NOVA SISTEMÁTICA DA PROTEÇÃO À INTIMIDADE

Fábio de Macedo Soares Pires Condeixa*

Resumo

O presente trabalho pretende abordar o regime jurídico brasileiro de proteção de dados relativos à intimidade e à privacidade do cidadão, com especial enfoque nas inovações trazidas pela Lei de Uso da Internet e pela Lei das Organizações Criminosas com relação aos registros de dados telefônicos, da internet e de viagens.

Juntamente com o avanço da tecnologia da informação e das comunicações vem a exposição da intimidade dos indivíduos. Os bancos de dados com informações pessoais proliferam-se a cada dia, tanto no âmbito das empresas do setor privado quanto das instituições governamentais, sem que, muitas vezes, haja a proteção necessária à privacidade das pessoas.

O ordenamento jurídico brasileiro, como todos ou quase todos os outros, prevê o respeito e a proteção à intimidade individual, ainda que, como sabemos, nem sempre essa proteção chegue a se efetivar [...]

O ordenamento jurídico brasileiro, como todos ou quase todos os outros, prevê o respeito e a proteção à intimidade individual, ainda que, como sabemos, nem sempre essa proteção chegue a se efetivar; é comum e até banal a violação a esse direito fundamental.

Com a edição das leis do Marco Civil da Internet e de organizações criminosas, foram trazidas, nesta seara, muitas inovações que, certamente, trarão muitas consequências de ordem prática.

A intimidade na constituição e no direito internacional

A Constituição Federal (CF) é o mais alto diploma normativo da República Federativa do Brasil; e orienta os demais e prevalece sobre eles. O seu art. 5º traz os

* É bacharel em direito e mestre em ciência política pela Universidade Federal do Rio de Janeiro (UFRJ). Oficial de Inteligência, atuando como professor e pesquisador da Escola de Inteligência da Agência Brasileira de Inteligência (ESINT/ABIN), autor de diversos artigos e dos livros Princípio da Simetria na Federação Brasileira (Lumen Juris, 2011) e Direito Constitucional Brasileiro (Lumen Juris, 2014).

direitos e garantias fundamentais, que, no jargão estadunidense, são chamados de direitos civis (*civil rights*). Entre eles, está o direito à liberdade (de expressão, de locomoção e de associação), à igualdade, à propriedade e à *intimidade* ou *privacidade*, que ora nos interessa.

Na doutrina jurídica, alguns autores costumam diferenciar intimidade de privacidade, ao afirmarem que a primeira "relaciona-se às relações subjetivas e de trato íntimo da pessoa, suas relações familiares e de amizade, enquanto vida privada envolve todos os demais relacionamentos humanos, inclusive os objetivos, tais como relações comerciais, de trabalho, de estudo etc".[1] Não obstante, tal distinção encerra escassa repercussão prática, razão pela qual optamos por usar os termos indistintamente neste trabalho.

O principal dispositivo sobre a proteção à privacidade da CF é o seu art. 5º, X, que dispõe o seguinte:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> [...]
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 1988).

Essa proteção genérica da privacidade desdobra-se em outras duas mais específicas, previstas dois incisos seguintes, que tratam, respectivamente, da inviolabilidade do domicílio e das comunicações. Assim, a proteção do direito à intimidade ou privacidade na CF divide-se em três grupos: 1) geral (imagem, dados, informações, etc.); 2) domicílio; e 3) comunicações.[2]

No direito internacional encontramos algumas disposições semelhantes. A Declaração Universal dos Direitos Humanos (DUDH)[3] traz a seguinte provisão de proteção à privacidade:

> **Artigo XII**
>
> Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.

Como se acreditava, entre os juristas, que tal declaração não tinha valor vinculante, isto é, não obrigava os Estados-membros da ONU, firmou-se o Pacto Internacional dos Direitos Civis e Políticos (PIDCP)[4] – este, sim, de observância obrigatória –, que trazia dispositivo semelhante:

1 MORAIS, Alexandre de. Direito Constitucional. São Paulo: Atlas, 2000. p. 73

2 Há controvérsia sobre a proteção do inciso XII refere-se ao sigilo de dados ou da comunicação de dados, prevalecendo, contudo, esta última posição, à qual nos filiamos.

3 Adotada e proclamada pela Resolução n° 217 A (III) da Assembléia-Geral das Nações Unidas, em 10 de dezembro de 1948 (NAÇÕES UNIDAS, 1948).

4 O PIDCP foi adotado em sessão da Assembléia-Geral das Nações Unidas em 1966, mas só veio a entrar em vigor, para o Brasil, quase trinta anos depois, tendo sido incorporado ao ordenamento jurídico pátrio pelo Decreto Presidencial n° 592, de 6 de julho de 1992 (BRASIL, 1992a).

