Cadernos Jurídicos

Ano 21 - Número 53 - Janeiro-Março/2020

Direito Digital e proteção de dados pessoais

Escola Paulista da Magistratura
São Paulo, 2020

Cadernos Jurídicos

Direito Digital e proteção de dados pessoais

ISSN 1806-5449
Cadernos Jurídicos, São Paulo, ano 21, nº 53, p. 1-202, Janeiro-Março/2020

CADERNOS JURÍDICOS / Escola Paulista da Magistratura
V. 1, nº 1 (2000) - São Paulo: Escola Paulista da Magistratura

Bimestral
2000, v. 1 (1 - 2)
2001, v. 2 (3 - 4 - 5 - 6)
2002, v. 3 (7 - 8 - 9 - 10 - 11 - 12)
2003, v. 4 (13 - 14 - 15 -16 - 17 - 18)
2004, v. 5 (19 - 20 - 21 - 22 - 23 - 24)
2005, v. 6 (25)
2006, v. 7 (26 - 27 - 28)
2007, v. 8 (29 - 30)
2008, v. 9 (31)
2009, v. 10 (32)
2011, v. 11 (33)
2012, v. 12 (34 - 35)
2013, v. 13 (36 - 37)
2014, v. 14 (38)
2015, v. 15 (39 - 40 - 41)
2016, v. 16 (42 - 43 - 44 - 45)
2017, v. 17 (46)
2019, v. 18 (47 - 48 - 49 - 50 - 51 - 52)
2020, v. 19 (53)

Direito CDU 34(05)
Jurisprudência CDU 35(05)

ISSN 1806-5449

Escola Paulista da Magistratura
Rua da Consolação, 1.483 – 1º ao 4º andar
CEP 01301-100 / São Paulo - SP
Fones: (11) 3256-6781 / 3257-0356
www.epm.tjsp.jus.br
imprensaepm@tjsp.jus.br

Ano 21
Número 53
Janeiro-Março
2020

SUMÁRIO

I — Direito Digital

II — Proteção de dados pessoais

Apresentação

O Direito Digital teve sua primeira aparição na Escola Paulista da Magistratura, sob esta denominação, no ano de 2013 quando o 1º Curso de Extensão Universitária em Direito Digital, coordenado pelo advogado especialista na área, Renato Opice Blum e pelo juiz Fernando Antonio Tasso, então Coordenador de Ensino à Distância, inaugurou uma nova abordagem das questões de tecnologia aplicadas ao direito.

Nesse ano, o Tribunal de Justiça de São Paulo empreendia sua transformação digital, com a unificação de seus 12 sistemas informatizados em apenas um, com o Plano de Unificação, Modernização e Alinhamento (PUMA), conforme preconizado pelo seu Planejamento Estratégico 2010/2014.

Temas como governança, novos riscos decorrentes das relações jurídicas travadas no ambiente digital, certificação digital, documento eletrônico e criptografia passaram a permear os debates e palestras no âmbito de nossa Escola.

Durante os anos de 2014/2015, enquanto o Tribunal se lançava à desafiadora meta de alcançar a propositura de novas ações exclusivamente pelo meio digital, com o Projeto 100% Digital, a Escola Paulista da Magistratura reafirmava seu compromisso de fomentar o intercâmbio de ideias e novas abordagens do direito à luz da tecnologia, promovendo o 2º Curso de Extensão Universitária em Direito na Era Digital.

No ano de 2017 a EPM realizou, em parceria com a Escola de Governança da Internet, o Curso de Extensão Universitária "Gestão e governança da Internet aplicadas à prestação jurisdicional – Escola Paulista da Magistratura e Escola de Governança da Internet no Brasil".

A profusão de temas relativos ao direito digital passou a ser objeto crescente das ações judiciais cíveis, criminais e no âmbito do direito público, trazendo à Escola a demanda pela criação do 1º Núcleo de Estudos em Direito Digital, entre os meses de setembro de 2017 e julho de 2018. Juízes passaram a se especializar nessa área e produzir conteúdo de qualidade junto a diversas instituições de ensino. Terminado este, seguiu-se o 2º Núcleo de Estudos em Direito Digital, iniciado em maio de 2019 com previsão de encerramento em abril de 2020. Em suas duas edições, doutrinadores de renome compartilharam generosamente seu conhecimento, ampliando os horizontes dos magistrados participantes.

O 1º Seminário "A magistratura paulista discute o direito digital alinhado à doutrina e jurisprudência modernas" foi realizado em agosto de 2018 para que os juízes participantes do Núcleo de Estudos transmitissem o conhecimento adquirido aos demais colegas, consistindo esse evento no primeiro fruto dessa colheita. No modelo de "juízes falando para juízes", suas realizações e estudos foram compartilhados com toda a carreira, beneficiando magistrados, servidores e participantes externos.

A Coordenadoria de Tecnologia da Informação, resultante da evolução da antiga Coordenadoria de Ensino a Distância, abarcou o Direito Digital, tornando-a disciplina a dividir o gosto e a audiência das tradicionais disciplinas do direito. Nascia em setembro de 2018 a Coordenadoria de Tecnologia da Informação e Direito Digital da Escola Paulista da Magistratura.

Novos temas relativos à proteção de dados, segurança da informação e governança digital encontraram no 2º Núcleo de Estudos um terreno fecundo para que profissionais

da área fossem trazidos a debater temas como a investigação digital, a prova eletrônica e as questões de privacidade, segurança da informação e proteção de dados pessoais.

Ao longo desse período, a Escola Paulista da Magistratura foi prestigiada em eventos acadêmicos que trataram de temas de Direito Digital ao lado de parceiros como o Departamento de Justiça dos Estados Unidos da América, o Comitê Gestor da Internet, Escolas de Magistratura coirmãs, como a do Rio Grande do Norte, Bahia e Santa Catarina, e a Procuradoria Geral do Estado do Rio de Janeiro.

Como resultado do trabalho consolidado até aqui, a EPM, por sua Coordenadoria de TI e Direito Digital, apresenta neste ano de 2020 a primeira edição dos Cadernos Jurídicos – Direito Digital e Proteção de Dados Pessoais. Nesse compêndio encontram-se os trabalhos de magistrados participantes e de acadêmicos que emprestaram aos encontros parte de seu conhecimento, sempre visando à aplicação concreta dos conceitos tecnológicos à prática jurídica.

Esperamos que os temas aqui tratados possam trazer novas perspectivas à prática jurisdicional e estimular seus leitores a perseverar na pesquisa e na produção acadêmica.

Wanderley José Federighi
Desembargador coordenador de Biblioteca e Revistas da EPM no biênio 2018/2019 e atual coordenador da Área de Direito Público da Escola

Luis Soares de Mello Neto
Desembargador coordenador de TI e Direito Digital da EPM no biênio 2018/2019 e atual vice-presidente do Tribunal de Justiça de São Paulo

Fernando Antonio Tasso
Juiz de Direito coordenador de TI e Direito Digital da EPM

I

Direito Digital

Do direito à desindexação face ao abuso de direito escorado em lei. Discussão sobre o alcance do art. 19 da Lei nº 12.965/14

Alexandre Jorge Carneiro da Cunha Filho[1]
Juiz de Direito no Estado de São Paulo

Sumário: 1. Introdução: um caso para se pensar; 2. Da responsabilidade civil nos termos do art. 19 da Lei nº 12.965/14; 3. O papel da hermenêutica jurídica na dicção da norma a partir do texto legal; 3.1. Interesses em disputa na construção e aplicação do texto normativo como critério de interpretação; 3.2. Art. 5º da LINDB – exigências do bem comum; 3.3. Do abuso de direito escorado na literalidade da lei; 3.4. Perspectivas à vista da Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/18); 4. Conclusão; 5. Bibliografia.

1. Introdução: um caso para se pensar

No presente ensaio vamos tratar da intepretação normalmente conferida ao art. 19 da Lei nº 12.965/14 pelas empresas de tecnologia e do efeito pernicioso dessa postura para aqueles que se sentem lesados pela exposição indevida de seu nome ou o nome de algum ente querido relacionado à matéria que acarrete constrangimento aos envolvidos.

Em especial trataremos de uma hipótese em que tal publicação não atenda sequer a um interesse público merecedor de tutela por parte de nosso ordenamento, dado que nos leva a refletir sobre o comportamento da empresa de mídia que, apesar de formalmente estar pautado em lei, não traz, ao menos à primeira vista, qualquer utilidade até mesmo para a fornecedora de serviços.

A inspiração para desenvolvermos o tema adveio de caso concreto que apreciamos quando em exercício na 2ª Vara do Juizado Especial Cível da Capital, no qual uma pessoa acionava o Google e determinado site pela divulgação de imagens da morte violenta de um ente querido. Pedia-se na ocasião desindexação (bloqueio de acesso a endereço eletrônico em que havia foto na qual as vísceras de um ser humano eram expostas em destaque em notícia sobre seu falecimento em acidente trágico envolvendo maquinário agrícola) e indenização por dano moral.

Na ocasião nos chamou a atenção a defesa apresentada pela Google resistindo ao pleito de interdição de acesso ao site sob o argumento de observância da prerrogativa que lhe é conferida pelo art. 19 da Lei nº 12.965/14 – Marco Civil da Internet e das garantias de liberdade de expressão/liberdade de informação, em nome das quais a empresa não poderia ser compelida a remover o conteúdo em tela de seu buscador.

O litígio em concreto teve suas peculiaridades, como, aliás, sói acontecer.

Com base na mesma notícia, ainda que com textos ligeiramente diversos e variação de ângulo da imagem da vítima dilacerada, houve veiculação da matéria em pelo

[1] Mestre e doutor em Direito do Estado. Integrante do NEDIG.

menos 10 sites, tendo a parte autora ingressado com uma ação individual contra cada um desses provedores em litisconsórcio com o Google. Ainda houve ação autônoma só contra o Google, esta proposta perante o Fórum Central da Capital.

Seguindo a tradição do nosso Judiciário na análise de casos análogos, apesar de os fatos, a nosso ver, reclamarem decisão uniforme no que se refere à aplicação do Direito ao questionamento de raiz comum[2], houve distribuição de todas essas demandas livremente, para diversos juízes, e até mesmo sob ritos distintos (o ordinário do CPC e o previsto na Lei nº 9.099/95).

Afora o risco real de decisões conflitantes, dado que milita a favor do descrédito de um sistema de Justiça que se pretenda racional e que zele pela isonomia entre aqueles que estão em situação equivalente[3], o acesso multiportas oferecido para tratamento do mesmo conflito, ao menos nos moldes em que hoje este é praticado entre nós, ainda implica movimentação desnecessária da máquina pública, que é chamada milhares de vezes a se pronunciar sobre uma mesma questão[4].

Nada obstante a complexidade descrita e a ressalva ora feita, sobre a qual sempre que possível alertamos aos colegas de modo a buscarmos, ao menos no futuro, uma forma mais adequada de lidar com esse tipo de lide[5], fizemos na ocasião o que se espera do julgador nos *"tempos modernos"*: sem inventar muito decidimos a faceta do problema tal como nos foi apresentada, fazendo alusão à parte do que já fora decidido a respeito por demanda julgada anteriormente.

Antes de revelarmos qual foi nossa conclusão sobre os pedidos formulados na ação, um percurso se faz necessário.

Eis o mote da presente reflexão.

---

[2] A complexidade do caso, no nosso sentir, envolve uma raiz comum (relação entre vítima e provedor de buscas) e várias outras relações que se estabelecem entre vítima do dano e responsáveis por sites que divulgam imagens que violam, sem justo motivo, a sua intimidade (mas para cujo dano imposto à vítima a conduta do *site buscador* é determinante).

[3] Sobre a importância de se *"tratar casos semelhantes de forma equivalente"* para fortalecimento da legitimidade do sistema de Justiça, crença que foi determinante para a valorização dos *precedentes* como fonte do Direito pelo Código do Processo Civil de 2015, ver: MANCUSO, Rodolfo de Camargo. *Sistema brasileiro de precedentes*. 2. ed. São Paulo: Revista dos Tribunais, 2016, p. 177 e ss. Para reflexos de tal preocupação no âmbito do Direito Administrativo, ver: MARQUES NETO, Floriano de Azevedo.; FREITAS, Rafael Véras de. *Comentários à lei nº 13.655/2018*. Belo Horizonte: Fórum, 2019, p. 160-161; LUVIZOTTO, Juliana Cristina. O art. 30 da Lei de Introdução às Normas do Direito Brasileiro e a sua relação com os precedentes administrativos. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Lei de Introdução às Normas do Direito Brasileiro*: anotada. São Paulo: Quartier Latin, 2019, v. 2, p. 490-498.

