Validade jurídica das provas digitais no processo administrativo disciplinar

Gustavo Henrique de Vasconcellos Cavalcanti

RESUMO

Este artigo busca explorar a validade da utilização de dados e documentos digitais, notadamente os obtidos em fontes abertas, como meio de prova na seara administrativo-disciplinar, bem como os requisitos necessários para a sua admissibilidade jurídica em processos administrativos disciplinares. Conclui-se que os documentos eletrônicos podem ser utilizados como prova no processo administrativo disciplinar, desde que assegurada a autenticidade, integridade e fé pública do conteúdo.

Palavras-chave: Processo Administrativo Disciplinar. Provas digitais. Inteligência em fontes abertas – OSINT (*Open Source Intelligence*).

Introdução

Uma das inovações mais marcantes da Terceira Revolução Industrial foi o advento da *Internet*. Consequência direta do crescimento, desenvolvimento e expansão das modernas tecnologias de telecomunicações, a rede mundial de computadores alterou profundamente a atividade humana e, por consequência, os paradigmas vigentes até então.

O Direito, como dimensão da atividade humana, não se quedou inerte a essas mudanças. Na medida em que as relações humanas passaram a se dar também por meios digitais como celulares, *tablets* e redes sociais, as relações jurídicas igualmente foram transformadas. O meio digital passou a ser o principal suporte para documentar as obrigações e responsabilidades entre as partes, mudança essa que trouxe consigo, naturalmente, inovações e desafios ao Direito, a exemplo da utilização de processos eletrônicos, discussões sobre a privacidade na rede e a apuração de crimes cibernéticos. Por outro lado, se é inconcebível cogitarmos viver em um mundo sem Internet, tampouco podemos admitir que esse novo "mundo digital" fira direitos e garantias individuais conquistadas arduamente ao longo de séculos de evolução jurídica.

Esse artigo busca explorar a validade da utilização de dados e documentos digitais, notadamente os obtidos em fontes abertas, como meio de prova na seara administrativo-disciplinar, bem como os requisitos necessários para a sua admissibilidade jurídica em processos administrativos disciplinares.

Conceito de prova digital

Antes de iniciarmos as discussões sobre a validade jurídica das provas digitais no processo administrativo disciplinar, cumpre definir o que chamamos de *prova digital*, ou *prova eletrônica*.

Sem a pretensão de se abordar com profundidade o tema sobre a Teoria Geral da Prova, podemos definir a prova como *um elemento capaz de dar ciência de um fato a alguém* (NETO, JESUS e MELO, 2014, p. 416).

Conforme explicado pelos autores, por mais simplista que seja essa definição, há que se admitir a sua completude quanto à descrição do que seja prova: ao se dizer que (a) a prova é um *elemento*, admite-se que qualquer meio, desde que lícito, moral e idôneo, pode servir de prova; b) esse elemento é capaz de dar *ciência*, temos que a prova tem por objetivo levar o conhecimento de um determinado fato a um destinatário, visando convence-lo de sua veracidade; c) tal elemento tem por objetivo dar ciência de um *fato*, eis que o objeto da prova são determinados fatos ocorridos, a respeito dos quais se torna necessário convencer alguém de sua existência.

O adjunto adnominal *digital*, por sua vez, destina-se a qualificar a natureza da prova, de modo a referir-se àquelas provas dispostas em uma sequência de bits e consignada em uma base física eletrônica. Uma *prova digital*, portanto, é um elemento digital/eletrônico capaz de dar ciência de um fato a alguém.

Tipos de prova digital

A despeito de não haver consenso na doutrina quanto às classificações das provas, é comum categoriza-las quanto ao seu objeto e sujeito.

Como bem esclarece LESSA (2009), citando a doutrina de Montenegro Filho, no tocante ao objeto, as provas podem ser diretas, quando levam por si só ao fato concreto (a exemplo de depoimentos de testemunhas e das partes, documentos e prova pericial) sem necessidade de elementos de associação, ou indiretas, quando precisam ser complementadas com elementos indutivos para a demonstração do *factum probandum* (a exemplo de indícios e presunções legais).

