Civil Procedure Review
AB OMNIBUS PRO OMNIBUS

5

O regime jurídico das provas digitais no Direito brasileiro

The discipline of digital evidence in Brazilian Law

João Paulo Lordelo Guimarães Tavares
PhD in Law (Federal University of Bahia). Federal Prosecutor, Brazil.

RESUMO: O presente artigo tem por objetivo descrever o panorama geral da disciplina das provas digitais no Direito brasileiro. Inicialmente, são explicados os conceitos fundamentais para a compreensão do tema, relativos ao funcionamento das tecnologias de conexão à internet e acesso às aplicações disponíveis. Essa explicação envolve, entre outros, conceitos disciplinados pelo Marco Civil da Internet (Lei n. 12.965/2014), a exemplo do endereço de protocolo de internet (endereço IP), provedores de conexão e de acesso a aplicações de internet. Em seguida, é descrito o regime processual estabelecido pela mencionada lei, para então ser proposta uma metodologia básica de identificação de usuários a partir da coleta de dados de conexão ou acesso. Também são estabelecidas distinções processuais relevantes, em especial entre as medidas de busca e apreensão virtual e de interceptação de fluxo de dados. Ao final, são feitas considerações acerca da cadeia de custódia da prova, perícia e *hashing,* bem como da preservação de conteúdo.

Palavras-Chave: Direito probatório. Provas digitais. Marco Civil da Internet. Provedores de conexão. Provedores de aplicações de internet.

ABSTRACT: This article aims to describe the general panorama of the discipline of digital evidence in Brazilian law. Initially, the fundamental concepts for understanding the theme, about the functioning of Internet connection technologies and access to available applications, are explained. This explanation involves, among others, concepts disciplined by the Law 12.965/2014, such as the concept of internet protocol address (IP address), connection providers and internet applications providers. Then, the procedural regime established by the aforementioned legal statute is described, so that a basic methodology for identifying users from the collection of connection or access data is proposed. Relevant procedural distinctions are also defined, in particular between search and seizure measures and interception of data flow. By the end, considerations are made about the chain of custody of evidence, expertise and hashing, as well as the preservation of content.

KEY-WORDS: Evidence law. Digital evidence. Civil Framework of the Internet. Connection providers. Internet application providers.

1. INTRODUÇÃO

A cada dia, cresce o uso de evidências digitais no Brasil. O que antes parecia se limitar aos processos penais – especialmente para fins de comprovação de crimes como o de divulgação de pornografia infantil pela internet, previsto no art. 241-A da Lei n. 8.069/1990 – passou a fazer parte também de processos cíveis.

Isso se deve, especialmente, ao crescente acesso à internet pela população brasileira, bem como à popularização das redes sociais, ferramentas que acabaram produzindo efeitos relevantes em campos como o da responsabilidade civil e o do processo eleitoral.

Lamentavelmente, diferentemente do que se observa na experiência estrangeira, a doutrina brasileira parece não se atentar ao tema, sendo raros os trabalhos voltados a uma descrição mínima do estado da arte no país.

Partindo dessa percepção, o presente artigo tem por objetivo descrever o panorama geral da disciplina das provas digitais no Direito brasileiro.

Civil Procedure Review, v. 11, n. 3: set.-dez. 2020.
ISSN 2191-1339 – www.civilprocedurereview.com

Inicialmente, são explicados os conceitos fundamentais para a compreensão do tema, relativos ao funcionamento das tecnologias de conexão à internet e acesso às aplicações disponíveis. Essa explicação envolve, entre outros, conceitos disciplinados pelo Marco Civil da Internet (Lei n. 12.965/2014), a exemplo do endereço de protocolo de internet (endereço IP), provedores de conexão e de acesso a aplicações de internet.

Em seguida, é descrito o regime processual estabelecido pela mencionada lei, para então ser proposta uma metodologia básica de identificação de usuários a partir da coleta de dados de conexão ou acesso.

Também são estabelecidas distinções processuais relevantes, em especial entre as medidas de busca e apreensão virtual e de interceptação de fluxo de dados.

Ao final, são feitas considerações acerca da cadeia de custódia da prova, perícia e *hashing*, bem como da preservação de conteúdo, ferramenta que tem se revelado essencial para a conservação das provas.

2. CONCEITOS FUNDAMENTAIS

Para que se possa conhecer a disciplina da produção de *provas digitais*, é necessária a prévia compreensão a respeito de alguns conceitos fundamentais, relativos ao funcionamento das tecnologias de conexão à internet e acesso às aplicações disponíveis.

O objetivo dos tópicos seguintes é o de, pressupondo-se o alheamento dos juristas em geral em relação a tais temas, desenvolvê-los de forma acessível e objetiva, focando em seus aspectos mais relevantes para fins probatórios.

2.1. Endereço de protocolo de internet (endereço IP), *domain names* e DNS

O conceito de endereço de protocolo de internet (endereço IP) é certamente o elemento nuclear para a compreensão do funcionamento da internet. Isso porque ela consiste num sistema global de redes de computadores conectados a partir de protocolos de comunicação padronizados que utilizam tais endereços como "caminhos" ou "rotas" de interconectividade[1].

