ANONIMATO, PROTEÇÃO DE DADOS E DEVIDO PROCESSO LEGAL: POR QUE E COMO CONTER UMA DAS MAIORES AMEAÇAS AO DIREITO À PRIVACIDADE NO BRASIL

Mariana Cunha e Melo[1]

Introdução

O objetivo deste artigo é analisar os aspectos procedimentais da defesa do anonimato na internet. A discussão sobre o anonimato hoje não envolve apenas a existência de assinatura em textos escritos, mas também tem implicações na proteção de dados pessoais. Não se trata apenas da liberdade para se manifestar com uma máscara ou sem assinatura, mas de impor limites à possibilidade de monitoramento de qualquer atividade online. Nesse sentido, fala-se muito, além do direito de escrever anonimamente, no direito de ler anonimamente[2].

Qualquer discussão sobre anonimato costuma atrair dois polos para o debate. Por um lado, há um receio razoável de que o anonimato seja utilizado para cometer toda espécie de abuso *online*. *Cyber-bullying*, ataques a grupos minoritários e calúnias em geral – tudo assume um alcance virtualmente impossível de ser previsto ou restringido[3]. A internet, portanto, reduz os custos envolvidos em cometer uma variedade de crimes relacionados ao discurso. A gravidade da

---

[1] Bacharel em direito pela UERJ, mestre em direito pela Nova York University (NYU) e doutoranda em direito no UniCEUB, sob orientação do Professor Luís Roberto Barroso. Autora do livro "The 'Marco Civil da Internet' and its unresolved issues: free speech and due process of law", publicado pela Editora CTV em 2016. Pesquisadora no Centro Brasileiro de Estudos Constitucionais, vinculado ao UniCEUB, comentarista do Observatório do Marco Civil, ex-integrante do conselho consultor da ONG Index on Censorship (mandato janeiro-julho de 2016) e advogada no escritório Barroso Fontelles, Barcellos, Mendonça, em Brasília.

[2] ELECTRONIC FRONTIER FOUNDATION, **Anonymity and Encryption** (Feb. 2015), p. 7. Disponível em: <https://www.eff.org/document/eff-comments-submitted-united-nations-special-rapporteur-promotion-and-protection-right> Acesso em: 23.03.17: "The ability to read and access information anonymously is also crucial for the exercise of free expression. Article 19 of the Universal Declaration of Human Rights, which enshrines the right to freedom of opinion and expression, includes the right to seek, receive, and impart information and ideas through any media. … In other words, the right to seek and receive information is chilled when the government or others have unchecked access to records that document the viewing or reading habits of individuals". Ver também: COHEN, Julie E. A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace. **28 Conn. L. Rev.**. 981-1039 (1996). Disponível em: <http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1815&context=facpub> Acesso em: 23.03.17: "Anonymous advocacy has always been controversial. Anonymous reading, in contrast, is something that is taken for granted".

[3] GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320 (2008).

situação é tal que Danielle Citron, uma das mais proeminentes especialistas em crimes de internet, compara o padrão de comportamento dos que cometem crimes de ódio na internet a grupos mascarados como a Ku Klux Klan[4].

Nesses casos, o anonimato dificulta a identificação dos responsáveis pelos abusos e provoca, ele mesmo, um efeito inibidor no discurso. Imagine-se a situação em que uma ativista pelos direitos dos animais defenda a alteração da legislação federal em um blog. E, como resultado, sofra toda espécie de ataque à sua intimidade e privacidade por um grupo de opositores. Seria plenamente possível que essa militante se sentisse insegura para defender suas posições publicamente. Consequentemente, o debate público se retrairia ao invés de se expandir pelo uso do anonimato.

Engana-se, contudo, quem imagina uma solução radical para o problema da nossa ativista. O anonimato é frequentemente utilizado pelos mais diversos grupos de pessoas para emitir opinião ou disseminar informações no debate público sem risco de represálias no mundo eletrônico ou físico. Imagine-se que a ativista tenha criado um blog, por meio de um pseudônimo, para fazer campanha contra um político local, acusado de corrupção. O político, em contrapartida, busca obter a identidade da ativista com o objetivo de prejudicá-la em seu emprego ou ameaçá-la de outra forma. Se o parâmetro para obtenção de sua identidade não levar em conta a ilicitude do que houver sido dito e a relevância de se divulgar esses dados pessoais, o político não terá dificuldades de prejudicar a ativista ainda que essa não tenha cometido qualquer ilícito.

Em apertada síntese, é possível identificar três motivos para se enxergar alguma relevância no anonimato na internet[5]. ***Em primeiro lugar***, o direito de evitar a vigilância – ou até a possibilidade de vigilância – é de extrema valia em um mundo que está progressivamente mais afeito a iniciativas de vigilância absoluta. E aqui vale lembrar que, ainda que não haja efetiva

[4] CITRON, Danielle Keats, Cyber Civil Rights, **89 Boston University Law Review** 81 (2009).

[5] Para mais informações sobre essa discussão, v.: CUNHA E MELO, Mariana. The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law. Curitiba, **CRV** (2016); ORGANIZAÇÃO DAS NAÇÕES UNIDAS, **Report on encryption, anonymity, and the human rights framework**: Disponível em: <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> Acesso em: 23.03.17; ELECTRONIC FRONTIER FOUNDATION, **Anonymity and Encryption** (Feb. 2015). Disponível em <https://www.eff.org/document/eff-comments-submitted-united-nations-special-rapporteur-promotion-and-protection-right> Acesso em: 23.03.17.

vigilância sobre todas as pessoas a todo o tempo, a *possibilidade* de vigilância provoca efeitos no comportamento das pessoas e na sua percepção de liberdade. É a ideia da sociedade no Panóptico.

Em segundo lugar, o anonimato na internet também tem um viés libertador, de empoderamento, que é permitir o controle do fluxo de informações sobre si. Trata-se de dar aos usuários o poder de proteger seus próprios dados da vigilância privada ou do Poder Público – essa é uma das funções mais poderosas do anonimato na internet[6].

Por fim, e ***em terceiro lugar***, a internet é considerada o grande mercado de ideias hoje, um fórum público. Muitas ideias e opiniões, contudo, são objeto de represálias de todas as formas – inclusive pela violência física. Nesse sentido, vale registrar o trabalho de ONGs como a Association for Progressive Communications (APC), que combate violência contra mulheres na internet, da Derechos Digitales, que promovem campanhas para o uso seguro da internet para fins de propagação de ideias[7], da Electronic Frontier Foundation[8] e da Access Now[9], duas das maiores organizações mundiais de defesa dos direitos civis na internet. Em muitos casos, esconder a identidade dos ativistas é a primeira fronteira de defesa contra violência na internet.

Há, portanto, um interesse na defesa do anonimato na internet – ao menos em alguma medida e em certas circunstâncias. E, apesar de a Constituição Federal vedar textualmente o anonimato no âmbito da manifestação do pensamento (art. 5º, IV), a mesma Carta também garante a inviolabilidade do sigilo de dados e a proteção da intimidade dos cidadãos (art. 5º, X e XII). No mundo de hoje, não há como compatibilizar uma interpretação literal da primeira com o sentido mais essencial dessas últimas[10].

Assumindo que há ao menos um interesse mínimo no anonimato enquanto direito de assumir pseudônimos e proteger seus dados de identidade, isso nos leva a um ponto de fundamental importância: o devido processo legal, que compreende o direito de participar do procedimento capaz de resultar em restrição da liberdade ou de seus bens. Envolve, ainda, o

---

[6] Confira-se em: <https://www.apc.org/en/node/15007/>. Acesso em: 23.03.17

[7] Confira-se em: <https://www.derechosdigitales.org/notemasainternet/>. Acesso em: 23.03.17

[8] Confira-se em: <https://www.eff.org/wp/blog-safely>. Acesso em: 23.03.17

[9] Confira-se em: <https://www.accessnow.org/issue/freedom-of-expression/> Acesso em: 23.03.17

[10] Para uma discussão hermenêutica sobre uma interpretação mitigada da vedação do anonimato, v.: CUNHA E MELO, Mariana, **The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law**. Curitiba, CRV, 2016.

direito à ampla defesa, ao contraditório: oportunidade de ser ouvido no processo.