[4] E normalmente sob os auspícios da Justiça Gratuita, dado que transfere o ônus financeiro respectivo ao Estado (ou seja, a todos os cidadãos), não sendo absorvido por aqueles que efetivamente estão interessados na solução de uma dada disputa. Sobre o impacto do fenômeno na organização dos serviços judiciais, ver: SILVA, Domicio Whately Pacheco e. O acesso à prestação jurisdicional e a responsabilidade das partes: reflexões sobre o papel da gratuidade processual, dos honorários sucumbenciais e da litigância de má-fé na distribuição da Justiça. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; OLIVEIRA, André Tito da Motta; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Direito, instituições e políticas públicas*: o papel do jusidealista na formação do Estado. São Paulo: Quartier Latin, 2017, p. 675-694.

[5] Seja via conexão de ações ou ao menos por meio da comunicação entre os juízes responsáveis pelo julgamento das facetas de um mesmo conflito, quiçá com o estabelecimento de atos de instrução comum. Note-se que ambas as medidas sugeridas contam com amparo legal expresso (art. 55, §3º e 69 do CPC, respectivamente), em mais um episódio a demonstrar que não é por falta de lei que não conseguimos uma atuação estatal mais eficiente em território nacional. Sugerindo que o problema não é exclusivo do nosso sistema, confira-se a exortação de Pietro Perlingieri quanto ao empenho cotidiano na aplicação das leis vigentes como mecanismo de aprimoramento da eficiência da magistratura, o que passaria pela recuperação ética de suas funções (PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Tradução: Maria Cristina de Cicco. Rio de Janeiro: Renovar, 2008, p. 20).

2. Da responsabilidade civil nos termos do art. 19 da lei nº 12.965/14

A empresa Google, resistindo ao pedido de bloqueio de acesso a site, socorreu-se do quanto previsto no *caput* art. 19 da Lei nº 12.965/14, cuja redação é a seguinte:

> *Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário*[6]*. (grifo nosso)*

Segundo o texto legislado, tem-se que houve uma opção pelo estabelecimento de um regime específico para a responsabilização do provedor de internet, excepcionando a regra geral do instituto da responsabilidade civil, pelo qual aquele que causa dano a outrem fica obrigado a repará-lo (desdobramento do postulado *neminen laedere*, que poderia ser alçado ao grau de princípio básico da convivência humana, a inspirar práticas do bem viver em coletivo desde tempos imemoriais e vocacionado à aplicação universal[7]).

E por que da especificidade? Qual seria a razão a mover o legislador no sentido de restringir as hipóteses em que tais empresas poderiam ser chamadas a indenizar prejuízos causados por meio dos seus serviços, ainda mais criando como filtro para desencadear tal efeito uma *"ordem judicial específica"*?

Os objetivos declarados no próprio dispositivo são os de *assegurar a liberdade de expressão* e *impedir a censura*.

Sem adentrarmos na seara sobre se houve móveis de diversa ordem a conduzir os trabalhos legislativos em tal direção, em especial a pressão de grupos de interesse economicamente poderosos desejosos de criar anteparo legal no afã de desenvolverem suas atividades com mais liberdade, delineados os fatos e a lei que lhes é aplicável,

---

[6] Os parágrafos do dispositivo são os seguintes: *"§ 1º A ordem judicial de que trata o* caput *deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal. § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais. § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação".* (Disponível em: http://bit.ly/2uNfNez. Acesso em: 17 set. 2019)

[7] *"Para conceber um ordenamento jurídico como reduzido a uma só norma particular, seria preciso erigir em norma particular a ordem de não prejudicar ninguém (neminem laedere)".* BOBBIO, Norberto. *Teoria do ordenamento jurídico*. 10. ed. Tradução: Maria Celeste Cordeiro Leite dos Santos. Brasília, DF: UNB, 1997, p. 33. Outras duas máximas do Direito que costumam acompanhar a do *neminen laedere* na construção dos pilares de uma ordem jurídica que aspire à Justiça são o *viver honestamente* (*honeste vivere*) e o *dar a cada o que é seu* (*suum cuique tribuere*), conforme famosa sentença atribuída a Ulpiano no Digesto 1.1.10.1, que é lembrada por Rogério José Ferraz Donnini em seu Bona fides: do direito material ao processual. *Revista de Processo*, São Paulo, v. 251, p. 113-126, 2016, p. 3. Disponível em: http://bit.ly/2tpCt4b. Acesso em: 16 jan. 2020.

resta saber se a conduta de uma empresa que ignore o apelo do particular para interditar lesão da qual este está sendo vítima é compatível com nosso ordenamento jurídico[8].

3. O papel da hermenêutica jurídica na dicção da norma a partir do texto legal

Seguindo a melhor doutrina que se debruçou até então sobre o assunto, compreendemos como *norma* um *dever ser* resultado de um processo de interpretação[9], o qual envolve não só um dado texto legal como sua leitura em conjunto com outras fontes do Direito, em uma operação que não se dá de forma cega[10], mas sim teleologicamente dirigida, ou seja, vocacionada a cumprir os fins que justificaram a criação de uma dada limitação à liberdade individual.

Neste mister não há fantasmas[11].

Ou melhor, os que há são só aqueles que transitam no nosso subconsciente, muitas vezes contaminado por uma formação idealizada do Direito tal qual esta continua a ser feita em muitos bancos escolares, despreocupada com a realidade que motiva sua criação e a qual é destinatária da sua aplicação[12].

3.1. Interesses em disputa na construção e aplicação do texto normativo como critério de interpretação

Se o texto aprovado pelo legislador é uma obra humana que, dessa forma, pode não necessariamente ser resultado de um esforço quase divino do seu criador com o propósito de conferir aos cidadãos o melhor regramento de conduta que sua razão/intelecto pôde alcançar[13], um dos caminhos para se buscar conferir alguma prudência na aplicação do

---

[8] A respeito vale registrar que o mesmo legislador, ao disciplinar a divulgação de cenas de nudez ou de atos sexuais sem o consentimento de seus participantes, optou por disciplina diversa, como se extrai do art. 21 da Lei nº 12.965/2014: *"O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. Parágrafo único. A notificação prevista no* caput *deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido".* (Disponível em: http://bit.ly/2uNfNez. Acesso em: 17 set. 2019)

[9] *"O direito é alográfico. E alográfico é porque o texto normativo não se completa no sentido nele expresso pelo legislador. A 'completude' do texto somente é atingida quando o sentido por ele expressado é produzido, como nova forma de expressão, pelo intérprete. Mas o 'sentido expressado pelo texto' já é algo novo, distinto do texto. É a norma".* (GRAU, Eros Roberto. *Ensaio e discurso sobre a interpretação/aplicação do direito*. São Paulo: Malheiros, 2002, p. 20)

[10] Para um maior desenvolvimento sobre nossa perspectiva sobre o ponto, ver: CUNHA FILHO, Alexandre Jorge Carneiro da. Ponto cego na aplicação da lei. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Lei de Introdução às Normas do Direito Brasileiro*: anotada. São Paulo: Quartier Latin, 2019, p. 321-329.

[11] MUÑOZ, Alberto Alonso. *Modelos de fundamentação filosófica do direito privado e seus limites*: contribuição à crítica do direito privado. 2015. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015, p. 14 e ss.

[12] Confira-se passagem da reflexão crítica sobre o ensino jurídico no país da lavra de San Tiago Dantas que, apesar de formulada há mais de meio século, continua atual: *"No estudo das instituições jurídicas apresentadas em sistema perde-se facilmente a sensibilidade da relação social, econômica ou política, a cuja disciplina é endereçada a norma jurídica. O sistema tem um valor lógico e racional, e por assim dizer, autônomo. O estudo que dele fazemos, com métodos próprios estritamente dedutivos, conduz a uma auto-suficiência, que permite ao jurista voltar as costas à sociedade e desinteressar-se da matéria regulada, como do alcance prático das suas soluções".* (DANTAS, San Tiago. A educação jurídica e a crise brasileira. *Revista Forense*, São Paulo, v. 159, n. 52, p. 449-458, 1955, p. 454).

[13] Sobre a concepção do Direito como um sistema fundado na razão e a importância desse pressuposto para linhas de pensamento que redundaram em escolas tidas por "positivistas", ver: LARENZ, Karl. *Metodologia da ciência do direito*. 8ª ed. Tradução:

art. 19 da Lei nº 12.965/14 é justamente uma visão crítica acerca dos interesses em disputa na sua aplicação[14].

Ainda que na construção do texto no âmbito do Legislativo determinados anseios tenham sido privilegiados em detrimento de outros, em um processo não raras vezes opaco e desfavorável à confecção de um ato normativo equilibrado, resultado de pesquisas empíricas e do sopesamento equidistante das diversas posições relevantes a serem afetadas pela sua aprovação[15], na sua aplicação pelos Tribunais desenha-se nova arena em que aqueles que não foram ouvidos quando da produção da lei passam a questioná-la, sobretudo ao entenderem que, apesar dela ou por ocasião da sua vigência, estão sendo lesados.

No caso que serve de mote para nossa reflexão temos uma ilustração bastante plástica do quanto exposto.

De um lado tem-se alguém que se sente intimamente ferido pela divulgação de cenas trágicas da morte de um ente querido. Pretende, assim, a cessação da conduta lesiva, que se dá por meio do serviço oferecido por provedores de internet, em especial aqueles que, disponibilizando busca aos seus usuários por meio de palavras-chave, apresentam links que conduzem ao material que causa dor e constrangimento a uma pessoa de carne e osso[16].

Do outro, há o site que veicula a notícia em tela, usando como chamariz para seu público a foto do falecido em condições ultrajantes, e uma das maiores empresas de tecnologias do globo[17], cuja principal fonte de renda seria a venda de espaços de publicidade, dado para o qual a difusão viral de conteúdos sensacionalistas impulsionada por terceiros pode simplesmente representar mais uma oportunidade de negócios.

José Malego. Lisboa: Fundação Calouste Gulbenkian, 2019, p. 39 e ss. Acerca da *paixão*, e não da *razão*, como principal móvel das ações humanas, inclusive no que diz respeito às deliberações relativas aos negócios públicos, ver: OLIVEIRA, Regis Fernandes de. *Indagação sobre os limites da ação do Estado*. São Paulo: Revista dos Tribunais, 2015, p. 187 e ss. Destacamos passagem: *"Nem por outro motivo é que o Estado é fruto das paixões. O Estado nem é nem pode ser racional, porque são seres humanos que instituem as leis, que deliberam sobre como exercer a vontade estatal, sobre como decidir os rumos do país"* (p. 193).

[14] Entendendo que a própria redação do dispositivo, ao enfatizar desde o seu início os direitos à liberdade de expressão e de vedação à censura, sem cotejá-los com outros bens jurídicos de valor ao menos equivalentes àqueles (como privacidade e dignidade da pessoa), fez a balança pesar em favor das empresas que exploram comercialmente a internet em detrimento dos seus usuários. É a posição de: SCHREIBER, Anderson. Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por dano gerado por terceiro. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*. São Paulo: Quartier Latin, 2015, t. 2, p. 277-305, p. 289 e ss.

[15] Investigando sobre como o instituto do *processo* pode contribuir para a produção de leis de maior qualidade, que evitem restrições arbitrárias à esfera de liberdade dos cidadãos, ver: NAGATA, Bruno Mitsuo. Questões atuais do devido processo legislativo. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Lei de Introdução às Normas do Direito Brasileiro*: anotada. *São Paulo*: Quartier Latin, 2019, v. 1, p. 91-97.

[16] Valendo aqui lembrar o teor do inciso X do art. 5º da Constituição: *"são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação"*. (Disponível em: http://bit.ly/2QXcM41. Acesso em: 26 set. 2019). O art. 12 do Código Civil, em consonância com o comando constitucional, prevê: *"pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau"*. (Disponível em: http://bit.ly/2R2iF02. Acesso em: 26 set. 2019).

[17] Esse é o dado constante do verbete presente na Wikipedia sobre a Google, conforme pode ser conferido em: http://bit.ly/2Rj0yli. Acesso em: 15 set. 19. No link referido ainda constam os seguintes dados: *"o* Alexa *classifica o Google como o* website *mais visitado do mundo. A Google é classificada pela revista* Fortune *como o melhor lugar do mundo para se trabalhar. Aparece na posição pelo sexto ano consecutivo e é a* marca *mais valiosa do mundo de acordo com o ranking* BrandZ *de 2017, avaliada em 245 bilhões de dólares. Em outro ranking de avaliação de marcas, ultrapassou em 2014 a* Apple, *que liderava por três anos consecutivos, com um valor estimado de US$ 159 bilhões. A posição dominante no mercado dos serviços do Google levou a críticas da sociedade sobre assuntos como* privacidade, direitos autorais *e* censura*"*.

Contrapostas as partes na arena do processo judicial, a vítima da conduta imputável ao gestor do site corréu, e potencializada pela suposta "neutralidade" do agente encarregado do sistema buscador, postula, com base nos ditames do instituto da responsabilidade civil, interdição de comportamento e reparação de danos. Os demandados, por sua vez, ou deixam de apresentar defesa em juízo (como o fez o site), ou sustentam liberdade de expressão e vedação de censura, na forma do art. 19 da Lei nº 12.965/14, a justificar seu comportamento.

