São Paulo, Brazil
November 4-5, 2019

The Eleventh International Conference on
FORENSIC COMPUTER SCIENCE and CYBER LAW

www.ICoFCS.org

DOI: 10.5769/C2019003 or http://dx.doi.org/10.5769/C2019003

Investigação cibernética no ordenamento jurídico brasileiro

Paulo Quintiliano[1], Dirceu Freitas Filho[2], Jefferson Plentz[3]

(1) Quintiliano Sociedade de Advocacia, Freitas Quintiliano Advogados Associados. E-mail: Paulo.Quintiliano@hotmail.com
(2) Freitas Quintiliano Advogados Associados, E-mail: dirceu@freitasquintiliano.com.br
(3) Techtools Ventures, E-mail: *Jeff.plentz@techtools.vc*

Abstract: Por meio deste artigo é apresentada abordagem para se levar a bom termo investigação cibernética em face de crimes cometidos por meio da internet, de forma não oficial, conduzida por advogado especialista em Direito Cibernético. A investigação cibernética pode também ser conduzida de forma oficial, no bojo de um inquérito policial, o que não será objeto de estudos desse artigo. São apresentadas técnicas de investigação cibernética para a identificação de usuários autores de práticas ilícitas na internet, envolvendo a busca e preservação dos registros de acesso à internet e demais dados necessários, por meio de ordens judiciais, bem como dos exames periciais. São discutidas as obrigações impostas aos provedores de acesso à internet e aos provedores de aplicações de internet de preservarem os registros de acesso à internet e às aplicações de internet.

Key words: Investigação cibernética, crimes digitais, Marco Civil da Internet, portas lógicas.

1. Introdução

A internet pode sim ser local de crimes. A diferença é que no caso de crimes cibernéticos as evidências que podem permitir a comprovação da materialidade, dinâmica e autoria dos crimes estão armazenadas em meios digitais. O sigilo dessas evidências digitais está protegido pela Lei Nº 12.965/2014 (Marco Civil da Internet), não podendo ser obtidas sem autorização judicial, sob pena de serem consideradas obtidas de forma ilegal.

Assim, a investigação desses crimes não pode ser conduzida somente por peritos em Computação Forense, pois depende de autorização judicial determinando o afastamento do sigilo telemático dessas informações. Nas investigações não-oficiais somente o advogado tem competência para peticionar em juízo e solicitar o afastamento do sigilo telemático dos registros de conexão e de acesso a aplicações de internet.

Nas investigações oficiais, o delegado de polícia cumpre esse papel, no bojo de um inquérito policial. Contudo, as investigações oficiais não serão abordadas neste artigo.

2. Acesso à internet

Para que seja possível o acesso à internet, o usuário precisa utilizar um endereço público e válido de IP, podendo ser do protocolo IPv4 ou IPv6, bem como se identificar e se apresentar de forma unívoca perante os recursos acessíveis no espaço cibernético.

Atualmente o endereçamento da Internet funciona por meio dos protocolos IPv4 (*Internet Protocol version 4*) e IPv6 (*Internet Protocol version 6*), que proporcionam endereços para o estabelecimento das conexões entre os computadores e demais recursos disponíveis. O antigo protocolo IPv4 disponibiliza cerca de 4,3 bilhões de endereços IP, sendo que tais endereços já foram esgotados, enquanto que o protocolo IPv6 disponibiliza cerca de 340 undecilhões de endereços IP. É uma quantidade absurdamente grande, suficiente para a implementação de novas tecnologias, como a IoT (*Internet of Things*), em que todas as pessoas poderão possuir grandes quantidades de endereços fixos de IP.

Atualmente, em decorrência do esgotamento do protocolo antigo, está em curso a migração do protocolo IPv4 para o IPv6, sendo que os dois protocolos estão funcionando paralelamente. Contudo, a migração está sendo feita de forma muito lenta, havendo pouco mais de 20% da migração efetivada.