> **Artigo 17**
>
> 1. Ninguém poderá ser objetivo de ingerências arbitrárias ou ilegais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais às suas honra e reputação.
>
> 2. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

Mais especificamente no âmbito da Organização dos Estados Americanos (OEA), foi firmada a Convenção Americana de Direitos Humanos (CADH), também conhecida como Pacto de San José da Costa Rica.[5] Esse tratado internacional é uma das bases do sistema interamericano de proteção aos direitos humanos e prevê, no tocante à privacidade, o seguinte:

> **Artigo 11 - Proteção da honra e da dignidade**
>
> 1. Toda pessoa tem direito ao respeito da sua honra e ao reconhecimento de sua dignidade.
>
> 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
>
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

Ambos o PIDCP e a CADH proíbem a prática de "ingerência arbitrária na vida privada, na família, no domicílio e na correspondência". Especificamente quanto ao sistema interamericano de proteção aos direitos humanos, a violação dessa proibição, por parte de Estado-membro, pode acarretar sua responsabilização perante a Côrte Interamericana de Direitos Humanos (CIDH) para indenizar a vítima.

Recordemos que tanto o PIDCP quanto a CADH são tratados internacionais sobre direitos humanos, que, de acordo com a orientação do Supremo Tribunal Federal (STF), gozam de "status normativo supralegal", isto é, na hierarquia normativa pátria, esses tratados estão acima das leis, sujeitando-se, no plano interno, apenas à CF.[6]

Além da possibilidade de responsabilização civil (interna) e internacional do Estado, o agente público que viola o direito à intimidade também pode responder nas esferas administrativa (funcional/disciplinar), cível (patrimonial) e criminal. O particular que viole o direito de privacidade de outrem também estará sujeito a sanções de natureza civil e penal e, às vezes, também administrativa.

Proteção legal da intimidade

Como estabelece o inciso X do art. 5º da CF, "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". Ao estabelecer a possibilidade de indenização por dano moral ou material, a própria CF prevê a respon-

[5] A CADH foi assinada em 1969, mas só entrou em vigor internacionalmente em 1978. Para o Brasil, internamente, o tratado só entrou em vigor 23 anos depois de sua assinatura, tendo sido definitivamente incorporado ao ordenamento jurídico pátrio pelo Decreto Presidencial n° 678, de 6 de novembro de 1992 (BRASIL, 1992b).

[6] STF. Recurso Extaordinário n° 349.703/RS. Plenário, relator Min. Gilmar Mendes. DJ, 5 .6.2009. (BRASIL, 2009a).

sabilização civil daquele que viola o direito de privacidade, seja agente público ou particular. O Código Civil (BRASIL, 2002, arts. 20 e 21) reforça a provisão e lhe acrescenta a possibilidade de tutela judicial inibitória.

[...] são consideravelmente numerosas e amplas as hipóteses de exceções à confidencialidade das informações pessoais, deixando-se, assim, uma vasta margem de discricionariedade ao agente público detentor delas para revelá-las.

A Lei de Acesso à Informação (LAI), Lei Federal nº 12.527 (BRASIL, 2011), prevê a proteção às informações que estiverem em poder do Estado relativas à intimidade, vida privada, honra e imagem das pessoas. Esse tipo de informação foi chamado pela lei de *informação pessoal* (art. 31). A maioria dos órgãos públicos detém esse tipo de informações nas suas bases de dados, pois estas abrangem toda sorte de dados pessoais, como nome, filiação, endereço, ocupação, renda, patrimônio, laudos médicos, litígios familiares, etc.

A LAI estabelece o prazo de 100 anos para a restrição de acesso às informações pessoais (art. 31, § 1º, I), que só poderão ser divulgadas antes disso com consentimento expresso da pessoa a quem se referem. Em razão disso, o Poder Público deve tomar todas as medidas necessárias para assegurar confidencialidade. A lei, no entanto, afasta a necessidade de consentimento para a revelação das informações pessoais em algumas hipóteses, como no caso de realização de estatísticas e pesquisas científicas, de prevenção e diagnóstico médico, cumprimento de ordem judicial, de defesa dos direitos humanos e de proteção do interesse público e geral preponderante (art. 31, § 3º).

Vê-se, pois, que são consideravelmente numerosas e amplas as hipóteses de exceções à confidencialidade das informações pessoais, deixando-se, assim, uma vasta margem de discricionariedade ao agente público detentor delas para revelá-las.

Não devemos confundir o sigilo das informações pessoais com outras modalidades de sigilo previstas na lei. Há casos em que o sigilo não visa à proteção da intimidade, mas, sim, à segurança da sociedade ou do Estado, como ocorre com a classificação sigilosa[7] ou com o segredo de justiça fundado no interesse público.[8]

[7] As informações sigilosas classificadas podem ser reservadas, secretas ou ultra-secretas, com os prazos máximos de restrição de acesso de cinco, 15 e 25 anos, respectivamente, podendo este último ser prorrogado por igual período uma única vez. As informações classificadas como reservadas cuja divulgação possa colocar em risco a segurança do presidente e vice-presidente da República e respectivos cônjuges e filhos podem permanecer sigilosas por mais de cinco anos, no caso reeleição (BRASIL, 2011, art. 24, § 2°).

[8] O art. 155, I, do Código de Processo Civil prevê a tramitação de processos em segredo de justiça quando houver interesse público para tanto, como ocorre nas investigações criminais sigilosas (BRASIL, 1973).