Toda pessoa conectada à internet o faz sob um endereço IP numérico. Esse número não é infinito. Cada endereço é distribuído pela *Internet Assigned Numbers Authority* (IANA), organização mundial sediada na Califórnia[2], encarregada de supervisionar e

1. HARGREAVES, Stuart; LOKMAN, Tsui. IP Addresses as Personal Data Under Hong Kong's Privacy Law: An Introduction to the Access My Info HK Project. *Journal of Law, Information & Science*, 2017, Vol. 25, p. 68-83, 16p. Borgesius, Frederik Zuiderveen. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. *European Data Protection Law Review (EDPL)*, 2017, Vol. 3, p. 130-137.
2. McGillivray, Kevin. Give it away now? Renewal of the IANA functions contract and its role in internet governance. *International Journal of Law & Information Technology*. Spring 2014, Vol. 22, p. 3-26. Cf. [http://www.iana.org].

atribuir IPs aos provedores de conexão de internet, possibilitando a atribuição aos seus usuários. Desde 1998, a IANA consiste em um departamento da *Internet Corporation for Assigned Names and Numbers* (ICANN)[3], entidade sem fins lucrativos responsável pelo desenvolvimento de políticas voltadas ao funcionamento e expansão da internet em todo o mundo[4].

Atualmente, as versões dos endereços de protocolo de internet utilizados são duas. A mais comum ainda é o IPv4, que utiliza endereços de 32 bits, limitando a sua atribuição para até 4.294.967.296 (2^{32}) endereços. O IPv4 utiliza quatro campos para definir o endereço IP (ex.: 225.109.4.98). A acelerada expansão da internet conduziu à necessidade de aumento dos números de protocolo de internet existentes, o que resultou na criação do IPv6, versão mais atual e com capacidade consideravelmente superior.

Cada vez que alguém se conecta à internet, o provedor de conexão atribui a ela um determinado endereço de IP. Normalmente, a cada conexão é atribuído um número de endereço distinto (endereço de IP dinâmico[5]), muito embora seja permitido aos provedores de internet atribuir endereços fixos aos seus usuários. Além disso, o normal é que cada endereço seja designado para apenas uma pessoa, permitindo o registro individualizado da sua atuação na internet.

Apesar de a designação de endereços IPs pela IANA ser individual para cada servidor, é possível que um determinado usuário se utilize de uma ferramenta chamada *Network Address Translation* (NAT), conhecida também como *masquerading,* em sua rede privada[6]. A título de exemplo, se alguém utiliza um roteador *wireless* em casa, muito embora esse roteador utilize um único endereço IP para se conectar à internet, ele distribui, para cada usuário doméstico, um número interno, conhecido como "IP privado" (ex.: 192.168.0.0/16). Esses números internos não são roteados na internet (e por isso, podem coincidir em casas diversas), mas apenas o número do endereço IP do roteador. Isso faz com que todos os usuários, ao final, se conectem à internet por um mesmo endereço IP público, embora por meio de portas lógicas distintas.

Situações assim dificultam a individualização de determinada conduta praticada na internet, para fins probatórios. Imagine-se um indivíduo que se conecta à rede *wireless* de um bar e pratica um delito por meio do seu celular. Como identificá-lo? Essa tarefa exige uma verificação mais acurada, a partir da análise dos registros de conexão que permanecem dentro do roteador (*logs*).

---

3. Saliba, Aziz Tuffi; Bahia, Amael Notini Moreira. A jurisdição da ICANN: desafios atuais e prospectivas futuras. *Revista de Direito Internacional*; 2019, Vol. 16, p. 335-345. Cf. [http://icann.org].
4. Mueller, Milton. Detaching Internet Governance from the State: Globalizing the IANA. *Georgetown Journal of International Affairs*, Vol. 15, 2014, p. 35-44.
5. EL KHOURY, Alessandro. Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat. *European Journal of Risk Regulation*, 2017, Vol. 8, p, 191-197.
6. Wing, Dan. Network Address Translation. *IEEE Internet Computing*. Jul/Aug 2010, Vol. 14, p. 66-70.

Por fim, é preciso esclarecer o conceito de nome de domínio (*domain name*). Cuida-se de uma forma de se conferir uma aparência mais compreensiva a um endereço IP. Toda vez que um usuário de internet digita em um navegador de internet (*internet browser*) um determinado endereço de registro (ex.: www.joaolordelo.com), esse endereço consiste num *domain name* que uma empresa de registros – chamada *Registrar* – alienou a alguém – chamado *Registrant*. Esses nomes de domínio facilitam a navegação pela internet e também se sujeitam ao controle da IANA. Cada vez que alguém adentra um *website,* o Sistema de Nomes de Domínio (*Domain Name System* – DNS) faz a associação entre o domínio e o respectivo endereço IP a ele atribuído, permitindo a conexão. Cada equipamento que hospeda um determinado *website* possui o seu endereço IP, que é alcançado pelo protocolo de conexão por meio do *domain name.*

2.2. Provedores de conexão à internet

Conforme disposto no art. 5º, V, do Marco Civil da Internet (Lei n. 12.965/2014), entende-se por conexão à internet "a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP". Os provedores de conexão, como o próprio nome sugere, são pessoas que prestam o serviço de habilitar os seus usuários ao acesso à internet. Quando algum consumidor paga uma determinada quantia para uma companhia habilitar o seu *smartphone*, possibilitando sua conexão à internet, essa companhia é um provedor de conexão.

Na forma do art. 13 da Lei n. 12.965/2014, na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. Essa responsabilidade não poderá ser transferida a terceiros (§ 1º).