Em virtude da necessidade da implantação do protocolo IPv6 para usuários que ainda precisam de conexões do protocolo IPv4, bem como do esgotamento do antigo protocolo, exsurge a necessidade da constante criação de novas técnicas de transição de um protocolo para outro. Em consequência, novas informações acessórias são criadas nos registros de conexões à internet, sendo elas imprescindíveis para a identificação dos responsáveis pela prática de atos ilícitos por meio da internet, já que milhares de usuários podem utilizar o mesmo endereço de IP (do protocolo IPv4) ao mesmo tempo.

3. Marco Civil da Internet

O Marco Civil da Internet regulamenta a atuação dos dois únicos grandes atores do espaço cibernético: usuários e provedores de serviços de internet. Há inúmeros tipos de usuários e de provedores de serviços de internet.

O artigo 7º do Marco Civil da Internet, que trata dos direitos e garantias dos usuários, por meio de seus incisos I e II, garante a inviolabilidade e o sigilo das comunicações privadas dos usuários, bem como dos fluxos de suas comunicações pela internet. Tais informações somente podem ser obtidas por meio de ordens judiciais determinando o afastamento do seu sigilo.

O inciso VII desse mesmo artigo 7º garante o não fornecimento a terceiros dos dados pessoais dos usuários, inclusive registros de conexão e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou por meio de ordens judiciais que determinem o afastamento do sigilo dessas informações.

Assim, resta clara a proteção do sigilo dos registros de acesso à internet e às aplicações de serviço de internet, devidamente conferida pelo Marco Civil da Internet.

O § 1º do artigo 10 estabelece que o provedor responsável pela guarda somente será obrigado a disponibilizar os registros de conexão e de acesso a aplicações de internet, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial.

O artigo 13 estabelece o dever do administrador de sistema autônomo de manter e preservar, pelo prazo de um ano, os registros de conexão de internet.

Observe-se que o legislador não menciona exatamente quais dados ou informações dos registros de conexões de internet devem ser preservados. Assim, deve-se entender que são todos os dados e informações necessários para a identificação do usuário responsável pela prática ilícita, visto que o objetivo dessa preservação é exatamente esse: identificar os usuários a partir de suas condutas praticadas nos meios disponibilizados na internet.

Conforme estabelece o legislador, apenas o administrador de sistema autônomo tem o dever de preservar tais informações. O artigo 5º, IV, define bem o administrador de sistema autônomo, que é 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 pela distribuição de endereços IP geograficamente referentes ao País.

Dessa forma, os hotéis, restaurantes, bares, aeroportos e outros centros comerciais não têm a obrigação legal de preservar os registros de conexão à internet, visto que não podem ser considerados administradores de sistemas autônomos.

3.1. Registros de conexão e de acesso a aplicações de internet

O Marco Civil da Internet se refere a "registros de conexão e de acesso a aplicações de internet", sem entrar em detalhamentos inúteis sobre quais seriam esses registros. Seguramente não poderia ser de outra forma, visto que a tecnologia se apresenta de forma muito dinâmica, surgindo novidades tecnológicas a todo momento, como a tecnologia NAT, que compartilha os endereços de IPv4, não sendo possível prever todas as possibilidades.

Assim, essas informações auxiliares, como a porta lógica de origem e o endereço de IP interno, são imprescindíveis para a identificação dos usuários na internet. O endereço de IP válido não é suficiente para a identificação do usuário, pois, conforme discutido alhures, milhares de usuários podem utilizar o mesmo endereço de IP (do protocolo IPv4) ao mesmo tempo.

Conforme conclusões apostas no Relatório Final de Atividades do GT-IPv6 [4], sobre a identificação unívoca de um determinado usuário que faz uso de um endereço IP compartilhado, restou acordado entre os vários especialistas envolvidos naquele trabalho técnico que a única forma que têm os provedores de serviços de internet de identificarem os usuários que utilizam endereços de IP compartilhados, em determinada data e horário exato, é por meio da porta lógica de origem da conexão utilizada.