Quanto ao sujeito, as provas podem ser pessoais, quando extraídas do depoimento pessoal das partes ou da oitiva de testemunhas, ou reais, quando originadas em um documento.

Os arquivos eletrônicos (ou digitais), por sua própria natureza, consistem em registros gravados em uma base física eletrônica, como um servidor, telefone celular, *HD* ou *pen drive*, e são produzidos por uma gama de instrumentos bastante variada.

Dentre os tipos de prova digital mais comuns, podemos citar os arquivos de texto, áudios, fotografias digitais, planilhas eletrônicas, imagens em qualquer formato, vídeos, depoimentos por videoconferência, etc. Esses arquivos eletrônicos, sejam públicos ou particulares, podem ser considerados para fins de direito como *documentos digitais (ou eletrônicos)*, e possuem a natureza de prova documental a que se refere o art. 212, inciso II do Código Civil[1].

A Prova eletrônica no Processo Administrativo Disciplinar

O Direito Administrativo Disciplinar é balizado, dentre outros, pelo princípio da verdade real, ou verdade material. Isso implica que a Administração tem o poder-dever de empreender as diligências necessárias e razoáveis à elucidação dos fatos tais como eles ocorreram, não se admitindo somente a versão dos fatos narrada pelos envolvidos ("verdade sabida"). Como bem coloca o Manual de Processo Administrativo Disciplinar da Controladoria-Geral da União (2017):

> *A prova visa à reconstrução dos atos e fatos que estejam compreendidos no objeto do processo. Busca-se, com ela, determinar a verdade, estabelecendo, na medida do possível, o que aconteceu e como aconteceu, em determinado tempo e lugar, fundamentando a convicção dos destinatários da prova.*

A prova no processo administrativo disciplinar não é destinada à formação da convicção do juiz, como no processo judicial, mas sim à comissão e, posteriormente, à autoridade julgadora. Para ambas, no entanto, a valoração probatória precisa estar demonstrada de maneira clara e fundamentada, já que em matéria disciplinar, ao menos em âmbito federal, a prova possui caráter decisivo, conforme se depreende do art. 168 da Lei n.º 8.112/90:

---

[1] *"Art. 212. Salvo o negócio a que se impõe forma especial, o fato jurídico pode ser provado mediante: I – confissão; **II – documento**; III – testemunha; IV – presunção; V – perícia".*

> *Art. 168. O julgamento acatará o relatório da comissão, salvo quando contrário às provas dos autos.*
>
> *Parágrafo único. Quando o relatório da comissão contrariar as provas dos autos, a autoridade julgadora poderá, motivadamente, agravar a penalidade proposta, abrandá-la ou isentar o servidor de responsabilidade. (BRASIL, 1990)*

Na seara administrativo-disciplinar, a Lei n.º 8.112/90 não traz distinções ou restrições quanto à natureza da prova. A Lei n.º 9.784/99, que regula de maneira genérica o processo administrativo na órbita federal, tampouco faz qualquer exigência a respeito, determinando somente que os atos devem adotar *formas simples, suficientes para propiciar adequado grau de certeza, segurança e respeito aos direitos dos administrados* (art. 2º, parágrafo único, inciso IX), critério este reforçado no art. 22 do mesmo diploma, que determina que *os atos do processo não dependem de forma determinada senão quando a lei expressamente o exigir (BRASIL, 1999)*.

Diante da lacuna normativa, cabe analisar o que dizem o Código Civil (Lei n.º 10.406/2002) e o Novo Código de Processo Civil (Lei n.º 13.105/15), uma vez que o artigo 15 do NCPC determina que *na ausência de normas que regulem processos eleitorais, trabalhistas ou administrativos, as disposições deste Código lhes serão aplicadas supletiva e subsidiariamente (BRASIL, 2015)*.