Havendo razões jurídicas para dar ganho de causa a uma ou a outra parte, qual seria a decisão mais adequada para a situação posta?

3.2. Art. 5º da LINDB — Exigências do bem comum

De acordo com o art. 5º da Lei de Introdução às Normas do Direito Brasileiro-LINDB (Decreto-Lei nº 4.657/1942), "na aplicação da lei, o juiz atenderá aos fins sociais a que ela se dirige e às exigências do bem comum"[18].

Em que pese a redação do dispositivo poder causar alguma surpresa ao leigo em matéria de leis, já que, se o próprio Estado tem por seu fundamento último a realização do bem comum[19], seria despropositado que a jurisdição, como uma das funções estatais, pudesse ser desenvolvida fora do escopo central que inspira o todo do qual ela faz parte, entre os versados nas letras jurídicas o comando em tela é um alerta não só oportuno como muitas vezes indispensável para que o Direito, em sua aplicação, não seja visto como um fim em si mesmo[20].

E quando se fala em Direito como fim em si mesmo, é valioso ressaltar que, como não estamos diante de um mundo ideal de anjos regidos por uma razão que lhes seja transcendente, estamos a discorrer sobre a defesa da sua interpretação de forma supostamente infensa aos interesses que atuaram na criação de atos normativos ou que estão em disputa na sua incidência em dramas humanos reais; ou seja, sobre uma operação cujo resultado não necessariamente esteja comprometido com sua utilidade para a vida das pessoas[21].

---

[18] Disponível em: http://bit.ly/2QZlQFH. Acesso em: 15 set. 2019.

[19] O que pressupõe o cumprimento contínuo dos fins sociais imanentes a uma organização política que tenha por foco primeiro a tutela do ser humano na sua relação com os demais, como a que é disciplinada por uma Constituição como a vigente no Brasil, em que a matéria encontra-se positivada, sobretudo, nos seus arts. 1º e 3º, que enunciam os fundamentos e objetivos da nossa República.

[20] A preocupação em evitar tal tipo de desfecho no exercício do dizer o Direito, seja na seara administrativa, seja na judicial, inclusive é o que, a nosso ver, em boa medida motivou a aprovação da Lei nº 13.655/2018, que trouxe alterações à Lei de Introdução às Normas do Direito Brasileiro. Dentre as mudanças, destacam-se os arts. 20 e 21 do referido diploma, os quais reforçam os deveres de motivação dos agentes executivos e de controle da atividade estatal no que concerne à ponderação quanto aos efeitos concretos de suas decisões. Confira-se as respectivas redações: *Art. 20. Nas esferas administrativa, controladora e judicial, não se decidirá com base em valores jurídicos abstratos sem que sejam consideradas as consequências práticas da decisão. Parágrafo único. A motivação demonstrará a necessidade e a adequação da medida imposta ou da invalidação de ato, contrato, ajuste, processo ou norma administrativa, inclusive em face das possíveis alternativas. Art. 21. A decisão que, nas esferas administrativa, controladora ou judicial, decretar a invalidação de ato, contrato, ajuste, processo ou norma administrativa deverá indicar de modo expresso suas consequências jurídicas e administrativas. Parágrafo único. A decisão a que se refere o* caput *deste artigo deverá, quando for o caso, indicar as condições para que a regularização ocorra de modo proporcional e equânime e sem prejuízo aos interesses gerais, não se podendo impor aos sujeitos atingidos ônus ou perdas que, em função das peculiaridades do caso, sejam anormais ou excessivos"*. (Disponível em: http://bit.ly/2QZlQFH. Acesso em: 22 set. 2019)

[21] Uma leitura dos textos normativos sem o norte das exigências do bem comum, pautada apenas na gramática de signos linguísticos, pode redundar em decisões nas quais prevaleçam interesses particulares em detrimento dos gerais ou ainda

Rejeitando tal hipótese por expressa vedação legal, no nosso caso o art. 5º da LINDB, tem-se que o art. 19 da Lei nº 12.965/14 deve ser interpretado conforme os motivos de utilidade pública plausíveis para sua existência no nosso ordenamento, independentemente do que pode ser extraído da gramática dos signos que compõe o dispositivo ou da intenção do legislador ao promulgá-lo.

3.3. Do abuso de direito escorado na literalidade da lei

Feitas tais considerações, inclusive tendo em conta os objetivos declarados para a incidência do art. 19 da Lei nº 12.965/14, não se vislumbra espaço para seu manejo em favor de provedores de internet fora de circunstâncias em que esteja clara a tutela do direito à liberdade de expressão por parte do emissor da mensagem e do direito à informação por parte do seu receptor.

Em outras palavras, o *bem comum* a ser perseguido com o comando sob exame é a garantia do livre trânsito de informações na sociedade, sem que possa haver constrangimento indevido aos veículos que sirvam de suporte a tal tipo de troca entre os cidadãos.

A liberdade sob exame, como praticamente todas as outras[22], não é ilimitada[23].

Isso significa que, se sob o pretexto de informar e garantir a desimpedida circulação de ideias, determinado agente econômico gera sofrimento e embaraços despropositados a terceiros, sua conduta é ilícita e, assim, passível, em última instância, de controle judicial.

O art. 19 do Marco Civil poderia, então, servir de anteparo para que uma empresa que permita acesso a conteúdo nitidamente ofensivo a direitos da personalidade nada faça para impedir tal lesão após provocada pela respectiva vítima, limitando-se a aguardar *ordem judicial específica* como condição para a adoção das providências pertinentes?

em escolhas interpretativas que podem não trazer qualquer utilidade para quem quer que seja. Um exemplo de aplicação do Direito que talvez se enquadre nessa segunda hipótese, que é intrigante, convenhamos, é, a nosso ver, a defesa que muitos fazem da proibição de acordo em ação de improbidade em razão de vedação legal expressa (art. 17, §1º), mas em um sistema que vem admitindo acordos para a prática de crimes relativos aos mesmos fatos tidos por violadores da Lei nº 8.429/92 (as condutas tipificadas como crimes, por definição, seriam aquelas mais lesivas à sociedade, a justificar a cominação de pena de prisão aos respectivos infratores). Ao se entender pela referida vedação em um caso concreto, quais interesses estariam sendo prestigiados? A interdição corresponde à medida mais adequada para a penalização dos envolvidos, recuperação de valores desviados e desbaratamento de um esquema criminoso? Umas das principais visões críticas à utilização de uma lógica meramente formal no âmbito jurídico pode ser conferida em: SICHES, Luis Recaséns. *Experiencia jurídica, naturaleza de la cosa y lógica "razonable"*. Cidade do México: Unam, 1971, p. 517 e ss.

[22] Usamos a expressão "praticamente todas as outras" já que há referências na doutrina, que nos parecem acertadas, a alguns direitos que seriam invioláveis, como o de não ser submetido a tortura ou à discriminação racista, esta, pertinente ressaltar, como claro limite à liberdade de expressão conferida ao emissor de tal tipo de manifestação. Sobre os embates possíveis entre liberdade de expressão e direitos da personalidade, ver: MARMELSTEIN, George. *Curso de direitos fundamentais*. 8. ed. São Paulo: Atlas: 2019, p. 133 e ss. e p. 430 e ss. Em seu estudo o autor trata do Caso Ellwanger, no qual o STF se pronunciou pela não tutela constitucional de manifestações discriminatórias proferidas em face do povo judeu e que lançavam dúvidas sobre a existência do Holocausto no contexto da Segunda Guerra Mundial (HC 82.424-RS).

[23] A ausência de regras no âmbito do tráfego de dados por meio da internet gera um ambiente especialmente propício à opressão, do qual são expressões fenômenos como o *cyberbullying* e os discursos de ódio, conforme ponderação feita por: SCHREIBER, Anderson. Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por dano gerado por terceiro. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*. São Paulo: Quartier Latin, 2015, t. 2, p. 277-305, p. 281.

Em uma situação na qual não seja possível, nem mesmo em tese, vislumbrar interesse público relevante na manutenção do link de acesso impugnado[24], entendemos que a resposta seja negativa.

Ainda que atores da mídia vejam potencial de venda para seus produtos via disseminação de informação sobre a morte de uma pessoa, atrelar tal relato a imagem que expõe a família da vítima fatal a inquietação e martírio corresponde a conduta abusiva, seja pela consternação gratuita imposta a terceiros, seja pela conduta empresarial estar descompassada com a preservação do bem jurídico que justifica a existência ao art. 19 da Lei nº 12.965/14 em nosso sistema[25].

3.4. Perspectivas à vista da Lei Geral de Proteção de Dados — LGPD (lei nº 13.709/18)

Não bastasse as críticas feitas ao art. 19 da Lei nº 12.965/14 à luz dos argumentos supramencionados, que exigem ao menos sua leitura conforme a Constituição e o art. 5º da LINDB de modo a não se amesquinhar a tutela de direitos da personalidade em nome de uma (por vezes apenas retórica) defesa da liberdade de expressão, vale ressaltar que a LGPD trouxe novo ingrediente para o debate[26].

O art. 18, IV da Lei nº 13.709/18 prevê o seguinte:

> *O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: […] IV — anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei*[27].

[24] Interesse público não corresponde necessariamente a interesse do público, como aponta Viviane Nóbrega Maldonado: *"a informação assegurada à sociedade é aquela que ostenta caráter de interesse público, não bastando, à evidência, o mero interesse do público em conhecer algum dado. Com efeito, acontecimentos que tão somente despertam a curiosidade não ganham o 'status', tecnicamente, de informação, porquanto cedem ao direito à privacidade de terceiros"* (MALDONADO, Viviane Nóbrega. *Direito ao esquecimento*. Barueri: Novo Século, 2017, p. 94).

[25] Para uma visão crítica quanto à constitucionalidade do art. 19 da Lei nº 12.965/14, ver: SCHREIBER, Anderson. Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por dano gerado por terceiro. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. t. 2, p. 277-305. O autor, de modo bastante perspicaz, abordando situações em que a manifestação ofensiva pela internet extrapola notícias jornalísticas de cunho sensacionalista alerta para a necessidade de cuidado com a *"invocação de liberdade de expressão no universo virtual"*, por tratar-se *"frequentemente de argumento falacioso, já que a imensa maioria dos casos concretos envolvendo pedidos e supressão de material lesivo na jurisprudência brasileira diz respeito a informações flagrantemente falsas, ofensas evidentes, comentários racistas e outras espécies de conteúdo que, muito ao contrário de exprimir um exercício legítimo de liberdade de expressão, pretendem canibalizá-la por meio de intimidação, do 'bullying' virtual, do ´online hate speech´ e de outras formas virtuais de opressão"* (p. 305). Em sentido próximo, ainda agregando outros argumentos para que se evite retrocesso na tutela de direitos da personalidade por uma aplicação literal do dispositivo em tela (como a garantia constitucional conferida à proteção dos consumidores e a responsabilidade inerente a cada empresa quanto à formulação de sua política de remoção de conteúdos), ver: GODOY, Cláudio Luiz Bueno de. Uma análise crítica da responsabilidade civil dos provedores na Lei nº 12.965/2014 (Marco Civil da Internet). *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III. São Paulo:* Quartier Latin, 2015, t. 2, p. 307-320, p. 316 e ss.; LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do marco civil da internet (Lei n. 12.965/14). *Revista da Faculdade de Direito, Universidade de São Paulo*. São Paulo, v. 110, p. 155-176, 2015, p. 172 e ss.

[26] Que inclusive teve sua repercussão geral reconhecida pelo Supremo Tribunal Federal no âmbito do RE nº 1.037.396, como pode ser conferido em: http://bit.ly/38bb9pd. Acesso em: 25 set. 2019. A mesma Corte ainda afetou para o julgamento em tal regime o RE nº 1.010.606, Tema nº 786, assim enunciado: *"aplicabilidade do direito ao esquecimento na esfera civil quando for invocado pela própria vítima ou pelos seus familiares"* (Disponível em: http://bit.ly/2u5xDJD. Acesso em: 26 set. 2019).

[27] http://bit.ly/2FViq0f. Acesso em: 25 set. 2019.

Considerando a clareza do quanto estipulado pela LGPD, para além dos fundamentos de Teoria Geral do Direito sobre caminhos possíveis para uma interpretação do art. 19 do Marco Civil consentânea com os bens jurídicos em disputa na aplicação da referida lei, tem-se que o novo diploma garante expressamente ao cidadão que se vê lesado pela manipulação desautorizada de seus dados por empresas de tecnologia a oportunidade de dirigir-se diretamente a elas em busca da respectiva desindexação[28].

No nosso caso, não parecendo haver dúvida que a exposição de imagem de pessoa morta em condições degradantes não é necessária para a divulgação de notícia sobre o trágico acidente, tem-se que, também por este novo fundamento legal, a conduta do site e do motor de buscas é ilegítima.

4. Conclusão

Em disputas envolvendo direito à informação e o resguardo de direitos da personalidade, nem sempre é simples decidir o que deve prevalecer.