Nesse sentido, os especialistas concluíram que os provedores de aplicação precisam fornecer o endereço de IP válido, da conexão de origem, bem como, necessariamente, também a porta lógica de origem. Sem a porta lógica, torna-se impossível a identificação e localização do usuário responsável pela conduta ilícita, visto que a o mesmo endereço de IP válido pode ser compartilhado por centenas e até milhares de usuários ao mesmo tempo [4].

Assim, ainda em consonância com as conclusões do Grupo de Trabalho GT-IPv6 [4], que enquanto os endereços de IPv4 estiverem sendo compartilhado por vários usuários ao mesmo tempo, em decorrência do esgotamento dos endereços desse protocolo, para que seja possível a identificação e localização dos usuários responsáveis por práticas ilícitas, é imprescindível que os provedores de acesso e os provedores de aplicações de internet preservem e forneçam as portas lógicas de origem utilizadas nas conexões, sob pena de se tornar inviável a investigação de crimes cometidos por meio da internet, em decorrência da impossibilidade da identificação desses usuários.

É importante destacar que, de fato, é imprescindível que tanto os provedores de acesso como os provedores de aplicações precisam preservar e fornecer as portas lógicas de origem para ser possível a identificação desses usuários. Essa imprescindibilidade exsurge devido ao fato de que a chave unívoca que permite a identificação desses usuários é composta, dela fazendo parte o endereço de IP público e a porta lógica de origem.

Se o provedor de aplicação somente fornecer o endereço de IP, não será possível a identificação do usuário perante o provedor de acesso, visto que inúmeros usuários compartilham o mesmo endereço de IP ao mesmo tempo.

4. Investigação cibernética

A investigação cibernética é muito dependente dos provedores de serviços de internet, visto que as informações que poderão permitir a comprovação da materialidade, dinâmica e autoria dos crimes estão em seu poder e estão protegidas por sigilo.

Com o objetivo de observar rigorosamente a legalidade das provas a serem produzidas, é imprescindível que todos as evidências sejam obtidas por meio de ordens judiciais que determinem o afastamento do sigilo telemático das informações.

Em caso de ocorrência de conduta criminosa, praticada por meio da internet, deve-se

imediatamente promover a coleta e a preservação das evidências digitais que poderão comprovar a materialidade do fato, por meio da emissão de Ata Notarial, em Cartório. A Ata Notarial, por ter fé-pública, é um meio de prova extremamente forte e que deve ser sempre utilizado nas investigações cibernéticas não-oficiais.

Ocorrendo, v.g., a publicação de mensagem criminosa em uma rede social, como o Facebook, deve-se solicitar imediatamente a emissão da Ata Notarial para a comprovação da materialidade do fato. Necessariamente devem ser coletados os endereços de URL do perfil do atacante, bem como de todas as mensagens ofensivas postadas.

Com base na Ata Notarial, o advogado especialista em Direito Cibernético ajuizará ação judicial em que pedirá o afastamento do sigilo telemático dos endereços de URL obtidos, bem como a imediata remoção do conteúdo ofensivo publicado na internet.

Uma vez deferido o afastamento do sigilo e obtidos os registros de conexão e de acesso a aplicações de internet, serão feitos exames periciais para a identificação do endereço de IP utilizado na conexão ilícita, bem como as informações acessórias como: porta lógica de origem, IP interno, endereço MAC, IMEI, localização geográfica, pontos de acesso Wi-Fi, identificação de torres de celulares, datas e horários exatos (início e término) da conexão ilícita, com informação de fuso horário e possível existência de horário de verão.

Na sequência, com base nos resultados dos exames periciais, deve ser solicitado o afastamento do sigilo telemático dos endereços de IP externo e interno e portas lógicas, em face do provedor de acesso à internet proprietário dos endereços de IP, no intervalo de tempo em que foram feitas as conexões ilícitas, de forma a serem obtidas informações sobre as linhas telefônicas utilizadas nessas conexões.

