

# O DIREITO À PRIVACIDADE E O SIGILO DE DADOS NA INTERNET

## THE RIGHT TO PRIVACY AND THE RIGHT TO INTERNET DATA CONFIDENTIALITY

FELIPE MARTINS PINTO\*

JOHNNY WILSON BATISTA GUIMARÃES\*\*

**RESUMO:** O presente artigo analisa as recentes tentativas de alteração do Marco Civil da *Internet* – Lei 12.965/2014, através dos Projetos de Lei 215/2015, 1.547/2015 e 1.589/2015. Os dispositivos dos projetos de lei, que parecem trazer uma tendência de limitação de direitos e garantias individuais, em favor de uma persecução penal inquisitiva, são confrontados com normas constitucionais vigentes e com princípios democráticos que devem nortear o uso da *internet* e o Processo Penal Constitucional.

**PALAVRAS-CHAVE:** Direitos e garantias individuais. Marco Civil da *Internet*. Processo Penal Constitucional. Privacidade. Sigilo de dados.

**ABSTRACT:** *This article analyzes the recent change attempts of Law 12,965 / 2014, which regulates the use of the Internet in Brazil, through the Law Projects 215/2015, 1,547 / 2015 and 1,589 / 2015. The provisions of law projects seem to bring a tendency of limiting individual rights and guarantees in favor of an inquisitive criminal prosecution. In this study, these law projects will be faced with constitutional norms and democratic principles that should guide the use of the Internet and the Constitutional Criminal Procedure.*

**KEYWORDS:** *Individual rights and guarantees. Internet law in Brazil. Constitutional Criminal Procedure. Privacy. Data confidentiality.*

## 1. INTRODUÇÃO

As últimas décadas foram testemunhas de uma radical mudança na forma de comunicação dos indivíduos e na maneira com que estes passaram a armazenar suas informações. O que era restrito

---

\* Professor de Direito Processual Penal da Faculdade de Direito da UFMG. Doutor em Direito pela UFMG. Vice-presidente do Instituto dos Advogados de Minas Gerais. Diretor Secretário da Academia Mineira de Letras Jurídicas.  
Email: felipempinto@hotmail.com

\*\* Mestre em Processo Penal pela Faculdade de Direito da Universidade Federal de Minas Gerais. Bacharel em Direito pela mesma Faculdade. Especialista em Ciências Penais pela Universidade Anhanguera, com extensão universitária em formação para o magistério superior. Escrivão da Polícia Federal.  
Email: johnnysioguimaraes@gmail.com

a pequenos grupos, difundiram-se nas redes sociais as capacidades globais de compartilhamento. O que era resguardado ao recanto do domicílio, passou a se virtualizar e a ser depositado na nuvem.

Frente à mudança revolucionária da sociedade e do indivíduo, catalisada pela *web*, houve algumas tentativas de normatizar o novo espaço criado, destacando-se, no ordenamento jurídico brasileiro, o Marco Civil da *Internet*, que veio a lume, recentemente, no ano de 2014, instrumentalizado pela Lei 12.965/2014.

Influenciado por um discurso vocacionado para a proteção da privacidade e da intimidade no ambiente de rede, ecoando a direção garantista prenunciada pela Constituição Federal de 1988, o novo Marco não escapou de receber, também recentemente, duras tentativas de desvirtuação.

Ainda em trâmite, os Projetos de Lei 215/2015, 1.547/2015 e 1.589/2015, que buscam alterar dispositivos essenciais da Lei 12.965/2014 – Marco Civil da *Internet*, são flagrantes exemplos dessa tentativa de ataque a direitos fundamentais (destacando-se o direito à privacidade) e a garantias processuais, conforme se analisará neste artigo.

## 2. UM NOVO MARCO PARA UM NOVO TEMPO

A conexão progressiva dos indivíduos no ambiente de rede traz a necessidade de regulação e balizamento dos usos e limites do fluxo de dados. Embora a presente geração esteja descortinando novas e instigantes plataformas de comunicação, com soluções inovadoras para este novo mundo, é de se pressupor que o aumento da convivência virtualizada aumente também a potencialidade lesiva de direitos por meio virtual. Portanto, nasce a necessidade de orientação e regramento do armazenamento e uso da informação em rede, sobretudo com vistas a buscar um norte de princípios que possa amainar essa torrente caótica, sem, contudo, instabilizar o sistema de garantias individuais.

Neste sentido, foi editado, pelo Comitê Gestor da *Internet* no Brasil, o conjunto de recomendações constante da Resolução CGI.

br/RES/2009/003/P<sup>1</sup>, intitulado “Princípios para a governança e uso da *Internet*”, documento que influenciou diretamente a elaboração do texto do Marco Civil da *Internet*, hoje inserido no ordenamento através da Lei nº 12.965, de 23 de abril de 2014.

**São dez princípios orientadores elencados na Resolução, sendo que, para o estudo aqui proposto, merecem destaque três:**

**1. Liberdade, privacidade e direitos humanos**

O uso da Internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.