Os registros de conexão conservam dados como o endereço IP atribuído ao usuário, a data e o horário da conexão, a duração da designação e o número da conta do usuário. O descumprimento das regras relativas à conservação desses dados poderá sujeitar o provedor a sanções que variam desde a advertência até a proibição de exercício de atividades (art. 12, I a IV).

É importante notar que, em respeito à intimidade e à privacidade dos usuários, aos provedores de conexão é vedado guardar os registros de acesso a aplicações de internet – a exemplo do acesso a um determinado *website* ou rede social –, devendo se limitar aos dados de conexão (art. 14). Em outras palavras, os provedores de conexão não podem monitorar, muito menos registrar informações relativas aos *websites* e aplicativos acessados pelos seus usuários.

2.3. Provedores de aplicações de internet

A Lei n. 12.965/2014 conceitua as aplicações de internet de forma ampla, compreendidas como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet" (art. 5º, VII). Após uma determinada pessoa se conectar à internet, o caminho natural consiste no acesso a determinadas aplicações, a exemplo de *websites*, redes sociais (*Twitter, Instagram, Facebook* etc.), ferramentas de comunicação instantânea (*Whatsapp, Telegram, Skype, Hangouts* etc.), caixas de mensagens de e-mail (*Hotmail, Gmail, Yahoo* etc.), buscadores (*Google, Yahoo, Bing* etc.), entre outras. Todas essas aplicações são mantidas por provedores específicos (ex.: o Google é o provedor da aplicação Gmail), que se ocupa de ofertar funcionalidades ao acesso à internet.

Vê-se, assim, que os provedores de aplicação, ao contrário dos provedores de conexão, não se ocupam do serviço de habilitação de um usuário para o acesso à internet, mas sim de ofertar funcionalidades variadas, gratuitas ou onerosas, que imprimem maior utilidade à rede mundial de computadores.

Na forma do art. 15 da Lei n. 12.965/2014, 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. Em termos mais simples, se alguém acessa o seu e-mail particular mantido pelo provedor Google (Gmail) em um determinado dia, num determinado horário, esse provedor possui a obrigação de guardar os dados desse acesso (endereço IP, data, horário e dados cadastrais) por pelo menos 6 (seis) meses. Igualmente, se alguém publica algo na rede social *Twitter,* os dados relativos a essa publicação devem permanecer guardados.

2.4. Servidores *proxy,* VPN e rede *TOR*

O uso de *proxies* e VPNs tem sido cada vez mais frequente por pessoas que buscam maior privacidade na internet mediante a ocultação do endereço IP. Até mesmo usuários comuns têm utilizado tais ferramentas, cuja compreensão é também necessária para fins de coleta de evidências digitais[7].

Um *proxy* consiste em um servidor que atua como intermediário – um verdadeiro "representante" – de um determinado usuário de internet, emprestando-lhe o seu endereço IP. A título de exemplo, um usuário brasileiro conectado à internet por meio do endereço IP 200.200.200.1 pode se utilizar de um servidor de *proxy* chinês com endereço IP diverso para acessar variadas aplicações na internet. Em tal caso, ao solicitar o acesso a um provedor de aplicação como uma rede social (*Twitter, Facebook,*

7. Morris, Antonio. How to surf privately (& watch 0/S TV). *APC (Bauer Media Group)*, Jun. 2010, Vol. 30, p. 84-84.

Civil Procedure Review, v. 11, n. 3: set.-dez. 2020.
ISSN 2191-1339 – www.civilprocedurereview.com

Instagram etc.), o usuário enviará esse pedido ao servidor *proxy,* conectando-se a ele. O *proxy,* por seu turno, fará a conexão com a rede social. Consequentemente, o tráfego de dados com o endereço IP da rede social será feito por um IP diverso (o endereço distribuído a um servidor *proxy* chinês), que encaminhará esses dados ao usuário brasileiro.

Em razão disso, no exemplo citado, os dados de conexão armazenados pelo provedor de aplicação não serão aqueles do usuário brasileiro, mas sim do servidor *proxy.* Assim, a identificação do usuário dependerá de uma prévia investigação a respeito do serviço de *proxy* oferecido, pode ser feito por meio do banco de dados existente em locais como a empresa *Domains by proxy8,* ou por medidas de cooperação internacional voltadas à coleta dos dados de conexão do servidor *proxy* estrangeiro.

De forma similar, uma *virtual private network* (VPN) também permite a ocultação do endereço IP de um determinado usuário, mas com algumas diferenças relevantes. De início, as VPNs conseguem redirecionar todo o tráfego de um terminal[9] – um computador, um *smartphone* etc. Um *proxy,* por outro lado, é utilizado em um aplicativo que permita conexão com a internet, a exemplo de um navegador ou mesmo um jogo, não sendo possível configurar todas as conexões de um computador ou roteador. Além disso, as VPNs submetem o tráfego de dados a um processo de criptografia, que pode ser traduzido como uma espécie de "envelopamento das informações e seu tráfego por um túnel totalmente seguro que interliga seu computador a uma rede remota"[10]. Por consequência desse procedimento, as VPNs costumam reduzir bastante a velocidade da navegação do usuário[11].