A Lei de Acesso à Informação determinou que fosse editado regulamento para detalhar as normas sobre o tratamento da informação pessoal, mas a matéria ainda se encontra pendente de regulamentação, embora a referida lei já tenha sido regulamentada por dois decretos presidenciais – um sobre o acesso à informação (Decreto nº 7.724 (BRASIL, 2012a)) e o outro sobre o tratamento da informação sigilosa classificada (Decreto nº 7.845 (BRASIL, 2012b)).[9]

A violação do sigilo das informações pessoais por parte de agentes públicos pode ensejar o enquadramento no delito do art. 325 do Código Penal[10] (BRASIL, 1940).

Na esfera administrativa, a revelação indevida de informações pessoais por agente público é considerada ilícita e deve ser tratada como transgressão militar média ou grave, no caso de ter sido cometida por militar das Forças Armadas no exercício de suas funções, ou, no caso de servidor público civil federal, como infrações administrativas apenadas, no mínimo, com suspensão, podendo ainda o servidor responder pela Lei de Crimes de Responsabilidade (Lei Federal nº 1.079 (BRASIL, 1950)) e/ou pela Lei de Improbidade Administrativa (Lei Federal nº 8.429 (BRASIL, 1992c)). Servidores estaduais, municipais e distritais responderão na forma dos seus respectivos estatutos.

O Decreto nº 7.724 (BRASIL, 2012a) prevê, no âmbito do Poder Executivo Federal, a multa de mil a 200 mil reais para o servidor ou pessoa natural com qualquer outro tipo de vínculo com o Poder Público por infrações ao dever de sigilo ou de divulgação da informação (art. 66). Prevê, ainda, sanção de advertência e rescisão do vínculo com o Poder Público.

No plano cível, o art. 34 da LAI (BRASIL, 2011) prevê não apenas a possibilidade de responsabilização do Estado, como também o direito de regresso deste contra o agente público responsável pela divulgação indevida, nos casos de dolo ou culpa. Recordemos que o direito de regresso do Estado contra agente por prejuízo por ele causado encontra assento no art. 37, § 6º, da CF.

E as informações pessoais em poder de pessoas ou entidades privadas? A LAI não se lhes aplica.[11] Entretanto, no tocante especificamente aos dados cadastrais, a Lei de Organizações Criminosas trouxe inovações que serão vistas adiante (BRASIL, 2013).

[9] No Grupo de Trabalho sobre a regulamentação da Lei de Acesso à Informação – do qual tivemos a honra de participar - , destacamos a necessidade de regulamentar o tratamento das informações pessoais, mas se entendeu que esse regramento deveria constar de instrumento próprio.

[10] No caso de militar, aplica-se o art. 326 do Código Penal Militar (BRASIL, 1969). Em linhas gerais, aplica-se esse código quando o crime é praticado por militar em situação de atividade.

[11] O art. 2° da lei permite, contudo, que suas disposições sejam aplicadas a "entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres" (BRASIL, 2011).

Há ainda uma discussão sobre o chamado "direito ao esquecimento", que consiste no direito da pessoa de não ter eternamente exposto ao público em geral um fato sobre determinado momento de sua vida [...]

A rigor, alguém que se sinta lesado por esse tipo de conduta pode, em tese, propor ação indenizatória, pois a aplicabilidade do art. 5º, X, da CF é imediata, isto é, independe de norma regulamentadora, por força do parágrafo 1º do mesmo artigo. Todavia, o fato é que, na prática, o que se vê é que as vítimas – cidadãos e consumidores – permanecem indefesas contra essas ações.

Não obstante, é sabido que há um imenso comércio de dados pessoais entre instituições financeiras e comerciais. Essas informações são utilizadas para diversas finalidades, entre as quais se destaca a oferta de produtos e serviços por mala-direta, e-mail, telefone, entre outros. Em face disso, tramita, na Câmara dos Deputados, o Projeto de Lei nº 4.060 (BRASIL, 2012c), que dispõe justamente sobre a proteção aos dados pessoais. Segundo nos informa Patrícia Eliane da Rosa Sardeto, diversos países na Europa e na América Latina já dispõem de instrumentos legais dessa natureza.[12]

Há ainda uma discussão sobre o chamado "direito ao esquecimento", que consiste no direito da pessoa de não ter eternamente exposto ao público em geral um fato sobre determinado momento de sua vida, ainda que verídico e público, de modo a lhe causar sofrimento e transtornos. Essa discussão ganhou bastante repercussão com o caso Lebach, de 1966, em que o Tribunal Constitucional Federal alemão acatou pedido de ex-condenado por homicídio para impedir emissora de TV de transmitir documentário sobre o crime. Com o advento da internet e o armazenamento indefinido de informações por provedores de aplicações como Google e Facebook, tal questão ganha ainda mais relevo. No Brasil, mesmo sem previsão legal, esse tipo de proteção já foi concedido pelo Superior Tribunal de Justiça (STJ).[13]

Vistas essas considerações gerais sobre o direito à intimidade, passemos à análise da nova sistemática legal dos dados cadastrais e telefônicos e dos registros de viagens e de internet.

