O anonimato da transição nas quebras de sigilo informático

Da necessidade ou não da indicação de porta lógica de origem para identificação de usuários de Internet

Recentemente, considerando a escassez de IPs na versão 4, inúmeros provedores de acesso começaram a implementar solução tecnológica a seus usuários, fazendo com que diversos clientes acessassem a Internet por meio de um único IP compartilhado, o que vale para telefonia móvel.

Deste modo, ao serem instados judicialmente a fornecerem dados cadastrais de seu cliente que em determinado dia e hora estava conectado à Internet com o um dado IP, os provedores recusam a ordem e como se não soubessem que a vítima não tem este dado, condicionam o fornecimento dos dados à indicação, pela vítima, da "porta lógica de origem", utilizada em cada conexão.

Justificam que o Comitê Gestor autorizou os provedores de acesso a compartilharem os IPs pré-existentes, nesta fase de transição para o IPV6. Deste modo, único elemento que distinguiria um usuário (computador) de outro, que no mesmo momento usa o mesmo IP para acesso a serviços a Internet, seria a porta lógica de origem.

A comunicação pela Internet é feita, basicamente, através de protocolos, de modo que o TCP (Transmission Control Protocol) é um dos mais importantes. O TCP está no contexto do conjunto de protocolos TCP/IP, base para as comunicações pela Internet.

Para permitir que computadores utilizem o mesmo IP público e usem a web o NAT (Network Address Translation) processa o IP interno e a porta local e gera uma numeração, que é gravada no campo "porta de origem". Assim, a transmissão web usa o IP

público do roteador e este número gerado é gravado no campo "porta de origem". No retorno do pacote o próprio NAT se encarrega de identificar em sua tabela o número de origem, encaminhando o pacote ao solicitante. Em síntese, vários computadores, praticando vários atos na Web, com o mesmo IP.

Ocorre que a vítima não tem conhecimento da "porta de origem" de um IP identificado como de origem de um ataque ou crime. Aliás, a vítima normalmente processa o provedor de acesso a aplicações para que este forneça o IP, data e hora relativo ao usuário que acessou o site, rede social ou serviço web para atividades ilícitas. Assim, o próprio provedor de aplicações, embora possa tecnicamente, não registra a porta de origem relativa aos IPs de usuários de seus serviços, nem está obrigado a assim proceder.

Tais aplicações devem guardar apenas os registros de acesso a aplicação, que nos termos do art. 5o., VI, do Marco Civil da Internet, são 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.

Neste sentido já entendeu o TJ/SP, em julgamento do Agravo de instrumento 2012094-24.2015.8.26.0000:

AGRAVO DE INSTRUMENTO – Obrigação de fazer – Provedor de serviços de internet – Decisão que antecipou a tutela e determinou a remoção do ar de fan pages e grupos fechados hospedados nas URLs indicadas e fornecimento de dados de cadastro disponíveis – Preliminar de conversão em retido – Não cabimento – Mérito – Insurgência da ré apenas no tocante à informação das "portas lógicas de origem" – Informação própria de provedor de conexão – Empresa/ré que exerce atividade de provedor de aplicação de internet (Facebook) – Impossibilidade de fornecimento dos dados relativos à "porta lógica de origem" – Decisão modificada – Preliminar rejeitada, recurso provido. (TJ-SP, Relator: Egidio Giacoia, Data de Julgamento:

28/04/2015, 3ª Câmara de Direito Privado)

Assim, não cabe ao Provedor de Acesso dificultar o fornecimento de dados cadastrais relativos aos IPs identificados pelo provedor de aplicações, para uma data e horário devidamente especificados, impondo-lhes a condicionante de apresentarem as "portas lógicas de origem" relacionadas aos referidos IPs. A vítima não tem este dado. Já o provedor de aplicações, por lei e decisões judiciais recentes, não tem obrigação de registrar a porta lógica de origem e caso venha a fazer, terá de prover mudanças consideráveis no sistema de registros.

Ademais, o número IP já permite identificar a conexão de computadores na Internet, sendo que, pela especificação de data e hora (as vezes até minutos e segundos), relacionada a ofensa ou golpes, seria possível restringir o fornecimento dos dados a somente aos que se enquadram no critério temporal, ou mesmo buscar a adoção de outros critérios.

Por outro lado, a questão da "privacidade" dos registos de outros usuários que coincidentemente estivessem conectados no mesmo horário da ofensa, no mesmo IP (Internet protocol) é fato a ser considerado. Uma alternativa seria um fornecimento mínimo de campos relativos aos registros de usuários identificados, pelo provedor de acesso, e diante das análises sobre estes dados (como por exemplo a cidade de origem) um outro pedido adicional relativo a um registro específico, com dados mais completos.

De se destacar que a eventual violação da privacidade não estaria relaciona a expor
"o que um usuário fez na Internet" em determinada data, mas expor que "ele estava conectado à Internet", em determinada data.

Enquanto alternativas não surgem, provedores de aplicações não registram tal "porta" (não há ajustamentos de conduta ou

decisões neste sentido) e crimes cibernéticos continuam ocorrendo, resta ao Julgador, sopesando a gravidade do caso concreto, ponderar entre eventual violação à privacidade e os direitos das vítimas em identificarem os autores dos delitos, para que possam responsabilizá-los nos termos da Lei. Este "anonimato" gerado pela transição tecnológica, sem previsão para acabar, precisa de uma resposta rápida da Autoridades.

Convite: Debate sobre aspectos jurídicos do IPV6

Tive a privilégio de ser chamado para o primeiro debate profundo sobre aspectos jurídicos do novo "protocolo IPV6". O evento é público e será realizado na casa da cidadania, na OAB/SP, tendo sido promovido pela atuante Comissão Estadual de Crimes de Alta Tecnologia, presidida por @CoriolanoAC. O debate, que será no dia 28 de janeiro de 2011, às 09:30 horas, contará com Antonio Moreiras, supervisor de projetos do NIC.br e que tem coordenado a transição na região metropolitana para o IPV6, contando também com a presença da Dra. Raquel Gatto, Diretora Executiva do NIC.br.

Logicamente, abordarei as mudanças nas conduções de processos de investigação de crimes digitais como IPV6, ponto ainda não petrificado e carecedor de profundos debates.

Todos estão convidados! Os vejo no evento!

Para ter acesso ao conteúdo completo do evento (programa): OAB-SP CAT temática IVP6-v12011F

Para ter acesso ao banner para divulgação: http://www.mokrejs.com/oabsp/20110111_IPv6/20110111_IPv6.html