 bits, suportando cerca de 4,3 bilhões de endereços únicos (ex: 192.168.0.1). O IPv6

usa endereços de 128 bits, permitindo um número muito maior de endereços (ex: 2001:0db8:85a3::8a2e:0370:7334). IPv6 foi criado para atender à crescente demanda por dispositivos conectados à internet.

Na prática, como funciona para identificar um cybercriminoso?

Apesar da sensação de anonimato, a internet é um espaço regulado e monitorado, onde as ações dos usuários podem ser rastreadas e os responsáveis por abusos e ilícitos podem ser identificados. Para identificar quem cometeu um ilícito na internet, é necessário uma autorização judicial.

O Marco Civil da Internet, em seus **artigos 22 e 23**, estabelece os fundamentos legais para a **solicitação judicial de registros de conexão e de acesso a aplicações**, que são essenciais para a investigação e compreensão das atividades online.

O **artigo 22 especifica os procedimentos** que devem ser seguidos pelas partes interessadas ao requisitar judicialmente esses registros. Ele destaca a necessidade de uma **ordem judicial específica**, que deve ser bem fundamentada e acompanhada de indícios suficientes de práticas ilícitas. Conforme o artigo, uma solicitação judicial de registros deve conter obrigatoriamente três requisitos:

- **Indícios fundados da ocorrência de um ilícito;**
- **Justificativa motivada da necessidade dos registros para a investigação ou como prova;**
- **Especificação do período a que os registros se referem.**

Se qualquer um desses três requisitos estiver ausente, o juiz deve rejeitar a solicitação judicial de registros, conforme estipulado no parágrafo único do artigo 22.

Por sua vez, o **artigo 23 direciona-se aos juízes**, enfatizando a obrigação do Poder Judiciário de assegurar o sigilo das informações obtidas e proteger a intimidade, a vida privada, a honra e a imagem dos usuários. O artigo permite, inclusive, que os pedidos de guarda de registros sejam tratados sob segredo de justiça, garantindo assim a confidencialidade das informações envolvidas.

CONSELHO DIGITAL
contato@conselhodigital.org.br

Mas as plataformas podem entregar dados cadastrais sem autorização judicial?

Em **caso de crimes graves**, como risco de vida ou ameaça de morte, dados cadastrais – como e-mail de criação da conta, e em alguns casos, IP de criação de conta – **podem ser fornecidos mesmo sem ordem judicial, desde que solicitado por autoridade policial dentro dos 6 meses previstos como prazo de guarda pelo provedor de aplicação**.

Category

1. Material educativo

Tags

1. anonimato

Date
18/10/2024
Date Created
13/06/2024