**2. Governança democrática e colaborativa**

A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.

**7. Inimputabilidade da rede**

O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.

Apesar da recepção recente de instrumentos com influências garantistas, como é exemplo a resolução acima citada e a nova Lei 12.965/2014 – Marco Civil da *Internet*, diante da irrefreável avalanche migratória para a virtualização<sup>2</sup> e da inevitável busca pelo equilíbrio normativo neste ainda estranho campo, cabe questionar se alguns pilares da cidadania, sobretudo direitos individuais consagrados pelo moderno constitucionalismo, têm-se mantido intactos neste embate, ou, por outra, como parece acontecer, sofrem ameaça iminente.

---

1 Disponível em: <<http://www.cgi.br/resolucoes/documento/2009/03>>. Acesso em: 04/11/2015.

2 Em levantamento datado de julho de 2015, a Associação Brasileira de Telecomunicações informa o montante de 1,6 milhões de novos acessos ativados em 12 meses. Disponível em: <<http://www.telebrasil.org.br/sala-de-imprensa/na-midia/7926-brasil-encerra-julho-com-221-3-milhoes-de-acessos-banda-larga-indica-telebrasil>>. Acesso em: 03/11/2015.

Analisando algumas propostas legislativas em trâmite e a manifestação de parcela considerável da opinião pública, ambas vertentes, muitas vezes, infladas pela opinião publicada da *mass media* e pelo apelo ao combate rigoroso à criminalidade<sup>3</sup>, podem-se pinçar amostras da atual tendência de inflexão sobre garantias constitucionais consagradas.

A última pressão sofrida pelas normas dos arts. 22 e 23 da Lei nº 12.965/2014, popularmente conhecida como Marco Civil da Internet, permite esta percepção. Cabe, inicialmente, citá-los na íntegra, para, posteriormente, pontuar o que se têm demonstrado como ataques frontais ao marco democrático da internet:

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.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Estes artigos do Marco Civil da *Internet*, de certa forma, vieram estabilizar o entendimento já sedimentado a partir da leitura do art. 5º, inciso XII, da Constituição Federal, segundo o qual somente ordem judicial (necessária e proporcional) seria capaz de, excepcionalmente, afastar o sigilo de dados. Coloca-se a autoridade

---

3 Um conjunto de crimes de especial gravidade para o contexto atual parece permitir a invasão da privacidade sem grandes questionamentos. A opinião pública, a despeito da violação de garantias constitucionais, parece não se importar com os espaços de invasão, desde que um dos “Quatro Cavaleiros do Infoapocalipse” esteja presente: pornografia infantil, terrorismo, lavagem de dinheiro e a guerra contra certas drogas (ASSANGE, 2013, p. 64).

judiciária como guardião da privacidade do indivíduo, num momento histórico de transição, onde o indivíduo transfere para a nuvem seus dados mais íntimos e particulares.

Ao passo que o constituinte de 1988 já antevia e protegia a coleta e armazenamento de dados dos indivíduos pelas autoridades públicas e empresas privadas, não lhe seria possível imaginar que a virtualização da esfera íntima (e seu depósito na nuvem) se desse em tal escala. Pode-se dizer que a virtualização dos aspectos da vida privada irrompeu como verdadeira revolução, mudando a concepção de sociedade e indivíduo.

A transição que se presencia é um momento de instabilidade de antigos valores, de desestabilização de dogmas e de fluidez, característica de momentos históricos de reagrupamento, de construção de novos valores. Zygmunt Bauman (2001, p. 10) tenta captar a época atual:

Os tempos modernos encontram os sólidos pré-modernos em estado avançado de desintegração; e um dos motivos mais fortes por trás da urgência em derretê-los era o desejo de, por uma vez, descobrir ou inventar sólidos de solidez duradoura, solidez em que se pudesse confiar e que tornaria o mundo previsível e, portanto, administrável.

Este é o momento em que alguns pilares de sustentação vêm abaixo e, nesta dinâmica, necessita-se saber quais pilares merecem esforços para a preservação.

No contexto específico dessa análise, é importante saber se a privacidade do indivíduo, no novíssimo contexto que se afigura, deve ser preservada, e, antes, se é possível sua preservação.

Bauman (2013, p. 114) chega a nomear a presente época como “modernidade líquida”<sup>4</sup>, justamente por sua fluidez e leveza, em dissonância com a modernidade, sólida e segura. Na

---

4 “Os fluidos se movem facilmente. Eles “fluem”, “escorrem”, “esvaem-se”, “respingam”, “transbordam”, “vazam”, “inundam”, “borrifam”, “pingam”, são “filtrados”, “destilados”, diferentemente dos sólidos, não são facilmente contidos – contornam certos obstáculos, dissolvem outros e invadem ou inundam seu caminho. Do encontro com sólidos emergem intactos, enquanto os sólidos que encontraram, se permanecem sólidos, são alterados – ficam molhados ou encharcados. A extraordinária mobilidade dos fluidos é o que os associa à idéia de leveza.” (BAUMAN, 2001, p. 8)

modernidade líquida, elimina-se a divisão antes sacrossanta, entre as esferas privada e pública, confundindo-se os dois planos. Nesta nova convivência, onde o indivíduo deposita desabafos, reflexões, confidências e toda sorte de informações numa rede compartilhada por um sem número de indivíduos, nasce a tentativa (endossada por este artigo) de marcar as fronteiras onde seria lícito arguir a proteção da privacidade.