O que existe hoje, por outro lado, é que os pedidos de fornecimento de dados sobre a identidade das pessoas são deferidos de forma quase automática. O autor não precisa ter uma boa razão para formular esse pedido. E pior: o maior interessado sequer é chamado ao processo. Se o direito que está em jogo aqui é o direito ao sigilo de dados sobre sua identidade, como o titular do direito poderia se defender sem revelar quem ele é e, portanto, derrotar todo o propósito dele ter uma chance de se defender?

Quando se discutem os procedimentos para defesa do anonimato, portanto, o que se pretende alcançar é um meio de permitir a defesa dos dados antes da entrega dos mesmos e da consumação do dano a importantes direitos fundamentais. É esse o objeto de investigação do presente artigo. *Em primeiro lugar*, será apresentado um panorama geral da legislação brasileira sobre anonimato e quebra de sigilo de dados sobre comunicações. Nesse ponto, serão delineadas justificativas para a interpretação mitigada do anonimato. *Em segundo lugar,* serão analisadas as repercussões do procedimento atual de fornecimento de dados para o princípio do devido processo legal. *Em terceiro lugar*, serão expostos os fatores mais relevantes para um procedimento adequado de fornecimento de dados.

Pedidos de identificação de usuários de Internet: entre a vedação ao anonimato e a proteção de dados

A jurisprudência brasileira sobre pedidos de identificação de usuários na internet é bastante permissiva. Em muitos casos, o pedido de fornecimento de dados é feito quase que de forma automática, com fundamento exclusivo na proibição constitucional ao anonimato. Em inúmeras oportunidades, as Turmas de Direito Privado do Superior Tribunal de Justiça afirmaram a obrigação dos provedores de serviço de internet garantirem a possibilidade de identificação de seus usuários para "coibir o anonimato"[11]. Aos poucos, a jurisprudência se

[11] BRASIL, STJ, DJe 02/05/2012, REsp 1306066/MT, Rel. Min. Sidnei Beneti: "RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. PROVEDOR. MENSAGEM DE CONTEÚDO OFENSIVO. RETIRADA. REGISTRO DE NÚMERO DO IP. DANO MORAL. AUSÊNCIA. PROVIMENTO. 1.- No caso de mensagens moralmente ofensivas, inseridas no site de provedor de conteúdo por usuário, não incide a regra de responsabilidade objetiva, prevista no art. 927, parágrafo único, do Cód. Civil/2002, pois não se configura risco inerente à atividade do

desenvolveu para passar a exigir que os provedores armazenassem dados de usuários por ao menos três anos – justamente para viabilizar a identificação por esse tempo[12-13].

A vedação constitucional e o interesse em viabilizar a responsabilização de autores de ilícitos na internet não são, contudo, os únicos elementos na resolução desse tipo de conflito. Com efeito, em oposição a essa linha jurisprudencial, precedentes que tratam sobre sigilo de dados parecem seguir um caminho diferente. No Brasil, a tutela dos sigilos constitucionais é dividida em duas categorias diferentes: a proteção prevista textualmente no art. 5º, XII da Constituição e aquela extraída de uma garantia geral à intimidade e à vida privada, no art. 5º, X. No primeiro grupo, estão os sigilos sobre o *conteúdo* das comunicações. No segundo, os demais

---

provedor. Precedentes. 2.- É o provedor de conteúdo obrigado a retirar imediatamente o conteúdo ofensivo, pena de responsabilidade solidária com o autor direto do dano. 3.- O provedor de conteúdo é obrigado a viabilizar a identificação de usuários, coibindo o anonimato; o registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na internet constitui meio de rastreamento de usuários, que ao provedor compete, necessariamente, providenciar".

12 BRASIL, STJ, DJe 18/06/2014, AgRg no REsp 1402104/RJ, Rel. Min. Raul Araújo: "A responsabilidade subjetiva do agravante se configura quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide; II) não mantiver um sistema ou não adotar providências, que estiverem tecnicamente ao seu alcance, de modo a possibilitar a identificação do usuário responsável pela divulgação ou a individuação dele, a fim de coibir o anonimato. O fornecimento do registro do número de protocolo (IP) dos computadores utilizados para cadastramento de contas na internet constitui meio satisfatório de identificação de usuários". No mesmo sentido, v.: BRASIL, STJ, DJe 23/05/2014, AgRg no REsp 1396963/RS, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 28/05/2014, AgRg no REsp 1285756/MG, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 26/05/2014, AgRg no REsp 1395803/RJ, Rel. Min. Raul Araújo; BRASIL, STJ, DJe 22/05/2014, AgRg no REsp 1395768/RJ, Rel. Min. Raul Araújo.

13 BRASIL, STJ, DJe 10/03/2014, REsp 1417641/RJ, Rel. Min. Nancy Andrighi: "2. Recurso especial que discute os limites da responsabilidade dos provedores de hospedagem de blogs pela manutenção de dados de seus usuários. 3. Ao oferecer um serviço por meio do qual se possibilita que os usuários divulguem livremente suas opiniões, deve o provedor de conteúdo ter o cuidado de propiciar meios para que se possa identificar cada um desses usuários, coibindo o anonimato e atribuindo a cada imagem uma autoria certa e determinada. Sob a ótica da diligência média que se espera do provedor, do dever de informação e do princípio da transparência, deve este adotar as providências que, conforme as circunstâncias específicas de cada caso, estiverem ao seu alcance para a individualização dos usuários do site, sob pena de responsabilização subjetiva por *culpa in omittendo*. Precedentes. 4. Uma vez ciente do ajuizamento da ação e da pretensão nela contida - de obtenção dos dados de um determinado usuário - estando a questão sub judice, o mínimo de bom senso e prudência sugerem a iniciativa do provedor de conteúdo no sentido de evitar que essas informações se percam. Essa providência é condizente com a boa-fé que se espera não apenas dos fornecedores e contratantes em geral, mas também da parte de um processo judicial, nos termos dos arts. 4º, III, do CDC, 422 do CC/02 e 14 do CPC. 5. As informações necessárias à identificação do usuário devem ser armazenadas pelo provedor de conteúdo por um prazo mínimo de 03 anos, a contar do dia em que o usuário cancela o serviço". No mesmo sentido, v.: BRASIL, STJ, DJe 26/11/2013, REsp 1398985/MG, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 25/03/2014, REsp 1403749/GO, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 26/09/2013, REsp 1383354/SP, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 26/06/2012, REsp 1300161/RS, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 02/08/2012, REsp 1192208/MG, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 19/06/2012, REsp 1308830/RS, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 31/08/2011, REsp 1186616/MG, Rel. Min. Nancy Andrighi; BRASIL, STJ, DJe 08/08/2011, REsp 1193764/SP, Rel. Min. Nancy Andrighi.

sigilos protegidos, como o bancário, o fiscal e dos *dados sobre comunicações* – **que constituem *informações sobre os atos de comunicação* efetuados pelos indivíduos.** Nessa categoria, se incluem o sigilo telefônico – lista das chamadas recebidas e efetuadas, com as respectivas datas e horários – e os registros eletrônicos relacionados à troca de e-mails – como o número de IP e as respectivas informações de data e horário.

Como se sabe, a proteção específica conferida pelo art. 5º, XII da Constituição é a mais substancial. Primeiramente, somente admite a quebra do sigilo em sede de investigação de crimes graves – nunca em processo cível. Além disso, nos termos da legislação de regência, exigem-se (i) "indícios razoáveis" do cometimento de um *crime*; (ii) demonstração da inexistência de meios alternativos (necessidade); (iii) o crime investigado deve ser punível por reclusão (crime grave) (Lei nº 9296/1996, art. 2º); (iv) limitação temporal (art. 5º).