Por fim, o *The Onion Router* (TOR) consiste em uma aplicação de internet que oculta a identidade do seu usuário, através não apenas da criptografia dos dados de tráfego, mas também pelo seu direcionamento por variados servidores operados por voluntários. Há aqui uma sobreposição de servidores que repassam os dados, o que gera uma espécie de "criptografia multicamadas".

Apesar da complexidade dessas ferramentas, é possível a obtenção de dados de conexão de usuários que se utilizam de *proxy,* VPN ou TOR[12], o que demanda atuações

8. Cf. [https://www.domainsbyproxy.com/AboutUs.aspx].
9. Brandt, Andrew. Easy VPNs Secure Wi-Fi at Home and on the Road. *PCWorld*. Abr. 2005, Vol. 23, p. 40-40.
10. Cf. [https://canaltech.com.br/seguranca/afinal-de-contas-qual-a-diferenca-entre-proxy-e-vpn-62225/].
11. Bandler, John. Network Cybersecurity in Your Home and Office. *GPSolo*, Mar/abr. 2018, Vol. 35, p. 52-55.
12. Chakravarty, Sambuddho; Portokalidis, Georgios; Polychronakis, Michalis; Keromytis, Angelos. Detection and analysis of eavesdropping in anonymous communication networks. *International Journal of Information Security*, Jun. 2015, Vol. 14, p. 205-220.

de órgãos especializados em combate a crimes cibernéticos (FBI, Ministério Público, Polícia Federal etc.).

3. O REGIME PROCESSUAL ESTABELECIDO PELO MARCO CIVIL DA INTERNET (LEI N. 12.965/2014)

Como expressamente anunciado em seu art. 1º, o Marco Civil da Internet (Lei n. 12.965/2014) tem por objetivo estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, além de determinar as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Entre os princípios elencados no art. 3º do diploma legal, destacam-se, para fins probatórios, a "proteção da privacidade" (inciso II) e a "proteção dos dados pessoais" (inciso III). Em decorrência desses dois princípios, o art. 7º estabelece, entre outros direitos dos usuários, a "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei" (inciso II), a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (inciso III), bem como o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;" (inciso VII).

Em reforço à disciplina estabelecida em seus dispositivos inaugurais, o art. 22 assegura genericamente à "parte interessada", com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, a possibilidade de requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet[13].

Para tanto, o seu parágrafo único estabelece três requisitos, sob pena de inadmissibilidade do requerimento: a) fundados indícios da ocorrência do ilícito; b) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e c) período ao qual se referem os registros.

É importante atentar, porém, a duas sutilezas.

A primeira delas consiste na compreensão de que o requerimento a que alude o art. 22 da Lei n. 12.965/2014 pode assumir duas naturezas bastantes distintas.

De um lado, é possível que ele se resuma a um pedido de quebra de dados informáticos ou telemáticos já armazenados em provedores de conexão, a exemplo um requerimento voltado ao conhecimento do endereço IP, dia e hora que um determinado usuário acessou a internet ou usou determinado aplicativo.

13. Nesse sentido, já decidiu o Superior Tribunal de Justiça: "O Marco Civil da Internet afirma a obrigatoriedade de ordem judicial para que os provedores de acesso e de aplicação apresentem dados considerados pessoais e sigilosos a interessados. Trata-se de a proteção necessária e esperada à privacidade e à intimidade dos usuários de aplicações da internet" (REsp 1782212/SP, Terceira Turma, Relatora: Min. Nancy Andrighi, DJe 7.11.2019).

Civil Procedure Review, v. 11, n. 3: set.-dez. 2020.
ISSN 2191-1339 – www.civilprocedurereview.com

De outro lado, é possível que o pedido consista na interceptação do fluxo de dados, mediante o monitoramento do fluxo de dados de conexão ou de acesso de um determinado usuário, caso em que são atraídos os requisitos adicionais relativos à interceptação de comunicações telefônicas, por força do que dispõe o art. 1º, parágrafo único, da Lei n. 9.296/1996, que regulamenta o inciso XII, parte final, do art. 5° da Constituição da República. Conforme estabelece o aludido diploma, essa medida somente pode ser determinada para fins de investigação de infração de natureza criminal punida com reclusão.

Outra diferença, conforme precedente do Superior Tribunal de Justiça, reside no requisito da indicação, no requerimento, do "período ao qual se referem os registros" (art. 22, parágrafo único, III). No julgamento do RHC n. 117.680/PR, o tribunal compreendeu que essa exigência somente se faz para a interceptação de fluxos de dados requisitados a provedores de aplicações de internet[14]. Isso se deve ao acentuado caráter interventivo, na medida em que a interceptação do fluxo de dados – a exemplo do acesso contínuo à caixa de e-mail ou das conversas em um determinado aplicativo de *chat* – não diz respeito a dados estáticos, interferindo diretamente na liberdade de comunicação em si, a merecer limitação temporal.

No particular, entende-se que o aludido precedente, embora com a melhor das intenções, chegou a uma conclusão equivocada. Em realidade, a partir das premissas elencadas, o resultado deveria ser o inverso: a necessidade de indicação de um lapso temporal preciso para o acesso a dados estáticos, algo que, para a interceptação do fluxo de dados, parece ilógico, na medida em que o objetivo da interceptação consiste na obtenção de informações *futuras* relativas a ilícitos penais.