Dados cadastrais

A nova Lei de Organizações Criminosas (BRASIL, 2013a) trouxe inovações no tocante aos dados cadastrais dos indivíduos. O art. 15 da lei admite que o delegado de polícia ou o membro do Ministério Público tenham, para fins de investigação

[12] A produção de dados pessoais em debate no Brasil. (SARDETO, 2013).

[13] STJ. Recurso Especial n° 1.335.153/RJ, da 4ª Turma, rel. min. Luís Salomão, DJ 10.9.2013 (BRASIL, 2013b). No mesmo sentido, Enunciado n° 531 do Conselho da Justiça Federal (BRASIL, 2013c).

criminal, acesso a informações sobre a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de internet e administradoras de cartão de crédito, *independentemente de autorização judicial*.

Ressalte-se que os dados passíveis de obtenção sem autorização judicial são apenas aqueles relativos à qualificação pessoal, à filiação e ao endereço, excluindo-se os demais dados mantidos pela entidade. Assim, por exemplo, uma empresa telefônica só está obrigada a transmitir, sem autorização judicial, aquelas informações sobre a qualificação pessoal, a filiação e o endereço do cliente, mas não pode fazê-lo quanto aos registros das suas ligações. O mesmo se pode dizer quanto às instituições financeiras e aos dados bancários dos clientes.

Questão que pode se colocar é com relação à abrangência da aplicabilidade do art. 15. Tendo em vista que o dispositivo consta de uma lei voltada à investigação de crimes que envolvem organização criminosa, seria o caso de se perguntar: o acesso direto a dados cadastrais pela polícia e pelo Ministério Público se dará apenas no caso de investigação de crimes que, de alguma maneira, envolvam organizações criminosas? A questão é controvertida. Luiz Flávio Gomes entende que sim, mas, majoritariamente, a leitura é que os meios de obtenção de prova previstos na Lei de Organizações Criminosas aplicam-se à apuração de qualquer infração penal.[14]

O sigilo dos dados telefônicos não se confunde com o sigilo das comunicações telefônicas. Os dados telefônicos consistem apenas no registro de ligações, sem qualquer acesso ao conteúdo das conversações.

Consoante disposição do art. 21 da lei, a negativa de se transmitir diretamente ao delegado ou ao Ministério Público os dados cadastrais configura crime, assim como a transmissão indevida dessas informações.

Embora o conceito de *dados cadastrais* da Lei de Organizações Criminosas abranja as informações mantidas pela Justiça Eleitoral, entendemos que, pelo princípio da especialidade e em respeito à isonomia, a divulgação indevida praticada pelos seus servidores constituirá o delito do art. 325 do Código Penal, e não o crime do art. 21, parágrafo único.

A Lei de Uso da Internet (Lei Federal nº 12.965 (BRASIL, 2014)), no seu art. 10, § 3º, ratificou a possibilidade de transmissão direta de dados cadastrais à polícia e ao Ministério Público ao dispor sobre a proteção dos registros relativos à internet.

Antes mesmo da edição da Lei de Organizações Criminosas, o STJ já havia se

[14] PEREIRA, Filipe Martins Alves; SILVA, Rafael de Vasconcelos. Análise jurídica da Nova Lei de Organizações Criminosas. Disponível em: http://www.atualidadesdodireito.com.br. Acesso em: 20 maio 2014.

posicionado no sentido da dispensa de autorização judicial para a obtenção, pela autoridade policial, de dados cadastrais, como o endereço de determinada pessoa.[15]

Dados telefônicos

O sigilo dos dados telefônicos não se confunde com o sigilo das comunicações telefônicas. Os dados telefônicos consistem apenas no registro de ligações, sem qualquer acesso ao conteúdo das conversações. Esses registros têm sido designados como "metadados".

É pacífico na jurisprudência do STF que a quebra do sigilo de dados telefônicos só pode acontecer mediante autorização judicial ou requisição de Comissão Parlamentar de Inquérito (CPI) no âmbito do Congresso Nacional ou de uma das suas casas, devido aos poderes de investigação próprios das autoridades judiciais que lhes confere o art. 58, § 3º, da CF[16]. À semelhança do que ocorre com os sigilos fiscal e financeiro, o poder de investigação também é reconhecido pelo STF às CPIs instauradas no âmbito das assembléias legislativas estaduais[17], mas não àquelas no âmbito das câmaras municipais de vereadores.[18]

A Lei de Organizações Criminosas determina, no seu art. 17, que as empresas de telefonia guardem os registros de ligações telefônicas pelo prazo de cinco anos. Curioso que a lei fala em manter os dados telefônicos "à disposição das autoridades mencionadas no art. 15" (delegado de polícia e membro do Ministério Público), dando a entender que a outorga judicial seria dispensável. Parece que a intenção do legislador foi deixar uma janela aberta para o futuro, sem dispensar expressamente a outorga judicial, o que, na atual conjuntura, ocasionaria a impugnação imediata do dispositivo.

Ademais disso, a manutenção dos registros telefônicos por um período tão longo aumenta bastante as chances do acesso indevido.