Para se identificarem os provedores de acesso proprietários dos endereços de IP encontrados, deve-se utilizar um serviço de “Who is”. O Registro.br oferece esse serviço para a identificação de domínios e endereços de IP brasileiros, por meio do link “https://registro.br/tecnologia/ferramentas/whois/”, em que são fornecidas as informações cadastrais das empresas.

Uma vez deferido o afastamento do sigilo dos endereços de IP e obtidos os dados solicitados, serão necessários novos exames periciais com a finalidade de se identificarem as pessoas responsáveis pelos ataques.

5. Perícia de Informática

A perícia de Informática, nos casos de crimes cibernéticos, normalmente envolve muitas atividades de investigação no espaço cibernético, sendo que tanto as atividades periciais quanto a investigação cibernética são muito dependentes dos provedores de serviços de internet, visto que as informações que podem elucidar o caso são protegidas por sigilo e, portanto, somente podem ser obtidas a partir de ordens judiciais determinando o afastamento do sigilo telemático dos registros de conexões à internet e de acesso a aplicações de internet.

Como são tratados dados e informações bastante técnicos, a perícia de Informática, realizada por perito não-oficial, especialista em Computação Forense, é de grande relevância. Assim, nas investigações cibernéticas não-oficiais, o advogado especialista em Direito Cibernético deverá atuar com o apoio do perito especialista em Computação Forense, de forma a se chegar a bom termo nas investigações.

6. Necessidade dos registros de conexão e de acesso a aplicações de internet

O Marco Civil da Internet, por meio de seu artigo 13, impõe aos provedores de acesso à internet (administradores de sistema autônomo) o dever de preservar e manter os registros de conexão à internet pelo prazo de um ano, sob sigilo, em ambiente controlado e de segurança. Impõe aos provedores de aplicações de internet (artigo 15) o dever de preservar os registros de acesso a aplicações de internet pelo prazo de 6 meses, em ambiente igualmente seguro.

Em nenhum momento a lei limita essa obrigação somente à preservação dos endereços de IP utilizados nas conexões criminosas. Ao contrário, o legislador impõe a exigência de forma aberta, referindo-se a “registros de conexão” para os provedores de acesso e “registros de acesso a aplicações de internet” para os provedores de aplicações de internet.

Dessa forma, considerando-se que a finalidade desses dispositivos legais (artigos 13 e 15) é garantir a possibilidade da identificação dos usuários da internet, a esses provedores de serviços de internet foram impostas as obrigações de preservarem dados suficientes para a sua identificação, em caso de prática de atos ilícitos por meio do espaço cibernético.

Portanto, esses provedores têm que preservar, além do endereço de IP válido, também todas as informações acessórias.

6.1. Jurisprudência

A jurisprudência do STJ, em consonância com o Marco Civil da Internet, firma o entendimento de que não cabe aos provedores de serviços de internet o monitoramento dos conteúdos publicados na internet, não podendo o serviço prestado ser considerado defeituoso caso haja publicações ofensivas, nos termos do CDC. Os provedores somente responderão civilmente se não tomarem as necessárias medidas para a remoção dos conteúdos ofensivos, dentro do prazo definido, em obediência a decisões judiciais.

Contudo, há decisões monocráticas do STJ equivocadas, estabelecendo a obrigatoriedade do fornecimento das portas lógicas de origem somente ao provedor de acesso e desonerando o provedor de aplicações dessa obrigação, seguramente por desconhecimento técnico. Decisões equivocadas como essa impossibilitam a identificação e localização do usuário responsável pela prática ilícita.

Os Tribunais de Justiça de Goiás, de São Paulo e de outros estados têm proferido decisões igualmente equivocadas, em que desobrigam os provedores de aplicações da obrigação de fornecerem as portas lógicas de origem das conexões utilizadas para propósitos ilícitos.

7. Conclusões

Conforme discutido, a investigação cibernética e a perícia de Informática são muito dependentes dos provedores de serviços de internet, visto que as informações que poderão esclarecer o caso estão sob a guarda desses provedores, bem como protegidas por sigilo, em conformidade com o Marco Civil da Internet.