De um lado, não é razoável permitir-se o acesso ilimitado a todos os dados telemáticos ou informáticos estáticos relativos a um determinado usuário, sob pena de exposição de dados temporalmente muito distantes dos fatos cuja comprovação se busca. De outro lado, na interceptação do fluxo de dados, é suficiente o estabelecimento de um lapso temporal para fins de análise da necessidade de prorrogações, tal como ocorre na disciplina que a Lei n. 9.296/1996 estabeleceu para a interceptação telefônica.

Há ainda uma segunda sutileza.

Embora o Marco Civil da Internet discipline a guarda e a exibição de dados de conexão – no caso dos provedores de conexão (art. 13, § 5º) – e de acesso – no caso dos provedores de aplicações de internet (art. 15, § 1º) –, existem outros dados igualmente relevantes, que podem ser fornecidos especialmente pelos provedores de aplicações de internet.

Cuida-se de dados que, embora também possam ser compreendidos, genericamente, como dados telemáticos – no caso de aplicação para *smartphone* –

14. RHC 11780/PR, Sexta Turma, Relator: Min. Nefi Cordeiro, DJe 14.2.2020.

ou informáticos – se utilizado outro tipo de terminal –, não dizem respeito apenas à conexão à internet ou acesso a uma determinada aplicação.

Curiosamente, o Marco Civil da Internet não parece se preocupar com essas informações, concentrando-se a Lei n. 12.965/2014 em disciplinar dados pessoais relativos à conexão à internet – a exemplo do endereço IP, data e hora do acesso, além da porta lógica, no caso do uso de ferramenta NAT[15] – e de acesso às aplicações – notadamente endereço IP, data, hora e duração do acesso. O que dizer de dados como as informações cadastrais em uma determinada rede social ou até mesmo o conteúdo de mensagens privadas de *chat* ou de e-mail? Certamente, não se trata de dados de conexão ou de acesso, mas são igualmente relevantes para fins probatórios.

No que diz respeito aos dados cadastrais, a lei confere uma proteção menor ao seu acesso, sendo permitida, por exemplo, a requisição direta por membros do Ministério Público ou por autoridades policiais, desde que limitados a informações referentes à qualificação pessoal, filiação e o endereço do usuário (art. 10-A, § 1º, II, c/c arts. 15 a 17 da Lei n. 12.850/2013). No caso de particulares ou outros órgãos públicos, a requisição desses dados dependerá de prévia autorização judicial.

Por seu turno, o acesso ao conteúdo de documentos e conversas armazenados em aplicativos – a exemplo de mensagens de e-mail, mensagens de aplicativos de comunicação instantânea, documentos e conteúdos armazenados na nuvem, dados de localização, dados relativos à utilização de aplicações de serviços de transporte (*Uber*, 99POP etc.), entre outros – deve sempre ser objeto de requerimento judicial prévio, da mesma forma que ocorre com documentos físicos ou correspondências obtidos por meio de busca e apreensão. E mais: na hipótese de interceptação do fluxo desses dados, ou seja, quando o que se deseja é o acesso simultâneo aos dados produzidos, será aplicado o regime das interceptações telefônicas (art. 1º, parágrafo único, da Lei n. 9.296/1996).

4. METODOLOGIA BÁSICA PARA A PRODUÇÃO DA PROVA DIGITAL

Um questionamento comum, frequentemente formulado por profissionais não especializados em evidências digitais, consiste em saber a forma de identificação de usuários a partir de um acesso a uma aplicação. Imagine-se que um determinado usuário anônimo de uma rede social publique uma mensagem ofensiva a alguém. Para

15. Segundo precedente do Superior Tribunal de Justiça, "Pelo cotejamento dos diversos dispositivos do Marco Civil da Internet mencionados acima, em especial o art. 10, caput e § 1º, percebe-se que é inegável a existência do dever de guarda e fornecimento das informações relacionadas à porta lógica de origem. 9. Apenas com a porta lógica de origem é possível fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela. Portanto, sua guarda é fundamental para a preservação de possíveis interesses legítimos a serem protegidos em lides judiciais ou em investigações criminais" (REsp 1777769/SP, Terceira Turma, Relatora: Min. Nancy Andrighi, Dje 8.11.2019).

Civil Procedure Review, v. 11, n. 3: set.-dez. 2020.
ISSN 2191-1339 – www.civilprocedurereview.com

além da comprovação da existência da mensagem, como identificar esse usuário? De igual modo, como proceder no caso de a prova de um determinado fato consistir em uma mensagem de e-mail enviada por um usuário?

Firmadas as premissas anteriores, é importante saber, em termos pragmáticos, a forma de postulação de acesso aos dados pessoais e aos documentos eletrônicos.

Em processos cíveis, o procedimento adotado será o da produção antecipada de provas, que, na disciplina do novo Código de Processo Civil, poderá ser proposta mesmo sem razões cautelares, bastando que o "prévio conhecimento dos fatos possa justificar ou evitar o ajuizamento de ação" (art. 381, III, do CPC).

Se o que se objetiva é a *identificação* de usuários responsáveis por determinada conduta praticada por intermédio de provedores de aplicações de internet – a exemplo do envio de mensagem de e-mail, publicações de imagens, mensagens em redes sociais, áudios, páginas etc. –, o primeiro passo consiste em saber o endereço IP que foi utilizado para a concretização dessa conduta. Isso porque, como já referido, o tráfego de dados entre um determinado usuário e um provedor de aplicações ocorre por intermédio de um endereço IP que lhe foi distribuído por um provedor de conexão à internet.