Registros de viagens

Especificamente quanto aos registros de viagens e de reservas de viagens, a Lei de Organizações Criminosas determinou que as empresas de transporte devem manter os dados acessíveis diretamente

[15] STJ. Recurso Especial n° 83.824/BA, 3ª Turma, rel. Min. Eduardo Ribeiro, DJ 17.5.1999 (BRASIL, 1999); Embargos de Declaração no Recurso em Mandado de Segurança n° 25.375/PA, 5ª turma, rel. Min. Félix Fischer, DJ, 2.2. 2009 (BRASIL, 2008).

[16] Mandado de Segurança nº 24.817/DF, Plenário, rel. Min. Celso de Mello, DJ, 06.11.2009 (BRASIL, 2009b).

[17] Ação Civil Originária nº 730/RJ, Plenário, rel. Min. Joaquim Barbosa, DJ, Brasília, DF, 11.11.2005 (BRASIL, 2004). Contudo especula-se que o STF possa mudar sua orientação no julgamento da Ação Civil Originária n° 1.390/RJ, rel. min. Marco Aurélio, em tramitação (BRASIL, 2009c).

[18] STF. Recurso Extraordinário n° 96.049/SP, 1ª turma, rel. min. Oscar Corrêa, DJ, 19.3.1983 (BRASIL, 1983).

às autoridades acima referidas e ao juiz pelo prazo de cinco anos (art. 16).

Ao estabelecer o prazo mínimo de cinco anos para a manutenção de registros de viagens e de reservas – assim como o fez para os registros telefônicos –, a Lei de Organizações Criminosas foi bem além do seu escopo, pois, uma vez disponíveis os dados, o acesso às informações poderá ser franqueado pela Justiça em qualquer processo judicial ou procedimento investigativo de CPI. Além disso, como já mencionado, a guarda dos dados por tanto tempo os expõe mais ao acesso ilícito e desautorizado.

Registros de conexão e de aplicação da internet

A Lei de Uso da Internet, Lei Federal nº 12.965 (BRASIL, 2014), também conhecida como Marco Civil da Internet, trouxe uma série de inovações no tocante à intimidade, naquilo que tange a rede mundial de computadores. No seu art. 7º, a lei estabelece uma sistemática de proteção à intimidade semelhante à que se encontra na CF, com uma cláusula geral prevendo o direito de indenização e dois desdobramentos: um relativo ao fluxo de comunicações e outro às comunicações armazenadas. Nestes dois últimos casos, a lei exige autorização judicial para violação do sigilo.

O inciso II do art. 7º refere-se à interceptação das comunicações telemáticas, hipótese abrangida pelo art. 5º, XII, da CF e pela Lei das Interceptações (Lei Federal nº 9.296 (BRASIL, 1996)). Essa lei incide tanto sobre as comunicações telefônicas quanto sobre o fluxo de comunicações em sistemas de informática e telemática (art. 1º, *caput* e parágrafo único).

As "comunicações armazenadas", referidas no inciso III, são justamente os registros de conexão à internet e de acesso a aplicações de internet. Aí é onde a Lei de Uso da Internet mais inova no tocante à privacidade na internet, chegando até a contrariar orientação consolidada da jurisprudência. Mas antes de adentrarmos na questão, é preciso distinguir esses dois tipos de registro.

Os *registros de acesso a aplicação da internet* consistem nas *ações virtuais* praticadas no mundo da internet, ao passo que os *registros de conexão à internet* apenas identificam de qual computador partiram tais ações. Veremos que cada tipo de registro recebe um tratamento da lei. A Lei de Uso da Internet conceitua cada um da seguinte forma (BRASIL, 2014, art. 5º, VI e VII):

> Registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados.
>
> Aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet.

Antes da promulgação da Lei de Uso da Internet, o STJ havia se manifestado no sentido de que os dados do usuário de Protocolo de Internet (*Internet Protocol* – IP), isto é, os registros de conexão, não

eram resguardados pelo sigilo.[19] Assim, a côrte entendeu não ser necessária a autorização judicial para a requisição de dados sobre a identificação e o endereço físico de terminal de computador.

[...] ao impor a necessidade de autorização judicial a lei criou um obstáculo à divulgação dos registros de conexão, por outro ampliou sobremaneira a possibilidade do acesso, ao obrigar os provedores de internet a guardarem tais registros pelo prazo mínimo de um ano.

Não obstante, a Lei de Uso da Internet, ao regular a matéria, impôs a necessidade de autorização judicial para a divulgação desses dados, bem como dos registros de aplicação da internet (BRASIL, 2014, art. 7º, III, art. 10, § 1º, art. 13, § 5º e art. 15, § 3º).

Se, por um lado, ao impor a necessidade de autorização judicial a lei criou um obstáculo à divulgação dos registros de conexão, por outro ampliou sobremaneira a possibilidade do acesso, ao obrigar os provedores de internet a guardarem tais registros pelo prazo mínimo de um ano.

Assim, os provedores de internet não apenas têm de ter à disposição os registros de conexão pelo prazo de um ano, como também estão proibidos de terceirizar a sua manutenção, e devem, ainda, mantê-los em ambiente controlado e de segurança, na forma de decreto presidencial a ser editado. Sem dúvida, essa obrigação implicará aumento de custos dos provedores, que, naturalmente, será repassado aos consumidores.