É o que se dá, por exemplo, em notícias que envolvam a investigação de crimes, nas quais as pessoas que se veem vinculadas a tais ilícitos podem ser expostas a constrangimentos só pelo fato de verem seus nomes enlaçados às referidas práticas, sem que haja qualquer decisão judicial avaliando o mérito da respectiva imputação.

Em tais hipóteses, seja pelos valores albergados em nossa Constituição, seja pelo quanto disciplinado pelo Marco Civil de Internet, os provedores têm lastro jurídico para só indisponibilizarem o acesso ao material após ordem judicial que assim os obrigue.

Em outras, como a que serve de mote para o presente ensaio, só se vê busca de publicidade à custa da aflição alheia.

Nestas, em que não há interesse público relevante, seja por parte das empresas em disseminar a dor, seja por parte dos destinatários da mensagem em terem instintos primitivos satisfeitos com um espetáculo lúgubre, não há, a nosso ver, campo legítimo para a incidência do art. 19 da Lei nº 12.965/2014.

Ah, e o nosso caso...

Na situação que examinamos envolvendo a matéria, a decisão, de forma harmônica com o raciocínio que ora tivemos oportunidade de melhor desenvolver, foi pela indisponibilização do link referido na inicial, mas com rejeição do pleito de indenização.

No que se refere ao bloqueio de acesso ao conteúdo ofensivo, a boa notícia é que o comando judicial foi cumprido, dado a desmentir a famosa tese de *"impossibilidade técnica"* veiculada à exaustão em defesas apresentadas por provedores de internet em situações análogas submetidas à apreciação judicial.

Já quanto ao pleito de reparação por dano imaterial, o entendimento foi pela necessidade de antes haver a notificação do site e do buscador para cessação do dano,

[28] Valendo quanto ao ponto registrar que, como nos dá notícia Viviane Nóbrega Maldonado, em importante precedente sobre a matéria proferido em 13 de maio de 2014 pelo Tribunal de Justiça da União Europeia (caso Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González), a atividade do motor de buscas da internet foi expressamente reconhecida como de "tratamento de dados pessoais", o que o torna responsável pela inadequação do serviço oferecido ao público por tal meio (MALDONADO, Viviane Nóbrega. *Direito ao esquecimento*. Barueri: Novo Século, 2017, p. 103 e ss.).

seguida da sua resistência ilegítima a respeito, como condição para configuração dos pressupostos da responsabilidade civil.

Como tal providência não fora demonstrada pela requerente, não chegamos a ter que nos pronunciar sobre a constitucionalidade ou a adequada interpretação dada pelas rés ao art. 19 do Marco Civil à vista do art. 5º, X da Constituição, dos arts. 12 e 927 do Código Civil, e/ou do art. 5º da LINDB, alguns dos principais anteparos previstos em nosso ordenamento para a tutela dos direitos do usuário frente a empresas que lucram, normalmente sem autorização informada, com o tratamento de dados pessoais relativos a si ou a entes queridos que, por qualquer circunstância, não estejam em condições de se defender.

5. Bibliografia

BOBBIO, Norberto. *Teoria do ordenamento jurídico*. 10. ed. Tradução: Maria Celeste Cordeiro Leite dos Santos. Brasília, DF: UNB, 1997.

CUNHA FILHO, Alexandre Jorge Carneiro da. Ponto cego na aplicação da lei. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Lei de Introdução às Normas do Direito Brasileiro*: anotada. *São Paulo:* Quartier Latin, 2019. v. 1, p. 321-329.

DANTAS, San Tiago. A educação jurídica e a crise brasileira. *Revista Forense*, São Paulo, v. 159, n. 52, p. 449-458, 1955.

DONNINI, Rogério José Ferraz. Bona fides: do direito material ao processual. *Revista de Processo*, São Paulo, v. 251, p. 113-126, 2016. Disponível em: http://bit.ly/2tpCt4b. Acesso em: 16 jan. 2020.

GODOY, Cláudio Luiz Bueno de. Uma análise crítica da responsabilidade civil dos provedores na Lei nº 12.965/2014 (Marco Civil da Internet). *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III. São Paulo:* Quartier Latin, 2015. t. 2, p. 307-320.

GRAU, Eros Roberto. *Ensaio e discurso sobre a interpretação/aplicação do direito*. São Paulo: Malheiros, 2002.

LARENZ, Karl. *Metodologia da ciência do direito*. 8. ed. Tradução: José Malego. Lisboa: Fundação Calouste Gulbenkian, 2019.

LIMA, Cíntia Rosa Pereira de. A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do marco civil da internet (Lei n. 12.965/14). *Revista da Faculdade de Direito, Universidade de* São Paulo, São Paulo, v. 110, p. 155-176, 2015.

LUVIZOTTO, Juliana Cristina. O art. 30 da Lei de Introdução *às* Normas do Direito Brasileiro e a sua relação com os precedentes administrativos. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Lei de Introdução às Normas do Direito Brasileiro*: anotada. *São Paulo:* Quartier Latin, 2019. v. 2, p. 490-498.

MALDONADO, Viviane Nóbrega. *Direito ao esquecimento*. Barueri: Novo Século, 2017.

MANCUSO, Rodolfo de Camargo. *Sistema brasileiro de precedentes*. 2. ed. São Paulo: Revista dos Tribunais, 2016.

MARQUES NETO, Floriano de Azevedo; FREITAS, Rafael V*éras* de. *Comentários à lei nº 13.655/2018*. Belo Horizonte: Fórum, 2019.

MARMELSTEIN, George. *Curso de direitos fundamentais*. 8. ed. São Paulo: Atlas: 2019.

MUÑOZ, Alberto Alonso. *Modelos de fundamentação filosófica do direito privado e seus limites*: contribuição à crítica do direito privado. 2015. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2015.

NAGATA, Bruno Mitsuo. Questões atuais do devido processo legislativo. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Lei de Introdução às Normas do Direito Brasileiro*: anotada. São Paulo: Quartier Latin, 2019. v. 1, p. 91-97.

OLIVEIRA, Regis Fernandes de. *Indagação sobre os limites da ação do Estado*. São Paulo: Revista dos Tribunais, 2015.

PERLINGIERI, Pietro. *O direito civil na legalidade constitucional*. Tradução: Maria Cristina de Cicco. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. Marco Civil da Internet: avanço ou retrocesso? A responsabilidade civil por dano gerado por terceiro. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira. de (coord.). *Direito & internet III. São Paulo:* Quartier Latin, 2015. t. 2, p. 277-305.

SICHES, Luis Recaséns. *Experiencia jurídica, naturaleza de la cosa y lógica "razonable"*. Cidade do México: Unam, 1971.

SILVA, Domicio Whately Pacheco e. O acesso à prestação jurisdicional e a responsabilidade das partes: reflexões sobre o papel da gratuidade processual, dos honorários sucumbenciais e da litigância de má-fé na distribuição da Justiça. *In*: CUNHA FILHO, Alexandre Jorge Carneiro da; OLIVEIRA, André Tito da Motta; ISSA, Rafael Hamze; SCHWIND, Rafael Wallbach (coord.). *Direito, instituições e políticas públicas*: o papel do jusidealista na formação do Estado. São Paulo: Quartier Latin, 2017. p. 675-694.

Links patrocinados — concorrência e comércio eletrônico — análise jurisprudencial das Câmaras Reservadas de Direito Empresarial

Paula da Rocha e Silva Formoso[1]
Juíza de Direito no Estado de São Paulo

Resumo: A era cibernética alterou o modo de realizar negócios. Em adição ao comércio convencional, surge o comércio eletrônico. Uma das principais ferramentas de publicidade utilizada para a difusão da atividade empresarial é o denominado *link* patrocinado, por meio do qual é possível vincular termos relacionados às marcas de terceiros, mediante pagamento feito pelo anunciante. O presente estudo visa analisar limites de utilização do motor de busca da *internet* nos *links* patrocinados, a partir da apresentação de conceitos de direito digital, propriedade intelectual e direito concorrencial, além de precedentes jurisprudenciais da Câmara Reservada de Direito Empresarial atinentes ao tema.

Palavras-chave: Direito Digital. Sociedade Informacional. Comércio Eletrônico. Buscadores da *Internet*. *Links* Patrocinados. Aquisição de Palavra-Chave Atrelada à Marca do Concorrente. Direito Concorrencial. Concorrência Desleal. Uso Parasitário da Marca Alheia. Jurisprudência das Câmaras Reservadas de Direito Empresarial.

Introdução

Uma pergunta extremamente pertinente no bojo do novíssimo universo do Direito Digital, que surge no contexto da contratação de *links* patrocinados, é: há atuação concorrencial lícita quando o anunciante vincula termos relacionados à marca registrada de um concorrente, para o direcionamento do público-alvo daquele terceiro ao seu próprio sítio eletrônico?

A revolução tecnológica, iniciada com a terceira revolução industrial e intensificada a partir da quarta, conduziu o futuro imaginado nas obras de ficção científica ao presente, tornando a informação disseminada pela rede mundial de computadores o epicentro da sociedade atual. O mercado, seguindo à risca a célebre frase de Zygmunt Bauman,

[1] Mestra em Direito Penal pela Pontifícia Universidade Católica de São Paulo.

qual seja, "na era da informação, a invisibilidade é equivalente à morte", tornou a *internet* uma grande ferramenta de publicidade, senão a maior, para o fomento da produção e circulação de bens ou serviços.

A neutralidade da rede estimula a livre concorrência e o acesso do consumidor à *internet*. Em outra perspectiva, possibilita que pequenos e médios empresários utilizem o comércio eletrônico (*e-commerce*) para adquirir maior visibilidade na oferta e circulação de produtos e serviços, a partir do uso de motores de buscas da *internet* (*Search Engine Marketing*), alcançando fatias do mercado até então de difícil ou inimaginável penetração.

O aumento expressivo da concorrência dos *players* do mercado, causado pela aceleração das inovações tecnológicas, traz como consequência a procura por opções que consigam maior destaque e atinjam maior número de pessoas. Com isso, novas "armas" são desenvolvidas e disponibilizadas pelos buscadores da *internet*, como é o caso dos *links* patrocinados, que nada mais são do que um serviço pago para alteração da ordem natural dos resultados advindos da busca de uma palavra-chave, para que o anunciante que contrata tal serviço pago tenha maior destaque com relação aos demais.

O escopo deste estudo é, justamente, analisar quais seriam os limites de utilização do motor de busca da *internet* nos *links* patrocinados. Para tanto, será necessário apresentar conceitos de Direito Digital, Propriedade Intelectual e Direito Concorrencial, além de precedentes jurisprudenciais da Câmara Reservada de Direito Empresarial atinentes ao tema, por meio dos quais poderão ser confrontadas as normas, delimitada a controvérsia e extraídas as conclusões.

1. A sociedade informacional e o comércio eletrônico

Os constantes movimentos de destruição criativa marcam o desenvolvimento humano. O fascínio pela mudança provoca imensas transformações econômico-sociais, como se observa a partir do advento das terceira e quarta revoluções industriais, com a disseminação mundial da *internet* no início do século XXI, proporcionando a fusão de tecnologias e o desaparecimento das linhas entre as esferas física, digital e biológica, interferindo diretamente nas relações jurídico-negociais.

A alteração do modo de convivência humana com o uso das novas tecnologias foi observada por Benacchio e Santos (2015, p. 154):

> *Nesta era, por meio da internet, os cidadãos sem sair de casa podem acessar os centros de documentos mais relevantes do mundo, realizar diversas operações financeiras e comerciais, usufruir de uma infinidade de entretenimentos de diversas espécies e se comunicar com outros usuários da rede sem limitações de quantidade e distância. Atualmente, por intermédio da internet cada domicílio de usuário da rede se torna um terminal que compõe um sistema universal integrado.*

Inegável que a mobilidade da *internet* auxilia a interação humana de forma dinâmica, imediata e em tempo real, a partir da difusão da informação de forma veloz e complexa, criando um incessante trânsito de dados que precisa ser cuidadosamente controlado, armazenado e distribuído.

A cultura digital transforma a sociedade em informacional, conferindo verdadeiro valor econômico ao conhecimento, com a criação e multiplicação de formas de fomento para produção e circulação de produtos e serviços, aprimorando em proporções antes inimagináveis os modelos de negócio até então existentes.

Observa Wachowicz (2015, p. 238):

> *A informação ganha na internet novas dimensões, já não mais o mero acesso às obras raras (livros, pinturas, esculturas), mas também o que contém o germe da nova invenção, da descoberta, que cria ou possibilita a criação do novo, que transforma, circula, e permeia todos os universos humanos, desde a esfera econômica, social e política, até planos éticos, culturais e ambientais.*

Nesse contexto de ampliação e avanços tecnológicos, surge o comércio eletrônico, ou e-*commerce*, que pode ser compreendido como a atividade que visa a alienação, em sentido amplo, de bens ou serviços por meio eletrônico. Trata-se, certamente, de um novo meio de desenvolver a atividade empresarial, que permite tanto a expansão da livre concorrência como o surgimento de novos modelos de negócio.

