PROVISÓRIO

WALTER ARANHA CAPANEMA

Manual de DIREITO DIGITAL

Teoria e Prática

2ª edição
Revista, Atualizada e Ampliada

2025

EDITORA JusPODIVM
www.editorajuspodivm.com.br

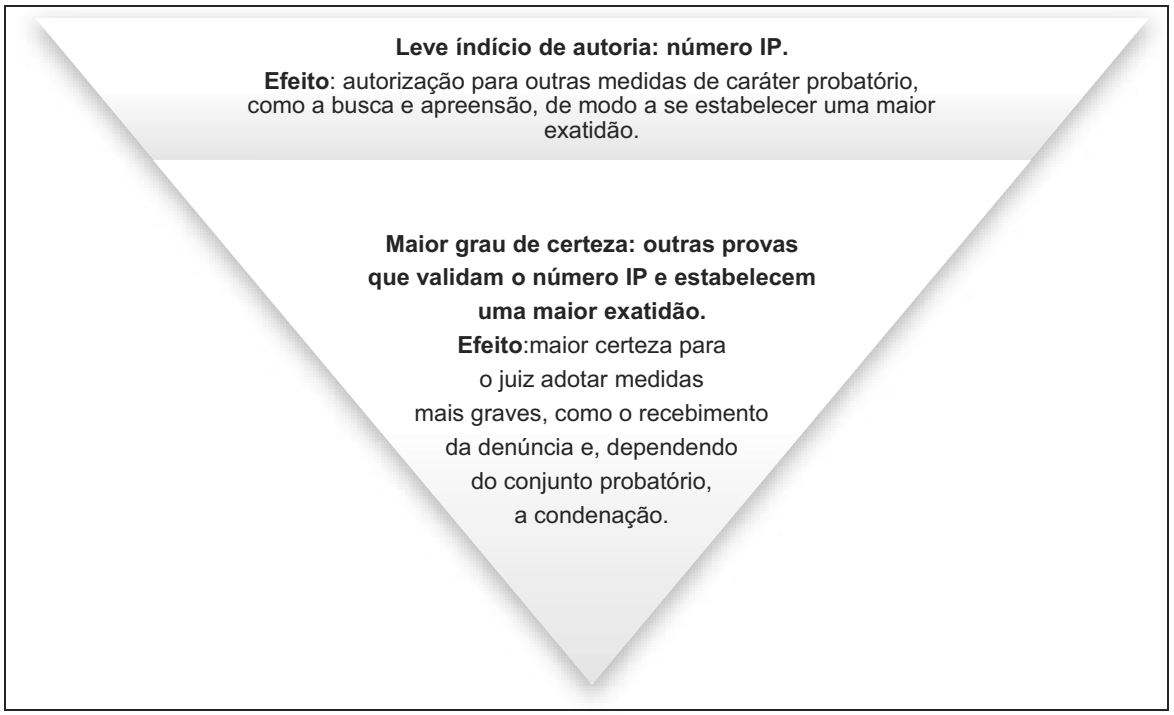

Figura 57: Esquema do Afunilamento Probatório

2. PROVAS DIGITAIS DOCUMENTAIS EM ESPÉCIE

Uma vez analisados os fundamentos das provas digitais, passa-se agora a estudar de forma detalhada as provas documentais em espécie:

2.1. Provas em provedores de conexão

Os provedores de conexão são as pessoas naturais ou jurídicas que, de modo oneroso ou gratuito, prestam o serviço de acesso à internet, permitindo, assim, a navegação pela *web*, o envio de e-mails e outras atividades úteis (e inúteis). Portanto, é quem faz a intermediação do usuário à grande rede.

A conexão de um computador à Internet pressupõe duas atividades:

1. **habilitação**: que o provedor atribua a esse dispositivo um número IP, único ou compartilhado ("nateado", conforme abordado no Capítulo 2);
2. **capacidade de troca de pacotes**: que se possa enviar e receber pacotes de dados, segundo os protocolos próprios da Internet[73].

73. O art. 5º, V do Marco Civil da Internet conceitua "conexão à internet" como "*a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP*".

O art. 13 do Marco Civil determina que os administradores de sistemas autônomos[74] dos provedores de conexão deverão "manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento".

Tal regulamentação se deu pelo Decreto 8.771/206, expedido pelo então Presidente Michel Temer.

As informações relativas aos **registros de conexão**[75], conforme mencionado anteriormente, dizem respeito à "data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (art. 5º, VI, do Marco Civil).

Contudo, o registro de conexão precisará conter outras informações.

A Resolução 73/1998 da ANATEL, que aprova o Regulamento dos Serviços de Telecomunicações, estabelece em seu art. 65-J, parágrafo único, o dever de guarda das portas lógicas "utilizadas quando do compartilhamento de IP público"[76].

