O PL 2630 e as portas "nateadas"

Enviado por admin em sab, 05/09/2020 - 22:59

Artigos do PL 2630 (conhecido como a “lei das fake news”)[1] contêm fragilidades técnicas que precisam ser esclarecidas. Em particular, o artigo 35 baseia-se em premissas falsas ou que correm o risco de obsolescência a curto prazo. Diz o artigo:

Art. 35. A Lei no 12.965, de 23 de abril de 2014 (Marco Civil da Internet), passa a vigorar com as seguintes alterações:
“Art. 5º .....
VIII – registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP e a porta lógica, quando o IP for nateado;
IX – nateamento de IP: o compartilhamento de um IP para mais de uma conexão ou usuário único, individualizadas através de diferentes portas lógicas; e
X – portas lógicas: os dispositivos que operam e trabalham com um ou mais sinais lógicos de entrada para produzir uma e somente uma saída.” (NR)
“Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, inclusive os registros que individualizem o usuário de um IP de maneira inequívoca, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Consideremos uma rede local de terminais (computadores, tabuletas, celulares, TVs etc) conectados a um roteador local que serve de “portal” (“gateway”) para a Internet (roteador de borda da rede local). Esta rede pode ser de uma grande instituição, um pequeno negócio ou uma típica rede caseira. Esse roteador local recebe um IP público (que pode variar com o tempo conforme a política de endereçamento do provedor), ou seja, um endereço numérico IP reconhecido como único na Internet, e para merecer seu nome roteia tráfego de dados através desse IP público entre os terminais da rede local e a Internet.

Os terminais da rede local são identificados por IP privado (um número IP que só é reconhecido como tal na própria rede local) de um bloco de números fornecido pelo roteador local. O tráfego de saída e entrante entre um terminal e seu IP privado e o roteador e seu IP público envolve a definição de número de porta arbitrário (tipicamente um número entre 1 e 1023, podendo teoricamente chegar a 65535), não permanente, para cada terminal. A combinação do IP privado com esse número de porta (incorretamente chamado de “porta lógica”) permite que o roteador local identifique de que terminal procede ou para qual terminal deve ser entregue cada datagrama enviado ou recebido. No jargão técnico é um método de endereçamento interno conhecido como NAT (“Network Address Translation”), que inclui um PAT (“Port Address Translation”). Há várias implementações de NAT, dependendo do firmware[2] que os fabricantes dos roteadores instalam por padrão.

Do lado externo, o datagrama enviado não contém o IP privado do terminal de origem – apenas o número de porta associado ao terminal e o IP público do roteador local, e o datagrama de retorno traz esse mesmo endereço embutido no cabeçalho do datagrama. O roteador local tem a tabela que associa o número de porta ao IP privado e assim pode entregar o datagrama ao endereço correto da rede local.

Na maioria dos casos, e por padrão, o roteador da rede local do usuário está configurado para oferecer os IPs privados por uma funcionalidade conhecida como DHCP (“Dynamic Host Configuration Protocol”) que entrega IPs privados (e as respectivos números de porta) aos terminais, geralmente em ordem numérica crescente assim que os terminais são conectados à rede. Isso significa que se um terminal for desligado, ao retornar à rede pode receber um outro IP privado e número de porta. Em resumo, a associação do IP privado e número de porta a um terminal em DHCP não é perene.

Na verdade, com a escassez de números IPv4, provedores de acesso adotam muitas vezes um NAT (com DHCP), conhecido pelo pomposo nome de “Carrier-Grade NAT” (CGNAT) para conectar redes locais de um bairro ou até uma área maior – neste caso o IP público do roteador local de sua casa ou escritório pode estar compartilhado com dezenas

de vizinhos e centenas de terminais com os decorrentes riscos de segurança (e quase impossibilidade de localizar inequivocamente que humano fez o que). Isso é comum na conexão de celulares por redes celulares de dados, ou em serviços de conexão via satélite, mas é também usado por outros provedores com escassez de IPs públicos disponíveis.

Um número de porta associado a um nome de domínio em uma rede local pode também ser configurada para oferecer algum tipo de serviço (um serviço Web por exemplo) que pode ser visitado diretamente por um usuário externo. Há empresas que oferecem a funcionalidade conhecida como “DNS dinâmico”, que assegura que o serviço em um terminal interno siga sendo visível mesmo que o provedor de acesso mude o IP público do roteador local. O número de porta (no caso do exemplo, em geral é a porta 80, por convenção reconhecida como serviço Web) entra no jogo apenas para definir o tipo de serviço/protocolo que, no roteador local, está associado a um terminal.

Em nenhum desses casos há como assegurar inequivocamente com esses dados quem estava usando um terminal em dado período de tempo. Ademais, o registro (“log”) da combinação de números de porta e IPs privados em uso, se existir, é feito em um ou mais dispositivos locais (roteador local de borda, pontos de acesso wi-fi e outros roteadores locais em redes mais complexas) sob controle do responsável pela rede local, e não necessariamente estão ao alcance do provedor de acesso. Há muitos casos em que pontos de acesso wi-fi distribuidos pela rede local operam DHCPs individuais utilizando blocos distintos de IPs privados, e esse encadeamento dificulta ainda mais o registro inequívoco do que ocorre na ponta (no terminal).

É importante notar que o artigo 35 do PL 2630 não leva em conta a natureza temporária da tecnologia envolvida. A Internet passa por uma transição para um novo sistema de endereçamento (IPv6) e o NAT ou CGNAT será substituido por novas formas de identificação de dispositivos na rede. Por essas e por outras, o artigo 35 na verdade carece de rigor técnico, já nasce com o risco de obsolescência e, da forma como está, seria inútil para o suposto propósito. A recomendação é que seja descartado.

A seguir os artigos do Marco Civil mencionados na redação do artigo 35 do PL 2630:

Art. 5º Para os efeitos desta Lei, considera-se:
I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito,com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
II - terminal: o computador ou qualquer dispositivo que se conecte à internet;
III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação,definido segundo parâmetros internacionais;
IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;
V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante aatribuição ou autenticação de um endereço IP;
VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet,sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
VIII - registros de acesso a aplicações de internet: o conjuntode informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 15º O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3º e 4º do art. 13.
§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência

[1] *https://www25.senado.leg.br/web/atividade/materias/-/materia/141944* [1]

[2] *Firmware* ou software embarcado é um programa de controle de um dispositivo que permite acesso a suas diferentes funções. Funciona como uma interface entre programas do usuário e as funcionalidades do dispositivo. Computadores em geral são fornecidos com *firmware* conhecido como BIOS (“basic input-output system”) que permite que os programas (incluindo o sistema operacional escolhido para o computador) possa acionar as funcionalidades do sistema e seus periféricos (rádio wi-fi ou bluetooth, discos, memória interna, teclado, mouse, vídeo etc etc).

Links
[1] https://www25.senado.leg.br/web/atividade/materias/-/materia/141944