A relevância do *e-commerce* é destacada por Teixeira (2015, p. 341):

> *E-commerce ou comércio eletrônico representa parte do presente e do futuro do comércio, existem várias oportunidades de negócio espalhadas pela internet, além de muitas que são criadas a todo momento. O crescimento do número de internautas na última década é espantoso, sendo que atualmente 45,6% da população brasileira têm acesso à internet (aproximadamente 90 milhões de pessoas).*

Inegável que a criação do mercado virtual trouxe inúmeros atrativos aos empresários, na medida em que os investimentos com a contratação de pessoal e montagem de local físico compatível com o modelo de negócio praticado são drasticamente reduzidos. Note-se que a redução de custos beneficia tanto o grande empresário já estabelecido no mercado, que pode diversificar e expandir seu negócio, quanto o pequeno/médio empresário, que deseja iniciar uma atividade empresarial ou que já atua com alcance territorial limitado.

Com a expansão da forma de exercício da livre iniciativa, houve o crescimento do número de *players* do mercado e a alteração de hábitos pelo consumidor, fato que conduziu à necessidade de adaptação do mercado e da comunidade jurídica.

Destaca Forgioni (2018, p. 406-407):

> *Nos últimos dez anos, o comércio pela internet passou a fazer parte do nosso dia a dia. Essa modificação dos hábitos de consumo em direção ao comércio eletrônico levou a doutrina a analisar os impactos jurídicos nesse horizonte que se expande cada vez mais. Foi preciso repensar os acordos e as restrições verticais nesse cenário, pois é evidente o aumento do grau de concorrência propiciado pela web: mercados antes apartados aproximam-se de outros, abrindo o leque de opções para o consumidor. Aqueles que, antes, adquiriam obras*

> *estrangeiras em uma pequena livraria situada na frente da faculdade, agora encomendam pelo computador.*

Expostos os principais aspectos da inovação causada pela *internet*, passa-se a examinar a concorrência dos *players* do mercado na era digital.

2. Concorrência na era cibernética

A era cibernética alterou sensivelmente os principais objetos do mercado, trazendo ao centro da discussão a propriedade intelectual, a qual se encontra abarcada pelo sistema de proteção à propriedade industrial (Lei n. 9.279/1996), com o fim de coibir eventuais abusos e concorrência desleal.

O valor da propriedade intelectual na era cibernética é bem apontado por Silveira (2001):

> *O sucesso do sistema de proteção à propriedade industrial, mediante a concessão de um título de exclusividade conferido pelo Estado, fez com que esse sistema se estendesse às marcas por meio do registro. Criou-se, assim, um novo bem imaterial, objeto dessa forma especial de propriedade, embora essa tutela não seja, no caso, conferida em reconhecimento de um ato de criação, mas para o fim de reprimir a concorrência desleal. Esse direito compete ao empresário, e não ao autor. […] Dessa forma, as marcas passaram a integrar o quadro da propriedade intelectual, ao lado dos direitos autorais e dos direitos sobre as criações industriais. Os direitos sobre os sinais distintivos e sobre as criações industriais compõem a propriedade industrial. No mundo moderno, porém, as obras intelectuais são também objeto do tráfico comercial, através da indústria editorial, gráfica, fonográfica e empresas de comunicações e diversões, sujeitando-se, em consequência, às normas reguladoras da concorrência.*

Assim, se os usuários do sistema eram, inicialmente, os autores e os inventores, hoje o usuário principal é a empresa, que exige do Estado e dos organismos internacionais uma proteção mais eficiente para sua propriedade intelectual, que passa a representar valor substancial em seus ativos.

De acordo com o sistema de proteção à propriedade industrial, propriedade da marca adquire-se pelo registro validamente expedido, sendo assegurado ao titular seu uso exclusivo em toda a abrangência do território nacional, conforme dispõe o artigo 129 da Lei n. 9.279/1996, sendo certo que "abrange o uso da marca em papéis, impressos, propaganda e documentos relativos à atividade do titular", de acordo com o que estabelece o artigo 131 da Lei n. 9.279/1996.

Se, por um lado, os direitos de propriedade industrial outorgam a exclusividade como forma de recompensa pela descoberta, criação ou inovação de determinado titular, de outra banda, desestimulam a força concorrencial dos demais agentes econômicos atuantes no mercado.

O contraponto é bem esclarecido por Forgioni (2018, p. 328-329):

> *Em suma: de uma parte, a garantia à propriedade intelectual pode estimular o desenvolvimento tecnológico, de outra, porém, é capaz de gerar situação propensa ao abuso, especialmente em ambientes nos quais a força concorrencial é arrefecida pela outorga da exclusividade. Nota-se potencial tensão entre as duas legislações. Tudo está em acertar o "tênue equilíbrio entre a justa recompensa do esforço intelectual humano [...] e o estímulo à evolução cultural e industrial do país".*

Nessa ordem de ideias, a exclusividade conferida ao titular de uma marca constitui-se exceção ao sistema jurídico que confere obediência ao princípio da livre concorrência.

Passa-se, agora, à verificação do uso dos motores de busca para fomento da atividade empresarial e o impacto em termos concorrenciais.

3. Concorrência e uso dos motores de busca para fomento da atividade empresarial

Por certo, um dos principais instrumentos para o desenvolvimento do comércio eletrônico é o motor de busca (*Search Engine Marketing*) oferecido pelos provedores de pesquisa, que nada mais é do que um mecanismo de páginas na *internet*, cujo resultado é, a princípio, orgânico, vale dizer, advém naturalmente da palavra-chave que foi objeto da pesquisa.

Ocorre que alguns provedores de busca oferecem um serviço pago de publicidade para alterar o referenciamento de um domínio, com base na utilização de certas palavras-chave. Isso significa dizer, em realidade, que o referido provedor expõe à venda palavras-chave, para que se exiba, com destaque e precedência, o conteúdo pretendido pelo anunciante.

Confere-se ao mecanismo pago oferecido pelos provedores de busca para dar publicidade aos produtos e serviços o nome de *links* patrocinados (*keyword advertising*). A ferramenta funciona, como era de se esperar, em prol de quem puder pagar o maior valor pela posição destacada da palavra-chave, que é escolhida livremente pelo próprio anunciante, de acordo com o público-alvo que se pretende atingir, sem imposição de qualquer restrição.

Elucidam Bueno e Idie (2016):

> *[...] as empresas têm se valido de um novo mecanismo on-line para dar publicidade aos seus produtos e serviços: a contratação de "links patrocinados". Trata-se de um serviço de publicidade disponibilizado por alguns dos principais sites de busca (Google, Bing, Yahoo! Search), que consiste na venda de determinadas palavras-chave atreladas ao negócio desenvolvido pela empresa, de modo que, quando pesquisadas pelos internautas, os sites de busca exibam, em um campo de destaque, o conteúdo do anunciante, proporcionando maior visibilidade para o público consumidor. [...] Nesse contexto, uma joalheria, por exemplo, pode comprar as palavras "joias", "ouro", "prata", "brincos", "colares", para que o seu anúncio apareça em um campo de destaque quando tais termos forem pesquisados no buscador, pelo seu consumidor alvo. [...] O contratante dos "links patrocinados", via de regra, paga pelo serviço de acordo com a sua efetividade,*

> *com base nos acessos proporcionados ao seu anúncio, o que tem ajudado a tornar essa forma de publicidade ainda mais procurada.*

Trata-se de prática publicitária que visa estimular que distintos agentes econômicos disputem a entrada ou manutenção num determinado mercado, em espaço geográfico bastante alargado em comparação ao mercado convencional.

Na medida em que a ordem econômica brasileira fundamenta-se na livre iniciativa, a partir da observância do princípio da livre concorrência, conforme prescrito na Constituição republicana de 1988, em seus artigos 1º, IV, e 170, IV, os atuantes no mercado procuram natural adaptação à nova realidade, adquirindo instrumentos que confiram destaque aos seus próprios produtos ou serviços.

A existência, de *per si*, de *links* patrocinados não merece a intervenção anormal do Estado, pois a prática de adquirir determinadas palavras-chave atreladas ao próprio negócio desenvolvido, para conferir maior destaque ao anúncio, situa-se dentro do comportamento esperado pelos *players* do mercado.

Exposto o conceito de *links* patrocinados e a sua relevância para o mercado, analisar-se-á a licitude da utilização de palavras-chave com termos vinculados à marca de terceiro.

4. Links patrocinados e marca do concorrente como palavra-chave do motor de busca

Questão tormentosa que exsurge com o direcionamento intencional do internauta é o limite desta escolha, na medida em que é permitido, porque o provedor não impõe restrição, utilizar a marca de uma empresa concorrente como palavra-chave para encaminhar o consumidor para seu próprio sítio eletrônico.

O estímulo à livre iniciativa, dentro ou fora da rede mundial de computadores, deve conhecer limite, pois inconcebível admitir que seja considerada lícita conduta que cause confusão ou associação proposital à marca de terceiro atuante no mesmo nicho de mercado.

A utilização da marca de determinado concorrente como palavra-chave para direcionamento ao seu próprio *link* patrocinado constitui prática ilegal, pois o anunciante vale-se do renome conquistado pelo concorrente para ludibriar o público-alvo de consumidores.

Esclarece Rodrigues Junior. (2015):

> *No caso específico das atividades comerciais dos motores de busca, o fornecimento de serviços de links patrocinados é capaz de gerar prejuízos vultosos aos interesses legítimos dos titulares de marcas comerciais e ao funcionamento do mercado. Os prejuízos são bem conhecidos: violação das diversas funções das marcas; concorrência desleal; parasitismo comercial. Sem contar que promoção de atos de concorrência desleal acaba por prejudicar o consumidor, pois tais atos enfraquecem os agentes econômicos leais.*

O uso por terceiros de esforços ou criações alheia, ao acionar um algoritmo no sistema, com o intuito de obter vantagem financeira, pode caracterizar concorrência desleal ou crescimento parasitário, a depender do ramo de atuação, identidade de público-alvo e disputa de clientela.

A diferença entre concorrência desleal e aproveitamento parasitário é bem explicada por Bueno e Idie (2016):

> *Para que se caracterize a concorrência desleal, é necessário que haja obrigatoriamente a concorrência entre os agentes, além dos seguintes pressupostos: 1. Os fatos têm que ocorrer na mesma época, pois se faz necessária a disputa de clientela, o que jamais ocorreria se atuassem em épocas distintas; 2. A identidade entre os produtos ou serviços (não precisam ser exatamente idênticos, caso possam ser substituídos pelo consumidor); e 3. Haja identidade do mercado, ou seja, estejam voltados ao mesmo mercado consumidor. […] Ademais, é necessário que haja a disputa da clientela de forma abusiva, de maneira desleal, nesse sentido pontua o professor Denis Borges Barbosa: "É preciso que os atos de concorrência sejam contrários aos "usos honestos em matéria industrial ou comercial" (Convenção de Paris, art. 10-bis) ou a "práticas comerciais honestas" (TRIPS, art. 39) – sempre apurados segundo contexto fático de cada mercado, em cada lugar, em cada tempo". […] O aproveitamento parasitário, por sua vez, independe da existência de concorrência entre os agentes, os quais podem não estar no mesmo ramo mercadológico ou não disputar a mesma clientela, mesmo que atuem em ramo idêntico, fato é que nestes casos, não haverá o desvio de clientes. […] Assim, pode-se afirmar que a essência do aproveitamento parasitário está nas situações em que "alguém procura vencer no mercado, não pela sua própria contribuição, mas explorando as contribuições alheias". Ainda, a doutrina francesa define o instituto como o ato ou atos de um empresário que tira ou procura tirar proveito das realizações pessoais de outrem, mesmo se não tem a intenção de prejudicar este último. […] Portanto, aquele que se utiliza dos nomes ou das marcas registradas de empresas diretamente concorrentes, ou simplesmente se aproveita da popularidade que estas possuem no mercado para posicionar melhor os seus produtos e serviços na internet, por meio de publicidade em links patrocinados, pode ser alvo de medida judicial, para que se abstenha da conduta e indenize eventuais prejuízos ao titular dos sinais distintivos.*

A conduta de aquisição de termo vinculado à marca alheia em *link* patrocinado, seja caracterizada como concorrência desleal pela atuação no mesmo nicho de mercado com desvio de clientela, ou como aproveitamento parasitário da marca por ausência de desvio de clientes, é ilícita e, como tal, deve ser coibida pelo Poder Judiciário.

5. Análise da jurisprudência das Câmaras Reservadas de Direito Empresarial do Tribunal de Justiça do Estado de São Paulo

Por certo, as Câmaras Reservadas de Direito Empresarial do Tribunal de Justiça, que detêm competência absoluta para o julgamento desde 2011, sedimentaram entendimento segundo o qual quem utiliza marca de concorrente como palavra-chave para o seu próprio *link* patrocinado, além do uso indevido de marca alheia, ainda comete ato de concorrência desleal.