Portanto, por mais que a exigência de autorização judicial – antes dispensada pelos tribunais – possa parecer ter aumentado a privacidade do usuário da internet, o fato é que, com a obrigação de manutenção de registros, todas as conexões à internet, assim como os acessos a aplicações, ficarão guardadas por prazo determinado. Na situação anterior, por mais que a autoridade policial ou o Ministério Público pudessem acessar diretamente os registros, podia acontecer de esses registros não mais existirem, logo, a privacidade estaria, forçosamente, resguardada.[20]

Talvez o maior problema da manutenção compulsória dos registros no tocante à intimidade seja o fato de que, por mais que a lei imponha cuidados com a guarda e penalidades para a sua violação, as informações sempre estarão sujeitas ao acesso desautorizado ou à transmissão

[19] Habeas-corpus n° 83.338/DF, da 6ª Turma, rel. Min. Hamilton Carvalhido. DJ, 26.10.2009 (BRASIL, 2009d); Carta Rogatória n° 297, Min. Rafael Monteiro. DJ, 29.09 2006 (BRASIL, 2006).

[20] Anteriormente, cada provedor, fosse de conexão ou de aplicação, estabelecia sua própria política de privacidade do usuário. Assim, alguns provedores entregavam os registros à autoridade policial e ao Ministério Público diretamente, mediante mera solicitação; outros, por sua vez, negavam-se a entregar os dados, fazendo-o apenas mediante autorização judicial.

clandestina. Se os registros não fossem guardados, não se correria esse risco.

O mesmo se aplica aos registros de acesso a aplicação da internet, com a diferença de que o prazo para a sua guarda é inferior, de apenas seis meses (BRASIL, 2014, art. 15º, *caput*),

Como o prazo de manutenção dos registros de conexão não é muito longo – apenas um ano –, a lei permite que a autoridade requeira, cautelarmente, a prorrogação do período de manutenção do registro, a fim de que possa providenciar, no prazo de 60 dias, a autorização judicial para obtê-lo (BRASIL, 2014, art. 13º, §§ 2º a 4º). O mesmo se aplica aos registros de aplicação (BRASIL, 2014, art. 15º, § 2º).

Convém destacar que, em ambos os casos dos registros de conexão e de aplicação, a lei faz menção à possibilidade de divulgação mediante ordem judicial. Mas quem teria legitimidade para requerer esta ordem? Segundo o art. 22 da lei, qualquer parte interessada poderá requerer ao juiz o fornecimento de registros de conexão ou de acesso a aplicações de internet.

Dito de outro modo, diferentemente do que ocorre com as interceptações das comunicações – cabíveis apenas na jurisdição criminal –, a quebra do sigilo dos registros de internet pode ser feita também em processos cíveis.

Até mesmo o pedido cautelar de manutenção do registro além do prazo da lei, previsto nos arts. 13º, § 2º, e 15º, § 2º, pode ser feito não apenas pela autoridade policial e pelo Ministério Público – que atuam na jurisdição criminal –, como também, diz a lei, por *autoridade administrativa*. Assim, por exemplo, autoridade da Receita Federal pode requerer a manutenção de registros de conexão e aplicação da internet a fim solicitá-lo judicialmente para instruir procedimento fiscal-tributário ou execução fiscal. Já quanto ao particular, não vemos óbice para o ajuizamento de medida cautelar com o mesmo objetivo, e há previsão expressa dessa possibilidade quanto aos registros de aplicações (art. 15º, § 1º).

A violação da privacidade do usuário pelo provedor, seja ele de conexão ou de aplicação, pode ensejar responsabilidade civil, penal e administrativa. A Lei de Uso da Internet traz, algumas penalidades de natureza administrativa, quais sejam:

> - Advertência, com indicação de prazo para adoção de medidas corretivas;
>
> - Multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> - Suspensão temporária ou proibição das atividades que envolvam operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações em território nacional; [...] (BRASIL, 2014, art. 12º)

A lei só se esqueceu de apontar a autoridade administrativa (governamental) responsável pela aplicação de tais penalidades. O diploma legal também proíbe que, contratualmente, os provedores se

eximam do dever de resguardar a privacidade dos usuários (art. 8º, I).

Se terceiro acessar esses dados remotamente, com violação de mecanismo de segurança (*hacker*), poderá responder criminalmente, em virtude da chamada Lei Carolina Dieckmann (Lei Federal nº 12.737 (BRASIL, 2012c)). Essa lei inseriu, no Código Penal, o crime de invasão de dispositivo informático alheio (art. 154-A) e decorreu da polêmica acerca da obtenção e divulgação desautorizadas de 36 fotos da atriz nua mantidas no seu computador pessoal. À época, não havia crime específico para aquela conduta, razão pela qual os seus autores foram enquadrados nos delitos de furto, extorsão e difamação, segundo a imprensa. Atualmente, tal conduta poderia ser enquadrada no dispositivo do art. 154-A do Código Penal.

O dispositivo abrange tanto a conduta dos particulares quanto de agentes públicos. Estes últimos, quando necessitarem de informações contidas em dispositivos informativos para investigações, podem socorrer-se do pedido judicial de busca e apreensão, para apreendê-los fisicamente.[21] A despeito disso, não enxergamos óbice para que o juiz autorize a invasão informática remota, caso a medida se mostre mais apropriada à situação. Nessa hipótese, não se configurará o delito do art. 154-A por não se caracterizar como *indevida* a violação.

