A INTIMIDADE E O ARMAZENAMENTO CAUTELAR DE CONEXÕES NO MARCO REGULATÓRIO DA INTERNET

THE INTIMITY AND INJUNCTIVE STORAGE OF CONNECTIONS IN INTERNET REGULATORY ACT

Pedro Lima Marcheri[1]

RESUMO: Este artigo busca a elucidar a constitucionalidade e adequação processual da medida de armazenamento cautelar do registro de conexões e acessos à aplicativos de Internet, introduzida pelo Marco Civil Regulatório em 2014. Para tanto é traçado um panorama da tutela constitucional da intimidade, privacidade e vida privada, com base no contexto atual de popularização no uso da Internet. Por meio de revisão bibliográfica, legislativa e jurisprudencial, apresentam-se aspectos teóricos e práticos das questões relativas ao armazenamento de tais dados no âmbito da investigação criminal e da violação do sigilo de acesso à rede mundial de computadores. Concluiu-se que a ausência de prazo para o armazenamento cautelar e a legitimação ativa da autoridade administrativa, sem qualquer regulamentação legal, ensejam a inconstitucionalidade da medida, havendo necessidade de aprimoramento. Ademais, o Marco Civil proporcionou um novo panorama da investigação de crimes eletrônicos, sendo que a obrigatoriedade no registro não necessariamente viola a intimidade.

PALAVRAS-CHAVE: Intimidade; *Internet*; Armazenamento Cautelar; Crimes Informáticos; Investigação.

ABSTRACT: This paper aims to elucidate the constitutionality and procedural adequacy of injunctive storage of connections and access to Internet applications, introduced by Internet Regulatory Act in 2014.To do so, is traced an overview of the constitutional protection of intimacy, privacy and private life, based on the current context of popularization the use of the Internet. Through a bibliographical, legislative and jurisprudential review, are presented theoretical and practical issues related to the storage of such data in the context of criminal investigation and the violation of secrecy aspect of access to the worldwide web. It was concluded that the absence of a deadline

[1] Doutorando em Direito pela Instituição Toledo de Ensino de Bauru – ITE. Mestre em Direito pelo Centro Universitário Eurípedes de Marília – UNIVEM. Pós-Graduando em Direito e Processo Penal pela Faculdade de Direito Damásio de Jesus. Advogado Criminalista.

for the injunctive storage and the active legitimacy of the administrative authority, without any legal regulation, generates the unconstitutionality of the measure, being necessary legal improvement. Furthermore, the Internet Regulatory Act provided a new landscape of electronic crime investigations, whereas obligation in the registry does not necessarily violate the intimacy

KEYWORDS: Intimacy; Internet; Injunctive Storage; Computer Crimes; Investigation.

INTRODUÇÃO

A incorporação das novas tecnologias no funcionamento do Estado e nas relações privadas tem proporcionado e ao mesmo tempo exigido do cidadão que informações pessoais sensíveis sejam transmitidas através da rede mundial de computadores. O próprio gerenciamento estatal é realizado, em boa parte, on-line e através da integração de diversos sistemas e bancos de dados; o denominado governo eletrônico ou e-gov.

A tutela constitucional à privacidade sofreu modificações conforme a evolução da sociedade, abrangendo novos aspectos como o sigilo eletrônico de dados e de acesso. Sua égide vem sendo progressivamente limitada por medidas legais que relativizam garantias do cidadão, sendo necessária a fixação de sua aplicabilidade no âmbito da *Internet*.

No ano de 2014 entrou em vigência no Brasil o Marco Regulatório da *Internet*, com o escopo de disciplinar os princípios, garantias direitos e deveres sobre o uso da rede mundial de computadores. À luz do direito brasileiro, o Marco trouxe à seara jurídica questões inéditas como a obrigatoriedade aos servidores em realizar o armazenamento dos registros de conexões e acesso à aplicativos de *Internet*. Ademais, além do monitoramento genérico, o Marco Regulatório também introduz a figura do armazenamento cautelar de tais registros, que constitui-se como medida investigatória específica para suspeito determinado.

A problemática proposta desemboca na reflexão do questionamento da pertinência constitucional da medida de armazenamento cautelar de conexões, em vistas à ausência de regulamentação quanto ao prazo e o rol de legitimados, e pretensa ofensa à garantia constitucional da intimidade.

Neste contexto, buscar-se-á, por meio de uma revisão bibliográfica, legislativa e jurisprudencial, analisar os aspectos jurídicos do armazenamento cautelar, sob uma dimensão constitucional, dando enfoque ao status jurídico conferido pela Constituição

Federal e pelo Marco Regulatório à intimidade, à luz do contexto social contemporâneo da *Internet*.

Para tanto, antes de analisar o enfoque processual da medida, necessário se torna promover o enfrentamento da contextualização da intimidade, da privacidade e da vida privada, nomeadamente no âmbito da investigação criminal em meio eletrônico, o que se fará a seguir.

1 O PARADIGMA DA PRIVACIDADE NA ORDEM JURÍDICA À LUZ DA INTERNET

Em um primeiro momento, a doutrina tenta sistematizar os conceitos de intimidade e privacidade. Nos dizeres de Ferraz Júnior (1993, p. 442) "a intimidade é o âmbito do exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance de sua vida privada, que por mais isolada que seja". Como parte integrante da dignidade humana, o âmbito privado encontra-se resguardado na égide dos direitos da personalidade humana, estando abarcado em seu conceito também as atividades e informações realizadas no meio eletrônico e na rede mundial de computadores.

Ratifica Marcacini (2002, p. 131), apregoando que o sigilo e a privacidade compõem a própria dignidade humana: "O direito ao sigilo e à privacidade são, entre nós, um aspecto dos chamados direitos da personalidade. Considerados pela doutrina como direitos absolutos, têm por finalidade proteger a dignidade da pessoa humana".

Pode-se ilustrar a vida social como um círculo maior, dentro do qual um menor, o da privacidade, que no interior seria aposto outro mais constrito e impenetrável, o da intimidade. À exemplo das relações bancárias, esta sorte de informação está contida dentro do círculo da privacidade, da mesma forma que seus relacionamentos profissionais e seu rol de clientes. Já os segredos mais íntimos, as dúvidas existenciais, a orientação sexual, comporiam o universo da intimidade (ARAÚJO, NUNES JÚNIOR, 2006).

Todas as Leis Maiores brasileiras já tutelavam a intimidade e a vida privada no âmbito constitucional. A evolução da tutela foi gradativa, de acordo com os seguintes dispositivos: Constituição do Império de 1824 (artigo 179 caput e incisos VII e XXVII); Constituição de 1891 (artigo 72 caput e parágrafos 11 e 18) asseguravam a

inviolabilidade domiciliar e da correspondência. A Carta de 1934 fez menção expressa as garantias da intimidade e vida privada (artigo 144), mantendo os direitos de sua antecessora. Nas constituições de 1937 (artigo 122), 1946 (artigos 141 e 144) e 1967 (artigo 150) foram mantidos o resguardo das constituições pretéritas. Com a promulgação da Constituição Cidadã de 1988, houve a garantia da inviolabilidade da intimidade, vida privada, honra e imagem, além da inviolabilidade da residência, o sigilo das correspondências, comunicações telegráficas, telefônicas e de dados (artigo 5º X, XI e XII), passando a tutela a constar do texto dos direitos e garantias fundamentais (SIMÓN, 2000).