A conclusão de unicidade de entendimento da Corte Paulista, pelo julgamento de 31 casos com idêntica questão de mérito, pode ser observada por meio da leitura do V. Acórdão que julgou a Apelação Cível n. 1002037-18.2016.8.26.0003, em que Eminente Relator o Desembargador Gilson Miranda, publicada no *Diário Oficial* em 12/07/2019:

> *DIREITO MARCÁRIO. Google Ads. Link patrocinado. Uso de marca de concorrente como palavra-chave. Prática ilegal. Violação de direitos sobre a marca e concorrência desleal. Jurisprudência uníssona das Câmaras Reservadas de Direito Empresarial do TJSP desde abril/2016. Conjunto probatório dos autos, porém, insuficiente para fundamentar a condenação pretendida. Ausência de prova do uso da marca da autora pela ré. Sentença mantida. Recurso não provido. […] Segundo pesquisa realizada pela Comissão de Estudo de Direito da Concorrência da Associação Brasileira de Propriedade Intelectual (ABPI) sobre a visão dos tribunais brasileiros com relação ao uso de links patrocinados com palavras-chave que imitem ou reproduzam sinais distintivos de concorrentes, até abril/2016 foram julgados 22 recursos acerca do tema, sendo que, dos 17 julgados que adentraram no mérito da questão, 13 foram favoráveis à tese de concorrência desleal e/ou violação de marca. Interessante anotar que dos 4 julgados restantes, que não adotaram essa tese, 3 deles assim decidiram porque o anunciante era revendedor autorizado (atraindo a incidência da regra específica do artigo 132, inciso I, da Lei de Propriedade Industrial) e o último foi proferido em demanda na qual não foi provada a utilização do sinal distintivo do concorrente no link patrocinado (Daniel Adensohn de Souza, Felipe Barros Oquendo, Ísis Moret Souza Valaziane e Lívia Barboza Maia, "A Jurisprudência sobre o Uso de Links Patrocinados como Instrumento de Concorrência Desleal", 'in' Revista da ABPI, edição 144, setembro-outubro/2016, p. 53 e ss.). […] Desde então, as Câmaras Reservadas de Direito Empresarial deste Tribunal de Justiça tiveram a oportunidade de enfrentar essa mesma questão, no mérito, em pelo menos mais 31 casos. E em 30 desses julgados, o entendimento foi exatamente o mesmo: aquele que utiliza marca de concorrente como palavra-chave para o seu próprio link patrocinado, além do uso indevido de marca alheia, ainda comete ato de concorrência desleal.*

O interessante julgado acima referido entendeu que, a depender da prova produzida em cada caso concreto, haveria a violação dos direitos sobre a marca quando o anunciante age como parasita do prestígio de marca alheia, atraindo para si a clientela sem ter realizado investimentos para isso. Ademais, a marca teria sua reputação diluída no mercado, deixando de alcançar posição de destaque no mercado. A função publicitária da marca restaria também prejudicada pela redução da visibilidade. Por fim, prejudicaria a função de investimentos da marca, pela necessidade de ampliar os investimentos em publicidade.

Restou assentado, ainda, que utilizar marca de concorrente como palavra-chave para o seu próprio *link* patrocinado provocaria confusão com o estabelecimento, os produtos ou a atividade praticada pelo concorrente, de modo a induzir o público, pelo que configuraria conduta desleal. A deslealdade residiria na forma de conduzir a captação de clientela.

Muito embora o julgado tenha entendido que as provas existentes naquele caso concreto eram insuficientes para o decreto de procedência dos pedidos, a conclusão extraída foi no sentido de que a conduta configuraria um ato de parasitismo, além de gerar confusão mercadológica, uma vez que o anunciante e o titular da marca tendem a atuar no mesmo nicho de mercado. Como via de consequência, a prática configuraria crime de concorrência desleal, prevista no artigo 195, III, da Lei n. 9.279/1996, e conferiria ao prejudicado o direito de haver perdas e danos pelos prejuízos sofridos, mercê do que dispõe o artigo 209, caput, da Lei n. 9.279/1996.

A título exemplificativo, os seguintes precedentes da 2ª Câmara de Direito Empresarial, os quais consideraram ilícita a conduta de direcionamento do usuário utilizando-se de termos vinculados à marca do concorrente:

> *Propriedade industrial. Vinculação do sítio eletrônico da corré à marca da autora e à expressão com que se identifica no âmbito virtual. Link patrocinado. Tutela devida para vedar o direcionamento do usuário. Vedação à concorrência desleal. Dano material presumido e cuja indenização se deve apurar em liquidação. Dano moral também devido, embora não no valor pretendido. Responsabilidade da corré que se vincula à exploração de serviço específico de publicidade pelo qual é remunerada e à contratação com quem viola, bem por meio do mesmo contrato que entabula, direito alheio. Sentença revista. Recurso provido em parte (Apel. N. 1019621-41.2015.8.26.0001, Rel. Des. Claudio Godoy, j. 09/04/2018).*
>
> *[…] MARCA. OBRIGAÇÃO DE NÃO FAZER C/C REPARAÇÃO DE DANO. LINK PATROCINADO. Uso marca da autora como palavra chave de link patrocinado contratado pela ré. O consumidor que fazia uma busca na internet pelo nome da autora obtinha como resposta, dentre as opções, o site da ré. Uso parasitário da marca. Dano moral presumido. Lesão à honra, reputação e imagem da autora que, ao lado do uso parasitário do nome da sociedade empresária, deve ser indenizado. Não comprovação de danos materiais. Provimento em parte, para determinar a abstenção do uso da marca da autora e fixar dano moral em R$ 20.000,00, que se ajusta aos parâmetros da jurisprudência. Sucumbência recíproca e honorários fixados em 20% do valor da condenação para cada qual. (Apelação 0175492-17.2011.8.26.0100, Rel. Enio Zuliani, 1ª Câmara Reservada de Direito Empresarial, j. 13/07/2016).*

Estes, em suma, os argumentos pelos quais a jurisprudência das Câmaras Reservadas de Direito Empresarial do Tribunal de Justiça do Estado de São Paulo entende pela ilicitude da conduta de vinculação à marca de terceiros em *links* patrocinados.

6. Conclusão

Inegável que a era cibernética trouxe novas ferramentas de publicidade e *marketing*, possibilitando o aumento da concorrência e a criação de novos modelos de negócio. Com a difusão da prática de venda pelo meio virtual, inúmeras pessoas com receio de iniciar uma atividade no mercado convencional lançaram-se a explorar novos modelos de negócio, atraídos pelas maravilhas e pelo baixo possível custo propiciado pelo *e-commerce*.

Esse avanço acelerado e um pouco difuso do exercício da atividade empresarial, provocado pelo comércio eletrônico, gerou situações inusitadas, até pelo novo mundo que se abre com a utilização intensa da *internet* em tão curto espaço de tempo. Ora, num ambiente em que poucas regras existem, justamente para não podar a fluência do tráfego de informação, fica mais difícil estabelecer limites para o exercício da livre iniciativa aos *players* do mercado.

Todavia, um limite inafastável para o exercício saudável da concorrência é a lealdade, vale dizer, a adoção de práticas mercadológicas pautadas na razoabilidade, dentro do padrão de condutas que é esperado por aqueles que integram o mercado. A forma na condução da atividade empresarial importa, e muito.

Por certo, utilizar marca de concorrente como palavra-chave para o seu próprio *link* patrocinado viola a previsibilidade do comportamento esperado pelos demais *players* do mercado, confunde a clientela do concorrente, induzindo-a em erro. Configura, certamente, concorrência desleal.

Vilipendia, ainda, os direitos sobre a marca alheia, pois parasita o prestígio de marca alheia atraindo para si a clientela, aumenta injustamente a posição de destaque do desleal no mercado, reduz a visibilidade e prejudica os investimentos da marca violada.

A conduta violadora da concorrência e dos direitos sobre a marca foi bem observada pelas Câmaras Reservadas de Direito Empresarial do Tribunal de Justiça de São Paulo, as quais estabeleceram em seus julgados, de forma bastante uniforme, que aquele que usa marca de concorrente como palavra-chave para o seu próprio *link* patrocinado, além do uso indevido de marca alheia, ainda comete ato de concorrência desleal.

Entretanto, os desafios proporcionados pela cultura digital estão apenas começando. A era cibernética é nova e as consequências advindas desta nova forma de relacionamento humano são inúmeras, desconhecidas e ilimitadas.

Um misto de sentimentos de animação e de receio permeia a comunidade jurídica que se dedica aos estudos do Direito Digital, especialmente quando envolvidas questões atinentes à livre iniciativa e à livre concorrência. Cada dia que surge, um questionamento diverso emerge. Que venham os próximos.

Referências bibliográficas

BUENO, Samara Schuch; IDIE, Renata Yumi. *Você investe em links patrocinados utilizando-se do nome do seu concorrente?* Veja por que você não deveria fazer isso, 2016. Disponível em: https://bit.ly/2FXKlws. Acesso em: 28 ago. 2019.

BENACCHIO, Marcelo; SANTOS, Queila Rocha Carmona dos. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III – tomo I*: Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 147-170.

FORGIONI, Paula A. *Os fundamentos do antitruste*. 10. ed. São Paulo: Revista dos Tribunais, 2018.

RODRIGUES JUNIOR, Edson Beas. Reprimindo a concorrência desleal no comércio eletrônico: links patrocinados, estratégias desleais de marketing, motores de busca na internet e violação aos direitos de marca. *Revista dos Tribunais*, São Paulo, v. 961, p. 35-93, 2015.

SILVEIRA, Newton. *O Sistema de Propriedade Industrial Brasileiro*, 2001. Disponível em: https://bit.ly/2FWpZUp. Acesso em: 30 ago. 2019.

TEIXEIRA, Tarcisio. Responsabilidade civil no comércio eletrônico: a livre-iniciativa e a defesa do consumidor. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III – tomo II*: Marco Civil da Internet (Lei n. 12.965/2014). São Paulo. Quartier Latin, 2015. p. 341-376.

WACHOWICZ, Marcos. Cultura digital e marco civil na internet: contradições e impedimentos jurídicos no acesso à informação. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III – tomo II*: Marco Civil da Internet (Lei n. 12.965/2014) – São Paulo. Quartier Latin, 2015. p. 235-246.

Outras referências

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Brasília, DF, 1988. Disponível em: https://bit.ly/2NylYtE. Acesso em: 29 ago. 2019.

BRASIL. *Lei n. 9.279, de 14 de maio de 1996*. Regula direitos e obrigações relativos à propriedade industrial. Brasília, DF, 1996. Disponível em: https://bit.ly/371Mq6r. Acesso em: 29 ago. 2019.

SÃO PAULO (Estado). Tribunal de Justiça. *Acórdão – Apelação Cível n. 0175492-17.2011.8.26.0100*. Apelante Instrutemp Instrumentos de Medição LTDA. Apelados Homis Controle e Instrumentação LTDA. e outro. Relator: Desembargador Enio Zuliani. Acórdão. Julgamento do caso em 13/07/2016. São Paulo, 2016.

SÃO PAULO (Estado). Tribunal de Justiça. *Acórdão – Apelação Cível n. 1019621-41.2015.8.26.0001*. Apelante L25 Moda Íntima Virtual LTDA. EPP. Apelado Miess Moda Íntima e E-commerce LTDA. ME. Apelado Google Brasil Internet LTDA. Relator: Desembargador Claudio Godoy. Acórdão. Julgamento do caso em 04/09/2018. São Paulo, 2018.

SÃO PAULO (Estado). Tribunal de Justiça. *Acórdão – Apelação Cível n. 1002037-18.2016.8.26.0003*. Apelante Bralyx Máquinas Indústria Comércio LTDA. Apelado Maqtiva Indústria e Comércio de Máquinas LTDA. ME. Relator: Desembargador Gilson Miranda. Acórdão. *Diário Oficial da União*, Brasília, DF, 12 jul. 2019.

A busca e apreensão em celulares: algumas ponderações em torno da proteção de dados, da privacidade e da eficiência do processo

Guilherme Madeira Dezem[1]
Juiz de Direito no Estado de São Paulo

Sumário: 1. Introdução; 2. Intimidade; 3. Domicílio em geral; 4. A necessidade de mudança do conceito de casa; Conclusão.

Resumo: Os celulares passaram a ser parte integrante da vida em sociedade; mais do que meios de comunicação, têm capacidade para guardar inúmeras informações. O STJ entende que somente é possível analisar esses dados com ordem judicial. Este artigo pretende dar outro ponto de vista para a questão.

Palavras-chave: Prova. Busca e Apreensão. Digital. Celular. Ordem Judicial.

1. Introdução

Uma das maiores conquistas dos chamados direitos de primeira dimensão é a proteção dada ao domicílio. Nos mais variados países, a proteção ao domicílio encontra-se erigida com status constitucional.