Recordemos que, para a configuração do crime do art. 154-A, é necessário que haja: 1) violação de mecanismo de segurança (*firewall, anti-vírus,* etc.); *e* 2) a finalidade de: 2.1) obter, adulterar ou destruir dados ou informações desautorizadamente; *ou* 2.2) instalar vulnerabilidades para obter vantagem ilícita (*key logger*, cavalo de tróia, etc.).

Não se deve confundir o crime do art. 154-A com as figuras delituosas dos arts. 313-A e 313-B do Código Penal. Estes últimos são crimes praticados por servidor público e consistem em inserir dados falsos em sistemas informatizados ou bancos de dados da Administração Pública, ou modificá-los ou alterá-los desautorizadamente.

Conclusão

Vimos, portanto, que tanto a Lei de Organizações Criminosas quanto a Lei de Uso da Internet trouxeram inovações bastante significativas, chegando, no caso dos registros de conexões à internet, a contrariar jurisprudência consolidada do STJ.

As principais mudanças aqui destacadas foram, portanto: 1) a necessidade de autorização judicial para a entrega de registros de conexão à internet e de acesso a aplicações da internet à polícia e ao Ministério Público; e 2) a exigência de manutenção de registros telefônicos, de viagens e das suas reservas, de co-

[21] STF. Recurso Extraordinário n°418.416/SC, Plenário, rel. Min. Sepúlveda Pertence. DJ, 19 dez. 2006 (BRASIL, 2006b).

nexão à internet e de acesso a aplicação da internet, pelos prazos de cinco anos para os dois primeiros, de um ano para o terceiro e de seis meses para o último. Vimos também que essa exigência implicará custos que, necessariamente, serão repassados ao consumidor.

Com relação aos dados cadastrais, embora se trate de uma novidade na lei, a entrega à autoridade policial e ao Ministério Público sem autorização judicial já era uma realidade avalizada pela jurisprudência do STJ. A novidade, nesse particular, foi a previsão de um crime específico de recusa da entrega e de divulgação indevida desse tipo de dado.

Essas inovações, do ponto de vista jurídico, mostram-se como um incremento à proteção da intimidade individual com relação ao que era praticado anteriormente. Todavia, ao estabelecerem a exigência de manutenção de registros, as leis, além de aumentarem os custos para o consumidor, ampliarão significativamente a possibilidade de acesso, autorizado e desautorizado, aos registros telefônicos, de viagens e de internet.

Referências

BRASIL. Código Civil (2002). Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>.

BRASIL. Código de Processo Civil (1973). Lei no 5.869, de 11 de janeiro de 1973. Institui o Código de Processo Civil. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/ l5869.htm>.

BRASIL. Código Penal (1940). Decreto-lei nº 2.848, de 7 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>.

BRASIL. Código Penal Militar (1969). Decreto-lei nº 1.001, de 21 de outubro de 1969. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del1001Compilado.htm>.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/ConstituicaoCompilado.htm>

BRASIL. Decreto nº 592, de 6 de julho de 1992a. Atos Internacionais. Pacto Internacional sobre Direitos Civis e Políticos. Promulgação. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm>.

BRASIL. Decreto nº 678, de 6 de novembro de 1992b. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm>.

BRASIL. Decreto nº 7.724, de 16 de maio de 2012a. Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7724. htm>.

BRASIL. Decreto nº 7.845, de 14 de novembro de 2012b. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm>.

BRASIL. Lei nº 1.079, de 10 de abril de 1950. Define os crimes de responsabilidade e regula o respectivo processo de julgamento. Disponível em: <http://www.planalto.gov.br/ ccivil_03 /leis/ L1079consol.htm>.

BRASIL. Lei nº 8.429, de 2 de junho de 1992c. Dispõe sobre as sanções aplicáveis aos agentes públicos nos casos de enriquecimento ilícito no exercício de mandato, cargo, emprego ou função na administração pública direta, indireta ou fundacional e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L8429compilado. htm>.

BRASIL. Lei nº 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/ leis/l9296.htm>.

BRASIL. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012c. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/ _ato2011-2014/2012/lei/l12737.htm>.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013a. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei no 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm>.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_ato2011-2014/2014/lei/l12965.htm>.

BRASIL. Câmara dos Deputados. Projeto de Lei 4.060, de 13 de junho de 2012c. Dispõe sobre o tratamento de dados pessoais, e dá outras providências. Disponível em: < http://www2.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066>.

BRASIL. Conselho de Justiça Federal. Enunciado nº 531, de 12 de março de 2013c. A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Disponível em: <http://www.cjf.jus.br/cjf/CEJ-Coedi/jornadas-cej/vijornada. pdf>

BRASIL. Superior Tribunal de Justiça. *Carta rogatória nº 297*, Brasília, DF, 18 de setembro de 2006. Relator: Ministro Barros Monteiro. Disponível em: <http://www.conjur.com.br/ 2006- out-09/uol_fornecer_dados_usuario_justica_alema>.