A ordem constitucional contemporânea estabelece a égide sobre a privacidade, a intimidade e também a vida privada no rol de direitos e garantias fundamentais previstos no artigo 5º, inciso X[2] da Constituição Federal. É fato que, com atual realidade do crescente e irrevogável uso da *Internet* e suas aplicações nas mais diversas tarefas do cotidiano, a tutela constitucional da privacidade e da intimidade, que outrora ficavam adstritas ao âmbito residencial do cidadão, hoje se estendem às informações relacionadas à ele ou de sua propriedade, que encontram armazenadas na rede mundial de computadores.

Contextualizando o processo descrito, Costa Júnior (1995, p. 24):

> O mais desconcertante não é a verificação objetiva do fenômeno, não é observar que a tecnologia acoberta, estimula e facilita o devassamento da vida privada; é tomar conhecimento de que as pessoas condicionadas pelos meios de divulgação da era tecnológica (a serviço, portanto, de seus desígnios, em termos estritamente apologéticos), sentem-se compelidas a renunciar à própria intimidade. [...] O conceito de vida privada, como algo precioso, parece estar sofrendo uma deformação progressiva em muitas camadas da população. Realmente, na moderna sociedade de massas, a existência da intimidade, privatividade, contemplação e interiorização vem sendo posta em xeque, numa escala de assédio crescente, sem que reações proporcionais possam ser notadas.

Deste modo, a inviolabilidade do sigilo dos dados e comunicações telegráficas, contidas no inciso XII[3] do aludido artigo, modulam uma complementação na própria garantia da privacidade, na mesma medida de crescimento da essencialidade e exposição das informações contidas na rede mundial de computadores.

[2] "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, 2016a).
[3] "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;" (BRASIL, 2016a).

Pérez e Badía (2012, p. 12)[4] dissertam sobre o tema, afirmando que:

> Isso tem levado, ao longo tempo, à proteção efetiva do direito migrou de ação individual para a incorporação diferentes graus e formas de tutela por parte das autoridades públicas; ou seja,os Estados e seus mecanismos de intervenção.
> A extensão generalizada de acesso e uso Internet mudou os parâmetros sobre aqueles anteriormente adotados para a proteção do direito à privacidade, devido ao aumento do efeito viral da rede mundial de computadores como a causa da multiplicação de agentes, modelos de negócio, serviços, utilidades, ferramentas, etc.

Anteriormente a este panorama, era possível vislumbrar uma linha divisória entre ambas as garantias, já que distinguia-se com facilidade a intimidade e o sigilo de dados e comunicações.

Badía (2012, p. 7)[5] pondera:

> Vale lembrar que uma das primeiras incorporações da intimidade ao ordenamento jurídico ocorreu com a tutela da inviolabilidade das correspondências e das comunicações telefônicas; em muitos casos, até mesmo dotada de status de constitucionalidade. Proteção, cuja tutela é geralmente atribuída à órgãos judiciais, sendo os únicos habilitados e legitimados para excepcionar a regra, nos casos de indícios de práticas de delitos, e somente para os prováveis autores da transgressão da lei penal. Igualmente ou mais controvertida ainda é a contraposição entre o direito à privacidade/intimidade e, o também constitucionalmente sancionado, direito à liberdade de informação e expressão. A profusão de litígios processuais para definir os limites e prevalências entre ambos os direitos vem ocorrendo de forma proporcional aos avanços e à multiplicação dos meios de comunicação, com uma jurisprudência, muitas vezes, oscilando entre a prevalência de um ou de outro, não só atendendo à uma comparação em tempo real entre diversos países, culturas e tradições, mas também dentro de um mesmo âmbito e com periodicidade definida.

[4] Tradução nossa. Original em espanhol: "*Esto ha llevado a que, a lo largo del tiempo, la protección efectiva de ese derecho haya migrado desde la acción individual a la incorporación de distintos grados y formas de tutela a cargo de los poderes públicos; esto es, los Estados y sus mecanismos de intervención. La extensión generalizada de acceso y uso de Internet ha variado los parámetros sobre los que se venía asentando la protección del derecho a la privacidad, tanto debido a la potenciación del efecto viral de la Red como a causa de la multiplicación de agentes, modelos de negocio, servicios, utilidades, herramientas, etcétera*".

[5] Tradução nossa. Original em espanhol: "*Vale la pena recordar que una de las primigenias incorporaciones del derecho a la intimidad en el ordenamiento ha sido declarar la inviolabilidad de la correspondencia y las comunicaciones telefónicas; en no pocos casos, incluso dotada de rango constitucional. Protección, cuya tutela queda por lo general asignada a órganos judiciales, siendo los únicos habilitados y legitimados para excepcionarla, en los casos o supuestos de presunta comisión delictiva y solo para los posibles autores de una transgresión de la ley. Tanto o más controvertida ha sido y sigue siendo la contraposición entre el derecho a la privacidad/intimidad y el también constitucionalmente sancionado a la libertad de información y expresión. La profusión de litigios procesales para sentar los límites y rozamientos entre ambos derechos ha discurrido de forma proporcional a los avances y a la multiplicación de los medios de difusión, con una jurisprudencia a menudo oscilante entre la prevalencia de uno u otro, no solo atendiendo a una comparativa en tiempo real entre distintos países, culturas y tradiciones, sino dentro de un mismo ámbito y con exigua cadencia tempora".*

Em sentido ligeiramente oposto, Huber (1997, p. 189)[6] entende que os avanços tecnológicos proporcionaram uma maior privacidade aos usuários da rede mundial de computadores, principalmente pela melhoria nas funções protetivas, à exemplo da criptografia de dados:

> Numa perspectiva técnica, a privacidade é agora garantida, ou pode ser para quem se preocupa em garanti-la. As demais ameaças à privacidade são: a ignorância pública, que eventualmente será dissipada, e a obstrução do governo, que não será [...].
> Além disso, todos os aspirantes à *hackers* têm que identificar as informações de relevância, dentro de uma infinidade de outros dados inúteis. Nas crescentes multidões eletrônicas, há mais privacidade do que nunca.

Muito embora a tutela da privacidade no âmbito constitucional já encontre-se sedimentada tanto na legislação infraconstitucional quanto na exegese jurisprudencial, a interpretação quanto à sua própria incidência ainda não é pacífica. Desta feita, a democratização dos meios de comunicação segue proporcionalmente inversa à capacidade ou a potencialidade do risco da exposição de dados pessoais ou informações da esfera privada do cidadão, ponderando que, embora a evolução dos meios de proteção da informação na *Internet* vem justamente ao encontro ao exponencial risco de sua exposição.

Com a disponibilidade de um grande volume de dados pessoais na *Internet* torna-se difícil a identificação do grau de vulnerabilidade de cada um deles. Utilizando a classificação de *dado e informação*[7] – na qual o primeiro tem o sentido de conteúdo pessoal sem relevância ou sem função vulnerante ao cidadão, enquanto o segundo apresenta-se como conteúdo de sensível interesse ou vulnerabilidade – em determinados casos, não há como objetivamente determinar tal aspecto, e mensurar o grau de publicidade de cada uma das publicações na *Internet*. Neste sentido, ratifica Marcacini (2002, p. 132): "Hoje, então, principalmente diante do impacto do avanço tecnológico,

[6] Tradução nossa. Original em inglês: "*From a technical perspective, privacy is now secure, or can be for anyone who cares to secure it. The remaining threats to privacy are public ignorance, which will eventually be dispelled, and government obstruction, which won't. [...] Beyond that, every would-be snooper has to search for messages of interest within cataracts of other, useless information. In the ever-growing eletronic crowds, there is more privacy than ever".*

[7] Dado – Simples registro de fato ou elemento, de fácil estruturação, transferível e quantificável. Informação – dados com propósito e relevância. Os dados servem de base para a sistematização de informações, que constituem-se como registros dotados de importância à atividade humana (DAVENPORT; PRUSAK, 1998).

mais difícil ainda se torna definir os limites da informação pessoal - e em que circunstâncias - pode ou não ser considerada sigilosa".