Há um limite onde possa o indivíduo se proteger da invasão e captura de seus registros? Qual o marco a ser fixado?

Numa perspectiva realista (pessimista?), Baumann (2013, p.113) assevera que:

Perdemos a coragem, energia e sobretudo disposição de persistir na defesa desses direitos, esses tijolos insubstituíveis na construção da autonomia individual. Em nossos dias, o que nos assusta não é tanto a possibilidade de traição ou violação da privacidade, mas o oposto: o fechamento das saídas. A área da privacidade está se transformando num local de encarceramento.

A privacidade, assim, seria uma trincheira, continuamente bombardeada por ouvintes ávidos por extrair nossos segredos, colocando-os em exposição pública e tornando-os propriedade comum (Baumann, 2013, p. 114).

### **3. VIOLAÇÕES AO DIREITO À PRIVACIDADE E CONTENÇÕES POSSÍVEIS**

A tentativa de requalificar o peso da importância da privacidade individual parece trazer repercussões negativas, a fragilizar a proteção à pessoa. Cabe ressaltar que, no campo restrito do processo penal, a apresentação de informações excepcionalmente retiradas da guarida da privacidade tem o condão de, com as garantias do devido processo legal, erigir-se ao *status* de prova, inquinando desfavoravelmente aquele que, até então, era seu único detentor. Por essa maximização de efeitos da invasão da privacidade no campo do processo penal, é preciso fazer a crítica à aparente irrefreável promiscuidade entre o público e o privado, em defesa do indivíduo.

Diante da relevância das consequências da quebra da privacidade em prejuízo do indivíduo, talvez seja necessário impedir

a vulgarização do conceito, seguindo o caminho apontado Cynthia Vianna (2004, p. 27):

É necessário deslocar o foco da privacidade como direito da personalidade, restrito ao direito privado, para o direito público, reconhecendo-a como essencial para a dignidade humana e lhe proporcionando proteção jurídica mais efetiva, ligado ao direito constitucional e aos tratados de direitos humanos.

No mesmo sentido, Túlio Vianna (2006, p. 84) reforça a ideia de que o direito à privacidade não se restringe ao direito privado, constituindo-se, antes, como fundamento das democracias:

O direito à privacidade, concebido como uma tríade de direitos – direito de não ser monitorado, direito de não ser registrado e direito de não ser reconhecido (direito de não ter registros pessoais publicados) – transcende, pois, nas sociedades informacionais, os limites de mero direito de interesse privado para se tornar em um dos fundamentos do Estado Democrático de Direito.

Este precioso espaço da opacidade privada deve ser protegido. Para Túlio Vianna (2006, p.163), uma maneira de colocar freio à invasão desse direito é com a amplificação da transparência pública. Para que a vigília da sociedade informacional não sufoque a esfera do indivíduo, é necessária a ampliação da possibilidade de controle de quem controla, através da otimização da transparência estatal, em proporção inversa à opacidade privada.

Nas palavras do autor (VIANNA, 2006, p. 163):

A opacidade privada que garante a confidencialidade dos registros pessoais só pode ser garantida se efetivada a transparência pública das atividades de monitoração e tratamento de dados pessoais. Destarte, o princípio da transparência pública veda qualquer monitoração eletrônica ou captura e armazenamento de dados pessoais de caráter secreto.

Reforçando o discurso da perniciosidade da falta de transparência pública, Hannah Arendt (2012, p.453) já denunciava que “a única regra segura num Estado totalitário é que, quanto mais visível é uma agência governamental, menos poder detém; e quanto menos se sabe da existência de uma instituição, mais poderosa ela

é.” Vê-se que a transparência pública é uma ferramenta eficaz para o controle da invasão da privacidade.

Percebe-se que a atual transformação dos meios de comunicação, sua radicalização virtual e a revolução que conduz tal mudança, tende a pressionar e fragilizar o espaço da privacidade, se não houver firmes contrapesos a sustentá-la.

Ao lado da efetiva transparência pública, já apontada como mecanismo de defesa, é preciso indagar quais outros institutos do direito estão disponíveis à salvaguarda da privacidade individual, neste momento líquido de instabilidade de valores.

A partir da premissa de que o Estado Democrático e Constitucional de Direito traz o princípio da legalidade ao trato das relações entre os particulares (e entre o poder público e os particulares)<sup>5</sup>, emerge daí, necessariamente, outro pilar que apoia a defesa da esfera íntima do indivíduo.