Tal norma, embora tenha sido publicada em 1998, foi alterada em 2020 pela Resolução 738 para se adequar à LGPD e, assim, estar em consonância com suas normas, especialmente os seus princípios.

E, em relação aos princípios da LGPD, nota-se a evidente influência do princípio da necessidade (art. 6º, III) no disposto do art. 65-I: "As prestadoras devem reter a menor quantidade possível de dados

---

74. Art. 5º, IV, do Marco Civil: "*administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País*".

75. Há um conceito muito semelhante, referente aos denominados "dados de conexão", no art. 10-A, § 1º, I, da Lei 12.850/2013: "informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão".

76. Art. 65-J, Resolução 73/1998 -ANATEL. A fim de assegurar a permanente fiscalização e o acompanhamento de obrigações legais e regulatórias, as prestadoras devem manter à disposição da Anatel os dados relativos à prestação do serviço, incluindo, conforme o caso e observada a regulamentação pertinente:

I – documentos de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada pelo prazo mínimo de 5 (cinco) anos, nos serviços que permitam a realização de tráfego telefônico; e,

II – registros de conexão à Internet pelo prazo mínimo de 1 (um) ano nos serviços que permitam a conexão à Internet.

Parágrafo único. Para fins do disposto neste artigo, considera-se registro de conexão à Internet o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal, assim como as portas lógicas utilizadas quando do compartilhamento de IP público, para o envio e recebimento de pacotes de dados.

de usuários, mantendo-os sob sigilo, em ambiente controlado e de segurança (...)".

A RFC 6302[77] apresenta algumas recomendações voltadas para provedores de conexão e servidores ligados à Internet, destacando-se o registro das portas lógicas e a necessidade de armazenamento do horário no padrão sugerido UTC – *Coordinated Universal Time* (Tempo Universal Coordenado)[78].

A utilização de um formato de horário como o UTC se justifica pela necessidade de se definir precisamente o exato momento da ocorrência de uma conduta, tendo em vista a multiplicidade de fusos horários que existem.

Com o acréscimo do fuso horário, teríamos, em resumo, no documento **registro de conexão** as seguintes informações:

- Número IP (+ porta lógica, se houver "nateamento");
- Data e hora do início e do término da conexão no formato UTC;
- Duração da conexão.

A exigência de sigilo, definida no *caput* do art. 13, é sensata. Afinal, são informações relativas à conexão da Internet de um ou vários usuários, constituindo-se, portanto, dados pessoais. E, por expressa previsão legal (art. 13, § 5º), tais registros só podem ser fornecidos mediante **prévia ordem judicial**.

O art. 13, § 1º do Marco Civil determina que o provedor de conexão não poderá delegar para terceiros a atividade de manutenção (leia-se "armazenamento") de registros.

Os §§ 2º, 3º e 4º do art. 13, tratam do "requerimento cautelar" de conservação de registros por período superior ao definido no *caput* (1 ano), de legitimidade da autoridade policial ou administrativa ou o do Ministério Público. Existe medida semelhante para o registro de aplicação (art. 15, § 2º).

Na verdade, não se trata de um "requerimento", mas de uma verdadeira requisição de preservação, sem a necessidade de ordem

77. INTERNET ENGINEERING TASK FORCE. **RFC 6302.** Disponivel em: https://datatracker.ietf.org/doc/html/rfc6302. Acesso em: 21 ago. 2022.

78. O formato UTC veio substituir o antigo e tradicional GMT (Greenwich Mean Time). O Horário de Brasília corresponde a UTC – 3.

judicial, afinal, o Marco Civil só a exige para o acesso àquele conteúdo previamente conservado (§ 4º).

Após a requisição, o interessado tem o prazo de 60 dias para ingressar com uma ação judicial (qualquer uma) pleiteando o acesso aos registros conservados. O provedor deverá manter sigilo em relação à requisição, o que permite concluir que o próprio procedimento judicial de acesso deverá ocorrer em segredo de justiça, nos termos do art. 23 do Marco Civil.

Caso a ação não seja proposta no prazo legal, ou na hipótese de indeferimento do pedido, cessará o dever de armazenamento (§ 4º).

Na jurisprudência, o STJ entendeu que esse "requerimento" é uma verdadeira "requisição", no que se denominou de **"congelamento de dados telemáticos"**:

> "É que, quem requer alguma coisa, pura e simplesmente pode tê-la deferida ou não, e, no caso, até mesmo pelo uso do termo "cautelarmente", seguido da previsão de pedido judicial de acesso no prazo de 60 (sessenta) dias, contados do requerimento administrativo, sob pena de caducidade, tem-se que o administrador de sistema autônomo e o provedor de aplicações de internet estariam obrigados a atender à solicitações da autoridade policial, administrativa ou o Ministério Público." (STJ – HC n. 626.983/PR, relator Ministro Olindo Menezes (Desembargador Convocado do TRF 1ª Região), Sexta Turma, julgado em 8/2/2022, DJe de 22/2/2022.)