A garantia geral à intimidade, ainda que mais branda, impõe também uma série de requisitos de validade à quebra dos demais sigilos[14]. A jurisprudência exige, também nesses casos, que a decisão de quebra de sigilo receba uma fundamentação específica, com a demonstração: (i) de indícios de que uma pessoa específica tenha cometido atos ilícitos[15]; dos

---

[14] BRASIL, STF, DJ 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello (Tribunal Pleno): "Essa diretriz jurisprudencial [de se exigir fundamentação adequada das decisões de quebra de sigilo] (...) reconhece que o direito à intimidade – que representa importante manifestação dos direitos da personalidade – qualifica-se como expressiva prerrogativa de ordem jurídica que consiste em garantir, em favor da pessoa, de qualquer pessoa, na esfera de sua vida privada, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros, notadamente a do Poder Publico. Daí a correta advertência feita por Carlos Alberto Di Franco, para quem 'um dos grandes desafios da sociedade moderna é a preservação do direito à intimidade. Nenhum homem pode ser considerado verdadeiramente livre, se não dispuser de garantia de inviolabilidade da esfera de privacidade que o cerca".

[15] TJSP, 13a Cam. Crim., HC 00430001-50.2014.8.26.0000/Franca, rel. Des. Augusto de Siqueira, j. 07/08/2014: "Muito embora os direitos sejam relativos, inclusive os constitucionais, sua flexibilização não pode ser indiscriminada, admitindo obtenção de informações sobre dados de quaisquer assinantes da empresa de telefonia, ao longo de um ano. A autorização deve ser concreta, ou seja, incidir sobre a prática de crimes específicos, cometidos por determinada ou determinadas pessoas e pelo tempo necessário à obtenção da prova. Nesse sentido já se decidiu: '(...) [A] **indicação do indivíduo ou do telefone objeto de investigação, e assim das razões que levam a autoridade a propor a quebra do sigilo legal, têm de ser deduzidas a 'priori'**, sem prejuízo do relatório posterior das diligência' (TJSP - Habeas Corpus n. 993.08.045010-2 Rel. Desembargador Aben-Athar). 'Habeas Corpus Sigilo de dados cadastrais de clientes de concessionárias de serviços telefonia **Não indicação de fato concreto e de pessoas individualizadas Autorização de quebra de sigilo genérica e sem fundamentação específica. Inadmissibilidade** Devassa que afronta as garantias constitucionais da intimidade e da privacidade (art. 5o, X, CF) e o princípio da dignidade da pessoa humana (art. 1o, III,CF) Receio fundado de represália jurídico-penal decorrente do descumprimento da sobredita ordem judicial genérica 'Mandamus' concedido, com extensão' (TJSP - Habeas Corpus n. 990.09.227159-8 Rel. Desembargador Moreira da Silva)".

fatos que se pretende comprovar com a quebra de sigilo[16], (ii) dos *indícios* de que os fatos serão comprovados por meio do provimento excepcional[17]; (iii) da necessidade da medida[18]; e (iv) do lapso temporal em que os dados deverão ser captados[19].

---

16 BRASIL, TJSE, Cam. Crim, HC 2010314476, rel. Des. Geni Silveira Schuster, j. 08/02/2011: "A determinação de fornecimento de senha franqueando a agentes policiais o acesso ilimitado a dados cadastrais de clientes afronta o disposto no inciso X, do art. 5o da Constituição Federal, já que qualquer pessoa pode ter devassado os seus dados, uma vez que a ordem judicial não é específica, não se vinculando a um caso concreto".

17 BRASIL, STF, DJ 04 ago. 2006, MS 25668/DF, Rel. Min. Celso de Mello: "A QUEBRA DE SIGILO - QUE SE APÓIA EM FUNDAMENTOS GENÉRICOS E **QUE NÃO INDICA FATOS CONCRETOS E PRECISOS REFERENTES À PESSOA SOB INVESTIGAÇÃO - CONSTITUI ATO EIVADO DE NULIDADE**. - A quebra do sigilo inerente aos **registros bancários, fiscais e telefônicos**, por traduzir medida de caráter excepcional, revela-se incompatível com o ordenamento constitucional, quando fundada em deliberações emanadas de CPI cujo suporte decisório apoia-se em **formulações genéricas, destituídas da necessária e específica indicação de causa provável**, que se qualifica como **pressuposto legitimador da ruptura, por parte do Estado, da esfera de intimidade a todos garantida pela Constituição da República**".

18 BRASIL, STF, DJ 23 fev. 06, MS 25812 MC, Rel. Min. Cezar Peluso.

19 BRASIL, STF, DJ 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello: "A QUEBRA DE SIGILO NÃO PODE SER UTILIZADA COMO INSTRUMENTO DE **DEVASSA INDISCRIMINADA**, SOB PENA DE OFENSA À GARANTIA CONSTITUCIONAL DA INTIMIDADE. - A **quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes**. É que, se assim não fosse, a quebra de sigilo converter-se-ia, ilegitimamente, em **instrumento de busca generalizada e de devassa indiscriminada da esfera de intimidade das pessoas**, o que daria, ao Estado, em desconformidade com os postulados que informam o regime democrático, o **poder absoluto de vasculhar, sem quaisquer limitações, registros sigilosos alheios**. (...) **Para que a medida excepcional da quebra de sigilo bancário não se descaracterize em sua finalidade legítima**, torna-se imprescindível que o ato estatal que a decrete, além de adequadamente fundamentado, também indique, de modo preciso, dentre outros dados essenciais, **os elementos de identificação do correntista (notadamente o número de sua inscrição no CPF)** e o lapso temporal abrangido pela ordem de ruptura dos registros sigilosos mantidos por instituição financeira". STF, DJ 23 fev. 06, MS no 25.812, Rel. Min. Cezar Peluso: "O outro requisito é a **existência de limitação temporal do objeto da medida** (d) [quebra de sigilo bancário], enquanto predeterminação formal do período que, constituindo a referência **do tempo provável** em que teria ocorrido o fato investigado, seja suficiente para lhe esclarecer a ocorrência por via tão excepcional e extrema. E é não menos cristalina a racionalidade desta condição decisiva, pois **nada legitimaria devassa ilimitada da vida bancária, fiscal e comunicativa do cidadão**, debaixo do pretexto de que Comissão Parlamentar de Inquérito precise investigar **fato ou fatos específicos, que são sempre situados no tempo, ainda quando de modo só aproximado**. Ou seja - para que se não invoque nenhuma dúvida ao propósito -, a Constituição da República não tolera devassa ampla de dados da intimidade do cidadão, quando, para atender a necessidade legítima de investigação de ato ou atos ilícitos que lhe seriam imputáveis, basta seja **a quebra de sigilos limitada ao período de tempo em que se teriam passado esses mesmos supostos atos**. **Que interesse jurídico pode enxergar-se na revelação de dados íntimos de outros períodos?** Só a concorrência de todos esses requisitos autoriza, perante a ordem constitucional, à luz do princípio da proporcionalidade, a prevalência do interesse público, encarnado nas deliberações legítimas de CPI, sobre o resguardo da intimidade, enquanto bem jurídico e valor essencial à plenitude da dignidade da pessoa humana". V. também: STF, *DJ* 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello (Tribunal Pleno): "A QUEBRA DE SIGILO NÃO PODE SER UTILIZADA COMO INSTRUMENTO DE DEVASSA INDISCRIMINADA, SOB PENA DE OFENSA À GARANTIA CONSTITUCIONAL DA INTIMIDADE. - A quebra de sigilo não pode ser manipulada, de modo arbitrário, pelo Poder Público ou por seus agentes. É que, se assim não fosse, a quebra de sigilo converter-se-ia, ilegitimamente, em instrumento de busca generalizada e de devassa indiscriminada da esfera de intimidade das pessoas, o que daria, ao Estado, em desconformidade com os postulados que informam o regime democrático, o poder absoluto de vasculhar, sem quaisquer limitações, registros sigilosos alheios"; STF, *DJ* 16 jun. 2006, HC 84758, Rel. Min. Celso de Mello (Tribunal Pleno): "Para que a medida excepcional da quebra de sigilo bancário não

Essas exigências se justificam, mesmo nas situações regidas pelo art. 5º, X da Constituição porque, nas palavras do Ministro Cezar Peluso, "não se pode sacrificar direito fundamental tutelado pela Constituição - o direito à intimidade -, mediante uso da medida drástica e extrema da quebra de sigilos, quando a existência do fato ou fatos sob investigação pode ser lograda com recurso aos meios ordinários de prova"[20]. Em uma única preposição: "[r]estrições absolutas a direito constitucional só se justificam em situações de absoluta excepcionalidade"[21] [22].