Pois bem. O Novo Código Civil parece caminhar na mesma direção dos demais diplomas aqui mencionados, quando determina no seu art. 107 que *a validade da declaração de vontade não dependerá de forma especial, senão quando a lei expressamente a exigir (BRASIL, 2002)*.

O Novo Código de Processo Civil, por sua vez, trouxe importante inovação no tocante à admissibilidade da prática eletrônica de atos processuais, permitindo ainda a convalidação dos atos praticados por meio eletrônico:

> *Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica.*
>
> *Art. 193. Os atos processuais podem ser total ou parcialmente digitais, de forma a permitir que sejam produzidos, comunicados, armazenados e validados por meio eletrônico, na forma da lei.*
>
> *Art. 1.053. Os atos processuais praticados por meio eletrônico até a transição definitiva para certificação digital ficam convalidados, ainda que não tenham observado os requisitos mínimos estabelecidos por este Código, desde que tenham atingido sua finalidade e não tenha havido prejuízo à defesa de qualquer das partes.*

Dessa forma, podemos concluir que não há, *prima facie,* nenhum óbice à utilização de documentos eletrônicos como prova no processo disciplinar, aqui entendido em sentido amplo, e não somente ao Processo Administrativo Disciplinar (PAD) a que se refere o Título V da Lei n.º 8.112/90. Em razão da lacuna normativa, contudo, se faz necessário esmiuçar no Código Civil e no Código de Processo Civil as regras para a utilização de documentos eletrônicos como meio de prova.

O documento eletrônico como prova

Os documentos digitais suscitam uma interessante discussão relacionada ao conceito de prova documental. A doutrina tradicionalmente associa a prova documental a um documento escrito, presumidamente, em um meio de papel para, a partir daí, debruçar-se sobre as questões relativas à sua forma – original ou cópia – e sua causa eficiente – autêntico ou particular. No entanto, a crescente tendência de diminuição no uso de documentos físicos nas relações jurídicas implica modificar o uso do papel como premissa lógica da manifestação da vontade das partes, sendo o papel nada mais que uma tecnologia como qualquer outra para o seu registro. Como acertadamente aponta PINHEIRO (2016, p. 259):

> *A problemática da substituição do papel, no entanto, é mais cultural que jurídica, uma vez que nosso Código Civil prevê contratos orais e determina que a manifestação da vontade pode ser expressa por qualquer meio. Quem disse que porque está no papel é o documento original? Afinal, todo fax é cópia, apesar de estar em papel. Já o e-mail eletrônico é o original, e sua versão impressa também é cópia.*

Os documentos digitais podem ser públicos, quando emanados de pessoa investida pelo poder público para a sua lavratura, ou particulares, quando produzidos pelas partes – não públicas – que eventualmente podem interferir na relação jurídica. Nesse sentido, o próprio Código de Processo Civil reconhece a possibilidade de lavratura de ata notarial contendo dados eletrônicos:

> *Art. 384. A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião.*
>
> *Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial.*

Sobre a questão, anote-se ainda que tanto o Código Civil quanto o Código de Processo Civil aceitam o seu uso, desde que assegurados os requisitos de autoria e integridade, conforme prelecionam o art. 225 do Código Civil e o art. 369 do Código de Processo Civil, *in verbis*:

> *Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão. (BRASIL, 2002)*

> *Art. 369. As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz. (BRASIL, 2015)*

Percebe-se, portanto, que a natureza digital do documento, *per se*, em nada altera sua valoração probatória quando comparado a um documento em papel, exigindo a lei algumas garantias para a admissibilidade de documentos eletrônicos como prova, quais sejam:

a) **autoria** (ou autenticidade): certeza inequívoca de quem o produz;

b) **integridade**: garantia de que o seu conteúdo não foi adulterado ou manipulado, devendo ser auditável e periciável;

c) **fé pública**: é pela fé pública que os documentos particulares, digitais ou em papel, adquirem a eficácia de prova plena, conforme art. 217 do Código Civil c/c art. 161 da Lei n.º 6.015/73 (Lei dos Registros Públicos).