Há um diferencial no julgado acima: o Ministério Público do Estado do Paraná havia requisitado à Apple e ao Google o congelamento não apenas dos registros de aplicação, mas também, dentre outros, **dos dados cadastrais, históricos de pesquisa e de localização, conteúdos de e-mail, fotos e contatos**. Para o STJ, não houve qualquer nulidade, afinal:

> "Considerando a facilidade do descarte dos conteúdos das aplicações de internet pelos usuários, a Lei do Marco Civil da Internet, a fim de viabilizar investigações criminais, que, normalmente, são de difícil realização em ambientes eletrônicos, tornou mais eficiente o acesso a dados e informações relevantes ao possibilitar que o Ministério Público, diretamente, requeira ao provedor apenas a guarda, em ambiente seguro e sigiloso,

> dos registros de acesso a aplicações de internet, haja vista que a disponibilização ao requerente dos conteúdos dos registros – dados cadastrais, histórico de pesquisa, todo conteúdo de e-mail e iMessages, fotos, contatos e históricos de localização etc. – deve sempre ser precedida de autorização judicial devidamente fundamentada, o que ocorreu no presente caso.
>
> Conforme a jurisprudência desta Corte Superior, não há nulidade sem prejuízo, ainda que essa nulidade seja absoluta".

A questão foi levada ao STF, e o relator do HC, o Ministro Ricardo Lewandowski, entendeu que o Marco Civil só admite o congelamento dos registros de conexão e de aplicação, o que importa na nulidade da apreensão do conteúdo das comunicações telemáticas:

> "Assim, vê-se que cabe ao Ministério Público requerer cautelarmente que os registros de conexão sejam guardados por prazo superior a 1 ano, quais sejam, aqueles exclusivos a informações de data e hora de acesso, duração e IP de origem, o que, como afirmado alhures, não se confunde com o conteúdo telemático armazenado dentro dos sistemas autônomos, tais como históricos de pesquisa, todo o conteúdo de e-mail e *Imessages*, fotos e dados de localização. Entendimento diverso levaria à autorização para que houvesse a busca e apreensão prévia de conteúdos e seu congelamento, para posterior formalização da medida por ordem judicial, em prática vedada por qualquer standard que se extraia da ordem constitucional vigente.
>
> Conclui-se, portanto, que, na hipótese sob exame, o Ministério Público do Estado do Paraná não observou a necessária reserva de jurisdição no que toca à ordem de indisponibilidade do conteúdo telemático por parte da sua legítima titular, contrariando, na forma acima delineada, a Constituição Federal e o Marco Civil da Internet, pois decretou verdadeira medida cautelar ao ordenar, *sponte propia*, o "congelamento" de todo o conteúdo de comunicações telemáticas da paciente. Em suma, retirou do seu legítimo proprietário o direito de dispor do conteúdo dos seus dados para quaisquer fins, sem que houvesse autorização judicial para tanto.
>
> Isso posto, concedo a ordem a fim de declarar nulos os elementos de prova angariados em desfavor da paciente a partir do congelamento prévio, sem autorização judicial, do conteúdo de suas contas eletrônicas, bem como de todos os demais que

> dele decorrem, nos autos da ação penal ora em comento. (STF – HC 222141 / PR – PARANÁ HABEAS CORPUS Relator(a): Min. RICARDO LEWANDOWSKI Julgamento: 01/12/2022. Publicação: 05/12/2022)

Dessa maneira, parece que a melhor estratégia é de se buscar por meio de uma medida judicial o acesso direto ao conteúdo das comunicações telemáticas do investigado.

Nada impede que outros atores processuais, não contemplados nesse rol, possam também garantir a conservação, não por meio de uma requisição direta, mas por uma medida judicial, como uma tutela de urgência.

Os provedores de conexão, poderão fornecer, também, os denominados **dados cadastrais,** que são aqueles relativos à qualificação pessoal, filiação e endereço do usuário (art. 10, § 2º Marco Civil), sendo que, os dados relativos à qualificação, são o prenome e o nome, o estado civil e a profissão (art. 11, § 2º do Decreto 8.771/2016)[79].