De forma específica, quanto à proteção dos *dados sobre comunicações* na internet, o Marco Civil da Internet, como esperado, incorporou os princípios gerais explorados pela jurisprudência constitucional. Em seu artigo 22, dispõe textualmente que ordens de quebra de sigilo dos registros de conexão ou de registros de acesso a aplicações de internet devem indicar: (i) "fundados indícios da ocorrência do ilícito"; (ii) "justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória"; e (iii) o "período ao qual

---

se descaracterize em sua finalidade legítima, torna-se imprescindível que o ato estatal que a decrete, além de adequadamente fundamentado, também indique, de modo preciso, dentre outros dados essenciais, os elementos de identificação do correntista (notadamente o número de sua inscrição no CPF) e o lapso temporal abrangido pela ordem de ruptura dos registros sigilosos mantidos por instituição financeira"; STF, *DJ* 04 ago. 2006, MS 25668/DF, Rel. Min. Celso de Mello (Tribunal Pleno): "A QUEBRA DE SIGILO - QUE SE APÓIA EM FUNDAMENTOS GENÉRICOS E QUE NÃO INDICA FATOS CONCRETOS E PRECISOS REFERENTES À PESSOA SOB INVESTIGAÇÃO - CONSTITUI ATO EIVADO DE NULIDADE. - A quebra do sigilo inerente aos registros bancários, fiscais e telefônicos, por traduzir medida de caráter excepcional, revela-se incompatível com o ordenamento constitucional, quando fundada em deliberações emanadas de CPI cujo suporte decisório apóia-se em formulações genéricas, destituídas da necessária e específica indicação de causa provável, que se qualifica como pressuposto legitimador da ruptura, por parte do Estado, da esfera de intimidade a todos garantida pela Constituição da República".

[20] BRASIL, STF, DJ 23 fev. 06, MS 25812 MC, Rel. Min. Cezar Peluso.

[21] BRASIL, STF, DJ 23 fev. 06, MS 25812 MC, Rel. Min. Cezar Peluso.

[22] No mesmo sentido, vale ver a manifestação do Ministro Celso de Mello: BRASIL, STF, DJ 14 fev. 2001, MS 23669, Rel. Min. Celso de Mello: "A GARANTIA CONSTITUCIONAL DA INTIMIDADE, EMBORA NÃO TENHA CARÁTER ABSOLUTO, NÃO PODE SER ARBITRARIAMENTE DESCONSIDERADA PELO PODER PÚBLICO. - O direito à intimidade - que representa importante manifestação dos direitos da personalidade - qualifica-se como expressiva prerrogativa de ordem jurídica que consiste em reconhecer, em favor da pessoa, a existência de um espaço indevassável destinado a protegê-la contra indevidas interferências de terceiros na esfera de sua vida privada. A transposição arbitrária, para o domínio público, de questões meramente pessoais, sem qualquer reflexo no plano dos interesses sociais, tem o significado de grave transgressão ao postulado constitucional que protege o direito à intimidade, pois este, na abrangência de seu alcance, representa o 'direito de excluir, do conhecimento de terceiros, aquilo que diz respeito ao modo de ser da vida privada' (HANNAH ARENDT). O DIREITO AO SIGILO BANCÁRIO - QUE TAMBÉM NÃO TEM CARÁTER ABSOLUTO - CONSTITUI EXPRESSÃO DA GARANTIA DA INTIMIDADE. - O sigilo bancário reflete expressiva projeção da garantia fundamental da intimidade das pessoas, não se expondo, em consequência, enquanto valor constitucional que é, a intervenções de terceiros ou a intrusões do Poder Público desvestidas de causa provável ou destituídas de base jurídica idônea".

se referem os registros".

O que se tem, portanto, é a proibição do anonimato, de um lado, e a garantia do sigilo dos dados sobre comunicações, de outro. Longe de se tratar de situação inconciliável, o aparente conflito entre as normas exige apenas uma acomodação hermenêutica dos dois comandos normativos[23]. A necessidade de interpretação temperada da proibição do anonimato sequer é inédita na história brasileira. No direito penal, a parte final do art. 5º, IV da Constituição é fundamento também para a proibição das denúncias anônimas. A proibição, contudo, foi mitigada para proibir o oferecimento de denúncias fundadas *exclusivamente* em acusações anônimas, mas admitir que essas sejam usadas como um dos elementos da denúncia[24]. A flexibilização da vedação constitucional foi justificada nesses casos para que fosse compatibilizada com o interesse constitucional na persecução criminal.

Ainda que essa circunstância não justifique, por si só, a interpretação mais branda da

---

[23] Para uma discussão mais profunda sobre a viabilização da flexibilização da interpretação da regra da vedação do anonimato, v.: Mariana Cunha e Melo, **The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law.** Curitiba: CRV, 2016.

[24] BRASIL, STJ, DJe 16/05/2013, RMS 38.010/RJ, Rel. Min. Herman Benjamin: "2. O simples fato de o Inquérito Civil ter-se formalizado com base em denúncia anônima não impede que o Ministério Público realize administrativamente as investigações para formar juízo de valor sobre a veracidade da notícia. Ressalte-se que, no caso em espécie, os servidores públicos já estão, por lei, obrigados na posse e depois, anualmente, a disponibilizar informações sobre seus bens e evolução patrimonial. (...) 5. **A vedação ao anonimato, constante no art. 5°, IV, da Constituição Federal, há de ser harmonizada, com base no princípio da concordância prática, com o dever constitucional imposto ao Ministério Público de promover o Inquérito Civil e a Ação Civil Pública, para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos (art. 129, III).** 6. Nos termos do art. 22 da Lei 8.429/1992, o Ministério Público pode, mesmo de ofício, requisitar a instauração de inquérito policial ou procedimento administrativo para apurar qualquer ilícito previsto no aludido diploma legal. 7. Assim, ainda que a notícia da suposta discrepância entre a evolução patrimonial de agentes políticos e seus rendimentos tenha decorrido de denúncia anônima, não se pode impedir que o membro do Parquet tome medidas proporcionais e razoáveis, como no caso dos autos, para investigar a veracidade do juízo apresentado por cidadão que não se tenha identificado. 8. Em matéria penal, o STF já assentou que 'nada impede, contudo, que o Poder Público provocado por delação anônima ('disque-denúncia', p. ex.), adote medidas informais destinadas a apurar, previamente, em averiguação sumária, 'com prudência e discrição', a possível ocorrência de eventual situação de ilicitude penal, desde que o faça com o objetivo de conferir a verossimilhança dos fatos nela denunciados, em ordem a promover, então, em caso positivo, a formal instauração da persecutio criminis, mantendo-se, assim, completa desvinculação desse procedimento estatal em relação às peças apócrifas' (Inq 1.957, Rel. Min. Carlos Velloso, voto do Min. Celso de Mello, julgamento em 11.5.2005, Plenário, DJ de 11.11.2005). 9. Em se tratando de suposto ato de improbidade que só pode ser analisado mediante documentos, descabe absolutamente adotar medidas informais para examinar a verossimilhança, ao contrário do que se passa, por exemplo, em caso de denúncia anônima da ocorrência de homicídio. 10. O STJ reconhece a possibilidade de investigar a veracidade de denúncia anônima em Inquérito Civil ou Processo Administrativo, conforme se observa nos seguintes precedentes, entre os quais se destacam a orientação já firmada por esta Segunda Turma e uma recente decisão da Primeira Turma: RMS 37.166/SP, Rel. Ministro Benedito Gonçalves, Primeira Turma, DJe 15.4.2013; RMS 30.510/RJ, Rel. Ministra Eliana Calmon, Segunda Turma, DJe 10.2.2010; MS 13.348/DF, Rel. Ministra Laurita Vaz, Terceira Seção, DJe 16.9.2009".

proibição do anonimato, indica que a vedação não merece – e não recebe – a interpretação absoluta defendida por alguns críticos do uso do anonimato na internet.

A questão do devido processo legal

O tópico anterior fez uma análise positiva dos dois polos da discussão sobre anonimato na internet no Brasil[25]. Sob o viés da proteção do sigilo constitucional (art. 5º, X), foram vistos alguns requisitos de fundamentação das decisões. Essas garantias estão no cerne da proteção procedimental da intimidade dos usuários de internet e devem ser feitas valer. Às previsões já aventadas pela jurisprudência e pelo Marco Civil, porém, devem ser acrescidas outras, igualmente importantes, mas frequentemente negligenciadas na prática brasileira.