BRASIL. Superior Tribunal de Justiça. *Embargos de Declaração no Recurso Mandado de Segurança nº 25.375/PA*, da 5ª Turma, Brasília, DF, 18 de novembro de 2008. Relator: Ministro Félix Fischer. Diário da Justiça Eletrônico, 2 fev. 2009. Disponível em: <https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA& sequencial=838243&num_registro=200702410579&data=20090202&formato=PDF>.

BRASIL. Superior Tribunal de Justiça. *Habeas corpus nº 83.338/DF*, da 6ª Turma, Brasília, DF, 26 de setembro de 2009d. Relator: Ministro Hamilton Carvalhido. Diário da Justiça Eletrônico, 26 out. 2009. Disponível em: <http://www.stj.jus.br/SCON/ jurisprudencia/doc.jsp?processo=83338&&b=ACOR&p=true&t=JURIDICO&l=10&i=2>.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 83.824/BA*, da 3ª Turma, Brasília, DF, 17 de maio de 1999. Relator: Ministro Eduardo Ribeiro. Disponível em: < https://ww2.stj.jus.br/processo/ita/documento/mediado/?num_registro=199500691329&dt_publicacao=17-05-1999&cod_tipo_ documento=>.

BRASIL. Superior Tribunal de Justiça. *Recurso Especial nº 1.335.153- RJ*, da 4ª Turma, Brasília, DF, 28 de maio de 2013b. Relator: Ministro Luis Felipe Salomão. Disponível em: < http://www.stj.jus.br/SCON/jurisprudencia/toc.jsp?tipo_visualizacao=null&livre=%28%22 LUIS+FELIPE+SALOM%3O%22%29.min.&processo=1335153&b=ACOR&thesaurus=JURIDICO>.

BRASIL. Supremo Tribunal Federal. *Ação Cível Originária nº 730/RJ*, Brasília, DF, 22 de setembro de 2004. Relator: Ministro Joaquim Barbosa. Diário da Justiça, 11 nov. 2005, p.5. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP = AC&docID=266125>.

BRASIL. Supremo Tribunal Federal. *Ação Cível Originária nº 1.390/RJ*, Brasília, DF, 25 de maio de 2009c. Relator: Ministro Marco Aurélio. Disponível em: <http://www.stf.jus.br/ portal/jurisprudencia/listarJurisprudencia.asp?s1=%28%281390%2ENUME%2E+OU+1390%2EDMS%2E%29%28%28MARCO+AUR%C9LIO%29%2ENORL%2E+OU+%28MARCO+AUR%C9LIO%29%2ENPRO%2E+OU+%28MARCO+AUR%C9LIO%29%2EDMS%2E%29%29+NAO+S%2EPRES%2E&base=baseMonocraticas&url=http://tinyurl.com/l3o3u9x>.

BRASIL. Supremo Tribunal Federal. *Mandado de Segurança nº 24.817/DF*, Brasília, DF, 5 de novembro de 2009b. Relator: Ministro Celso de Mello. Diário da Justiça Eletrônico, 6 nov. 2009. Disponível em: <http://www.stf.jus.br/portal/processo/ver ProcessoAndamento.asp?incidente=2205427>.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 96.049-SP*, da 1ª Turma, Brasília, DF, 30 de junho de 1983. Relator: Ministro Oscar Corrêa. Diário da Justiça, 19 ago. 1983, p. 12.195. Disponível em: <http://www.stf.jus.br/portal/ jurisprudencia/listarJurisprudencia.asp?s1=%2896049.NUME.+OU+96049.ACMS.%29& base=baseAcordaos&url=http://tinyurl.com/kf72xmo>.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 349.703-RS*, Brasília, DF, 5 de junho de 2009a. Disponível em: <http://www.stf.jus.br/portal/processo/ver ProcessoAndamento.asp?incidente=2035659>.

BRASIL. Supremo Tribunal Federal. *Recurso Extraordinário nº 418.416/SC*, Brasília, DF, . 19 de dezembro de 2006b. Relator: Ministro Sepúlveda Pertence. Disponível em: < http://www.stf.jus.br/portal/diarioJustica/verDiarioProcesso.asp?numDj=242&data PublicacaoDj=19/12/2006&incidente=2205705&codCapitulo=5&numMateria=43&cod Materia=1>.

MORAIS, Alexandre de. Direito Constitucional. São Paulo: Atlas, 2000.

NAÇÕES UNIDAS. Assembléia Geral das Nações Unidas. Declaração Universal dos Direitos Humanos. Disponível em: <http://www.onu.org.br/img/ 2014/09/DUDH.pdf>.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. Convenção Americana de Direitos Humanos, de 22 de novembro de 1969. Pacto de San José da Costa Rica. Disponível em: <http://www.pge.sp.gov.br/centrodeestudos/ bibliotecavirtual/instrumentos/sanjose.htm>.

SARDETO, Patricia Eliane da Rosa. *A proteção de dados pessoais em debate no Brasil*. In: Âmbito Jurídico: o seu portal jurídico na internet. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_ leitura&artigo_id=9455>. Acesso em: 15 maio 2013.