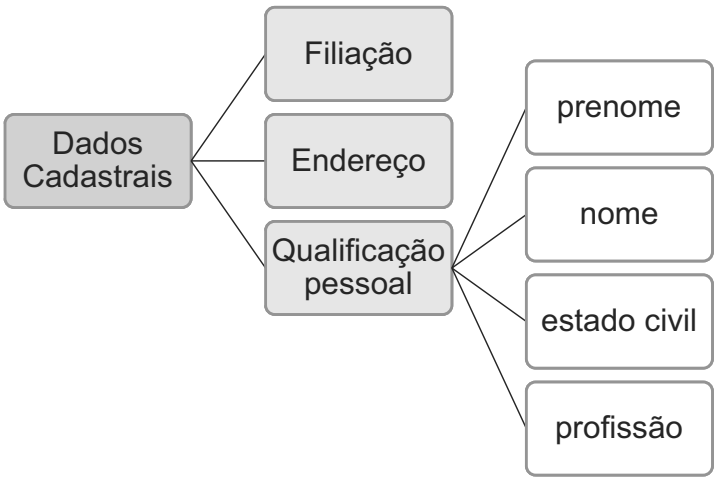

Figura 58: Esquema relativo aos dados cadastrais

Há, para os provedores de conexão, um dever de guarda dos documentos fiscais e dos dados cadastrais dos assinantes, conforme determina o art. 65-J, I da citada Resolução 73/1998 da ANATEL.

Serão disponibilizados, como regra geral, mediante ordem judicial, exceto nos termos do art. 10, § 3º, para as **autoridades administrativas**

79. Há um conceito específico de dados cadastrais no art. 10-A, § 1º, II, da Lei 12.850/2013: "informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão".

"que detenham competência legal para a sua requisição", as quais poderão requisitar diretamente tais dados.

Para tanto, tais autoridades deverão indicar a base legal para o acesso e o motivo, de acordo com o art. 11, *caput*, do Decreto 8.771/2016.

Há aqui alguns dos maiores mistérios do Marco Civil: por qual razão o legislador restringiu a legitimidade dessa espécie de requisição apenas para as autoridades administrativas? E, principalmente, quais seriam essas autoridades?

Pode-se apontar algumas autoridades com atribuições genéricas de requisição de informações e documentos, como o Conselho Administrativo de Defesa Econômica – CADE[80].

Contudo, o STJ, no supracitado julgado amplia a legitimidade para as autoridades policiais e o Ministério Público:

> "6. Dispõe, ainda, que a autoridade policial, administrativa ou o Ministério Público poderão requerer cautelarmente que os registros de conexão sejam guardados por prazo superior a 1 (um) ano (art. 13, § 2º), e os registros de acesso a aplicações de internet por prazo superior a 6 (seis) meses (art. 15, § 2º), devendo, nas duas situações, e no prazo de 60 (sessenta) dias, contados do requerimento administrativo, ingressar com o pedido de autorização judicial de acesso aos (dois) registros (arts. 13, § 3º, e 15, § 2º):
>
> 7. A lei dispõe que a autoridade policial, administrativa ou o Ministério Público poderão requerer cautelarmente – que os registros de conexão sejam guardados por prazo superior a 1 (um) ano (art. 13, § 2º), e os registros de acesso a aplicações de internet por prazo superior a 6 (seis) meses (art. 15, § 2º) –, parecendo dizer menos do que pretendia."

É importante frisar que o acesso não será à integralidade do cadastro do investigado/réu, **mas apenas aos dados referentes à filiação e qualificação pessoal (identificação) e endereço (localização).**

Nos demais casos, o acesso aos dados cadastrais dependerá de prévia ordem judicial. Contudo, o Marco Civil não definiu quais seriam os requisitos para tanto. A partir de uma interpretação sistemática da lei e do seu decreto regulador, é possível estabelecer os seguintes:

---

80. As requisições de documentos podem ser realizadas pelos Conselheiros do Tribunal Administrativo de Defesa Econômica (art. 11, III, Lei 12.529/2011) e pela Superintendência-Geral (art. 13, VI, a).

1. **individualização do investigado/réu**: art. 11, § 3º, Decreto 8.771/2016;
2. **utilidade/necessidade da prova:** pode-se buscar o fundamento de validade desse argumento no seguinte trecho do art. 10, § 1º do Marco Civil: "informações que possam contribuir para a identificação do usuário ou do terminal".

O art. 13 do Decreto 8.771/2016 definiu os padrões de segurança necessários para os registros, dados pessoais e comunicações privadas.

Chama atenção o inciso III, que estabelece o dever de "criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014".

Tal documento, portanto, é um controle interno dos provedores (de conexão e de aplicação) em que se listam quais empregados, servidores públicos ou colaboradores que tiveram acesso (e qual tipo de acesso) aos registros. Como não há cláusula de reserva de jurisdição expressa, ele poderia ser requisitado pelo Ministério Público e pela autoridade policial, com base em suas normas gerais de requisição.