Com efeito, o conteúdo básico do devido processo legal (art. 5º, LIV) impõe que não se afaste a proteção constitucional ao conteúdo de e-mails sem ao menos a intimação do interessado para que esse possa, se achar necessário, defender seu direito fundamental. Importantes argumentos de ampla defesa que impõem a comunicação do titular do sigilo sujeito à quebra. ***Em primeiro lugar***, há uma restrição à liberdade do criador do conteúdo sem que ele tenha a possibilidade de defender previamente sua própria liberdade. Trata-se de um golpe de morte no sentido mais básico do devido processo legal.

A Constituição dispõe no artigo 5º, LIV que "ninguém será privado da liberdade ou de seus bens sem o devido processo legal". O princípio, portanto, pressupõe uma oitiva prévia de quem está por ter sua liberdade restringida. No caso da quebra de sigilo, a hipótese dificilmente poderia ser mais grave. Trata-se, afinal, da revogação da garantia de segredo sobre dados de alguém antes que ele possa defender seu direito fundamental.

Não se descuida aqui da possibilidade de concessão de decisões liminares sem a prévia oitiva do réu. A existência dessa prática, no entanto, não resolve o problema constitucional. Primeiramente, porque a própria ideia de provimento de tutela satisfativa *inaudita altera par* em restrição direta a direitos fundamentais é, em si, questionável. Não por outra razão, os tribunais superiores registram em diversos julgados e o Congresso, na Lei nº 8.437/92, a impossibilidade

[25] Para uma análise normativa desta autora sobre a matéria, v.: CUNHA E MELO, Mariana, **The Marco Civil da Internet and its Unresolved Issues**: free speech and due process of law. Curitiba, CRV, 2016.

de concessão de liminar satisfativa em processo civil[26], penal[27], trabalhista[28] e contra a fazenda pública[29].

Além disso, mesmo quando há provimento liminar antes da citação do réu, a parte interessada, ao ser intimada para cumprimento da decisão, têm o direito constitucional de pedir sua reconsideração ou mesmo impugná-la via recurso. Esse direito à revisão de qualquer provimento jurisdicional de primeiro grau foi inclusive reconhecido pelo Pacto de São José da Costa Rica (art. 8º, 2, *h*). A mesma possibilidade não se coloca quando o direito de um cidadão brasileiro é restringido à sua revelia, em processo proposto contra um terceiro (provedor de serviço na internet).

Em segundo lugar, a exemplo do que ocorre em conflitos de outros direitos fundamentais[30], quando o autor de um pedido de quebra aciona o provedor de serviço de internet, a discussão sobre a necessidade e pertinência do fornecimento dos dados é substancialmente mitigada[31]. No mínimo, o peso argumentativo de um terceiro defender a liberdade alheia é consideravelmente menor do que o peso da defesa do próprio interessado. Isso porque a demanda perde o enfoque de conflito entre direitos fundamentais e passa a assumir contornos de direito do consumidor – o cidadão que se sentiu ofendido, de um lado, e a empresa provedora de serviço de internet, de outro. Além disso, do ponto de vista do conteúdo da defesa do conteúdo impugnado, quando se retira o foco da discussão da relação autor-ofendido para a relação provedor-ofendido, uma série de questões podem passar despercebidas. O provedor não terá subsídio para deduzir razões específicas da legalidade da conduta do usuário cujo sigilo seria quebrado. Tampouco poderia a empresa defender de forma precisa a relevância da manutenção do sigilo de dados em

---

[26] BRASIL, STJ, DJ 20 jun. 2005, AgRg no REsp 584.527/RN, Rel. Min. Laurita Vaz.

[27] BRASIL, STF, DJ 21 mai. 2012, HC 112487/PR, Rel. Min. Celso de Mello.

[28] BRASIL, STF, DJ 29 ago. 2003, RE 162309/PE, Rel. Min. Marco Aurélio.

[29] BRASIL, Lei nº 8.437/1992, art. 1°, § 3º.

[30] V. CUNHA E MELO, Mariana, **O significado do Direito ao Esquecimento**, Jota (Nov. 2016), disponível em <http://jota.info/artigos/o-significado-direito-ao-esquecimento-22112016> Acesso em: 23.03.17.

[31] GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 330 (2008). "Finally, although a motion to quash may well be appropriate, without proper notice, John Doe subpoenas can easily become ex parte proceedings. In many jurisdictions, defendants must rely on the business policies of the subpoena's target or the goodwill of the plaintiff to receive notice. Even if the plaintiff does attempt to notify the defendant, he could fail—the defendant is, after all, anonymous. If the subpoena becomes ex parte, one of the defendant's most important defenses—his own vigorous advocacy—is eliminated. This combination of severe consequences meted out after limited trial process, possibly without opposition from the defendant whose identity is at risk, is a dangerous recipe that demands a carefully balanced standard".

cada caso.

Não por outra razão, o Código de Processo Civil restringe o alcance subjetivo dos efeitos da sentença. O art. 473 dispõe que a sentença faz coisa julgada para as partes da demanda e que não beneficia nem prejudica terceiros. Além disso, o art. 6º prevê que a nenhuma das partes é dado defender, em nome próprio, direito alheio. Nesse particular, a legislação processual pretende evitar que se criem substitutos processuais fora das hipóteses legais taxativas. Essa proibição tem o claro objetivo de proteger ao menos três classes de interesse: (i) o da parte em não ter seu direito defendido por terceiros sem seu consentimento; (ii) o do *ex adverso* em litigar com seu real opositor, inclusive como requisito para a obtenção de um provimento válido; (iii) o do intermediário, que seria prejudicado com o ônus excessivo de proteger, além dos seus próprios interesses, o direito de outrem – e sem condições materiais para fazê-lo de forma plenamente adequada.

Em terceiro lugar, além dos riscos para o usuário titular do direito ameaçado pelo pedido de fornecimento de dados, há também dois graves problemas procedimentais que agridem a esfera jurídica dos provedores de serviço da internet e que merecem destaque. O primeiro é o ônus de ser o único capaz de contraditar ordens abusivas direcionadas a seus usuários. Trata-se de uma situação difícil em que o provedor de serviços ou assume o ônus – financeiro e de imagem – inerente à impugnação reiterada de ordens judiciais ou abandona seus usuários ao risco de uma quebra de sigilo sem contraditório nem controle externo. O segundo, relacionado ao primeiro, é que frequentemente o provedor de serviço é condenado a arcar com os ônus sucumbenciais em caso de deferimento do pedido de fornecimento de dados. Ocorre que, a intervenção do Poder Judiciário para a legitimidade da quebra de sigilo é exigência legal e constitucional. Ou seja: em princípio, a empresa não "dará causa" ao processo judicial[32], ao resistir a uma pretensão legítima do autor da demanda. Afinal, não poderia legalmente fornecer os dados de identificação de usuários sem uma decisão judicial. Assim, a "causa" do processo, nesses casos, é a exigência constitucional de judicialização do conflito. Nesses casos, não parece

[32] Na doutrina processual civil brasileira, a parte que dá causa ao processo arca com os custos da ação. Ou seja: o autor, caso esse tenha ajuizado a demanda sem que tivesse o direito material pleiteado ou o réu, caso esse tenha resistido a uma pretensão legítima do autor, obrigando-o a se valer da estrutura judicial para garantir seu direito. V.: DINAMARCO, Cândido Rangel, **Instituições de Direito Processual Civil**, vol II, 6ª ed. São Paulo: Malheiros, 2009.

coerente com a teoria processual a empresa ser obrigada a arcar com a sucumbência.

Em suma: já vimos que há boas razões jurídicas para que pessoas ofendidas por atos ilícitos na internet tenham meios de identificar os responsáveis pelas ilicitudes. Vimos também, contudo, que a Constituição brasileira protege os sigilos de dados em geral e, em especial, aqueles que dizem respeito às comunicações. Nesse cenário, a quebra de sigilos sem a oitiva do interessado é providência no mínimo pouco usual no panorama processual e constitucional.