Assim, por exemplo, temos o caso dos EUA, em que a proteção contra buscas arbitrárias encontra-se na 4ª Emenda. Da mesma forma, a Itália no artigo 14 de sua Constituição, e a Alemanha no artigo 13.

Tantos outros países poderiam ser citados de exemplo, mas o que importa neste momento é compreender a importância da proteção do domicílio apresentada pelos mais variados ordenamentos jurídicos. Percebe-se claramente a preocupação com a proteção de um dos núcleos da dignidade humana, que se expressa na proteção do domicílio.

No plano internacional, a situação também não é diferente. Diversos tratados buscam proteger o domicílio contra ingerências arbitrárias por parte do Estado. Assim, temos o Pacto Internacional Sobre Direitos Civis e Políticos, o Pacto de São José da Costa Rica e, no âmbito europeu, a Convenção Europeia de Direitos Humanos.

Percebe-se, porém, no plano internacional importante mudança de tônica: a proteção ao domicílio é ligada diretamente à proteção da honra, da dignidade e da vida familiar. Nada mais natural, afinal de contas a proteção dada ao domicílio está indissociavelmente ligada à proteção da intimidade e da privacidade.

[1] Mestre e doutor em Direito Processual pela Universidade de São Paulo. Professor da Universidade Presbiteriana Mackenzie (graduação e pós-graduação). Autor do curso de Processo Penal pela editora Revista dos Tribunais.

Quando se pensa nos primórdios da proteção do domicílio, bem como o que motivou a sua inclusão nos textos constitucionais e tratados internacionais, é possível identificar descompasso entre o objeto inicial da proteção e as mudanças surgidas com a pós-modernidade. E justamente é esta falta de sincronia que precisa ser pensada para atualizar a proteção constitucional e internacional.

O objetivo deste texto está em demonstrar esse descompasso e propor alterações na percepção do que se entenda por domicílio. Essa alteração é necessária para que se possa estender a proteção do domicílio, a fim de que o texto constitucional continue atual e tendo a abrangência idealizada pelos constituintes. Da mesma forma, procura-se demonstrar que o Marco Civil da Internet representa a positivação deste novo conceito de domicílio.

2. Intimidade

A proteção da intimidade e da vida privada foi positivado pela primeira vez no Brasil com o advento da Constituição Federal de 1988, o que não significa dizer que antes o direito à privacidade não era tutelado, apenas não constava na Constituição como direito fundamental individual.

A Constituição, em seu artigo 5º, X, garantiu de maneira detalhada os direitos da personalidade e não somente o direito à intimidade e à vida privada, mas também tutelou especificamente os direitos inerentes à dignidade da pessoa humana. Assim nos ensina Luiz Alberto Davi Araújo:

> *A Constituição de 1988, no entanto, acompanhando os textos constitucionais modernos de Portugal e Espanha, tratou de garantir os direitos da personalidade de forma específica e explícita. No entanto, enquanto os documentos ibéricos citados garantiram apenas um ou outro (a Constituição portuguesa de 1976 garantiu a "reserva da intimidade da vida privada e familiar" – art. 26, 1 – a Constituição da Espanha de 1978 garantiu o direito à honra, à intimidade pessoal e familiar, em seu art. 18.1), o Texto Constitucional brasileiro cuidou de garantir a privacidade, a intimidade, a imagem, os sigilos de correspondência, além de outros direitos no seu art. 5.º, da CF/1988 (LGL\1988\3)*[2].

A preocupação com a proteção da intimidade e da vida privada alcança status de direitos humanos, dada a preocupação mundial sobre o tema. Assim, está ela assegurada em tratados internacionais:

> *O princípio do respeito pela vida privada e familiar encontra-se consagrado, desde logo, no art. XII da Declaração Universal dos Direitos do Homem, segundo o qual "ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação".*

[2] ARAUJO, Luiz Alberto David. A correspondência eletrônica do empregado (e-mail) e o poder diretivo do empregador. *Revista de Direito Constitucional e Internacional*, v. 40, p. 96, 2002.

> *Este artigo remata dizendo que "toda a pessoa tem direito à protecção da lei contra as interferências ou ataques". Em termos similares, o art. 8.º, n. 1, da CEDH dispõe que "qualquer pessoa tem direito ao respeito pela sua vida privada e familiar, do seu domicílio e da sua correspondência", acrescentando no n. 2 que "não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros"*[3].

A proteção à vida privada surge da necessidade do homem de viver em sociedade e, ao mesmo tempo, resguardar-se da exposição de certos dados sensíveis a ele perante essa mesma sociedade.

O direito à intimidade é próprio do homem, é inato, nasce juntamente com ele, sendo consagrado pelo princípio da dignidade humana. Mas o que devemos entender como intimidade?

Primeiramente, cumpre salientar que não adentraremos na celeuma sobre intimidade e vida privada terem conceitos diferentes ou não, para efeito do presente trabalho ambas serão tratadas como sinônimos.

A dificuldade de conceituação se dá pelo fato de que a sociedade muda constantemente. Dependerá da cultura social, do espaço e do tempo em que se encontra o indivíduo.

Basta que se imagine os dados das pessoas que eram conhecidos pela sociedade em geral nos anos 1950 e o que hoje conhecemos sobre elas. O advento das redes sociais alterou a forma como lidamos com essas informações e o que sabemos das pessoas, senão de todas, de expressiva parcela delas.

Em geral, é o próprio indivíduo quem determina o que é de interesse público e o que será devidamente privado no que diz respeito a sua vida íntima e particular, não devendo ser ofendido este direito de escolha nem pelo Estado e nem por terceiros.

Essa lição fica especialmente clara quando se pensa que na era digital as próprias pessoas são responsáveis pelas exibições de suas vidas íntimas nas redes sociais, em geral.

A intimidade traz a ideia de que certas atitudes do indivíduo não devem ser de conhecimento público, isto é, a pessoa tem o direito de realizar escolhas e comportamentos sem que seja do conhecimento alheio, sendo protegidos pela esfera da privacidade.

Para José Afonso da Silva, a privacidade pode ser entendida como:

> *O conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, se mais isso poder ser legalmente sujeito. Embarca todas as manifestações das esferas íntimas, privadas e da personalidade, que o texto constitucional consagrou. A esfera de*

[3] GONÇALVES, Pedro Correia. O direito ao respeito pela vida privada e familiar dos doentes mentais à luz da jurisprudência do Tribunal Europeu de Direitos Humanos. *Revista Brasileira de Ciências Criminais*, v. 79, p. 303, 2009.

> *inviolabilidade, assim, é ampla, abrange modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo*[4].

No mesmo sentido, Jean Rivero:

> *A vida privada é a esfera de cada existência em que ninguém pode imiscuir-se sem ser convidado. A liberdade da vida privada é o reconhecimento, em proveito de cada qual, de uma zona de atividade que lhe é própria*[5].

Vale dizer, privado é aquilo que o indivíduo opta por não compartilhar, dentro de sua esfera de autonomia. No entanto, essas restrições de informações não possuem caráter absoluto justamente porque há informações que devem ser de conhecimento público.

Daí porque Jean Rivero nos ensina que deve haver delimitação dessa esfera, devendo haver espaço para que a sociedade conheça aqueles que a compõem, fator essencial para as relações sociais. Desse modo, o autor assim conceitua vida privada:

> *Tendo em conta essa relativização da delimitação, considera-se como normalmente dependente da vida privada tudo o que diz respeito à saúde pessoal, às convicções religiosas ou morais, à vida familiar e afetiva, às relações de amizade, aos lazeres, e, com as ressalvas já indicadas, à vida profissional e à situação material. É esse conjunto que o legislador e os juízes pretenderam preservar contra as invasões tanto dos terceiros como do poder*[6].

É o direito fundamental do indivíduo em obstar a invasão de terceiros e do Estado a sua vida privada e familiar. A proteção ao direito à intimidade preserva dois aspectos: a invasão e a divulgação da vida íntima e familiar. A agressão a qualquer um destes aspectos leva a indenização por danos materiais e ou morais, de acordo com o próprio texto constitucional.

Hannah Arendt também explica a importância da intimidade para o indivíduo, em sua obra *A condição humana*, ensinando:

> *A segunda saliente característica não privativa da privatividade é que as quatro paredes da propriedade privada de uma pessoa oferecem o único refúgio seguro contra o mundo público comum — não só contra tudo o que nele ocorre, mas também contra a sua própria publicidade, contra o fato de ser visto e ouvido. Uma existência vivida inteiramente em público, na presença de outros, torna-se, como se diz, superficial. Retém a sua visibilidade, mas perde a qualidade resultante de vir à luz a partir de um terreno mais sombrio que deve permanecer oculto a fim de não perder sua profundidade em um sentido muito real,*

[4] SILVA, José Afonso da. *Curso de Direito Constitucional positivo*. 19. ed. São Paulo: Malheiros, 2009, p. 206.

[5] RIVERO, Jean; MOUTOUH, Hugues. *Liberdades públicas*. São Paulo: Martins Fontes, 2006, p. 447.

[6] RIVERO, Jean; MOUTOUH, Hugues. *Liberdades públicas*. São Paulo: Martins Fontes, 2006, p. 447-448.

> *não subjetivo. O único modo eficaz de garantir a escuridão do que deve ser escondido da luz da publicidade é a propriedade privada, um lugar possuído privadamente para se esconder*[7].

Como dito acima, o direito à intimidade não é absoluto, podendo sofrer restrições. Porém, essa limitação não pode ser transformada em extinção do direito sob nenhuma hipótese, nem mesmo para beneficiar a coletividade.

Dworkin[8] sustenta que a função mais importante do sistema jurídico são os direitos individuais, estando à frente dos direitos sociais coletivos, e que os objetivos da sociedade só serão legítimos se não ofenderem os direitos individuais.

Não se pode esquecer que a intimidade e a privacidade ligam-se diretamente a uma categoria oposta, qual seja, à vigilância. A limitação da privacidade e da intimidade normalmente está ligada à ideia de vigilância por parte do Estado, como bem observa Anthony Giddens:

> *[…] a vigilância liga dois fenômenos afins: o cotejo de informação usada para coordenar atividades sociais de subordinados e a supervisão direta da conduta desses subordinados. Em cada um destes aspectos, o advento do Estado moderno, com sua infra-estrutura capitalista-industrial, distinguiu-se por uma vasta expansão da vigilância. Ora, por sua própria natureza, a "vigilância" envolve abertura, tornar visível. A acumulação de informação revela os padrões de atividade daqueles aos quais essa informação se refere, e a supervisão direta mantém abertamente tal atividade sob observação a fim de a controlar. A minimização ou manipulação de condições de abertura está, pois, de ordinário, nos interesses daqueles cujo comportamento está sujeito à vigilância – cuja extensão depende do grau de desinteresse ou nocividade que há no que esses indivíduos são chamados a fazer em tais cenários*[9].

Intimidade e privacidade de um lado e vigilância de outro são elementos indissociáveis para a compreensão da busca e apreensão em celulares. Para analisar de maneira mais ampla esses elementos, precisamos agregar ainda um outro, que é o conceito de domicílio. Vejamos no próximo tópico.

3. Domicílio em geral

Como extensão da privacidade e, consequentemente, da dignidade da pessoa humana, temos a inviolabilidade do domicílio, tutelado pela Constituição Federal em seu artigo 5º, XI, a título de direito individual.

[7] ARENDT, Hannah. *A condição humana*. 11. ed. Rio de Janeiro: Forense Universitária, 2013, p. 87.

[8] DWORKIN, Ronald. *Levando os direitos a sério*. São Paulo: Martins Fontes, 2002, p. XI-XVIII.

[9] GIDDENS, Anthony. *A constituição da sociedade*. 3. ed. São Paulo: Martins Fontes, 2009, p. 150.

Constitucionalmente, o caráter abrangente de casa, diferentemente do conceito do direito civil, é qualquer espaço em que o indivíduo exerça a sua intimidade, podendo ser temporário ou não, mas imprescindível que seja espaço privado e não aberto ao público[10].

Nesse sentido, temos o ensinamento de Manuel da Costa Andrade:

> *Por isso é que, de todos os lados, se reconhece que o domicílio ou a habitação de que aqui curamos se estende muito para além do conceito físico de casa e do conceito jurídico de residência ou de conceitos equivalentes ao "nível da esfera do leigo" ou do "sentido comum" e mediatizados pela linguagem corrente. Domicílio é, com efeito, todo o espaço fisicamente circunscrito e delimitado (fechado) onde, por mais ou menos tempo a(s) pessoa(s) se entrincheira(m) ou se refugiam para realizar a sua vida privada, imune(s) às perturbações, ruídos ou olhares indesejados do ambiente, resguardadas da indiscrição e devassa arbitrárias*[11].

A Constituição visou à proteção do domicílio sem vincular ao direito de propriedade; portanto, o morador tem a garantia da inviolabilidade de seu domicílio ainda que não seja seu proprietário, ou até mesmo em detrimento deste.

Trata-se de espaço privativo destinado a possibilitar intimidade e sossego do indivíduo, sabedor ele de que em seu domicílio não haverá indevidas ingerências do Estado.