Assim, nesse caso, a postulação deve seguir o seguinte roteiro: a) requerimento de quebra do sigilo de dados informáticos, de modo que o provedor de aplicações (*Twitter*, *Facebook, Google* etc.) exiba o endereço IP utilizado para a publicação de determinada mensagem, informando-se as suas circunstâncias (usuário, dia e hora); b) requerimento de quebra de sigilo de dados pessoais, para que esse mesmo provedor de aplicações forneça as informações utilizadas pelo usuário para abrir a sua conta. No caso de mensagens de e-mail, o destinatário da mensagem, ao recebê-la, já é informado também sobre o endereço IP do usuário que a enviou, tornando-se desnecessário o primeiro requerimento.

Com frequência, os dados pessoais informados por ocasião do cadastro (nome, endereço etc.) são falsos. Nesse caso, será necessário passar para um segundo passo, consistente na identificação do provedor de conexão a partir do endereço IP informado pelo provedor de aplicações. Essa identificação não é difícil, na medida em que cada endereço é distribuído pela *Internet Assigned Numbers Authority* (IANA). Para tanto, basta inserir o número do endereço IP em uma ferramenta *Whois*[16], o que pode ser feito pelo próprio requerente.

Existem diversos *websites* que permitem o acesso gratuito ao *Whois*, a exemplo daqueles que podem ser acessados pelos endereços http://registro.br (para endereços nacionais) e http://www.whois.net. Outros são pagos, ofertando informações mais

16. Elliott, Kathryn. The Who, What, Where, When, and Why of WHOIS: Privacy and Accuracy Concerns of the WHOIS Database. *SMU Science and Technology Law Review*, Vol. 12, 2009, p. 141-172. Cf. também Sobek, Jeffrey Stephen. Balancing Individual Privacy Rights and the Rights of Trademark Owners in Access to the WHOIS. *John Marshall Law Review*, Vol. 38, 2004, p. 357-380.

detalhadas. O *Whois* informa, entre outros, os seguintes dados, que são relevantes para a identificação do usuário: a) o local do endereço IP (país, geralmente); b) *Host name*; c) *Whois server* (mantenedor do IP); d) *IP range* (bloco de números IP que o provedor de conexão possui) etc.[17]

Identificado o provedor de conexão (Claro, Vivo, Velox, NET etc.), o terceiro passo consistirá no requerimento de quebra de sigilo de dados, possibilitando-se o acesso às informações cadastrais do usuário junto a essas empresas. Esse último passo dispensará a mediação judicial, na hipótese de o requerente ser o Ministério Público ou autoridade policial, por força do que dispõe a Lei n. 12.850/2013 (art. 10-A, § 1º, II, c/c arts. 15 a 17). Ainda que essas informações sejam falsas, é possível identificá-lo por metodologias empregadas a partir dos dados relativos à forma de pagamento do serviço.

Por outro lado, se o que se quer é a *obtenção de um documento virtual* – a exemplo do acesso à caixa de e-mail de um determinado usuário em um período específico, o acesso aos documentos armazenados em uma conta na "nuvem", o histórico de buscas de um determinado buscador, o histórico de localização ou de uso de aplicações de transporte, entre outros –, o prévio conhecimento do endereço IP do usuário pode ser desnecessário. Para tanto, será suficiente a indicação de informações como o endereço de e-mail, nome ou número de identificação do perfil nas redes sociais.

5. BUSCA E APREENSÃO VIRTUAL *X* INTERCEPTAÇÃO DE FLUXO DE DADOS: DISTINÇÕES NECESSÁRIAS

No clássico precedente formado por ocasião do julgamento do RE 418416/SC, o Supremo Tribunal Federal consolidou o entendimento no sentido de que "a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador"[18]. Naquela oportunidade, foi feita uma clara distinção entre a obtenção de dados informáticos "estáticos" – ex.: mensagens de e-mail e documentos armazenados em um dispositivo – e a comunicação ("fluxo") de dados.

No primeiro caso, os dados já existem e estão armazenados em algum local, que pode ser um terminal do usuário (*smartphone,* computador etc.) ou um servidor (caixa de e-mail, *iCloud, Google Drive* etc.). O que temos aqui são dados estáticos que podem ser objeto de um pedido judicial de busca e apreensão "física" – no caso de celulares, computadores etc. – ou busca e apreensão "virtual" (quebra de sigilo telemático/informático).

17. Aaron, Tara M. Availability of WHOIS Information after the GDPR - Is It Time to Panic. *The Trademark Reporter*, Vol. 108, 2018, p. 1.129-1.142.
18. RE 418416/SC, Tribunal Pleno, Relator: Min. Sepúlveda Pertence, j. 10.5.2006. cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270.

Civil Procedure Review, v. 11, n. 3: set.-dez. 2020.
ISSN 2191-1339 – www.civilprocedurereview.com

Situação diversa consiste na interceptação de fluxos de dados, medida que, por força do art. 5º, XII, da Constituição da República, regulamentado pelo art. 1º, parágrafo único, da Lei n. 9.296/1996, somente pode ser judicialmente deferida para fins de investigação criminal ou instrução processual relativa a crime punido com reclusão. Assim, não é possível formular, em processos de natureza cível, pedidos de interceptação de mensagens em aplicativos de *chat* ou de e-mail, nem mesmo o acesso à senha do usuário em aplicativos dessa natureza, o que permitiria o monitoramento da comunicação.