O próximo tópico irá analisar alternativas para conciliar os dois polos: (i) o interesse na identificação dos responsáveis pelo cometimento de ilícitos; e (ii) a garantia do sigilo de dados e do devido processo legal.

Modelos de proteção do devido processo legal aplicado à proteção de dados

Nos Estados Unidos, o anonimato é considerado um direito fundamental decorrente da liberdade de expressão[33]. Essa proteção especial do anonimato pode soar estranha no sistema brasileiro que, nesse particular, adotou postura diametralmente oposta. No Brasil, longe de ser direito fundamental decorrente da liberdade de expressão, o anonimato é vedado pelo mesmo dispositivo constitucional que garante a livre manifestação do pensamento. Como já mencionado, no entanto, a parte final do art. 5º, IV da Constituição não encerra todas as discussões sobre a identidade de usuários de internet. Isso porque a proteção dos sigilos constitucionais deve também ser equacionada nesses casos.

Por outro lado, essa proteção especial aos sigilos e à privacidade de forma geral não encontra paralelo no direito constitucional norte-americano. Esse enfoque especial na liberdade de expressão nos Estados Unidos e na privacidade no Brasil é marca de uma dicotomia clássica entre as tradições jurídicas norte-americana e europeia, muitas vezes caracterizada como um enfoque maior na liberdade, de um lado, e na dignidade da pessoa humana, de outro[34].

Seja qual for o fundamento constitucional e o ponto de vista da proteção material – seja a liberdade de expressão (anonimato), seja a privacidade (sigilo de dados) –, é possível concluir

---

[33] SUPREMA CORTE DOS ESTADOS UNIDOS, **Mclntyre v. Ohio Elections Commission**, 514 U.S. 334, 342 (1995)

[34] WHITMAN, James Q., The Two Western Cultures of Privacy: Dignity versus Liberty, **113 The Yale Law Journal** 1165 (Apr., 2004), disponível em: <http://www.jstor.org/stable/4135723> Acesso em: 23.03.17.

que o ato de fornecer dados pessoais capazes de identificar usuários de internet é de considerável gravidade constitucional nos dois países. Os Estados Unidos possuem vasta experiência na elaboração de procedimentos destinados a garantir a proteção do anonimato dos usuários de internet, de um lado, e a possibilidade de responsabilização dos autores de ilícitos, de outro.

Apesar das grandes diferenças nos parâmetros aplicados e em alguns detalhes procedimentais, é possível identificar um procedimento geral que se generalizou entre os Estados: trata-se dos litígios ajuizados contra *John Doe's* ou *Jane Doe*'s. O termo se refere a um nome genérico, algo como, no Brasil, chamaríamos de "Fulano de Tal". Em linhas gerais, o processo contra um *John* ou *Jane Doe* é formalizado por um autor contra uma pessoa ainda desconhecida. Nesses casos, a primeira fase do procedimento é, naturalmente, desvendar a identidade do réu – o que muitos denominam de "*unmask John Doe*" (desmascarar John Doe)[35].

Existem diversos procedimentos diferentes para processar um John Doe, a depender do Estado da federação americana[36]. A depender das opções específicas locais, o processo pode ser mais favorável aos autores[37] ou aos réus[38]. É possível, contudo, extrair uma ideia geral a partir de uma análise conjunta desses procedimentos. Com efeito, e de forma geral, duas características importantes devem ser destacadas: (i) viabilizam a tutela procedimental do direito fundamental a ser restringido (liberdade de expressão ou privacidade) sem desguarnecer a proteção dos interesses daqueles ofendidos por ilícitos praticados na internet por usuários anônimos[39]; e (ii)

---

35 ELECTRONIC FRONTIER FOUNDATION, **Test for Unmasking Anonymous Speech. Internet Law Treatise**. Disponível em <http://ilt.eff.org/index.php/Speech:_Anonymity#Tests_for_Unmasking_Anonymous_Speakers> Acesso em: 23.03.17.

36 Nathaniel Gleicher identifica ao menos sete modelos: Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (W.D. Wash. 2001); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999); Mobilisa, Inc. v. Doe 1, 170 P.3d 712 (Ariz. Ct. App. 2007); Krinsky v. Doe 6, 72 Cal. Rptr. 3d 231 (Ct. App. 2008); Doe No. 1 v. Cahill, 884 A.2d 451 (Del. 2005); Dendrite Int'l, Inc. v. Doe, No. 3, 775 A.2d 756 (N.J. Super. Ct. App. Div. 2001); *In re* Subpoena Duces Tecum to Am. Online, Inc. (*In re AOL)*, 52 Va. Cir. 26 (Cir. Ct. 2000), *rev'd on other grounds sub nom.* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001). GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320 (2008).

37 V., por exemplo: ESTADOS UNIDOS DA AMÉRICA, CORTE FEDERAL DE VIRGÍNIA, **In re AOL**, 52 Va. Cir. 26.

38 V., por exemplo: ESTADOS UNIDOS DA AMÉRICA, CORTE SUPERIOR DE NEW JERSEY, **Dendrite**, 775 A.2d 756.

39 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 325 (2008): "Although John Doe subpoenas are procedural tools, the standards governing them define the extent of First Amendment rights online. A standard that is too permissive severely weakens the ability of citizens to speak anonymously, limiting freedom of speech online. Too restrictive a standard leaves the increasing litany of targets of

permitem uma análise individualizada da justiça e da necessidade de se fornecer os dados dos usuários, o que favorece um rigor maior na apreciação da matéria.

De forma mais específica, vale destacar o profundo e sistêmico estudo desenvolvido por Nathaniel Gleicher. Em artigo antológico, o especialista em cyber-segurança condensou o complexo material jurisprudencial sobre o tema e extraiu seis fatores principais para a formulação de uma moldura legal que regule com justiça e segurança o processo de fornecimento de dados de usuários.

A ***primeira*** é a oportunidade de o interessado participar do procedimento e apresentar defesa sem que precise desvendar sua identidade. Esse é o ponto central da defesa do devido processo legal nesses casos. Sem dúvida, é uma questão que, por si só, provoca muitas dificuldades. Como notificar o usuário objeto da ordem? Qual deve ser o meio adequado? Quem deve ter o ônus da notificação e suportar os custos? Como permitir a representação de uma pessoa nos autos de um processo sem sua adequada qualificação? Qual seria o prazo de resposta do usuário?

Não cabe no propósito deste artigo desenvolver todos esses questionamentos. As três primeiras perguntas demandam uma reflexão mais urgente e merecem uma consideração adicional. Quanto à distribuição do ônus da notificação, dentre as diversas alternativas, existem jurisdições que exigem que o próprio autor empregue um "esforço razoável" para notificar o usuário do ajuizamento da ação e o seu teor[40]. Como o interesse na obtenção da informação é exclusivamente do autor, parece fazer sentido, ao menos em princípio, que ele arque com esse ônus.

Por outro lado, o esforço razoável de alguém se comunicar com um usuário anônimo nem

---

online harassment with no defense. Only a consistent nationwide standard for John Doe subpoenas will ensure balanced protection for both anonymous online speakers and the targets of anonymous online speech".

[40] SUPREMA CORTE DE DELAWARE, **Doe No. 1 v. Cahill**, 884 A.2d 451, 461 (Del. 2005). V., também: ELECTRONIC FRONTIER FOUNDATION, **Test for Unmasking Anonymous Speech. Internet Law Treatise**, disponível em <http://ilt.eff.org/index.php/Speech: Anonymity#Tests for Unmasking Anonymous Speakers>. Acesso em: 23.03.17.; "As best practices, those third parties should: **Make reasonable efforts** to notify the person whose identity is sought; If possible, agree to a timetable for disclosure of the information to the party seeking it that provides a reasonable opportunity for the Internet user to file an objection with a court before disclosure; Forward the exact statements and material provided by the person seeking the identity, including information about the cause of action alleged in the lawsuit and the evidence provided by the identityseeker to the court where provided to the service provider".

sempre será uma tarefa simples[41]. Assim, outras jurisdições optam por requerer que o próprio destinatário da ordem de fornecimento de dados se comunique com o titular dos dados requeridos – ou seja: o prestador do serviço utilizado pelo usuário anônimo. A empresa, em geral, está em posição privilegiada para contactar seus usuários e, portanto, teria maior probabilidade de sucesso no propósito de notificar o interessado[42].