Luigi Ferrajoli (2011, p. 104), quando delimita o conceito de Estado de Direito, parece concordar com sua função de contenção de abusos:

*Entendiendo por esta expresión un tipo de ordenamiento en que el poder público, y específicamente el penal, está rígidamente limitado y vinculado a la ley en el plano sustancial (o de los contenidos penalmente relevantes) y bajo el procesal (o de las formas procesalmente vinculantes).*

É no limite ditado pela lei (material e formalmente hígida), sobretudo no limite trazido pela regulação processual de acesso e uso dos dados do indivíduo, que repousa a segurança que requer a plena cidadania. Ora, não se pode, como pretende o recente e ainda em tramitação Projeto de Lei 215/2015, retirar, por exemplo, do controle judicial o acesso dos dados do investigado/demandado, como se a privacidade estivesse encoberta com frágil película e não integrasse a estrutura da dignidade humana, com estatura de direito fundamental. A Constituição Federal em seu artigo 5º, incisos VI e

---

5 Cite-se o art. 5º da Constituição Federal em seus incisos II (ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei) e LIV (ninguém será privado da liberdade ou de seus bens sem o devido processo legal).



XII, já ponderou o valor da privacidade e do sigilo das informações íntimas do indivíduo e não cabe à legislação ordinária (ou mesmo ao constituinte derivado<sup>6</sup>) abolir tal conquista. Lembre-se que “a democracia trouxe exigências de que o homem tenha uma dimensão jurídica que o Estado ou a coletividade não pode sacrificar *ad nutum*.” (LOPES JÚNIOR, 2008, p. 11)

A privacidade é um direito fundamental que, em que pese a revolução nos meios de comunicação e armazenamento de dados, na concepção de sociedade e indivíduo, não deve ser dilapidado, sob pena de desconstruir-se importante faceta da dignidade humana. Além disso, a privacidade, para ser exercida em sua plenitude, não precisa de qualquer parcimônia ou autorização estatal. Como observa Juarez Tavares (2003, p. 162), a “garantia e o exercício da liberdade individual não necessitam de qualquer legitimação, em face de sua evidência”.

Dessa maneira, é elogiável o art. 2º, inciso II, da Lei 12.965/2014 – Marco Civil da *Internet* que traz como fundamento da disciplina do uso da *internet* no Brasil “os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais”.

Também o art. 10, parágrafos 1º e 2º, do mesmo Marco Civil vem explicitar a preocupação, já inscrita na Constituição Federal, com a preservação da intimidade, da vida privada, da honra e da imagem dos indivíduos:

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de *internet* de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, **devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.**

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser

---

6 Art. 60, parágrafo 4º, inciso IV, da Constituição Federal.

disponibilizado **mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º. (grifos nossos)

Denota-se do texto do Marco Civil da *Internet* o conhecimento de que a defesa da imagem e da honra de uns é completamente conciliável com a privacidade e intimidade de outros. A persistência das garantias constitucionais guarda harmonia com o Processo Penal vocacionado à realização do projeto democrático (LOPES JUNIOR, 2008, p. 07).

Bem por isto, quando a Constituição Federal entrega ao judiciário a guarda dos dados e informações do indivíduo, o faz na busca do resguardo máximo das liberdades públicas, sem as quais o conceito de cidadania seria esvaziado. Pode-se dizer que o judiciário, quando realiza o controle da legalidade e conveniência da quebra dos sigilos, o faz orientado pelo sistema de *checks and balances*, uma vez que, em nosso sistema, ao executivo é confiada a sorte da investigação criminal, sendo de inconsistência lógica a entrega simultânea da discricionariedade sobre a invasão dos dados da pessoa.

Luigi Ferrajoli (2011, p. 10) apresenta hipótese que parece ser coerente com essa argumentação:

*La hipótesis teórica en que se basa es la existencia de un nexo indisoluble entre garantía de los derechos fundamentales, división de poderes y democracia. Sólo un derecho penal reconducido únicamente a las funciones de tutela de bienes y derechos fundamentales puede, en efecto, conjugar garantismo, eficiencia y certeza jurídica.*

Alerte-se, ainda, que cabem ao governo as políticas de gestão, expansão e uso da *internet* (através das agências reguladoras, comitês gestores etc), ficando ao seu facilitado alcance e regulação o banco de dados disponível dos provedores. Sem uma exigência legal de ordem judicial para o franqueamento de dados individuais, este mesmo governo, também detentor dos aparatos estatais de investigação, seria a raposa a tomar conta do galinheiro. Traga-se o testemunho cético de Julian Assange (2013, p.66), segundo o qual “os governos democráticos têm um interesse próprio, que é o controle.”

A reforçar esta denúncia e o cuidado que se deve ter ao entregar ao Estado, sem o filtro racional da decisão judicial, a quebra do sigilo de dados, poder-se-ia citar episódios históricos lamentáveis onde a crença na boa intenção estatal municiou aparatos repressivos.