Os provedores de conexão possuem a capacidade técnica de analisar os pacotes de dados dos seus usuários e de monitorar o os sites e serviços utilizados[81]. Essas condutas são lícitas? Essa prova poderia ser utilizada em juízo?

O Marco Civil, ao prever a neutralidade da rede em seu art. 9º, que consiste em um dever de se tratar os pacotes de dados de forma isonômica ("isonomia de pacotes"), proibiu, no § 3º, todo comportamento que implicasse em bloqueio, monitoramento, filtragem ou análise do conteúdo desses pacotes[82]. Essa eventual atividade de

81. O´DRISCOLL, Aimee. **Your ISP can see your browsing history; here's how to stop it.** Disponível em: https://www.comparitech.com/blog/vpn-privacy/stop-isp-tracking-browsing-history/. Acesso em: 7 maio 2021.

82. Essa atividade de controle da conexão do usuário, de forma a privilegiar ou degradar a conexão da internet atender pelo nome técnico de ***traffic shaping*** ("modelagem de tráfego"). Há alguns sites que se propõem a verificar se a sua conexão sofre desse fenômeno. Um deles é o Glasnost – http://broadband.mpi-sws.org/transparency/bttest-mlab.php.

monitoramento, portanto, é ilícita, e até poderia constituir o crime do art. 10 da Lei 9.296/96.

O art. 16, I determina que os provedores de conexão não podem guardar registros de acesso sem o consentimento do usuário[83]. A eventual guarda também constituiria prova ilegal.

Uma outra prova documental possível de ser encontrada nos provedores de conexão diz respeito aos números de cartão de crédito utilizados pelo investigado/réu, caso o provedor de conexão exerça a atividade de forma comercial e ofereça essa forma de pagamento.

As atividades de operações com cartão de crédito são consideradas operações financeiras, conforme o art. 5º, § 1º, da Lei Complementar 105/2001, cujo sigilo só pode ser quebrado mediante ordem judicial (art. 1º, § 4º).

Os provedores de conexão também podem documentar o consumo de Internet do usuário[84].

Em caso de desobediência aos deveres impostos aos provedores de conexão no art. 13, determina o § 6º que poderão ser impostas sanções que terão como parâmetros a natureza e a gravidade da infração; os danos dela resultantes (a sua extensão); eventual vantagem auferida pelo infrator; bem como "as circunstâncias agravantes, os antecedentes do infrator e a reincidência".

Quem é o responsável por impor tais sanções? Em qual procedimento? Quais são as hipóteses de aplicação? Quais seriam essas sanções? Qual o alcance da expressão "circunstâncias agravantes"?

Victor Hugo Gonçalves entende que o presente parágrafo pode ser aplicado pelo Judiciário, criticando a opção do legislador em definir critérios indeterminados, tornando a norma de difícil aplicação[85].

---

83. Um ponto que precisa ser refletido é o de se a guarda dos referidos registros pelo provedor de conexão tem como requisito apenas o consentimento, ou, interpretando-se o Marco Civil no contexto do microssistema de proteção de dados, poderia-se aplicar, também, as demais hipóteses de tratamento dos arts. 7º e 11 da LGPD. Por outro lado, a restrição do armazenamento, leia-se, "tratamento de dados pessoais", apenas na hipótese de prévio consentimento não seria uma interpretação mais favorável ao usuário/titular de dados pessoais, a afastar a "importação" das bases legais da LGPD? Privilegiar o consentimento seria prestigiar a autodeterminação informativa.

84. O provedor de conexão Claro possui um sistema que permite ao usuário acompanhar o seu gasto pela Internet – https://melhorplano.net/claro/consumo-claro.

85. GONÇALVES, Victor Hugo Pereira. **Marco Civil da Internet Comentado**. São Paulo: Atlas, 2017. p. 81.

O Marco Civil, na verdade, não limita a aplicação dessas sanções em ações judiciais, razão pela qual é possível imaginar o seu cabimento em processos administrativos.

No caso, o "descumprimento ao disposto nesse artigo" importa à desobediência aos seguintes deveres:

1. armazenamento, guarda cautelar e fornecimento dos registros de conexão;
2. segurança e sigilo dos registros de conexão;
3. disponibilização dos registros de conexão mediante ordem judicial;
4. sigilo sobre a guarda cautelar.

Pode-se imaginar, por exemplo, uma situação em que uma associação civil de defesa dos usuários da Internet ajuíze uma ação civil pública em face de um provedor de conexão que está armazenando os registros de conexão em ambiente inseguro, fornecendo tais informações sem a necessária ordem judicial. O autor poderia, assim, pleitear a adoção de medidas de segurança, a obrigação de se atender ao art. 13, § 5º, e, principalmente, à condenação da ré ao pagamento de quantia indenizatória, a título de dano moral coletivo, tendo, como parâmetros, as balizas do § 6º.