Lewis (2012, p. 47) distingue a mera privacidade do conceito de *cibersegurança*, afirmando que a porosidade das conexões eletrônicas fixam um novo panorama na tutela dos bens jurídicos:

> A porosidade e vulnerabilidade das redes cibernéticas e a facilidade com que o agente com intenções maliciosas logra êxito em ter acesso à informação sem permissão do proprietário, supõe novos riscos para os indivíduos, empresas e nações, e ao mesmo tempo gera uma nova dimensão a qualquer esforço para preservar a privacidade individual.
> A privacidade e a cibersegurança não são sinônimos. A cibersegurança é a proteção dos serviços e infra-estruturas essenciais contra qualquer invasão, bem como a proteção da informação contra acessos não autorizados. A privacidade é o direito que todo indivíduo tem no controle e acesso de sua informação pessoal e em seu uso[8].

Obviamente que a inovação das condutas sociais pressupõe uma consequente evolução jurídica na tutela do bens tangenciados. No meio eletrônico e informático surgem diariamente novas violações anteriormente não concebidas pelo legislador constitucional, contudo, não mostra-se necessária adequação textual na Lei Maior, posto que a própria seara principiológica aporta as situações inéditas. A exegese doutrinária e jurisprudencial, que contempla a mutação constitucional e a reinterpretação dos antigos princípios de privacidade e intimidade, vem tendendo à eles incorporar novos conceitos, a fim de modular a crescente relevância das relações no meio eletrônico.

No mesmo sentido, o novo panorama proporcionado pelas novas práticas delitivas na *Internet* requer um repensar na questão material e probatória do Direito Penal. Uma nova técnica legislativa de criminalização mais ampla, relativizando a legalidade e outras garantias do Direito Penal classicamente concebido. Esta tendência é o que Moraes (2011) denomina de terceira velocidade do Direito Penal.

É necessário ponderar até que ponto justificar-se-ia a mitigação conceitual clássica de princípios constitucionais em nome da eficácia probatória criminal.

[8] Tradução nossa. Texto original em espanhol: "*La porosidad y vulnerabilidade de las redes cibernéticas y la facilidad con la que quienes poseen intención maliciosa logran acceder a la información sin el permiso del proprietario supone nuenos riesgos para los individuos, empresas y naciones, y al mismo tiempo añade una nueva dimensión a cualquier esfuerzo por preservar la privacidad individual. La privacidad y la ciberseguridad no son lo mismo. La ciberseguridad es la protección de los servicios e infraestructuras críticas frente a cualquier irrupción, así como la protección de la información contra accesos no autorizados. La privacidad es el derecho que todo individuo tiene a controlar el acceso a sua información personal y el uso de la misma*".

2 OS NOVOS LIMITES DA PRIVACIDADE NA INTERNET FIXADOS PELO MARCO CIVIL REGULATÓRIO

Em 23 de abril de 2014 foi promulgada a Lei Federal nº 12.965/14 também denominada de Marco Civil da *Internet* ou Marco Civil Regulatório.

Anteriormente à edição da Lei, havia um hiato no caso dos servidores que ofereciam serviços em *sites* ou aplicativos de *Internet*, onerosos ou gratuitos ao consumidor: não existia a obrigação legal na guarda dos registros de conexões ou de conteúdo destes serviços. Muito embora a recomendação, poucas empresas adotavam a prática em razão dos elevados custos da medida.

O cenário anterior era favorável à impunidade, já que muito embora a legislação material penal estivesse adequada a subsumir tipicamente[9] as práticas criminosas do *modus operandi* da *Internet*, a atividade investigatória enfrentava sérios óbices na identificação da autoria de tais delitos. Ademais, a ausência de sede nacional das pessoas jurídicas prestadoras de serviços na rede mundial de computadores, que geralmente hospedavam seus servidores em território estrangeiro, fazia com que as decisões judiciais brasileiras fossem impostas apenas pela via diplomática; e nos casos em que não houvesse cooperação internacional, a coercibilidade da jurisdição brasileira era inexistente.

Do mesmo modo, como a maior parte dos serviços consumidos na *Internet*, sejam eles em aplicações, bancos de dados ou endereços eletrônicos, a operacionalização destes servidores seguem parâmetros internacionais, geralmente dos países em que estão sediados, gerando outra incongruência com o Direito brasileiro. Ademais, a guarda dos registros de conexões e aplicações era facultativa, e geralmente não realizada, por questões financeiras.

A ausência de legislação específica para as relações no meio eletrônico da *Internet*, notadamente que regulamentasse a obrigatoriedade na guarda de registros de conexão e aplicação criava um contexto de maior violação da segurança jurídica e da própria privacidade (FURLANETO NETO; SANTOS; GIMENES, 2012).

[9] Neste mesmo sentido, Santos (2013) afirma que embora a rede mundial de computadores apresente uma nova modalidade de cometimento de delitos, que potencializa alguns riscos preexistentes (como a disseminação ou publicidade do crime), a legislação penal é adequada na tarefa de incriminação de tais condutas, sendo desnecessária a edição de lei própria.

O Comitê Gestor da *Internet* no Brasil emite a seguinte recomendação às práticas de segurança para as empresas que administram servidores *on-line*, sobre os *logs*:

> [...] não podem ser mantidos on-line por tempo indeterminado, pois acabam por consumir muito espaço em disco. A melhor estratégia para resolver esta questão é transferir periodicamente os logs do disco para dispositivos de armazenamento off-line, tais como fita, CD-R ou DVD-R. [...]
> Os logs armazenados off-line devem ser mantidos por um certo período de tempo, pois podem vir a ser necessários para ajudar na investigação de incidentes de segurança descobertos posteriormente. O Comitê Gestor da Internet no Brasil recomenda que logs de conexões de usuários de provedores de acesso estejam disponíveis por pelo menos 3 anos. É aconselhável que os demais logs sejam mantidos no mínimo por 6 meses. É importante que os logs armazenados on-line sejam incluídos no procedimento de backup dos seus sistemas [...] (BRASIL, 2016d).

Frisa-se que em seu artigo 3º, inciso II[10], a Lei firma a proteção à privacidade como um dos princípios do uso da rede mundial de computadores no Brasil.

Com a edição do Marco Civil Regulatório, ficou estabelecido, em artigo 11 e seu parágrafo 2º[11], que tais empresas e servidores deverão sujeitar-se à legislação pátria, desde que oferte serviço ao público brasileiro ou tenha ao menos uma sede em território nacional. Esta nova medida torna obrigatória a adequação técnica dos sistemas informáticos às disposições legais brasileiras. No que tange à privacidade de acesso e navegação na *Internet*, os artigos 13 e 14[12] fixam o prazo obrigatório para armazenamento dos registros de conexão em 1 ano e de aplicações de *Internet* por 6 meses. Complementa ainda que o armazenamento dos registros de conexões de aplicações de *Internet* deve ser realizado pelos provedores constituídos na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos.