Embora não exista no Brasil nenhuma regra jurídica a respeito da valoração probatória de documentos eletrônicos, há intenso debate sobre a admissibilidade do uso destes como meio de prova. As posições contrárias ao seu uso, em geral, estão fundamentadas na suposição de que estes seriam mais facilmente adulteráveis que os documentos em papel, o que comprometeria a sua autoria ou integridade.

Ora, tal premissa não encontra respaldo na realidade fática, notadamente após o advento de soluções computacionais que asseguram a autoria e integridade de um arquivo digital – as chamadas assinaturas digitais. Nesse particular, juntamos ombros com PINHEIRO (2016, p. 261), quando afirma que "é *ilusão acreditar que o papel é o meio mais seguro. O papel me si não confere garantia de autenticidade e integridade, tampouco amarra a assinatura das partes com o conteúdo".* Ademais, um documento em papel que tenha sido forjado desde o seu nascedouro não terá reconhecida sua validade jurídica por estar em papel, tampouco por ter sido autenticado em cartório.

A respeito das soluções de assinatura digitais, cumpre destacar a edição da Medida Provisória 2.200-2, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), cuja finalidade é justamente "*garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras".* O art. 10 dessa MP equipara os documentos eletrônicos aos tradicionais, bem como sua admissibilidade como meio de prova, independentemente se assinados pelo sistema de assinatura digital ou não:

> *Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.*
>
> *§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art. 131 da Lei no 3.071, de 1o de janeiro de 1916 - Código Civil.*
>
> *§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil, desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento. (BRASIL, 2001)*

Embora o texto citado faça referência ao art. 131 do Código Civil de 1916, o art. 219 do Novo Código Civil prescreve comando similar:

> *Art. 219. As declarações constantes de documentos assinados presumem-se verdadeiras em relação aos signatários.*
>
> *Parágrafo único. Não tendo relação direta, porém, com as disposições principais ou com a legitimidade das partes, as declarações enunciativas não eximem os interessados em sua veracidade do ônus de prová-las. (BRASIL, 2002).*

Feita essa breve exposição sobre documentos eletrônicos e prova eletrônica, passamos a discorrer sobre as principais fontes de provas digitais e as discussões jurídicas decorrentes.

Fontes de provas digitais

BARRETO, WENDT e CASELLI (2017) definem uma *fonte* como:

> *(...) qualquer dado ou conhecimento que interesse ao profissional de inteligência ou de investigação para a produção de conhecimentos e ou provas admitidas em direito, tanto em processos cíveis quanto em processos penais, e, ainda, em processos trabalhistas e administrativos (relativos a servidores públicos federais, estaduais e municipais).*

Embora os autores tenham como foco a investigação criminal e o levantamento de inteligência[2], entendemos que a classificação das fontes por eles proposta se adequa também às investigações administrativas, especialmente aquelas destinadas a apurar irregularidades praticadas por servidores no exercício de suas funções ou a elas relacionadas. Segundo aqueles, as fontes de conteúdo são divididas em *fechadas* e *abertas*.

Fontes fechadas são aquelas que não estão disponíveis ao público de maneira irrestrita, cujo acesso depende de algum tipo de credenciamento ou autorização. Como exemplos de fontes fechadas de informação, temos as informações relativas a sigilo fiscal ou bancário, interceptações telefônicas ou ambientais, para as quais exige-se autorização judicial, bem como aquelas informações constantes em bancos de dados que exijam algum tipo de credenciamento/obstáculo de acesso, como *login* e senha.

Fontes abertas, por outro lado, são aquelas disponíveis ao público e que não exigem credenciamento ou restrição para seu acesso, a exemplo de jornais, revistas, periódicos acadêmicos, livros e, de maneira mais pronunciada, dados disponíveis na Internet. O processo de obtenção de dados em fontes abertas que sejam úteis para a apuração dos fatos é conhecido como inteligência em fontes abertas (*Open Source Inteligence – OSINT)*.