O legislador se esqueceu em definir quais seriam essas "circunstâncias agravantes". Aliás, pior ainda: não trouxe as circunstâncias atenuantes, que seriam fundamentais para se poder definir uma sanção justa e equânime. No silêncio, portanto, o alcance da expressão dependerá do intérprete, e pode-se apontar as seguintes sugestões:

- ausência de adoção das diretrizes sobre padrões de segurança, elencadas no art. 13 do Decreto 8.771/2016;
- prática de condutas que violem a intimidade e a privacidade do usuário, como o *traffic shaping* (art. 9º, § 3º). A referida conduta, por si só, não permite a aplicação das sanções, afinal, só se referem ao art. 13. Contudo, pela sua gravidade, pode funcionar como circunstância agravante;
- a adoção de medidas para ocultar a ocorrência do dano, como a destruição de registros, arquivos e documentos (inspiração da circunstância agravante do art. 61, II, b, CP)

2.2. Provas em provedores de telefonia

Os provedores de telefonia também guardam informações que podem ser fundamentais para a investigação policial ou para o processo, sendo relevantes a Lei 9.472/97 e as Resoluções 73/1998 (Regulamento dos Serviços de Telecomunicações), 477/2007 (Regulamento sobre Serviço Móvel Pessoal) e 632/2014 (Regulamento Geral de Direito do Consumidor de Serviços de Telecomunicações) da ANATEL, bem como o Código de Processo Penal.

Os seguintes documentos devem ser armazenados pelas prestadores de serviços de telefonia: (art. 65-J, inciso I, Resolução 73/1998 da ANATEL):

a) Documentos de natureza fiscal;
b) Dados cadastrais dos assinantes;
c) Metadados das ligações telefônicas ("dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada").

O art. 3º, IV da Lei 12.850/2013 (Lei das ORCRIM) admite, como meio de obtenção de prova, o "acesso a registros de ligações telefônicas e telemáticas, a dados cadastrais constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais".

O art. 17 da supracitada norma determina que as concessionárias de telefonia fixa ou móvel armazenarão, pelo prazo de 5 anos, o histórico de ligações telefônicas, que poderão ser acessados sem ordem judicial pelas autoridades policiais e pelo Ministério Público.

Uma outra prova que pode ser fornecida pelos provedores de telefonia é a triangulação das Estações de Rádio Base (ERBs), que permite a localização aproximada de um indivíduo em um determinado espaço. As ERBs são aparelhos de comunicação que realizam a intermediação entre os telefones celulares e a empresa de telefonia, sendo que a sua área de cobertura constitui uma célula[86].

Por meio de um processo de triangulação entre diversas ERBs, é possível se ter a localização aproximada de um indivíduo. Tal localização,

86. Ministério Público do Estado de Goiás. **Estação Rádio Base**: telefonia celular. Disponível em: http://www.mpgo.mp.br/portal/news/estacao-radio-base-telefonia-celular. Acesso em: 6 jun. 2021.

não se compara àquela realizada por meio do geoposicionamento (GPS), que possui uma acurácia de 4.9 metros em *smartphones*, em condições meteorológicas de céu aberto[87].

O art. 65-E da Resolução 73/98 confere às prestadoras de telefonia móvel o dever de disponibilizar às autoridades responsáveis pelos serviços públicos de emergência acesso às informações sobre a localização do aparelho de onde partiu uma chamada ou mensagem de texto destinada a elas.

O Código de Processo Penal permite o acesso à ERB apenas para hipóteses específicas, envolvendo a prevenção e a repressão de crimes relacionados ao tráfico de pessoas.

O art. 13-B do CPP determina a prerrogativa do Ministério Público e da autoridade policial de "requisitar, mediante autorização judicial" (leia-se, requerer) às empresas de telefonia sinais, informações que permitem a localização da vítima ou dos suspeitos desses crimes.

E, para os efeitos desse artigo, o conceito de "sinais" abrange "posicionamento da estação de cobertura, setorização e intensidade de radiofrequência", o que significa, portanto, acesso à ERB.

Os juízes devem se manifestar sobre o pedido em até 12 horas, caso em que, ultrapassado esse prazo sem decisão, poderá a autoridade requisitar diretamente às empresas de telecomunicação os sinais e informações necessários (art. 13-B, § 4º, CPP).

O acesso aos sinais não compreende, obviamente, o conteúdo das comunicações, que dependerá de outra ordem judicial, nos termos da Lei 9.296/96; e poderá ser fornecido pelo prazo de 30 dias, renovável por igual período. Uma renovação por período maior necessitará de apresentação de ordem judicial (art. 13-B, § 2º, III).