[10] "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade; [...]Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet." (BRASIL, 2016b).

[11] "Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. [...] § 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil" (BRASIL, 2016b).

[12] "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. [...]
Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento" (BRASIL, 2016b).

Neste novo sentido, as empresas responsáveis por prover a conexão à rede mundial de computadores ao usuário do terminal eletrônico devem registrar os acessos de seus clientes por prazo de 1 ano, enquanto que os servidores que se amoldarem aos termos do artigo 11 ficam obrigados a armazenar os acessos aos aplicativos aos quais sediem e mantenham na *Internet* por 6 meses; possibilitando que a autoridade investigativa rastreie o fluxo de acessos de um determinado usuário tanto através do seu provedor quanto por solicitação direta ao servidor responsável pelo endereço eletrônico acessado.

A modelagem de armazenamento obrigatória contempla, no caso dos registros de conexão, o IP (*Internet Protocol*) do terminal no sistema data-hora e fuso-horário, referentes ao início e ao fim da conexão. Com relação ao registro de acesso a aplicações na *Internet*, são armazenadas as mesmas informações, com o acréscimo da identificação da aplicação utilizada, nos termos do artigo 5º[13].

Furlaneto Neto, Santos e Gimenes (2012, p. 163) realizam a ressalva de que nem sempre é necessário o deferimento do juízo para a obtenção do *IP*:

> Ressalte-se que nem sempre há, em um primeiro momento, a necessidade de autorização judicial para se chegar ao *protocol internet* (IP) do suspeito, diante de esse dado ser de domínio público e ser acessado por qualquer um que tenha conhecimento técnico para tal. Após a identificação do IP, deverá o provedor fornecer os dados cadastrais do cliente, sem que, para tanto, seja necessário autorização judicial, porém, para a confirmação dos dados obtidos no ato da investigação criminal preliminar, com os arquivos *logs* mantidos pelo provedor, necessário se faz ordem judicial, em decorrência do disposto no inciso XII do art. 5º da CF, regulamentado pela Lei nº 9.292/1996.

Com vistas no avanço tecnológico informático, foi necessária a fixação de um prazo para o armazenamento das atividades de cada um dos usuários da rede. Em consonância com a exegese constitucional clássica, os direitos fundamentais da intimidade e da privacidade não são absolutos; havendo a necessidade da mitigação do anonimato virtual, a fim de possibilitar a investigação e instrução processual, nos crescentes casos de criminalidade informática, cometidos na rede. Como bem lembra Reis (1997, p. 20) "o conhecimento da vulnerabilidade dos computadores pode ser mais nefasto que o próprio crime".

Complementarmente Lins (2014, p. 7) ressalta:

[13] "Art. 5º Para os efeitos desta Lei, considera-se: [...]VI - 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; [...] VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" (BRASIL, 2016b).

> A Internet traz um agravante: a rede é mundial e o fato poderá ser divulgado em escala nunca antes alcançada por outros meios de comunicação de massa. Tal circunstância levanta, inclusive, aspectos de natureza técnica: os fatos podem ser divulgados a partir de países que, por não dispor de legislação para tal, não punirão a ocorrência, dando um caráter de impunidade à atitude delituosa.

A privacidade na esfera da Internet, além dos registros de logs, relaciona-se naturalmente ao modo que os usuários da rede utilizam os dispositivos tecnológicos. Na medida em que alguém disponibiliza, por qualquer motivo, determinadas informações sensíveis, sua esfera de privacidade diminui; *contrariu sensu*, se tomar postura reservada, a privacidade é preservada. Garcia e Furlaneto Neto (2012) destacam a função da autotutela na esfera da Internet, afirmando que a intimidade não está apenas no armazenamento de dados e postagens, nem no Estado que promulga legislação específica sobre o dever ou não de armazenar os *logs*, mas sim uma responsabilidade individual, a fim de determinar o grau de privacidade de cada usuário.

Pondera-se que o conteúdo dos acessos não foi contemplado pelo Marco Regulatório, dependendo de requisição específica ao servidor detentor do conteúdo (que facultativamente poderá ou não armazenar tais dados) e excluindo-se o provedor da questão. Desta forma, em havendo eventual requisição policial ou judicial, será possível a obtenção dos endereços e aplicações acessados por determinado terminal eletrônico, contudo, seu conteúdo dependerá de acesso autônomo, ou seja, realizado pelo próprio agente. Se o conteúdo for de acesso restrito, sua cognição dependerá de determinação judicial.

As linhas de investigação informática linear e não linear são mencionadas por Furlaneto Neto, Santos e Gimenes (2012, p. 163-164), que ressaltam a dificuldade existente na identificação da autoria dos delitos cometidos em terminais públicos:

> A investigação linear se dá por meio de informações obtidas junto ao provedor, no que tange ao cadastro do cliente que utilizou determinado IP.
> Processo mais complexo, porém, muito mais eficiente, se dá por meio da investigação não linear. Por meio de uma engenharia regressiva, busca-se a localização de onde o IP originário está instalado, sem que haja invasão da privacidade ou violação a direito e garantia fundamental[14]. A engenharia

[14] Importante ressaltar que a linha investigatória adotada irá indicar o grau ostensividade e perturbação à privacidade constitucional. Nesta mesma equação, a violação e eventual inconstitucionalidade da medida deverá ser verificada *in casu*. Embora a tendência da política criminal da contemporaneidade seja tendente à relativização dos direitos e garantias fundamentais no que tange ao uso da *Internet*, sendo esta ratificada pela legislação em vigor, relega-se à discricionariedade da autoridade policial a utilização dos novos métodos investigativos ou a condução das diligências de forma menos incisiva.

> regressiva ou engenharia social é realizada por meios de mecanismos disponíveis na própria rede mundial de computadores.
> Importa salientar que a engenharia regressiva poderá levar a um computador instalado em cibercafés, escolas de informáticas ou espaços públicos, o que imporá em um empecilho para a identificação da autoria em face de, em regra, não haver controle de acesso e uso por parte dos responsáveis.

Com a edição do Marco Civil Regulatório, a privacidade no âmbito da *Internet*, à princípio, permanece incólume. Não obstante, o armazenamento dos registros de conexão, anteriormente facultativo, pode representar uma modulação da garantia constitucional para fins penais, de acordo com a teoria da *Terceira Velocidade do Direito Penal* de Moraes (2011). Nos termos do referido artigo 13, a tutela destas informações deverá ser sigilosa e segura, evitando o acesso e divulgação indevidos. Esta regra somente poderá ser relativizada, no caso de requisição da autoridade policial ou judicial, devendo obedecer aos mesmos ditames da legislação processual penal, a saber, a materialidade do delito e indícios razoáveis de sua autoria.

Tal qual a justificativa da prescritibilidade geral dos crimes, a interferência estatal não poderá ser *ad perpetuam* na esfera do indivíduo. Trilhando tal juízo, deve haver adequação entre o interesse social na elucidação criminal e o interesse individual na preservação da privacidade no âmbito da *Internet*; não admite-se uma regra que obrigue registros vitalícios ou demasiadamente prolongados das atividades da rede, em respeito ao contemporâneo *direito ao esquecimento*.