Portanto, entre o conhecimento dos dados sigilosos e o interesse “elucidatório” dos agentes do Estado deve estar o dique da decisão judicial, necessária e proporcional.

Nessa linha de ideias, cite-se novamente Túlio Vianna (2006, p. 160/161):

O princípio da opacidade privada é o mais importante corolário princípio do interesse público do direito à privacidade. Com base nele, pode-se afirmar que, nas hipóteses em que a ponderação de translucidez recomendar o sacrifício do direito fundamental à privacidade com a finalidade de resguardar um bem jurídico de maior ou igual valor, a pessoa física ou jurídica responsável pela monitoração só poderá ter acesso às gravações por meio de autorização judicial.

Outro ponto deve ser considerado: uma vez que os dados individuais depositados na nuvem virtual extrapolam evidentemente a barreira nacional (as grandes empresas que dominam a *internet* são, em sua maioria, sediadas nos EUA, onde também se concentram os maiores *datacenters*) e que, noutra faceta, as maiores capacidades invasivas são de órgãos de inteligência das grandes potências, não é difícil imaginar a que ponto de fragilidade chegou o sigilo de dados.

Em recentíssimo artigo sobre os atentados terroristas de 13 de novembro de 2015 em Paris, o jornalista Helio Gurovtz reforça a opinião sobre o equívoco da limitação das garantias constitucionais em prol de medidas autoritárias na luta (ilusória<sup>7</sup>) contra a criminalidade:

Os partidários das restrições às comunicações têm afirmado que empresas como Apple ou Google deveriam dar ao governo a capacidade

---

7 A existência da criptografia derruba por terra o discurso da necessidade da quebra indiscriminada dos espaços de privacidade no interesse da investigação criminal. A invasão demonstra atingir em primeiro lugar o indivíduo desavisado do que o criminoso prudente: “a criptografia é a derradeira forma de ação direta não violenta. (...) uma criptografia robusta significa que um Estado, mesmo exercendo tal violência ilimitada, não tem como violar a determinação de indivíduos de manter segredos inacessíveis a ele.” (ASSANGE, 2013, p. 28)

de quebrar todos os códigos das mensagens trocadas por meio de seus programas. Trata-se de um disparate. Primeiro, porque qualquer porta ou janela que pudesse ser aberta ao governo seria também usada pelos criminosos. Segundo, porque a criptografia é uma ciência robusta, à disposição de todos. Ninguém precisa de nenhuma para trocar mensagens 100% secretas e seguras. É impraticável a qualquer governo ter acesso a todas as comunicações digitais, quando remetentes e destinatários realmente querem mantê-las em segredo.

É nessa linha de raciocínio, denunciando a tentativa de invasão da esfera íntima do indivíduo pelo Estado, sempre sob a bandeira do combate à criminalidade (e, modernamente, ao terror) outro alerta de Julian Assange (2013, p. 53), que chega a nomear o fenômeno de “militarização do ciberespaço”:

Quando nos comunicamos por *internet* ou telefonia celular, que agora está imbuída na *internet*, nossas comunicações são interceptadas por organizações militares da inteligência. É como ter um tanque de guerra dentro do quarto. É como ter um soldado entre você e sua mulher enquanto vocês estão trocando mensagens de texto. Todos nós vivemos sob uma lei marcial no que diz respeito às nossas comunicações, só não conseguimos enxergar os tanques – mas eles estão lá.

O fenômeno de banalização da invasão dos espaços de privacidade, para além das organizações de inteligência (vocacionados à atuação sob a sombra), é também presenciado na rotina de instituições democráticas e, por isso, somente legitimadas pela transparência. Tal mania é sentida na rotina das instruções preliminares no Brasil, onde diversos fatores (inclusive a desídia dos órgãos policiais, que preferem restringir o trabalho às diligências realizadas sob o conforto de salas refrigeradas) parecem catalisar a prioritária coleta de indícios através da quebra do espaço privado de comunicação e armazenamento de dados. Geraldo Prado (2014, p. 43) registra esta tendência de vulgarização da quebra de sigilo:

A indispensabilidade de um eficiente sistema de controles epistêmicos goza de especial importância nos dias atuais, porque vulgarizou-se o apelo, no âmbito da investigação, aos métodos ocultos de pesquisa (interceptação das comunicações e afastamento de sigilos) e de um modo geral a totalidade dos elementos informativos que subsidiam acusações encontra-se alicerçada em elementos obtidos dessa maneira.

Diante do contexto descrito, parece difícil a tarefa de frear a usurpação da esfera da privacidade do indivíduo. Uma saída de contenção, outra trincheira nesta batalha, pode ser o uso do direito como via de resguardo do sagrado espaço de privacidade. Nessa missão, o direito deve vir a inquirir de ilegalidade os abusos cometidos pelo Estado e por empresas privadas e deve chancelar como ilícita a violação dos dados do indivíduo que fuja da cartilha do devido processo legal, sobretudo da inarredável ordem judicial de quebra do sigilo de informações privadas.