A utilização das fontes abertas, em especial, tem ganhado crescente importância e destaque no mundo jurídico, tendo sido inclusive admitida nos tribunais como meio válido de prova. O surgimento das redes sociais, em especial, fez com que as pessoas passassem a expor cada vez mais suas preferências, *hobbies* e personalidade na Internet, compartilhando-as com amigos, familiares e até mesmo o público em geral.

Essa crescente exposição social digital, no entanto, trouxe consigo outras implicações não antevistas pelos seus usuários. A divulgação de dados como número de telefone, endereço, fotos de familiares e locais frequentados, por exemplo, facilitaram sobremaneira o planejamento e a prática de um ato delitivo, na medida em que disponibilizam aos seus perpetradores as informações críticas de que necessitam.

---

[2] O Decreto n.º 8.793/16 define a atividade de inteligência como o "*exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado*".

Noutro giro, o surgimento das mídias sociais permitiu também às autoridades ter acesso aos mesmos registros publicados por eventuais criminosos, sonegadores e delinquentes, que, não raro, divulgam mensagens, textos e fotos do produto de sua atividade criminosa ou informações a respeito do seu *modus vivendi*. A riqueza dessas informações não passou despercebido às autoridades públicas: um estudo de 2014 revelou que 73% dos órgãos de investigação utilizam as redes sociais para solucionar delitos de forma mais célere, com 25% dos policiais acessando-as diariamente para auxílio de seu trabalho (BARRETO, WENDT e CASELLI, op. cit.). Mesmo no âmbito dos tribunais, a pesquisa em fontes abertas digitais – sendo as redes sociais sua expressão mais visível – vem servindo como elemento de convicção dos juízes em suas decisões, a exemplo de um magistrado do Rio Grande do Norte que negou o benefício da gratuidade após pesquisa em redes sociais, fundamentando da seguinte forma (idem):

> *Ao analisar as redes sociais, especialmente o Facebook, observo claramente que a promovida alterou a verdade dos fatos para tentar a isenção do pagamento das custas processuais, quando na verdade tem perfeitas condições para o pagamento, isso partindo do pressuposto que uma pessoa, ao divulgar a presença no 'showzão de Jorge e Mateus com os friends' na Vaquejada de Currais Novos, não está preocupada com o sustento da família, conforme alegou na contestação. Do mesmo modo, a "prainha show", bem como os momentos felizes, E CAROS, assistindo aos Jogos da Copa do Mundo FIFA 2014, dão conta de que tem perfeitas condições de arcar com as custas processuais, bem como que é litigante de má-fé ao afirmar o contrário...*

O uso de informações obtidas em fontes abertas como meio de prova tem suscitado questionamentos quanto à legalidade de sua obtenção, bem como questões relacionadas à proteção da intimidade e privacidade. Sem a pretensão de se esgotar o tema, até mesmo em função de sua complexidade, cumpre um breve apanhado sobre as questões mais relevantes para o objeto deste artigo.

A publicidade da rede a o Direito à intimidade

De início, importante ressaltar que na *Internet* reina o princípio da *presunção de publicidade*, o que implica que nada do que é transmitido na rede mundial pode ser considerado sigiloso, salvo aquelas que estejam protegidas por senha ou outra espécie de autorização (fontes fechadas). Da mesma forma, não há lesão a direito quando um indivíduo consente, ainda que de maneira implícita, em divulgar aspectos de sua vida privada na Internet, como comumente ocorre nas redes sociais – cujo modelo de negócios, diga-se, é inteiramente baseado em oferecer "gratuitamente" seus serviços em troca do uso dos dados dos seus usuários. Como oportunamente coloca PINHEIRO (2016, fls. 100), citando Manuel Castells, "*Aquele que decide se conectar aceita, mesmo que tacitamente, o resultado da 'socialização dos seus dados', ou melhor, a perda do controle de suas próprias informações"*.