Quanto ao meio de notificação, Gleicher aventa três possibilidades, em escala decrescente de confiabilidade em sua eficácia: (i) notificação direta – via e-mail ou outro meio privado; (ii) notificação pelo meio de comunicação utilizado para a suposta ofensa; e (iii) notificação via publicação[43]. As opções naturalmente não são excludentes e podem ser combinadas de múltiplas formas. E a notificação direta nem sempre será possível em razão da falta de informação sobre o usuário em questão.

Nos Estados Unidos, organizações de defesas de direitos civis na internet, como a *Electronic Frontier Foundation* atuam na representação de *John Doe*'s em juízo[44].

O direito brasileiro não admite a tramitação de processo contra pessoa indeterminada. De outra forma, não seria possível a autuação do processo (CPC, art. 206), a citação (CPC, art. 238) ou a representação da parte por advogado constituído nos autos (CPC, art. 104). Há, por outro lado, uma figura no processo civil brasileiro, que atua em casos que a parte, apesar de titular de direitos, não possui capacidade de estar em juízo. Trata-se da figura da curatela especial, que o Código de Processo Civil e a Lei Complementar nº 80 atribuem à Defensoria Pública. A curatela especial se presta a garantir a presença nos autos de quem, de outra forma, não poderia. O art. 72 do Código de Processo Civil prevê a atuação do curador especial para assistir (i) a parte incapaz sem representante legal ou quando os interesses desse e daquele forem conflitantes; e (ii) o réu revel, quando esse estiver preso ou em casos de citação ficta (por edital ou por hora certa), até que seja constituído advogado nos autos.

---

41 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 346 (2008).

42 É o caso da regulação no Estado da Virginia. Confira-se em DIGITAL MEDIA LAW PROJECT, **Legal Protections for Anonymous Speech in Virginia**, disponível em <http://www.dmlp.org/legal-guide/legal-protections-anonymous-speech-virginia>. Acesso em: 23.03.17.

43 GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 347 (2008)

44 Uma lista dos processos em que o EFF atua pode ser encontrada em: <https://www.eff.org/issues/free-speech>. Acesso em: 23.03.17.

Do ponto de vista prático, a atividade da Defensoria Pública nos casos previstos no art. 72 do Código de Processo Civil não se distancia grandemente da atividade das organizações sem fins lucrativos nos Estados Unidos. Ambos se prestam a viabilizar a defesa nos autos em casos em que o próprio titular do direito se vê impossibilitado de fazê-lo por seus próprios meios – seja porque não é civilmente capaz (impossibilidade jurídica), seja porque não foi localizado (impossibilidade fática), seja porque o comparecimento aos autos faria perecer o próprio direito que se defenderia em juízo (impossibilidade lógica).

Nesse contexto, seria de se imaginar a possibilidade de se chamar a Defensoria Pública à responsabilidade de defender o sigilo de dados dos usuários, inclusive fazendo esforços razoáveis para tentar contactá-los para fins de alinhamento da estratégia de defesa. Isso, é claro, sem prejuízo de, uma vez comunicado da pendência de processo judicial, o usuário poder optar por constituir seu próprio representante. A providência estaria alinhada com os objetivos e funções básicos da Defensoria Públicas, esculpidos nos arts. 3º e 4º de sua lei orgânica: a "primazia da dignidade da pessoa humana"; a "prevalência e efetividade dos direitos humanos"; a "garantia dos princípios constitucionais da ampla defesa e do contraditório"; e a promoção da "mais ampla defesa dos direitos fundamentais dos necessitados, abrangendo seus direitos individuais, coletivos, sociais, econômicos, culturais e ambientais, sendo admissíveis todas as espécies de ações capazes de propiciar sua adequada e efetiva tutela".

O ***segundo*** fator relevante é que se exija um nível mínimo de plausibilidade da pretensão do autor. A exigência faz muito sentido se considerarmos que, até que seja confirmada a ilicitude da conduta do usuário, deve ser protegido o sigilo de dados, no caso brasileiro, e o anonimato, na tradição norte-americana. Além de se tratar de uma exigência própria do direito material em jogo, o requisito também assume um claro contorno de proteção da presunção de inocência (CF, art. 5º, LVII).

No Brasil, esse tipo de exigência aparece no direito processual civil sob a forma do requisito do *fumus boni juris*. Nos Estados Unidos, por outro lado, há uma grande variedade de níveis de exigências. São eles: (i) boa-fé (*good faith*), um requisito muito brando e que no direito brasileiro aparece como uma exigência geral para todos os litigantes, a todo momento, sob pena

de multa[45]; (ii) sobreviver a um pedido de arquivamento (*motion to dismiss*), que exige apenas que a pretensão do autor supere o nível de *especulação*, assumindo que todas as alegações sejam verdadeiras; (iii) sobreviver a um pedido de julgamento sumário (*summary judgement*), que exige a prova de um elemento essencial para a fundamentação da pretensão do autor; (iv) estabelecer um caso *prima facie* (*a prima facie evidentiary showing*), que exige que nenhuma prova em contrário tenha sido apresentada até o momento[46].

Antes de qualquer consideração quanto ao parâmetro legal de plausibilidade do direito do autor, vale notar que a possibilidade de provimento de tutela satisfativa em restrição direta a direitos fundamentais deve ser considerada com grande cautela[47]. Do ponto de vista material, os já referidos requisitos impostos pela jurisprudência do Supremo Tribunal Federal em matéria de quebra de sigilo de dados sobre comunicações e pelo art. 22 do Marco Civil da Internet já estabelecem sarrafo suficientemente alto para garantia do direito fundamental à privacidade – se observados com rigor pelas Cortes, naturalmente. Trata-se, vale lembrar, da exigência de demonstração da ilegalidade da conduta, na necessidade da providência e do período de tempo compreendido pela ordem.

Quanto ao ***terceiro*** fator, a relevância da obtenção das informações requeridas, seu fundamento central repousa também na circunstância de se estar diante da restrição de um princípio fundamental. E que, por dever de razoabilidade[48], essas restrições devem ser mantidas em um mínimo indispensável para proteger outros princípios de mesma estatura constitucional. Nesse ponto, mesmo as jurisdições com procedimentos mais vantajosos aos autores exigem que a "informação sobre a identidade requerida seja centralmente necessária para viabilizar a pretensão material do autor"[49]. Outros Estados exigem que a "informação seja suficiente para estabelecer

---

[45] BRASIL, Código de Processo Civil, arts. 5º e 79-81.

[46] CORTE DE APELAÇÕES DO TERCEIRO DISTRITO, **Valencia v. Citibank Int'l**, 728 So. 2d 330.

[47] Não por outra razão, os tribunais superiores registram em diversos julgados e o Congresso, na Lei nº 8.437/92, a impossibilidade de concessão de liminar satisfativa em processo civil (BRASIL, STJ, *DJ* 20 jun. 2005, AgRg no REsp 584.527/RN, Rel. Min. Laurita Vaz), penal (BRASIL, STF, *DJ* 21 mai. 2012, HC 112487/PR, Rel. Min. Celso de Mello), trabalhista (BRASIL, STF, *DJ* 29 ago. 2003, RE 162309/PE, Rel. Min. Marco Aurélio) e contra a fazenda pública (BRASIL, Lei nº 8.437/1992, art. 1°, § 3º).

[48] V.: BARROSO, Luís Roberto; DE BARCELLOS, Ana Paula. **O começo da história: o Papel dos Princípios no Direito Brasileiro**, p. 65, disponível em <http://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista23/revista23_25.pdf> Acesso em: 23.03.17.

[49] ESTADOS UNIDOS DA AMÉRICA, CORTE FEDERAL DE VIRGÍNIA, **In re AOL**, 52 Va. Cir. 26.

ou contradizer que a pretensão ou a defesa seria inviável com o uso de qualquer outro meio"[50]. Apesar da pluralidade de níveis de exigência, a noção é muito próxima da exigência brasileira de interesse de agir nos procedimentos cíveis em geral e, em especial, quando se trate de restrição a direitos fundamentais.