#### **4. RECENTES TENTATIVAS DE DETURPAÇÃO DO RECENTE MARCO CIVIL DA INTERNET**

Nesse caminho, é preciso denunciar o canto de sereia do Projeto de Lei 215/2015 (com o apensamento e incremento dos Projetos de Lei nºs 1.547/2015 e 1.589/2015), que, a pretexto de aumentar a punição dos crimes contra a honra, cometidos através das redes sociais, deixa ao relento o segredo dos dados do indivíduo.

Com efeito. O Projeto de Lei 1.547/2015, de autoria do Deputado Federal Expedito Neto, apensado ao Projeto de Lei 215/2015, busca “promover o recrudescimento do tratamento penal dispensado ao agente que pratica crimes contra a honra em sítios ou por meio de mensagens eletrônicas difundidas pela *Internet*”<sup>8</sup>, em autêntica mensagem punitivista. Numa reação à avalanche de opiniões e críticas, antes confinadas a pequenos grupos, e, hoje, difundidas, compartilhadas nas teias da sociedade informacional, a primeira reação do Estado Totalitário é ameaçar com o braço pesado do Direito Penal. Tenta-se a contenção, através do sistema punitivo, de uma prática que, levando em consideração os milhões de usuários das redes sociais, é incontrolável. Aqui, o Direito Penal servirá apenas para instrumentalizar a seletividade do sistema e contribuir para o esfacelamento do Estado Garantista.

---

8 Vide justificação do próprio Projeto de Lei 1547/2015. Disponível em: <[http://www.camara.gov.br/proposicoesWeb/prop\\_mostrarintegra;jsessionid=8B056EE17AC8702CA108E0CBFB66927F,proposicoesWeb2?codteor=1334460&filename=PL+1547/2015](http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=8B056EE17AC8702CA108E0CBFB66927F,proposicoesWeb2?codteor=1334460&filename=PL+1547/2015)>. Acesso em: 03/11/2015.

Seria possível instaurar uma investigação para cada crime contra a honra veiculado na *web*? Ou o sistema seria seletivo o bastante para instaurar quando o controle e o cabedal do difamado o exigissem? As garantias processuais seriam atropeladas em nome de um Estado Policial e de vigilância?

Aury Lopes Júnior (2008, p. 18) lembra que “a ideia de que a repressão total vai sanar o problema é totalmente ideológica e mistificadora. Sacrificam-se direitos fundamentais em nome da incompetência estatal em resolver os problemas que realmente geram a violência.”

Noutra frente de ataque às garantias do indivíduo, aparece o Projeto de Lei 1.589/2015, de autoria da Deputada Federal Soraya Santos, também apensado ao Projeto de Lei 215/2015, que conclama a atuação “mais enérgica” do Estado contra os crimes contra a honra levados a cabo via *internet*, “dando poderes imediatos às autoridades de investigação para o acesso a registros de conexão à *internet* e aos registros de navegação na *internet* em casos de crimes contra a honra cometidos mediante publicação no meio virtual”<sup>9</sup>.

De uma forma desinibida frente às garantias mínimas de resguardo do sigilo dos dados, referido projeto apregoa o acesso das informações diretamente pela autoridade policial ou pelo Ministério Público, escanteando a proteção das liberdades públicas pelo judiciário.

Veja-se a sugestão de inclusão do art. 23-A à Lei 12.965/2014, trazida, sem rubor de face, pelo combatido projeto de lei:

Art. 23-A. A autoridade policial ou o Ministério Público, observado o disposto neste artigo, poderão requerer, ao responsável pela guarda, registros de conexão e registros de acesso a aplicações de *internet*, para instruir inquérito policial ou procedimento investigatório iniciados para apurar a prática de crimes contra a honra cometidos mediante conteúdo disponibilizado na *internet*.

§ 1o O requerimento apenas será formulado se presentes fundados indícios da ocorrência do crime e quando a prova não puder ser feita

---

9 Vide, igualmente, a justificação do Projeto de Lei 1589/2015. Disponível em <[http://www2.camara.leg.br/proposicoesWeb/prop\\_mostrarintegra?codteor=1336275&file name=PL+1589/2015](http://www2.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1336275&file name=PL+1589/2015)>. Acesso em: 03/11/2015.

por outros meios disponíveis, sob pena de nulidade da prova produzida.

§ 4º Cabe à autoridade requerente tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário.

É certo que os pressupostos elencados nos parágrafos 1º e 4º do citado artigo, tais como “fundados indícios da ocorrência de crime” e “providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário”, tornam-se verniz a disfarçar a destituição do Poder Judiciário como guardião da liberdade pública assaltada.