Para que as investigações sejam levadas a bom termo, é imprescindível que os provedores de acesso e de aplicações forneçam todos os dados necessários para a identificação dos usuários responsáveis pela conduta ilícita, incluindo-se os endereços de IP público, as portas lógicas de origem, as datas e horários exatos da conexão utilizada para a prática criminosa, com a indicação de fuso horário e possível ocorrência de horário de verão, endereço MAC, IMEI, localização geográfica, pontos de acesso Wi-Fi, identificação de torres de celulares, se for o caso.

Referências Bibliográficas

[1] BRITO, Auriney. Direito Penal Informático. Editora Saraiva, 2013. ISBN 978-85-02-20942-8.

[2] CASSANTI, Moisés de Oliveira. Crimes Virtuais, Vítimas Reais. Editora Brasport Livros e Multimídia Ltda. 2014.

[3] DE LUCA, Newton (obra coletiva). Direito & Internet. Editora Quartier Latin do Brasil. 2ª edição, 2005.

[4] GT-IPv6, Grupo de Trabalho para implantação do protocolo IPVersão 6 nas redes das Prestadoras de Serviços de Telecomunicações, Relatório Final de Atividades, 2014.

[5] MALAQUIAS, Roberto Darós. Crime Cibernético e prova: A investigação Criminal em Busca da Verdade. ISBN 978-85-362-5383-1. Curitiba: Editora Juruá, 2º edição revista e atualizada, 2015.

[6] PINHEIRO, Patricia Peck. Direito Digital. São Paulo: Editora Saraiva, 6º edição: 2016. ISBN 978-85-02-63561-6.

[7] PINHEIRO, Patrícia Peck (obra coletiva). Direito Digital Aplicado 2.0. São Paulo: Editora Thomson Reuters, 2ª edição: 2016. ISBN 978-85-203-6864-0.

[8] QUINTILIANO, Paulo. Crimes Eleitorais Cibernéticos nas Campanhas Eleitorais pela Internet. The Tenth International Conference on

Forensic Computer Science and Cyber Law. DOI 10.5769/C2018011. ISBN 978-85-65069-15-1. São Paulo, Brasil, 2018, pp 88-99.

[9] QUINTILIANO, Paulo; CAMARGO, Coriolano, e REYES, Anthony. Brasil como principal alvo de ataques cibernéticos. The Tenth International Conference on Forensic Computer Science and Cyber Law. DOI 10.5769/C2018012. ISBN 978-85-65069-15-1. São Paulo, Brasil, 2018, pp 100-105.

[10] REYES, Anthony (obra coletiva). Cyber Crime Investigations. Editora Amorette Pedersen, 2007. ISBN 978-1-59749-133-4.

[11] SCHJOLBERG, Stein. A global framework on cybersecurity and cybercrime, and a contribution for peace, security and justice in cyberspace. A Geneva Convention or Declaration for Cyberspace. VFAC Review, No. 12, October 2016, Korean Institute of Criminology.

[12] SILVA, Nilton; et. al. Document type classification for Brazil's supreme court using a Convolutional Neural Network. The Tenth International Conference on Forensic Computer Science and Cyber Law. DOI 10.5769/C2018001. ISBN 978-85-65069-15-1. São Paulo, Brasil, 2018. pp 7-11.

Paulo Quintiliano, *Ph.D.*
Presidente HTCIA Brazil Chapter
Quintiliano Sociedade de Advocacia
Freitas e Quintiliano Advogados Associados
Advogado especialista em Direito Cibernético
(www.quintiliano.adv.br)
paulo.quintiliano@hotmail.com

Dirceu Freitas Filho
Freitas e Quintiliano Advogados Associados
Advogado especialista em Direito Tributário e Compliance
(www.freitasquintiliano.com.br)

Jefferson Plentz
1º Vice-Presidente da HTCIA Brazil Chapter
Presidente da Techtools Ventures
(www.techtools.vc)
Jeff.Plentz@techtools.vc)