Por outra perspectiva, advogar a favor da inconstitucionalidade do armazenamento de *logs* e registros de conexões na rede mundial de computadores é impróprio, posto que o contexto atual de uso abusivo e ilícito dos meios eletrônicos gerou a necessidade de investigar os atos ilegais praticados em tal meio, de modo a garantir a segurança jurídica necessária para o uso adequado da *Internet* no Brasil. Não se pode abrir mão dessa segurança que parece preponderar sob a aludida privacidade. Ademais, a relativização da privacidade contida na medida de guarda das informações mostra-se razoável e não abusiva, sendo tal medida já adotada há tempos com sucesso em outras áreas, como na telefonia móvel e fixa.

Partido das premissas até então estabelecidas, é pertinente a análise acerca da admissibilidade constitucional do armazenamento cautelar dos registros imposto pelo Marco Civil Regulatório.

3 A INTERCEPTAÇÃO TELEMÁTICA E O ARMAZENAMENTO CAUTELAR DE CONEXÕES

A lógica na investigação dos crimes no âmbito da *Internet*, que pressupõe a guarda dos registros de conexão, parte da solicitação das informações referentes aos terminais em que as conexões foram realizadas; posteriormente, há a identificação do proprietário/usuário do dispositivo eletrônico e a sua correlação com o autor da prática criminosa.

Em determinados casos, surge a necessidade do monitoramento cautelar das mensagens interpostas pelo investigado; é o que denomina de interceptação telemática ou de dispositivo informático. Sua regulamentação específica é encontrada na Lei 9.296/96 obrigando, dentre outras medidas, a solicitação judicial, o exaurimento de outros meios investigatórios e a obediência ao prazo máximo fixado em lei.

Por outra perspectiva, aventa-se a possibilidade de que a interceptação seja vertida para os próprios registros de conexões e aos acessos à aplicativos de *Internet* em período de guarda inclusive superior à aquele já fixado pelo Marco Civil Regulatório. Esta situação ocorrerá quando o interesse da instrução recair sobre dados de acesso de provedores de aplicações de Internet, que não se amoldem à tutela compulsória da Lei, ou seja, não exerçam atividade de forma organizada, profissional e com fins econômicos. Tais empresas, a princípio, não estariam obrigadas a realizar a guarda dos registros, contudo, através de ordem judicial, é possível a fixação da obrigatoriedade no registro por período determinado e versando sobre fatos específicos.

Nota-se que a determinação da medida de armazenamento cautelar poderá ser realizada por duas ordens: por meio de requisição judicial ou diretamente pela autoridade policial, administrativa ou pelo Ministério Público.

A requisição judicial (e consequentemente a pretérita solicitação ao magistrado) deverá discriminar, ao servidor solicitado, o período exato dos registros de conexões (artigo 15, §1º[15]), a medida cautelar cria a obrigação do servidor em armazenar os dados por período indeterminado, evitando o perecimento dos dados de conexões vincendas e não determináveis[16]. Nos termos da Lei nº 12.965/14 os registros de conexão podem ser

[15] "§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no *caput* a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado." (BRASIL, 2016b).

[16] Outra alternativa, mais dispendiosa, que supriria o armazenamento cautelar seria a expedição de requisições sucessivas, de acordo com o vencimento da obrigação legal de armazenamento dos dados (a

cauterlamente armazenados por período superior à 1 ano (artigo 13, §2º) e os registros de aplicações de *Internet* por período superior à 6 meses (artigo 15, §2º) [17]. Em ambos os casos, a medida cautelar poderá ser solicitada pelo Ministério Público, autoridade policial ou administrativa.

Na outra situação descrita, à luz do aludido parágrafo §2º, é possível que a cautela seja solicitada ao provedor diretamente pelos legitimados ativos para tanto, dispensando em um primeiro momento a ordem judicial. A requisição direta é medida excepcional e somente deverá ser utilizada em caso de risco de perecimento da prova em razão da mora no lapso da solicitação judicial. O provedor será desobrigado no cumprimento da medida caso o pedido formulado ao judiciário seja indeferido ou não houver comprovação da formulação do pedido ao juízo competente no prazo de 60 dias, na sistemática dos parágrafos 3º e 4º do artigo 13[18]. Assim, em caso de urgência a análise judicial é diferida, podendo a medida ser determinada de plano pela própria autoridade solicitante.

Como função principal, o armazenamento cautelar presta-se à preservar a prova, enquanto a formação da plena cognição que o fundamente é instruído em juízo. Ao contrário da guarda geral dos registros, a medida cautelar volta-se para o futuro, ou seja, cria-se a obrigação que a atividade de determinado terminal seja efetivamente monitorada e registrada, levando em conta a morosidade geral do judiciário para atender as solicitações. Outrossim, o armazenamento cautelar poderá servir para obrigar aqueles provedores que legalmente não estariam, em tese, obrigados à armazenar os registros de conexões de seus usuários.

De tal sorte, as informações coletadas pelos servidores só podem ser prestadas ao solicitante com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, formalizada através de requerimento

cada seis meses ou um ano). Nota-se, contudo, que foi adequada a opção legislativa, otimizando a instrução penal.

[17] "Art. 13§ 2º: A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no *caput*.[...] Art. 15 § 2º: A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no *caput*, observado o disposto nos §§ 3o e 4o do art. 13". (BRASIL, 2016b).

[18] "§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no caput. § 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º". (BRASIL, 2016b).

motivado, contendo o *fumus boni juris* e *periculum in mora* do pleito, nos termos do artigo 22[19] da Lei.

As diligências investigatórias que mantenham, de qualquer forma, uma interferência oculta do investigado, excepcionam temporariamente a esfera de garantias constitucionais do cidadão. Na medida em que há a ponderação de interesses conflitantes, tutelados pela Constituição brasileira, há a prevalência de determinado princípio sobre outro que, naquela oportunidade, mostra-se mais relevante, de acordo com o Estado democrático de Direito. À exemplo da interceptação telemática, prevista na Lei 9.296/96, o armazenamento de registros de conexões e aplicativos na *Internet*, sem dúvida, consubstancia uma medida preventiva de rastreabilidade das condutas praticadas no âmbito virtual, relativizando a garantia constitucional à privacidade.

Partindo desta premissa, tal sorte de medida probatória, assim como qualquer outra que influa na seara garantidora do cidadão, deverá ser modulada nos limites da razoabilidade, de acordo com o seguinte guia: a) a fixação legal de prazo determinado, balanceando a privacidade e a instrução processual à luz do princípio da intervenção mínima; b) a determinação da excepcionalidade da prorrogação da medida, assim como seu respectivo prazo; c) a vedação de seu deferimento *ad perpetuam*, sem prazo determinado ou para investigar fatos incertos; d) a restrição da legitimação postulatória da medida aos pólos que ostentem real interesse no processo, como o Ministério Público, a autoridade policial ou o assistente da acusação.

Traçando um paralelo entre a interceptação do fluxo de comunicações informáticas da Lei 9.296/96 e o armazenamento cautelar dos registros de conexões previsto no Marco Regulatório da *Internet*, ambos constituem-se em medida de natureza semelhante. Verifica-se que estes institutos vertem-se na excepcional investigação de pessoa determinada a fim de elucidar a materialidade e autoria de pretenso delito. Por tal razão, além da evidente recenticidade do tema e da falta de regulamentação da medida, será tomada como teoria de base os estudos sobre a interceptação telefônica, a fim de realizar a crítica reflexiva sobre o armazenamento cautelar de conexões.

[19] "Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
I - fundados indícios da ocorrência do ilícito;
II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
III - período ao qual se referem os registros".(BRASIL, 2016b).