Permitir o distanciamento do controle judicial da coleta de dados e quebra de sigilo para instrução processual penal é aceitar o perigoso agigantamento do Estado Policial, característica afeta aos Estados totalitários. É tirar do caminho o crivo da decisão judicial fundamentada para entregar aos inquisidores e à sua sanha a construção unilateral do discurso punitivo<sup>10</sup>.

A trilhar a linha desejada pelos projetos de leis trazidos a exame, estar-se-ia maculando o ideal Processo Penal Constitucional, delineado assim por Maurício Zanoide (2010, p. 236):

Em um Estado Democrático de Direito, em cujos primados fundamentais estão a dignidade da pessoa humana, a igualdade e o cidadão como fonte primaz do poder – logo, como princípio e fim dos atos (públicos e privados) -, a persecução não pode ter aquele matiz despótico, inquisitivo ou arbitrário. Por essa razão, nossa atual Constituição não autoriza a realização de “qualquer” processo penal, mas apenas de um devido processo penal, feito em moldes a respeitar aqueles primados na busca da melhor reconstrução possível dos fatos penalmente relevantes.

A alteração legislativa pretendida equipara a ordem judicial, exigida pela Constituição Federal quando da excepcional

---

10 Geraldo Prado (2014, p. 49/50) traz o parâmetro recente do processo penal alemão, onde é característico o fortalecimento das posições processuais de poder das autoridades preventivas, para denunciar o que ele nomeia de “aglomeração quântica de poder”, identificada como a concentração de poder nas mãos da polícia e/ou Ministério Público. O autor alerta que muitas vezes tal combinação descamba para o abuso de poder, com uso de práticas do chamado subsistema policial e de emergência.

quebra de sigilo de dados, à requisição da autoridade competente, desconsiderando que a redoma judicial vem proteger o indivíduo justamente da autoridade competente e, muitas vezes, sem limites do Estado Inquisidor.

Segue a almejada nova redação do parágrafo 1º do art. 10 da Lei 12.965/2014:

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial ou requisição da autoridade competente**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º. (grifo nosso)

O que dizer desta tentativa de amputação de garantia individual, tão cara à construção do substantivo desenho do indivíduo, sustentáculo de toda ideia liberal de Estado?

A Constituição Federal de 1988 exigiu a ordem judicial para a quebra do sigilo de dados. Desta forma, e trazendo o ensinamento de Maurício Zanoide de Moraes (2010, p. 74), sem a determinação judicial para a quebra do sigilo de dados, a intervenção estatal seria ilegítima ou não permitida, violadora, portanto.

Explicitando o tema, o mesmo Maurício Zanoide é enfático (2010, p. 74):

Os direitos fundamentais *prima facie* são direitos restringíveis e esta redução em seu âmbito pode se dar apenas por meio de uma norma que também seja uma “norma constitucional”. No caso, por constitucional, devem ser entendidas tanto normas cuja natureza e posição hierárquica se vinculem diretamente ao capítulo constitucional dos direitos fundamentais, como também aquelas normas de nível inferior, mas elaboradas por determinação constitucional.

No caso em exame, tem-se, de um lado, o sigilo de dados trazido pela Constituição Federal expressamente como direito fundamental e, de outro lado, a tentativa, via legislação ordinária, de burla da magna proteção, transformando o instrumento legislativo em porta-voz da intervenção estatal ilegítima já denunciada.

Diante do espaço da individualidade, resguardado pela Carta de Direitos da República, a exceção à quebra do segredo ali contido se dará ou, voluntariamente, pelo indivíduo detentor do sigilo, ou,



motivadamente, pelo Estado, cumprida as regras do devido processo legal, sendo a indispensabilidade de ordem judicial uma norma de ouro. Postura contrária a esse entendimento libera o Estado para desconfiar de todos e vasculhar a esmo os indivíduos, bastando um protocolo formal de aparente obediência à lei. Vislumbra-se, aqui, outra inconstitucionalidade, por descumprimento de outro direito fundamental: a presunção de inocência.

É a presunção de inocência que garante ao indivíduo a salvaguarda do direito à privacidade, o direito de exigir uma decisão judicial fundamentada para a quebra de seu espaço privado, deixando nas mãos do Estado inquisidor a obrigação de apresentar em juízo o conjunto indiciário contrário. Para adentrar a esfera íntima, deverá o Estado Inquisidor demonstrar a necessidade e proporcionalidade da medida à autoridade judiciária competente.

Até que uma decisão judicial, necessária e proporcional, excepcione o sigilo de dados, todo indivíduo tem o direito de salvaguarda de suas informações, que não podem ser devassadas, como se suspeitas fossem, em princípio.

Não é à toa que a indispensabilidade de decisão judicial para a quebra de sigilo de dados é um obstáculo ao Estado Arbitrário.