É permito, porém, o empréstimo de prova produzida por meio de interceptação do fluxo de dados, em processo ou investigação criminal, para processos cíveis e até mesmo processos administrativos, conforme a jurisprudência do Supremo Tribunal Federal[19] e do Superior Tribunal de Justiça[20].

6. BUSCA E APREENSÃO DE DISPOSITIVOS INFORMÁTICOS OU TELEMÁTICOS, CADEIA DE CUSTÓDIA DA PROVA, PERÍCIA E *HASHING*

Em processos cíveis ou criminais, é comum a formulação de pedidos de busca e apreensão de dispositivos informáticos (computadores, *laptops* etc.) ou telemáticos (*smartphones*) para fins de obtenção de provas.

Questão relevante consiste em saber se, apreendido o dispositivo, seria necessária a formulação de novo pedido, voltado à extração do conteúdo já armazenado. Quanto a isso, a jurisprudência do Superior Tribunal de Justiça é sólida no sentido de que, se ocorreu a busca e apreensão da base física dos aparelhos de telefone celular, ante a relevância para as investigações, "não há óbice para se adentrar ao seu conteúdo já armazenado, porquanto necessário ao deslinde do feito, sendo prescindível nova autorização judicial para análise e utilização dos dados neles armazenados"[21].

Por outro lado, o STJ considera ilícito o acesso aos dados do celular extraídos do aparelho celular apreendido em flagrante delito, "quando ausente de ordem judicial para tanto, ao entendimento de que, no acesso aos dados do aparelho, se tem a devassa de dados particulares, com violação à intimidade do agente".[22]

Apreendido o dispositivo mediante ordem judicial, a atividade pericial exige cuidados relativos à *cadeia de custódia* da prova, assim compreendido "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte" (art. 158-A do CPP).

19. RMS 36434 AgR/DF, Primeira Turma, Relator: Min. Alexandre de Moraes, DJe 11.10.2019; RMS 30295 AgR/DF, Primeira Turma, Relatora: Min. Rosa Weber, Dje 12.2.2019.
20. MS 24031/DF, Primeira Seção, Relatora: Ministra Regina Helena da Costa, DJe 16.10.2019.
21. HC 372.762/MG, Quinta Turma, Relator: Ministro Felix Fischer, DJe 16.10.2017.
22. AgRg no HC 542940/SP, Sexta Turma, Relator: Nefi Cordeiro, DJe 10.3.2020.

Um método valioso para a sua preservação consiste no uso de ferramentas de *hashing.* Cuida-se de operação realizada por meio de aplicativo que cria um código único (*hash*) para quaisquer dados que sejam nele inseridos, tornando-se extremamente relevante para fins de preservação da integridade de uma evidência digital coletada. A título de exemplo, ao se utilizar o aplicativo de *hashing* no conteúdo de um disco rígido (HD) externo ou no conteúdo armazenado por um aparelho celular, será gerado um número de *hash* único. Se um único arquivo daquela base de dados for modificado, o número *hash* será diverso. Assim, qualquer alteração no conteúdo poderá ser identificada pela comparação entre o número *hash* inicial e o número após a suposta alteração, tornando-se inservível a prova[23].

7. PEDIDOS DE PRESERVAÇÃO DE CONTEÚDO

O Marco Civil da Internet (Lei n. 12.965/2014) também disciplina um instrumento bastante utilizado na experiência estrangeira, consistente nas requisições de preservação de conteúdo. A sua relevância decorre não apenas da limitação temporal que a legislação estabelece para a guarda dos dados de conexão e acesso, mas, sobretudo, da facilidade com que os usuários de aplicações de Internet podem excluir o registro de dados, especialmente após a edição da Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709/2018).

Na forma do art. 13, § 2º, e art. 15, § 2º, do Marco Civil da Internet, a autoridade policial ou administrativa ou o Ministério Público poderão "requerer" cautelarmente que os registros de conexão ou os registros de acesso a aplicações de Internet sejam guardados por prazo superior ao previsto na lei (um ano, para os registros de conexão; seis meses, para os de acesso a aplicações).

Apesar da literalidade do texto legal, compreendemos que a regra em questão não trata propriamente de um *requerimento*, mas sim de uma verdadeira *requisição*, com conteúdo de ordem direta aos provedores de conexão e de aplicação, como a experiência estrangeira ensina. Isso porque, à luz do que dispõem o art. 13, § 3º, e o art. 15, § 2º, a autoridade "requerente" terá o prazo de 60 (sessenta) dias, contados a partir do "requerimento", para ingressar com o pedido de autorização judicial de acesso aos registros previstos no *caput*. Se acaso fosse necessária a prévia autorização judicial para a mera preservação de dados, essa ferramenta careceria de utilidade, na medida em que o lapso temporal entre o requerimento e o deferimento judicial a tornaria inócua. Além disso, bastaria o requerimento judicial de acesso imediato aos dados, não havendo utilidade em primeiramente se pedir judicialmente a sua preservação.

23. Truong, Tri. Hashing in the Cloud: The Private Search Defense Is Active and Potent. *MU Law Review*, Vol. 72, p. 343-350; Branham, Rebekah. Hash it out: fourth amendment protection of electronically stored child exploitation. *Akron Law Review*, 2019, Vol. 53, p. 217-244.