Pondera-se que, muito embora a função aventada entre ambos os institutos seja semelhante, não se pode confundir a interceptação do fluxo das comunicações informáticas com o armazenamento cautelar de registros. No primeiro caso, há efetiva interceptação de conteúdo (sendo mais invasiva) enquanto que no segundo apenas há a guarda dos registros de acesso[20].

Em preliminar definição, Castro (2003, p. 131) lembra que: "A telemática é uma ciência que trata da manipulação de dados e informações, conjugando o computador, sistema de informática, com os meios de comunicação, telefônicos ou não". Portanto, conforme o parágrafo único do artigo 1º[21] da Lei 9.296/96, é possível que a interceptação seja determinada em face da comunicação dos sistemas informáticos (conectados ou não à rede mundial de computadores).

Conforme Avolio (2010, p. 118) é fundamental para a estrutural conceitual da interceptação o fato de que a comunicação tenha sido realizada por terceiro estranho à medida, de forma que possibilita-se a cognição de informações e circunstâncias, que de outro modo, permaneceriam ocultas; justificando o exaurimento pretérito dos outros métodos investigatórios.

Na lição de Badaró (2008, p. 287) a autorização da interceptação telemática ou informática depende da comprovação da impossibilidade dos demais meios investigatórios ordinariamente disponíveis, à exemplo da busca e apreensão, da prova testemunhal ou do labor dos agentes policiais. Em outras palavras, a reconstrução fática deverá ser impossível sem a interceptação. Outrossim, Fernandes (2007, p. 107) ressalta que a interceptação será lícita somente se constituir-se no único meio hábil à evidenciar a materialidade ou autoria do crime, ou colher relevante elemento de prova.

Mendes (1999, p. 192) ressalta que a medida, por óbvio, é deferida *inaudita altera pars*, caracterizando a natureza velada do meio:

[20] Em situação semelhante ao que ocorre com a interceptação telefônica, também regulamentada pela Lei 9.296/96, as operadoras de telefonia (fixa ou móvel) registram por tempo determinado a relação das ligações e mensagens multimídia (texto, imagem e som) enviadas e recebidas de cada uma das linhas registradas em sua competência. No caso da interceptação telefônica, passa-se a monitorar o conteúdo das ligações, ou seja, as chamadas efetivamente, enquanto que no caso da solicitação policial ou judicial da bilhetagem das ligações corresponderia à medida de armazenamento geral. Contudo, não há previsão específica no caso da telefonia para que seja solicitado *ad cautelam* o registro das ligações futuras ou determinado diretamente pela autoridade policial/ministerial (dispensando a ordem judicial). Nota-se que, em ambas as medidas, a natureza inquisitiva é a mesma, havendo a variação quanto à relativização da garantia individual da privacidade.

[21] "O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática" (BRASIL, 2016c).

> O deferimento da medida é *inaudita altera pars*, não tendo o investigado conhecimento de que sua conversa está sendo captada, mas, ao se concluírem as diligências, será levantado o sigilo, podendo o investigado valer-se de *habeas corpus* para impugnar a medida se tiver havido nulidade. Entende Gomes que se o pedido for indeferido o Ministério Público pode ingressar com mandado de segurança.

Pondera Marcacini (2002, p. 146) sobre a natureza dos dados interceptados e sua possibilidade de interceptação, de acordo com seu posicionamento nos sistemas ou conexões:

> Assim, quando se fala no direito à privacidade de dados, cumpre destacar suas situações distintas. Pela primeira, dados estão sendo transmitidos estabelecendo uma forma de comunicação por redes públicas ou privadas; esta goza de larga proteção constitucional, insculpida no inciso XII, do artigo 5º de nossa Carta. Estes dados transmitidos não podem ser licitamente interceptados, nem mesmo diante autorização judicial. Uma vez armazenados os dados transmitidos, esta informação passa a ser considerada uma informação fixa, caso em que deixa de incidir o inciso XII.

Conforme ressalta Aranha (2008, p. 288) o procedimento de validade da interceptação telemática passa pela observância do prazo de 15 dias, com a possibilidade de renovação por igual período, em caso de comprovada necessidade. No mesmo sentido, Castro (2003, p. 131-132): "A interceptação, desta forma, poderá ser feita nas comunicações telefônicas e telemáticas, desde que preenchidos os requisitos enumerados na lei [...]. O prazo para a diligência será de 15 dias, prorrogável por igual período, desde que comprovada a indispensabilidade do meio de prova (artigo 5º da Lei nº 9.296/96)".

O ponto fundamental da crítica ao armazenamento cautelar de dados da *Internet*, com base na legislação aplicável à interceptação telemática é que esta apresenta prazo máximo de duração para a diligência, não havendo regulamentação legislativa neste sentido para aquela.

Há que se diferenciar o armazenamento geral de dados, realizado pelos servidores, com fulcro na obrigação fixada pelo Marco Civil Regulatório, o qual decorre de Lei e é inespecífico (atingindo todos os usuários do servidor que gerencia as conexões/aplicativo) e o armazenamento cautelar, que é determinado pelo juiz com caráter individual. Neste último caso, trata-se de medida excepcional, que deve ser fundamentada em indícios de materialidade e autoria de delito ou ilícito civil (*fumus boni juris e periculum in mora*), enquanto que o primeiro serve como garantia geral para a adimplência das obrigações fixadas na *Internet*, além da prevenção criminal.

Enquanto que a interceptação deve ser realizada com a finalidade específica de elucidar os delitos que fundamentaram sua requisição, nenhum objeto é indicado como pressuposto do armazenamento cautelar; o que poderia ensejar o deferimento de medidas de vigilância preventivas, sem fundamento fático, como uma espécie de preempção de determinados grupos sujeitos à medida.

Com esteio na natureza jurídica do armazenamento cautelar de dados, é possível indicar que este assemelha-se, em muitos pontos, à interceptação telemática, sendo necessária a sua regulamentação, especialmente quanto ao prazo de duração e possibilidade de prorrogação da medida, a fim de conferir segurança jurídica na instrução criminal. Ademais, relegar tal função ao magistrado não indica ser o melhor juízo, visto que estar-se-ia conferindo demasiada arbitrariedade ao julgador, ficando ao seu talante a decisão da fixação ou não de prazo cautelar ou sua duração[22], o que possivelmente geraria incongruências na aplicação da medida.

3.1 Sanção Administrativa

A Lei 12.965/14 também cuidou da eventual aplicação de penalidades no caso do descumprimento de seus preceitos fixados na coleta, guarda e armazenamento dos registros de conexões e aplicações. Estas sanções de natureza administrativa são aplicáveis quando tais atividades dos provedores não atenderem à preservação da privacidade e da honra das pessoas envolvidas no processo eletrônico, e também e caso de violação do sigilo das informações armazenadas na coleta, armazenamento, guarda e tratamento de tais dados.

Pela inteligência e compatibilização dos artigos 13, §6º[23] e 15, §4º[24] a aplicação de sanções também se estende à hipótese de descumprimento do servidor da requisição

[22] À título de exemplo no *Habeas Corpus* 143.697 - PR (2009/0148654-5) foi reconhecida a nulidade absoluta das provas obtidas por meio de medida de interceptação da Lei 9.296/96, em razão das excessivas prorrogações: 16 vezes. Na oportunidade, o tribunal identificou a ocorrência de abuso à razoabilidade e a privacidade do réu (BRASIL, 2016e).
Ainda que existente o disposto do artigo 5º, que regulamenta o prazo e a prorrogação da interceptação telefônica/telemática, constatam-se diversos abusos no uso da medida. Conforme o posicionamento deste trabalho especula-se que a ausência de normatização semelhante na cautela de armazenamento de registros e conexões de *Internet* poderá agravar a situação.