Ademais, não se pode ignorar que as plataformas sociais podem ser também utilizadas para o cometimento de crimes, o que não pode ser tolerado pelo direito em nome da proteção à privacidade. Em verdade, o entendimento jurisprudencial caminha no sentido de que é válida a utilização de provas obtidas na rede mundial, inclusive em grupos fechados (comunidades virtuais, grupos de *WhatsApp*, etc), quando divulgados por um de seus

participantes, a exemplo de decisão da Primeira Turma do Tribunal de Justiça do Rio de Janeiro, cujo excerto destacamos (TJRJ, 2013):

> *É lícita a prova fornecida por um dos integrantes do ato comunicativo. Precedentes das Cortes Supremas brasileira e alemã. Situação que equivale à gravação ambiental de conversas por um dos interlocutores, manobra cuja legalidade é afirmada de maneira uníssona pela jurisprudência. De todo modo,* ***a disponibilização do conteúdo na rede mundial de computadores levanta seu sigilo.*** *Entendimento do Superior Tribunal de Justiça e deste TJRJ.* **(grifos nossos)**

Casos como o acima demonstram que se por um lado há limites naturais ao direito à informação, por outro há também limites naturais ao direito à privacidade, nas situações em que o interesse coletivo é atingido. Mas como delimitar a fronteira na obtenção e uso das informações pessoais dos serviços digitais por empresas e autoridades públicas?

No intuito de tentar dar uma resposta a essas questões, foi aprovada a Lei n.º 12.965/2014, conhecida como Marco Civil da Internet, que veio regular as exigências de transparência e aviso prévio do usuário acerca da forma a que seus dados serão coletados e o que pode ser feito com os mesmos, além de outras obrigações a provedores de conexão e aplicações na *Internet* quanto à manutenção de registros de acesso (*logs*) e as condições de acesso aos dados por autoridades policiais, administrativas e Ministério Público.

Nesse particular, cabe esclarecer confusão bastante comum entre que dados exatamente as autoridades públicas poderão ter acesso nos termos do Marco Civil da Internet.

Quando tratamos de informações transmitidas ou arquivadas na rede mundial, podemos nos defrontar com dois tipos de informação: *dados cadastrais* ou *dados do conteúdo*. Embora ambos tenham proteção legal, os graus de proteção conferido a cada um deles – e, portanto, os requisitos para sua obtenção – não são os mesmos.

Dados de conteúdo são aqueles relativos ao teor das mensagens e dados transmitidos ou armazenados de forma digital, e somente podem ser obtidos por medida de interceptação telemática, a qual que exige determinação judicial, conforme art. 10, §2º do Marco Civil da Internet (BRASIL, 2014):

> *Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.*
>
> *§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, 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, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.*
>
> *§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.*

Dados cadastrais são aqueles relativos à identificação do usuário (nome, CPF, endereço, etc) aos registros de conexão (data e horário, endereço IP[3]), e podem ser obtidos por quebra de sigilo telemático ou por requisição de autoridade administrativa que tenha competência para tanto, conforme dispõe o art. 10, §3º do mesmo diploma:

> *§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.*

A Lei n.º 12.965/14 estabelece o prazo de 1 (um) ano para que os provedores de conexão mantenham os registros de acesso, embora preveja a possibilidade da autoridade policial ou administrativa ou o Ministério Público requerer cautelarmente que estes sejam guardados por prazo superior (art. 13, §2º), contanto que o requerimento judicial seja apresentado em até 60 (sessenta) dias após o requerimento (§3º).

Por fim, o dispositivo acima não faz distinção sobre qual a finalidade do requerimento, exigindo somente que a autoridade administrativa tenha competência para tanto, de modo que não se vislumbra óbice à utilização desses dados em processos disciplinares cujo objeto de apuração exija acesso a tais informações.

Interceptação telemática e quebra de sigilo telemático

Embora constituam medidas distintas, é comum haver confusão entre a *interceptação telemática* e a *quebra de sigilo telemático*.