O ***quarto*** fator, ponderação de interesses entre o autor e o réu não representa qualquer novidade ao direito brasileiro. De toda forma, é um fato importante de ser destacado para que não se perca de vista que pedidos de fornecimento de dados são conflitos entre direitos fundamentais. O ***quinto*** aspecto relevante é a exigência de que as provas produzidas sejam específicas, para evitar que o autor afogue a corte e o réu em documentos desnecessários, dificultando a defesa. Por fim, o ***sexto*** fator destacado por Gleicher consiste na demonstração de que o autor esgotou todos os meios extrajudiciais disponíveis para identificar o usuário antes de submeter a matéria à corte.

Conclusão: regras e procedimentos para fornecimento de dados de usuários.

A correta calibragem do procedimento a ser adotado para fornecimento de dados de usuários é de extrema relevância e complexidade[51]. Sua definição impacta o nível de proteção à privacidade, ao devido processo legal, à presunção de inocência, de um lado, e ao direito à honra e à intimidade, de outro. Ainda que a sintonia fina do procedimento demande uma análise mais detida dos riscos e benefícios de cada detalhe, espera-se que a presente análise ajude a traçar linhas gerais de uma moldura legal adequada para o fornecimento de dados. E que o presente estudo sirva de propulsor para pesquisas complementares nessa área.

---

[50] ESTADOS UNIDOS DA AMÉRICA, CORTE FEDERAL DE WASHINGTON, *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001)

[51] GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320, 329 (2008): "John Doe subpoenas can have severe consequences, potentially causing irreparable harm to defendants if granted, and denying plaintiffs the opportunity to seek relief for their harms if denied. A defendant who is exposed could be subject to reprisals or severe social and professional sanctions, making extreme care necessary when exposing potentially innocent defendants. At the same time, a plaintiff who is denied the identity of his defendant is left with no recourse and has his suit effectively denied without a hearing on the merits".

BIBLIOGRAFIA

ACCESS NOW, **Freedom of Expression**, disponível em: <https://www.accessnow.org/issue/freedom-of-expression/> Acesso em: 23.03.17.

APC, **End violence: Women's rights and safety online**, disponível em: <https://www.apc.org/en/node/15007/> Acesso em: 23.03.17

BARROSO, Luís Roberto; DE BARCELLOS, Ana Paula. **O começo da história: o Papel dos Princípios no Direito Brasileiro**, p. 65, Disponível em <http://www.emerj.tjrj.jus.br/revistaemerj_online /edicoes/revista23/revista23_25.pdf> Acesso em: 23.03.17.

BRASIL, Código de Processo Civil.

BRASIL, Lei nº 8.437/1992.

BRASIL, STF, DJ 04/08/2006, MS 25668/DF, Rel. Min. Celso de Mello (Tribunal Pleno).

BRASIL, STF, DJ 14/01/2001, MS 23669, Rel. Min. Celso de Mello.

BRASIL, STF, DJ 16/06/2006, HC 84758, Rel. Min. Celso de Mello (Tribunal Pleno).

BRASIL, STF, DJ 21/05/2012, HC 112487/PR, Rel. Min. Celso de Mello.

BRASIL, STF, DJ 23/02/06, MS 25812 MC, Rel. Min. Cezar Peluso.

BRASIL, STF, DJ 29/08/2003, RE 162309/PE, Rel. Min. Marco Aurélio.

BRASIL, STJ, DJ 20/06/2005, AgRg no REsp 584.527/RN, Rel. Min. Laurita Vaz.

BRASIL, STJ, DJe 02/05/2012, REsp 1306066/MT, Rel. Min. Sidnei Beneti.

BRASIL, STJ, DJe 02/08/2012, REsp 1192208/MG, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 08/08/2011, REsp 1193764/SP, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 10/03/2014, REsp 1417641/RJ, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 16/05/2013, RMS 38.010/RJ, Rel. Min. Herman Benjamin.

BRASIL, STJ, DJe 18/06/2014, AgRg no REsp 1402104/RJ, Rel. Min. Raul Araújo.

BRASIL, STJ, DJe 19/06/2012, REsp 1308830/RS, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 22/05/2014, AgRg no REsp 1395768/RJ, Rel. Min. Raul Araújo.

BRASIL, STJ, DJe 23/05/2014, AgRg no REsp 1396963/RS, Rel. Min. Raul Araújo.

BRASIL, STJ, DJe 25/03/2014, REsp 1403749/GO, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 26/05/2014, AgRg no REsp 1395803/RJ, Rel. Min. Raul Araújo.

BRASIL, STJ, DJe 26/06/2012, REsp 1300161/RS, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 26/09/2013, REsp 1383354/SP, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 26/11/2013, REsp 1398985/MG, Rel. Min. Nancy Andrighi.

BRASIL, STJ, DJe 28/05/2014, AgRg no REsp 1285756/MG, Rel. Min. Raul Araújo.

BRASIL, STJ, DJe 31/08/2011, REsp 1186616/MG, Rel. Min. Nancy Andrighi.

BRASIL, TJSE, Cam. Crim, HC 2010314476, rel. Des. Geni Silveira Schuster, j. 08/02/2011.

BRASIL, TJSP, 13a Cam. Crim., HC 00430001-50.2014.8.26.0000/Franca, rel. Des. Augusto de Siqueira, j. 07/08/2014.

CITRON, Danielle Keats, Cyber Civil Rights, **89 Boston University Law Review** 81 (2009).

COHEN, Julie E. A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace. **28 Conn. L. Rev**.. 981-1039 (1996). Disponível em:

<http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1815&context=facpub> Acesso em: 23.03.17.

CORTE DE APELAÇÕES DO TERCEIRO DISTRITO, **Valencia v. Citibank Int'l**, 728 So. 2d 330.

CORTE FEDERAL DE VIRGÍNIA, **In re AOL**, 52 Va. Cir. 26.

CORTE FEDERAL DE WASHINGTON, *Doe v. 2theMart.com*, 140 F. Supp. 2d 1088, 1095 (W.D. Wash. 2001).

CORTE SUPERIOR DE NEW JERSEY, **Dendrite**, 775 A.2d 756.

CUNHA E MELO, Mariana, The Marco Civil da Internet and its Unresolved Issues: free speech and due process of law. Curitiba, CRV (2016).

DERECHOS DIGITALES, **No temas a Internet**. Disponível em: <https://www.derechosdigitales.org/notemasainternet/> Acesso em: 23.03.17.

DIGITAL MEDIA LAW PROJECT, **Legal Protections for Anonymous Speech in Virginia**. Disponível em <http://www.dmlp.org/legal-guide/legal-protections-anonymous-speech-virginia> Acesso em: 23.03.17.

ELECTRONIC FRONTIER FOUNDATION, **Anonymity and Encryption** (Feb. 2015). Disponível em <https://www.eff.org/document/eff-comments-submitted-united-nations-special-rapporteur-prom
otion-and-protection-right> Acesso em: 23.03.17.

ELECTRONIC FRONTIER FOUNDATION, **Blog safely**, disponível em: <https://www.eff.org/wp/blog-safely> Acesso em: 23.03.17.

ELECTRONIC FRONTIER FOUNDATION, **Test for Unmasking Anonymous Speech. Internet Law Treatise**. Disponível em: <http://ilt.eff.org/index.php/Speech:_Anonymity#Tests_for_Unmasking_Anonymous_Speakers> Acesso em: 23.03.17.

GLEICHER, Nathaniel, John Doe Subpoenas: Toward a Consistent Legal Standard, **118 Yale L.J.** 320 (2008).

ORGANIZAÇÃO DAS NAÇÕES UNIDAS, **Report on encryption, anonymity, and the human rights framework**. Disponível em: <http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.aspx> Acesso em: 23.03.17.

SUPREMA CORTE DE DELAWARE, **Doe No. 1 v. Cahill**, 884 A.2d 451, 461 (Del. 2005).

SUPREMA CORTE DOS ESTADOS UNIDOS, **Mclntyre v. Ohio Elections Commission**, 514 U.S. 334, 342 (1995)

WHITMAN, James Q., The Two Western Cultures of Privacy: Dignity versus Liberty, **113 The Yale Law Journal** 1165 (Apr., 2004), disponível em: <http://www.jstor.org/stable/4135723> Acesso em: 23.03.17.