[23] "Art. 13, § 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência." (BRASIL, 2016c).

[24] "Art. 15, § 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida

do armazenamento cautelar de registros de conexão ou de aplicações de *Internet*, tanto pela autoridade policial quanto pela autoridade administrativa ou policial. Assim, uma vez havendo a solicitação, dentro dos parâmetros legais estabelecidos pelo Marco, estará obrigado o provedor ou servidor cível e criminalmente à acatar a solicitação; no caso de o armazenamento não ser realizado ou se a operação violar algum dos princípios norteadores da Lei como a intimidade ou a honra do investigado, é cabível a penalidade para atender o fiel cumprimento da medida de armazenamento cautelar.

Nos termos do artigo 12, no caso de infração às normas reguladoras das referidas operações de guarda e armazenamento na rede (previstas nos artigos 10 e 11) poderão ser aplicadas as seguintes sanções, de forma isolada ou cumulativa: I - advertência; II - multa de até 10% do faturamento do grupo econômico no Brasil, referente a seu último exercício fiscal; III - suspensão temporária das atividades que envolvam as práticas arroladas no artigo 11; IV - proibição das atividades que envolvam as práticas arroladas no artigo 11 (BRASIL, 2016c). Ademais, o dispositivo não deixa claro a titularidade do mister de processar e julgar os processos administrativos do Marco Civil. Tomando como base a natureza das sanções, parece-nos que a competência de seu julgamento e aplicação fica a cargo da Agência Nacional de Telecomunicações (ANATEL).

Nota-se que o legislador estabeleceu como base determinados critérios objetivos e subjetivos, a fim de estabelecer a espécie e dosimetria da sanção aplicável. Tanto no caso da violação dos registros de conexões (artigo 13) quanto nas aplicações de *Internet* (artigo 15) obedece-se aos mesmos critérios: I) natureza da infração; II) gravidade da infração; III) danos resultantes; IV) vantagem auferida pelo infrator; V) circunstâncias agravantes; VI) antecedentes do infrator; VII) reincidência.

Ao dispor sobre os parâmetros ou circunstâncias que compõe a dosimetria da sanção administrativa, não houve qualquer regulamentação da Lei 12.965/14 acerca do conceito de reincidência Traçando um paralelo com o Direito Penal, acredita-se que a especificação técnica do termo obedece à mesma sistemática estabelecida no artigo 63 do *Codex* Penal, assim adotando sentido idêntico em ambos os casos: considera-se reincidente a parte que incidir em infração administrativa, ostentando prévia condenação transitada em julgado por outra penalidade nos termos do artigo 12 do Marco. Do mesmo modo, não há a fixação de um rol de agravantes específico para as violações no âmbito da rede mundial de computadores. Não obstante a existência do rol

pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência." (BRASIL, 2016c).

de agravantes criminais (artigo 61, CP) este mostra-se dissociado das circunstâncias congruentes à égide da Lei, provando a necessidade da regulamentação do tema.

CONSIDERAÇÕES FINAIS

A tutela constitucional da privacidade vem sendo progressivamente modificada pelas novas tecnologias, notadamente pelo contexto da ascedente relevância das atividades praticadas na rede mundial de computadores. Na contemporaneidade é necessário repensar a abrangência da intimidade e da privacidade no âmbito do cidadão, que outrora era adstrita ao âmbito residencial, hoje contempla novas perspectivas como a identidade digital do cidadão e o sigilo de suas atividades e acessos na *Internet*.

Por meio da mutação constitucional nota-se a convergência de garantias do cidadão, inicialmente concebidas em searas diversas, a fim de complementarem-se mutuamente, à exemplo da inviolabilidade da intimidade e vida privada (artigo 5º, inciso X, CF) e da inviolabilidade das comunicações telegráficas (inciso XII), sistematizando a tutela constitucional da privacidade na rede mundial de computadores.

Cresce na mesma proporção a importância do uso dos dispositivos eletrônicos conectados à *Internet* no exercício da cidadania e outras atividades relevantes no contexto social, como também a necessidade de aprimorar a proteção legal da privacidade sobre as informações que são transmitidas pelo meio eletrônico, visto que os dados sensíveis e de alto risco circulam diariamente na *web*.

No cenário anterior à promulgação do Marco Civil Regulatório da *Internet*¸ o armazenamento dos registros de conexões e acessos à aplicativos na *Internet* era facultativo e, geralmente não adotado pela maioria dos servidores. Embora este panorama conferisse maior grau de privacidade no uso da *Internet*, na ocorrência de práticas ilícitas, a atividade investigativa restava prejudicada (em alguns casos), já que para a identificação do terminal de origem da conduta era necessária a cooperação entre os órgãos públicos (policiais e judiciários) e as empresas que hospedavam os dados de acesso.

Com a obrigatoriedade do armazenamento dos registros de conexão pelo prazo de 1 ano e dos acessos à aplicativos por 6 meses, permitiu-se uma nova etapa no cenário jurídico da *Internet*. Não houve regressão quanto à privacidade, já que embora exista a obrigatoriedade do registro de atividades, sua divulgação é excepcional, pressupondo

decisão judicial embasada na ocorrência de fato ilícito e seu acesso é restrito aos interessados processuais.

A inovação possibilitou a investigação eficaz dos delitos cometidos via *Internet*, estabelecendo prazo razoável para que os agentes policiais elucidem a materialidade e autoria desta estirpe de crimes, nos moldes da evolução das velocidades do Direito Penal, relativizando garantias, com base na modulação da instrução processual. Não obstante, pondera-se que o uso de métodos mais ou menos ostensivos faz parte da discricionariedade da autoridade policial, que poderá fazer uso de métodos menos invasivos, ou seja, de acesso público, a fim de exercer o mister investigatório no âmbito da *Internet*.

Não se justifica a inconstitucionalidade no registro dos dados de conexões, inexistindo a violação à privacidade. A pacificação social gerada pelo uso adequado da *Internet* e a investigação dos crimes eletrônicos, exclusivamente possível através da medida, prepondera sobre o direito individual neste caso. Ademais, a exigência legal fixada para o sigilo das informações garante sua razoabilidade.

O Marco Regulatório estabeleceu a medida de armazenamento cautelar de registros de conexões e acessos à aplicativos de *Internet*, de forma judicial e extrajudicial. Tal medida antecipa a morosidade no processamento das solicitações ao judiciário, que prejudicaria a efetivação da grande parte das medidas, além de possibilitar o enquadramento da obrigatoriedade à servidores que não estariam contemplados na norma geral, no contexto de investigação específica de pessoa determinada.

Tal medida assemelha-se, em alguns aspectos, à interceptação telemática/informática da Lei 9.296/96 (a qual possui austeras limitações quanto à natureza do delito, prazo e renovação) já que vale-se da individualização motivada, não se constituindo mais como medida abstrata e genérica. O armazenamento cautelar verte-se na investigação de um único suspeito, enquanto o armazenamento dos dados de conexões e acessos à *Internet* é indistintamente aplicável a todos.