A *interceptação telemática*, à exemplo da interceptação telefônica, consiste em ter acesso, em tempo real ou não, às mensagens e dados transmitidos de forma digital, tais como correio eletrônico, mensagens de texto, *chats* e VoIP[4], sem que disso se apercebam os que o emitem e recebem. Trata-se de medida voltada à investigação criminal que exige autorização judicial, por conter informações a respeito da intimidade e vida privada. A interceptação telemática está resguardada pelo art. 5º, incisos X e XII da Constituição Federal e pela Lei n.º 9.296/96 (Lei do Sigilo Telefônico), e só é admitida para apuração de infrações penais punidas com pena de reclusão[5].

A *quebra de sigilo telemático*, por sua vez, consiste em obter os dados cadastrais relacionados à identificação do usuário de um determinado serviço, como, por exemplo, o endereço de um determinado número de IP no momento da prática de um ilícito ou a data, hora e responsável por determinada página ou conteúdo na Internet. Nesses casos, não é exigida a reserva de jurisdição, bastando a existência de representação da autoridade policial para que um provedor de conexão ou de acesso a conteúdo forneça os dados requisitados. Nesse sentido, citamos decisão emanada no HC 83.338/DF do STJ, rel. Min. Hamilton Carvalhido:

> *II. O conhecimento de dados meramente cadastrais, inclusive de e mail, quando disso não se extrapola para a dimensão de informações sobre o status ou modus*

---

[3] Endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais.

[4] Sigla de V*oice over IP*, ou seja, softwares de comunicação de voz através da Internet, a exemplo do Skype®.

[5] Lei n.º 9.296/96, art. 2º, inciso III.

vivendi da pessoa, não atinge a intimidade ou a vida privada de alguém, não estando submetido à cláusula de reserva de jurisdição. Licitude da prova produzida nesses termos.

Oportuno ainda trazer a jurisprudência do Supremo Tribunal Federal a respeito, mencionada pelo Ministro Raphael de Barros Monteiro Filho, na Carta Rogatória nº 297/DE, in DJ 29/9/2006, e citado no voto do Ministro Hamilton Carvalhido:

> *Não entendo que se cuide de garantia com status constitucional. Não se trata da 'intimidade ' protegida no inciso X do art. 5º da Constituição Federal. Da minha leitura, no inciso XII da Lei Fundamental, o que se protege, e de modo absoluto, até em relação ao Poder Judiciário, é a comunicação 'de dados' e não os 'dados', o que tornaria impossível qualquer investigação administrativa, fosse qual fosse. (voto proferido pelo Ministro Sepúlveda Pertence no MS n. 21.729-4/DF, DJ 19.10.2001)*

Importante frisar que a garantia constitucional da proteção à intimidade e privacidade diz respeito ao teor das comunicações, e não do conhecimento dos dados cadastrais em si. Por conseguinte, a exigência constitucional e legal de reserva de jurisdição diz respeito somente à interceptação telemática, e não à quebra de sigilo de dados telemáticos que não tragam em si informações sobre a intimidade e vida privada do agente.

Conclusão

Como demonstrado ao longo deste artigo, a legislação brasileira vem buscando equilibrar o direito à informação com o direito à privacidade, sem olvidar da possibilidade de atuação das autoridades quando o interesse coletivo estiver em jogo, inclusive nas hipóteses de inquérito administrativo destinado a apurar responsabilidade de servidor público. Se por um lado é garantido o sigilo dos dados e informações de um indivíduo na rede mundial de computadores, por outro é certo que essa proteção não é absoluta, notadamente quando o próprio indivíduo consente, ainda que tacitamente, em divulgar aspectos de sua vida na rede.

Demonstramos também ser possível a obtenção de informações mais detalhadas dos registros de conexão (dados cadastrais) e até mesmo do teor do conteúdo das mensagens, desde que devidamente atendidas as exigências legais para seu acesso e utilização.