O STJ já entendeu que não há ilegalidade na conduta de autoridade policial que requisitou à empresa de telefonia o registro de todos os números telefônicos que acessaram determinada ERB no dia e hora da prática de um determinado crime[88]. O mesmo julgado determinou que não há necessidade de autorização judicial para o acesso aos dados

87. GPS.gov. **GPS Accuracy.** Disponível em: https://www.gps.gov/systems/gps/performance/accuracy/. Acesso em: 6 jun. 2021.

88. STJ – HC 247.331/RS, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 21/08/2014, DJe 03/09/2014.

cadastrais[89]. As informações relativas ao histórico de chamadas (dia e hora) são, na verdade, metadados das ligações telefônicas.

E a Corte já decidiu[90] que não são exigíveis, para o acesso aos dados cadastrais, os mesmos rigores da Lei 9.296/96, que trata das interceptações telemáticas e telefônicas.

Contudo, a Lei 10.703/2003, que trata do cadastramento dos telefones celulares pré-pagos, determina em seu art. 1º, § 3º, que esses dados cadastrais deverão ser imediatamente disponibilizados, salvo motivo justificado, para "**atender solicitação da autoridade judicial**" (grifou-se).

2.3. Provas em provedores de aplicação

2.3.1. Regras Gerais

Os provedores de aplicação[91] são aqueles que disponibilizam serviços, aplicativos e outros funcionalidades aos usuários, de forma gratuita ou onerosa, podendo ser constituídos como pessoas naturais ou jurídicas, sem formalidades específicas para tanto.

Se os provedores de conexão permitem que o usuário acesse a Internet, os provedores de aplicação, por sua vez, "são a Internet", propriamente dita.

Esses provedores de aplicação coletam, registram e armazenam informações basicamente por dois fundamentos: para atender a uma exigência legal e para dar suporte à eventual relação contratual com o usuário.

---

89. "Nos termos da jurisprudência do Superior Tribunal de Justiça, a quebra de sigilo dos dados cadastrais dos usuários, relações de números de chamadas, horário, duração, dentre outros registros similares, que são informes externos à comunicação telemática, não se submetem a disciplina da Lei n.º 9.296/96, que trata da interceptação do que é transmitido pelo interlocutor ou do teor da comunicação telefônica" (AgRg no REsp 1760815/PR, Rel. Ministra LAURITA VAZ, SEXTA TURMA, DJe 13/11/2018).

90. "2. Não se confundem as medidas de quebra de sigilo telefônico com a interceptação de comunicação telefônica, esta última albergada, ademais, pela cláusula de reserva de jurisdição. Daí, não são exigíveis, no contexto da quebra de sigilo de dados, todas as cautelas insertas na Lei 9.296/1996. In casu, o magistrado, em cumprimento do inciso IX do artigo 93 da Constituição da República, motivou a quebra do sigilo de dados, com base na intensa utilização de certo terminal telefônico, havendo a franca possibilidade de se desvendar, com base em dados cadastrais oriundos das registros de companhia telefônica, a autoria de um quarto agente no concerto delitivo. 3. Ordem não conhecida." (HC 237.006/DF, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, SEXTA TURMA, julgado em 27/06/2014, DJe 04/08/2014).

91. O Marco Civil conceitua aplicações de internet como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet" (art. 5º, VII).

Enquanto no primeiro caso temos leis pontuais que especificam esses deveres, na segunda hipótese tem-se praticamente uma quantidade ilimitada de provas possíveis, especialmente porque os Termos de Uso (contratos de adesão) e as Políticas de Privacidade (declarações unilaterais de informações sobre o tratamento de dados pessoais) não são muito transparentes a respeito dessas informações.

No caso das obrigações legais, tem-se o dever de produção e armazenamento dos registros de acesso a aplicações de Internet pelo prazo de 6 meses (art. 15, Marco Civil).

Tendo em vista que a implantação de uma estrutura tecnológica para tanto é onerosa, e que a sua exigência indiscriminada poderia ofender a livre iniciativa (art. 170, *caput*, CF), o legislador limitou tal exigência para os provedores que forem constituídos como pessoas jurídicas que exerçam "essa atividade de forma organizada, profissionalmente e com fins econômicos", ou seja, atuem empresarialmente.