A medida de armazenamento cautelar não é regulamentada em sua totalidade pelo Marco Regulatório, posto que não apresentada prazo determinado ou número de prorrogações, o que mostra-se inadmissível, violando a privacidade do âmbito da *Internet*. Ademais, a solicitação da medida poderá ser realizada por "autoridade administrativa", termo genérico e não regulamentado pela Lei, equivocadamente

ampliando o rol de legitimados. Neste aspecto, especula-se que a legislação em comento queria tratar das autoridades administrativas com função investigatória sobre ilícitos cíveis, criminais ou administrativos (como no caso de membros do poder legislativo em Comissão Parlamentar de Inquérito). Independentemente, frisa-se a necessidade do referido arrolamento de maneira expressa.

As incongruências apresentadas no armazenamento cautelar demonstram sua tendência à inconstitucionalidade, por violação à privacidade e à legalidade. Por conseguinte, sugerem-se os seguintes aprimoramentos: a) fixação de prazo determinado para o armazenamento cautelar por 1 ano (registros de conexão) e 6 meses (acesso à aplicações), no caso da modalidade judicial da medida; b) possibilidade de prorrogação fundamentada por igual prazo; c) na hipótese do armazenamento cautelar solicitado diretamente pelas autoridades investigatórias, a possibilidade da perpetuação da medida até a análise judicial do pleito e, posteriormente, a fixação do prazo de 6 meses ou 1 ano; d) regulamentação do rol de autoridades administrativas legitimadas para solicitar a medida.

Por fim, conclui-se que as sanções administrativas fixadas mostram-se necessárias para a efetivação do estrito cumprimento a normatização estabelecida no âmbito da rede mundial de computadores, especialmente no tocante ao tratamento e guarda dos dados de conexão. Paralelamente à questão do armazenamento cautelar, as sanções também merecem regulamentação própria, especialmente quanto à competência e critérios de dosimetria, a fim de viabilizar sua implementação.

REFERÊNCIAS

ARANHA, Adalberto José Queiroz Teles de Camargo. *Da Prova no Processo Penal.* 7. ed. São Paulo: Saraiva, 2008.

ARAÚJO, Luiz Alberto David. NUNES JÚNIOR, Vidal Serrano. *Curso de Direito Constitucional.* 10. ed. São Paulo: Saraiva, 2006.

AVOLIO, Luiz Francisco Torquato. *Provas ilícitas: interceptações telefônicas, ambientais e gravações clandestinas*. 4. ed. São Paulo: Revista dos Tribunais, 2010.

BADARÓ, Gustavo Henrique Righi Ivahy. *Direito Processual Penal*. Rio de Janeiro: Elsevier, 2008.

BADÍA, Enrique. *Marco conceptual. Derecho ¿pendiente?* In: PÉREZ, Jorge Pérez; BADÍA, Enrique (Coord.). El debate sobre la privacidad y seguridad en la Red: Regulación y mercados. Fundación Telefónica. Barcelona: Editorial Ariel, 2012.

BRASIL. Constituição da República Federativa do Brasil de 1988. *Planalto.* Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 03 jan. 2016a.

BRASIL. Lei nº 12.965, de 23 de Abril de 2014. *Planalto.* Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 03 jan. 2016b.

BRASIL. Lei nº. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. *Planalto.* Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9296.htm>. Acesso em: 03 jan. 2016c.

BRASIL. Ministério das Comunicações e o Ministério da Ciência e Tecnologia. Comitê Gestor da Internet no Brasil. *Práticas de Segurança para Administradores de Redes Internet.* Disponível em: <http://www.cert.br/docs/seg-adm-redes/>. Acesso em: 03 jan. 2016d.

BRASIL. *Superior Tribunal de Justiça.* Habeas Corpus nº 143.697 - PR (2009/0148654-5). Relator: Min. Napoleão Nunes Maia Filho. PR, 2009. Disponível em: <http://stj.jusbrasil.com.br/jurisprudencia/5971077/habeas-corpus-hc-143697-pr-2009-0148654-5/inteiro-teor-12107439>. Acesso em: 03 jan. 2016e.

CASTRO, Carla Rodrigues Araújo de. *Crimes de Informática e Seus Aspectos Processuais.* 2. ed. Rio de Janeiro: Lumen Juris, 2003.

COSTA JÚNIOR, Paulo José. *O Direito de Estar Só: tutela penal da intimidade*. 2. ed. São Paulo: RT, 1995.

DAVENPORT, Thomas H.; PRUSAK, Laurence. *Conhecimento Empresarial*. 14 ed. Rio de Janeiro: Campus, 1998.

FERRAZ JÚNIOR, Tércio Sampaio. *Sigilo de dados:* o direito à privacidade e os limites à função fiscalizadora do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, São Paulo, v. 88, 1993, p. 439-459. Disponível em: <http://www.revistas.usp.br/rfdusp/issue/view/5421 >. Acesso em: 02. Jan. 2016.

FERNANDES, Antonio Scarance. *Processo Penal Constitucional.* 5. ed. São Paulo: Revista dos Tribunais, 2007.

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. *Crimes na Internet e Inquérito Policial Eletrônico*. São Paulo: Edipro, 2012.

GARCIA, Bruna Pinotti; FURLANETO NETO, Mário. *Guarda dos registros de conexão e de aplicação: estudo sobre o conflito privacidade vs segurança jurídica na proposta do Projeto de Lei nº 2.126/11*. CONPEDI, 2012. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=56c82ccd658e09e8>. Acesso em: 01 jan. 2016.

HUBER, Peter. *Law and Disorder In Cyberspace*. Oxford. New York: Oxford University Press, 1997.

LEWIS, James A. Contribuciones para Modelos Reguladores de proteccíon de datos para una era global.In: PÉREZ, Jorge Pérez; BADÍA, Enrique (Coord.). *El debate sobre la privacidad y seguridad en la Red: Regulación y mercados*. Fundación Telefónica. Barcelona: Editorial Ariel, 2012.

LINS, Bernardo F. E. Privacidade e Internet. *Consultoria Legislativa*: Estudo Março/2000. Disponível em: <http://www2.camara.leg.br/documentos-e-pesquisa/publicacoes/estnottec/tema4/pdf/001854.pdf >. Acesso em: 20 jan. 2016.

MARCACINI, Augusto Tavares Rosa. *Direito e Informática*: uma abordagem jurídica sobre a criptografia.Rio de Janeiro: Forense, 2002.

MENDES, Maria Gilmaise de Oliveira. *Direito à intimidade e interceptações telefônicas*. Belo Horizonte: Mandamentos, 1999.

MORAES, Alexandre Rocha Almeida. *Direito Penal do Inimigo: A Terceira Velocidade do Direito Penal*. Curitiba: Juruá, 2011.

PÉREZ, Jorge Pérez; BADÍA, Enrique (Coord.). *El debate sobre la privacidad y seguridad en la Red: Regulación y mercados*. Fundación Telefónica. Barcelona: Editorial Ariel, 2012.

REIS, Maria Helena Junqueira. *Computer Crimes: a criminalidade na era dos computadores*. Belo Horizonte: Del Rey, 1997.

SANTOS, José Eduardo Lourenço dos. *Preconceito e Discriminação Racial Pela Internet: Legitimidade da Incriminação*. 2013. 306 f. Tese (Doutorado em Direito) - Setor de Ciências Jurídicas, Universidade Federal do Paraná, Curitiba. 2013.

SIMÓN, Sandra Lia. *A Proteção Constitucional da Intimidade e da Vida Privada do Empregado*. São Paulo: LTR, 2000.