Por fim, a despeito de não haver normativo específico no Direito Administrativo Disciplinar, a lacuna é preenchida pelas regras do Direito Civil e Processual Civil, que preveem e autorizam o uso de documentos eletrônicos, inclusive aqueles obtidos em fontes abertas como a *Internet* e redes sociais, como meio de prova no processo, desde que obtidas por meio lícito e com boa técnica que garanta sua autoria, integridade e fé pública.

REFERÊNCIAS

BARRETO, Alesandro G., WENDT, Emerson e CASELLI, Guilherme**. Investigação Digital em Fontes Abertas:** *Busca de dados em redes sociais, coleta de informações na Deep Web, Análise de metadados*. 2ª ed. – Rio de Janeiro: Brasport, 2017

BARRETO, Alesandro G., BRASIL, Beatriz S**. Manual de Investigação Cibernética à Luz do Novo Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016.

BAZELL, Michael**. Open Source Intelligence Techniques***: resources for searching and analyzing online information*. 5ª ed. Lexinton, KY, Estados Unidos da América. 2016, 407p.

BRASIL. Lei n.º 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. **Portal da Legislação**, Brasília, dez. 1990. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/L8112cons.htm>. Acesso em 17.01.2018.

_____. Lei n.º 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal (Lei do Sigilo Telefônico). **Portal da Legislação,** Brasília, jul. 1996. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em 15.01.2018.

_____. Lei n.º 9.784, de 29 de janeiro de 1999. Regula o processo administrativo no âmbito da Administração Pública Federal. **Portal da Legislação**, Brasília, jan. 1999. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/l9784.htm>. Acesso em 15.01.2018.

_____. Medida Provisória n.º 2.200-2, de 24 de agosto de 2001. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. **Portal da Legislação,** Brasília, ago. 2001. Disponível em <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em 20.01.2018.

_____. Lei n.º 10.406, de 10 de janeiro de 2002. Institui o Código Civil**. Portal da Legislação**, Brasília, jan. 2002. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406compilada.htm>. Acesso em 19.01.2018.

_____. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Portal da Legislação,** Brasília, abr. 2014. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 04.02.2018.

_____. Lei n.º 13.105, de 16 de março de 2015. Código de Processo Civil. **Portal da Legislação**, Brasília, mar. 2015. Disponível em <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm>. Acesso em 19.01.2018.

_____. Ministério da Transparência e Controladoria Geral da União. **Manual de Processo Administrativo Disciplinar**. Brasília, dez. 2017. Disponível em <https://www.cgu.gov.br/Publicacoes/atividade-disciplinar/arquivos/manual-pad-dezembro-2017.pdf/view>. Acesso em 16.02.2018.

_____. Superior Tribunal de Justiça. HABEAS CORPUS: HC 83.338/DF (2007/0116172-1) Relator: Min. Hamilton Carvalhido. DJe: 26/10/2009. **Pesquisa Jurisprudencial.** Disponível em <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=200701161721&dt_publicacao=26/10/2009> . Acesso em 24.02.2018.

_____. Tribunal de Justiça do Rio de Janeiro. Primeira Turma Recursal Fazendária. RECURSO INOMINADO: RI 02539109620138190001. Relator: Juiz Luiz Fernando de Andrade Pinto. DJ: 30/10/2014. **Jusbrasil**, 2013. Disponível em <https://tj-rj.jusbrasil.com.br/jurisprudencia/149496982/recurso-inominado-ri-25391096201381900 01-rj-0253910-9620138190001> . Acesso em 24.02.2018.

LESSA, Breno Minucci. **A Invalidade das Provas Digitais no Processo Judiciário**. Disponível em <http://www.conteudojuridico.com.br/artigo,a-invalidade-das-provas-digitais-no-processo-judiciario,25613.html>. Acesso em 16.01.2018.

PINHEIRO, Patrícia Peck. **Direito Digital**. 6ª ed., rev., atual. e ampl. – São Paulo: Saraiva, 2016.