Civil Procedure Review, v. 11, n. 3: set.-dez. 2020.
ISSN 2191-1339 – www.civilprocedurereview.com

Em atenção à disciplina legal, diversos provedores de aplicações de Internet já estabeleceram ferramentas automatizadas de preservação de conteúdo, acessíveis em *websites* específicos. É o caso do *Facebook,* rede social que desenvolveu uma plataforma específica, denominada *Facebook Records* (https://www.facebook.com/records/login/), destinada a "solicitações online para autoridades de aplicação da lei".

Embora a *preservação* do conteúdo seja alcançada extrajudicialmente, o seu *acesso* depende de prévia autorização judicial. Excepcionalmente, a experiência revela que os provedores de aplicações de Internet disponibilizam diretamente dados de acesso e até mesmo conteúdos privados, em hipóteses como as de flagrantes de crimes ou de indícios de planejamento de suicídios de usuários.

8. CONCLUSÃO

O regime jurídico da produção de provas digitais ainda é pouco conhecido pelos profissionais do Direito, sendo raras as produções acadêmicas sobre esse tema no Brasil.

Analisando-se o exposto, foi possível perceber que essa disciplina demanda uma prévia compreensão concernente a conceitos fundamentais, relativos ao funcionamento das tecnologias de conexão à Internet e acesso às aplicações disponíveis. Essa compreensão envolve os conceitos disciplinados pelo Marco Civil da Internet (Lei n. 12.965/2014), a exemplo do endereço de protocolo de Internet (endereço IP), provedores de conexão e de acesso a aplicações de Internet, além de outros, como os de *domain name,* DNS, *hashing,* VTN, *proxy* etc.

Firmadas tais premissas, o regime geral de produção de provas digitais foi descrito por meio da análise da mencionada lei, que estabelece obrigações específicas para os provedores, além de prever a necessidade de prévia autorização judicial para a coleta dos dados de conexão e de acesso por eles armazenados.

A análise desse regime permitiu a construção de uma proposta metodológica básica de identificação de usuários a partir do exame dos dados de conexão e de acesso, possibilitando ainda a realização de distinções processuais relevantes, em especial entre as medidas de busca e apreensão virtual (quebra de sigilo de dados) e de interceptação de fluxo de dados.

REFERÊNCIAS

AARON, Tara M. Availability of WHOIS Information after the GDPR - Is It Time to Panic. *The Trademark Reporter*, Vol. 108, 2018, p. 1.129-1.142.

BANDLER, John. Network Cybersecurity in Your Home and Office. *GPSolo*, Mar/Apr 2018, Vol. 35, p. 52-55.

BORGESIUS, Frederik Zuiderveen. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. *European Data Protection Law Review (EDPL)*, 2017, Vol. 3, p. 130-137.

BRANDT, Andrew. Easy VPNs Secure Wi-Fi at Home and on the Road. *PCWorld*. Apr2005, Vol. 23, p. 40-40.

BRANHAM, Rebekah. Hash it out: fourth amendment protection of electronically stored child exploitation. *Akron Law Review*, 2019, Vol. 53, p. 217-244.

CHAKRAVARTY, Sambuddho; Portokalidis, Georgios; Polychronakis, Michalis; Keromytis, Angelos. Detection and analysis of eavesdropping in anonymous communication networks. *International Journal of Information Security*, Jun. 2015, Vol. 14, p. 205-220.

EL KHOURY, Alessandro. Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat. *European Journal of Risk Regulation*, 2017, Vol. 8, p, 191-197.

ELLIOTT, Kathryn. The Who, What, Where, When, and Why of WHOIS: Privacy and Accuracy Concerns of the WHOIS Database. *SMU Science and Technology Law Review*, Vol. 12, 2009, p. 141-172.

HARGREAVES, Stuart; LOKMAN, Tsui. IP Addresses as Personal Data Under Hong Kong's Privacy Law: An Introduction to the Access My Info HK Project. *Journal of Law, Information & Science*, 2017, Vol. 25, p. 68-83.

MCGILLIVRAY, Kevin. Give it away now? Renewal of the IANA functions contract and its role in internet governance. *International Journal of Law & Information Technology*. Spring 2014, Vol. 22, p. 3-26.

MORRIS, Antonio. How to surf privately (& watch 0/S TV). *APC (Bauer Media Group)*, Jun. 2010, Vol. 30, p. 84-84.

MUELLER, Milton. Detaching Internet Governance from the State: Globalizing the IANA. *Georgetown Journal of International Affairs*, Vol. 15, 2014, p. 35-44.

SALIBA, Aziz Tuffi; Bahia, Amael Notini Moreira. A jurisdição da ICANN: desafios atuais e prospectivas futuras. *Revista de Direito Internacional*; 2019, Vol. 16, p. 335-345.

SOBEK, Jeffrey Stephen. Balancing Individual Privacy Rights and the Rights of Trademark Owners in Access to the WHOIS. *John Marshall Law Review*, Vol. 38, 2004, p. 357-380.

TRUONG, Tri. Hashing in the Cloud: The Private Search Defense Is Active and Potent. *MU Law Review*, Vol. 72, p. 343-350.

WING, Dan. Network Address Translation. *IEEE Internet Computing*. Jul/Aug 2010, Vol. 14, p. 66-70.