É, deveras, porque a presunção de inocência é uma norma de juízo, uma exigência que “incide em toda decisão, no instante de se analisar o material probatório já produzido para a formação da convicção judicial.” (ZANOIDE, 2010, p. 468) Portanto, manifesta-se em todas as decisões proferidas na persecução penal, qualificando e legitimando o ato. Justamente por seu caráter protetor das garantias individuais, não pode o filtro do Poder Judiciário ser alijado da quebra do sigilo de dados. Por acaso alguma individualidade resistiria à perquirição indiscriminada dos inquisidores?

Note-se que a celeridade da persecução penal tenta fundamentar a tentativa de alteração legislativa que visa dar “poderes imediatos às autoridades de investigação”. Sob o manto da urgência e da pronta resposta à sociedade<sup>11</sup>, inscritas na exposição de motivos

---

11 A função simbólica atribuída à instrução preliminar, qual seja a de contribuir para amenizar o mal-estar causado pelo crime, demonstrando a atuação dos órgãos do

do Projeto de Lei 1.589/2015, confere-se uma presunção de que as autoridades investigantes estariam atuando corretamente ao vigiar e esmiuçar os indivíduos (a esta altura, presumivelmente, culpados).

Conforme relatado por Mauro Fonseca Andrade (2012, p. 284) e por tantos pesquisadores do período inquisitorial, a confiança no inquisidor não parece ser um guia a orientar o Processo Penal na direção da realização democrática:

Nesses casos havia uma presunção *in favorem fidei* de que o inquisidor estaria atuando corretamente, e que aquele que recorria sistematicamente tentava, na realidade, dilatar o tempo de duração do processo. A Igreja Católica abandonava sua preocupação com a legalidade do procedimento ou comportamento do imputado, para centrar sua atenção exclusivamente na celeridade do processo.

É preocupante notar que a busca pela celeridade, que norteia o projeto de lei comentado, também esteve presente nos processos da cruel Inquisição Espanhola, quando “havia uma explícita e insistente preocupação com a celeridade do processo.” (ANDRADE, 2012, p. 291).

A busca pela rápida elucidação do fato criminoso não pode justificar o atropelo de garantias processuais, uma vez que se insere dentre as finalidades do processo penal, justamente, a instrumentalização da “máxima eficácia dos direitos e garantias fundamentais, em especial da liberdade individual”. (LOPES JUNIOR, 2008, p. 25)

## REFERÊNCIAS

ANDRADE, Mauro Fonseca. *Sistemas Processuais Penais e seus Princípios Reitores*. Curitiba: Juruá, 2012.

ARENDETT, Hannah. *Origens do totalitarismo*. Tradução de Roberto Raposo. São Paulo: Companhia das Letras, 2012.

ASSANGE, Julian ...[et al.] *Cypherpunks: liberdade e o futuro da internet*. Tradução de Cristina Yamagami. São Paulo: Boitempo, 2013.

---

Estado, evitando a impunidade, tem-se desvirtuado e “explorada para muito além do limite razoável.” (LOPES JÚNIOR, 2013, p. 106/107)

BAUMAN, Zygmunt. *Danos colaterais. Desigualdades sociais numa era global*. Tradução de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

\_\_\_\_\_, Zygmunt. *Modernidade líquida*. Tradução de Plínio Dentzein. Rio de Janeiro: Zahar, 2001.

FERRAJOLI, Luigi. *Derecho y Razón. Teoría del Garantismo Penal*. 10. ed. Trad. Perfecto Andrés Ibáñez; Alfonso Ruiz Miguel; Juan Carlos Bayón Mohino; Juan Terradillos Basoco; e Rocío Cantarero Bandrés. Madrid: Trotta, 2011.

LOPES JUNIOR, Aury. *Direito Processual Penal e sua Conformidade Constitucional*. v.I. 3ª ed., Rio de Janeiro: Lumen Juris, 2008.

\_\_\_\_\_. *Investigação Preliminar no Processo Penal*. São Paulo: Saraiva, 2013.

MORAES, Maurício Zanoide. *Presunção de Inocência no Processo Penal Brasileiro: análise de sua estrutura normativa para a elaboração legislativa e para a decisão judicial*. Rio de Janeiro: Lumen Juris, 2010.

PRADO, Geraldo. *Prova penal e sistema de controles epistêmicos. A quebra da cadeia de custódia das provas obtidas por métodos ocultos*. São Paulo: Marcial Pons, 2014.

TAVARES, Juarez. *Teoria do Injusto Penal*. Belo Horizonte: Del Rey, 2003

VIANNA, Cynthia Semíramis Machado. *Em busca da privacidade perdida: do direito à privacidade à privação de direitos*. Belo Horizonte, 2004. Dissertação (Mestrado em Direito). Faculdade de Direito, Pontifícia Universidade Católica de Minas Gerais.

VIANNA, Túlio Lima. *Transparência pública, opacidade privada: o Direito como instrumento de limitação do poder na sociedade de controle*. 181 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade Federal do Paraná, Curitiba. 2006.

**Recebido em 11/03/2016.**

**Aprovado em 14/06/2016.**