Não há, até o presente momento, previsão normativa para a guarda das portas lógicas relativas aos números IPs "nateados". Há, contudo, um importantíssimo precedente do STJ:

> "RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE APLICAÇÕES. IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO À APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. INTERPRETAÇÃO TELEOLÓGICA DOS ARTS. 5º, VII, E 15 DA LEI N. 12.965/2014. RECURSO ESPECIAL PROVIDO.
>
> 1. O recurso especial debate a extensão de obrigação do provedor de aplicações de guarda e fornecimento do endereço IP de terceiro responsável pela disponibilização de conteúdo ilícito às informações acerca da porta lógica de origem associada ao IP.
>
> 2. A previsão legal de guarda e fornecimento dos dados de acesso de conexão e aplicações foi distribuída pela Lei n. 12.965/2014 entre os provedores de conexão e os provedores de aplicações, em observância aos direitos à intimidade e à privacidade.
>
> 3. Cabe aos provedores de aplicações a manutenção dos registros dos dados de acesso à aplicação, entre os quais se inclui o endereço IP, nos termos dos arts. 15 combinado com o art. 5º, VIII, da Lei n. 12.965/2014, os quais poderão vir a ser fornecidos por meio de ordem judicial.

> 4. A obrigatoriedade de fornecimento dos dados de acesso decorre da necessidade de balanceamento entre o direito à privacidade e o direito de terceiros, cujas esferas jurídicas tenham sido aviltadas, à identificação do autor da conduta ilícita.
>
> 5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso à internet e às aplicações.
>
> 6. A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária.
>
> 7. Nessa fase de compartilhamento do IP, a individualização da navegação na internet passa a ser intrinsecamente dependente da porta lógica de origem, até a migração para o IPv6.
>
> 8. A revelação das portas lógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP.
>
> 9. Recurso especial provido."
>
> (REsp 1784156/SP, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA TURMA, julgado em 05/11/2019, DJe 21/11/2019)

Levando-se em consideração o que já foi mencionado a respeito dos registros de conexão, bem como levando-se em consideração o art. 5º, VIII do Marco Civil, os registros de aplicação ou registros de acesso a aplicações de internet devem conter:

- Número IP (+ porta lógica, se houver "nateamento");
- Data e hora do uso no formato UTC;

Excepcionalmente, o dever de guarda dos registros de aplicação poderá abranger outras espécies de provedores de aplicação, como, por exemplo, os que sejam pessoas naturais ou os que forem constituídos como pessoas jurídicas que não explorem a atividade empresarial, desde que sejam atendido três requisitos:

a) **exista uma ordem judicial determinando essa obrigação**, podendo decorrer de um juízo criminal, civil ou trabalhista;

b) **que seja por prazo determinado**: muito embora o legislador não tenha definido qual seria esse prazo, deve-se entender que

não poderá ser superior ao do *caput*, de 6 meses, sob pena de se ofender a isonomia;

c) **que os registros sejam relativos à fatos específicos**: o registro não deve ser realizado de forma indiscriminada, mas apenas dos serviços relacionados à prova.

Muito embora o Marco Civil seja silente, os ônus financeiros da estruturação do sistema de registros de aplicação deverão ser suportados pelo requerente.

Há uma diferença entre esses dois dispositivos: no *caput*, determina-se o registro e o armazenamento para que, em havendo um ilícito, esses dados permitam a identificação do possível causador. No § 1º, o registro é feito com vistas ao futuro: para uma conduta que irá ser realizada. Nesse caso, não se deve trabalhar com "futurologia", mas com probabilidades.

Imagine, por exemplo, que uma pessoa natural tenha criado um site com um fórum de discussão sobre dicas de viagens. Certo dia, surge um usuário que que, reiteradamente, ofende os demais colegas. Como o cadastro que ele preencheu era falso, e o site não era obrigado a armazenar os registros de aplicação, não há provas para individualizar esse agressor.

Como se acredita que ele irá "atacar" novamente, o ofendido requer que o dono do site instale um sistema de registro de aplicações, de forma a poder identificar o número IP daquele usuário "problemático".

Logo, o a hipótese do § 1º é para registrar uma conduta lesiva que tenha grande probabilidade de ocorrer, **como no caso de reiteração**.

O Marco Civil trata de forma idêntica à do registro de conexão as questões relativas à requisição de armazenamento (§ 2º)[92], à cláusula de reserva de jurisdição para o acesso ao conteúdo (§ 3º), bem como às sanções (§ 4º), razão pela qual se remete o leitor para a seção correspondente.

---

92. Os grandes provedores de aplicação possuem portais próprios para atender as solicitações e requisições das autoridades policiais e Ministério Público:
    a) Facebook – *https://www.facebook.com/records*
    b) WhatsApp – *https://www.whatsapp.com/records/*
    c) Google – *https://lers.google.com/*
    d) Microsoft – *https://lers.google.com/*

    Outros, como a Apple, estabelecem suas interações com as autoridades por *email*: *lawenforcement@apple.com*. O Zoom possui um formulário em uma página Web: *https://zoom.us/trust=-form/?enter-Law%20Enforcement%20Request*.