Tem-se entendido ainda como casa o lugar habitado por qualquer pessoa que realize atividades profissionais com intenção de estabelecimento, que exclua terceiros. Com esta ideia, Jean Rivero afirma que domicílio é:

> *Não é somente "o lugar do principal estabelecimento de uma pessoa" que se beneficia de uma proteção fundamental, mas os diferentes locais de sua vida privada: residências secundárias, veículos, trailers ou barcos. E, graças à jurisprudência do Tribunal Europeu, cumpre igualmente incluir neles os locais profissionais*[12].

Da mesma forma, temos Kildare Gonçalves Carvalho analisando especificamente o caso brasileiro:

> *O termo "casa" empregado no texto constitucional compreende qualquer compartimento habitado, aposento habitado, ou compartimento não aberto ao público, onde alguém exerce profissão ou atividade (Código Penal, art. 150, § 4°). É a projeção espacial da pessoa; o espaço isolado do ambiente externo utilizado para o desenvolvimento das atividades da vida e do qual a pessoa pretenda normalmente excluir a presença de terceiros. Da noção de casa fazem parte as ideias de âmbito espacial, direito de exclusividade em relação a todos,*

[10] AMARAL, Cláudio do Prado. Inviolabilidade do domicílio e flagrante de crime permanente. *Revista Brasileira de Ciências Criminais*, v. 95, p. 165, 2012.

[11] ANDRADE, Manuel da Costa. Domicílio, intimidade e Constituição (anotação crítica do Acórdão 364/2006 do Tribunal Constitucional). *Revista Brasileira de Ciências Criminais*, v. 100, p. 55, 2013.

[12] RIVERO, Jean; MOUTOUH, Hugues. *Liberdades públicas*. São Paulo: Martins Fontes, 2006, p. 453.

> *direito à privacidade e à não-intromissão. De se considerar, portanto, que nos teatros, restaurantes, mercados e lojas, desde que cerrem suas portas e neles haja domicílio, haverá a inviolabilidade por destinação, circunstância que não ocorre enquanto aberto*[13].

A inviolabilidade do domicílio é a garantia dada ao indivíduo de que ninguém irá adentrar em sua casa sem que haja sua expressão permissão, salvo as exceções apresentadas na Constituição, quais sejam: a) caso de flagrante delito ou desastre; b) para prestar socorro; ou, c) durante o dia, por determinação judicial.

José Afonso da Silva esclarece que a Constituição, ao tutelar a casa como inviolável, está "reconhecendo que o homem tem direito fundamental a um lugar e que, só ou com sua família, gozará de uma esfera jurídica privada íntima, que terá que ser respeitada como sagrada manifestação da pessoa humana"[14].

A proteção constitucional também recai sobre o livre uso do domicílio, como assim nos ensina Jean Rivero:

> *O domicílio é o lugar onde as liberdades assumem sua dimensão máxima, trata-se das liberdades da pessoa física, da expressão do pensamento, do trabalho ou dos lazeres; consequência essencial desse princípio, os poderes de regulamentação das autoridades de polícia administrativa terminam normalmente no limiar do domicílio e não se estendem às atividades nele sediadas*[15].

Segundo o autor, este direito de uso se dá com a condição de que as atividades desenvolvidas permaneçam restritas ao interior do domicílio, bem como sejam respeitadas as regras de segurança e higiene da sociedade; do contrário, é possível a limitação deste direito.

4. A necessidade de mudança do conceito de casa

O conceito de casa como sendo o espaço físico onde se exerce a intimidade e a vida privada não é mais condizente com a realidade tecnológica que transforma a sociedade moderna.

Com o avanço tecnológico, um simples aparelho celular não se atém mais a exclusividade de fazer e receber ligações e ter uma agenda telefônica.

Os modernos aparelhos telefônicos são verdadeiros computadores portáteis, onde se pode acessar e-mail, redes sociais, tirar fotografias, além de armazenar uma infinita quantidade de informações íntimas e de cunho privado do proprietário.

De acordo com Helena Regina Lobo da Costa e Marcel Leonardi:

> *O conceito técnico de computador é o seguinte: "máquina capaz de receber, armazenar e enviar dados, e de efetuar, sobre estes, sequências previamente programadas de operações aritméticas*

[13] CARVALHO, Kildare Gonçalves. *Direito Constitucional*. 10. ed. Belo Horizonte: Del Rey, 2004, p. 386.

[14] SILVA, José Afonso da. *Curso de Direito Constitucional positivo*. 19. ed. São Paulo: Malheiros, 2009, p. 206.

[15] RIVERO, Jean; MOUTOUH, Hugues. *Liberdades públicas*. São Paulo: Martins Fontes, 2006, p. 454.

> *(como cálculos) e lógicas (como comparações), com o objetivo de resolver problemas". Entretanto, a palavra é muito utilizada para se referir, de modo coloquial, aos microcomputadores destinados ao usuário individual, de uso doméstico ou profissional, instalados em empresas ou casas, e foi empregada nessa acepção na ordem judicial de busca e apreensão*[16].

Deste modo, sendo o computador uma máquina capaz de receber, armazenar e enviar dados, temos que em nada difere das funções exercidas pelo aparelho telefônico dos dias atuais.

Diante das inúmeras funcionalidades do aparelho celular, ele passou a ser um local onde o indivíduo exerce a sua vida privada, podendo conter fotos íntimas do proprietário e de terceiros, conversas reveladoras de segredos, entre outras particularidades que dizem respeito tão somente ao seu dono, cabendo a ele o direito de tornar público ou não essas intimidades.

O cerne da questão está no fato de que o conceito atual de domicílio, embora amplo, restringe-se a um local físico, fechado e privativo. Quando analisamos o disposto no Código Penal, o domicílio é o local para onde o indivíduo vai; portanto, não serviria para a proteção da privacidade do celular, na medida em que o indivíduo leva o celular consigo.

Ocorre que o celular, embora não possa ser considerado um local físico, permite a realização de atividades pertinentes à intimidade e à vida privada do indivíduo, características próprias do domicílio.

De acordo com Manuel da Costa Andrade:

> *O que não deve, em qualquer caso levar-se à conta de contestação ou de negação da relação privilegiada que medeia entre o domicílio e a privacidade/intimidade: o domicílio é o espaço normal da intimidade. Dito de novo com o Tribunal Constitucional Federal, o "desenvolvimento da personalidade na área nuclear da intimidade pressupõe a possibilidade de expressar livremente sentimentos e emoções bem como reflexões, opiniões e vivências de cariz eminentemente pessoal sem medo de ser vigiado por instâncias estaduais. A tutela abrange também a expressão das sensações e da experiência inconsciente bem como as manifestações da sexualidade. A possibilidade de um tal desenvolvimento pressupõe que o indivíduo disponha de um espaço adequado para o efeito […] a habitação é, como último refúgio (lestztes Refugium), um meio para garantia da dignidade humana"*[17].

No mesmo sentido, temos Cláudio do Prado Amaral:

> *Conforme Sérgio Iglesias: "A moradia, conceitualmente, é um bem da personalidade, com proteção constitucional e civil. É, portanto, um bem irrenunciável da pessoa natural, indissociável da sua vontade*

[16] COSTA, Helena Regina Lobo da; LEONARDI, Marcel. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais*, v. 88, p. 203, 2011.

[17] ANDRADE, Manuel da Costa. Domicílio, intimidade e Constituição (anotação crítica do Acórdão 364/2006 do Tribunal Constitucional). *Revista Brasileira de Ciências Criminais*, v. 100, p. 55, 2013.

> *e indisponível, exercendo-se de forma definitiva pelo indivíduo; secundariamente, recai o seu exercício em qualquer pouso ou local, mas é objeto de direito e protegido juridicamente. O bem da 'moradia' é inerente à pessoa e independe de objeto físico para a sua existência e proteção jurídica. Existe independentemente de lei, porque também tem substrato no direito natural. Atualmente, é uma situação de direito reconhecida pelo ordenamento jurídico, é uma qualificação legal reconhecida como direito inerente a todo o ser humano, notadamente, em face da natureza de direito essencial referente à personalidade humana"*[18].

Desse modo, se o domicílio pode ser entendido como o espaço normal da intimidade, onde ela se expressa livremente, sendo inerente à pessoa, e, o mais importante, independe de objeto físico para a sua existência, não vislumbramos óbice para que o aparelho celular não possa vir a ser considerado um domicílio e receber a tutela constitucional fundamental da inviolabilidade domiciliar.

Por vezes, o aparelho celular contém mais dados e informações íntimas sobre a nossa vida privada do que nossa própria residência, não sendo pertinente não ser abrangido como domicílio somente, e tão somente, por não ser dotado de espaço físico, tendo, portanto, todas as demais características para ser protegido como tal.

Assim como o conceito de privacidade e intimidade se altera de acordo com o tempo, o espaço e a sociedade, o conceito de domicílio também deve evoluir conforme os avanços sociais e principalmente tecnológicos, para que sua proteção seja a mais absoluta possível, de forma que toda pessoa tenha direito a que se respeite sua integridade física, psíquica e moral para o exercício do direito adequado de domicílio[19], consagrando o direito da dignidade humana, essencial ao Estado Democrático de Direito.

Por fim, entendemos que o avanço tecnológico nos permitiu que levássemos o domicílio conosco, isto é, ao utilizarmos o aparelho telefônico ou similar para exercer o direito à nossa intimidade, estamos carregando conosco o espaço destinado a este exercício.

A Constituição Federal não define o que seja domicílio no artigo 5, inciso XI. Esta definição é dada pela doutrina, que sempre se valeu do disposto no artigo 150 do Código Penal.

Para que se possa entender os motivos pelos quais o conceito de domicílio deve ser atualizado, é preciso que se compreenda, ontologicamente, porque merece o domicílio proteção tão especial por parte do legislador.

Inicialmente, a proteção ao domicílio estava diretamente ligada à ideia de proteção da propriedade. Vale dizer, protegia-se o domicílio porque ele representava o direito à propriedade do nobre.

[18] AMARAL, Cláudio do Prado. Inviolabilidade do domicílio e flagrante de crime permanente. *Revista Brasileira de Ciências Criminais*, v. 95, p. 165, 2012.

[19] AMARAL, Cláudio do Prado. Inviolabilidade do domicílio e flagrante de crime permanente. *Revista Brasileira de Ciências Criminais*, v. 95, p. 165, 2012.

Posteriormente, a ideia de propriedade sai do âmbito principal de necessidade de proteção do domicílio, sendo desenvolvido outro critério, qual seja, a necessidade de proteção da intimidade e da vida privada, dissociada das práticas públicas[20].

Esta mentalidade, formada em especial com o advento da Renascença, iria permear o imaginário humano nos séculos vindouros, de forma que o domicílio passou a ser considerado o local sagrado por excelência da proteção do indivíduo.

No entanto, como já dito, a pós-modernidade acaba por trazer uma nova nota a este imaginário: se antes o domicílio era visto como um local físico, um local para onde nos dirigíamos a fim de lá guardarmos nossos segredos, hoje este local é levado com cada um de nós.

Uma das características mais interessantes da pós-modernidade e da tecnologia ligada à computação em nuvem reside justamente na espiritualização de determinados bens, ou seja, na desmaterialização de determinadas coisas que antes somente podiam ser acessadas em um local físico.

No século passado, e até pouco tempo atrás, os arquivos eram todos guardados em enormes armários com fichas catalogadoras do local em que se encontrava cada um dos documentos. Para ter acesso a tais fichas e a tais documentos, era necessário ir até o local físico onde se encontravam.

Hoje isso não é mais necessário. Qualquer pessoa com um smartphone com acesso à internet pode acessar o local em que se encontram armazenados esses dados e ter acesso a eles onde quer que se encontre.

Um dos grandes teóricos da internet, o sociólogo Manuel Castells, nos ensina que ela não é apenas uma tecnologia. Na verdade, a internet representa meio de comunicação e a própria infraestrutura da organização da rede[21].

A internet afetou de maneira profunda a própria noção de soberania, na medida em que os Estados foram obrigados a repensar sobre o efetivo controle que detém sobre a informação existente na internet e sobre os espaços a serem ocupados.

---

[20] Nesse sentido, esclarecem Yves Castan, François Lebrum e Roger Chartier: "[…] os limites móveis da esfera do privado – quer abranja a quase totalidade da visa social, quer, ao contrário, se restrinja ao foro íntimo, doméstico e familiar – dependem antes de tudo da maneira como se constitui, em doutrina e em poder, a autoridade pública e, em primeira instância, aquela reivindicada e exercida pelo Estado. É, pois, a progressiva construção do Estado moderno – nem sempre absolutista, mas em toda parte administrativo e burocrático – que se revela condição necessária para se poder definir; pensar como tal ou apenas vivenciar de fato um privado doravante distinto de um público claramente identificável. Esse elo essencial entre a afirmação do Estado e o processo de privatização permite várias interpretações. A que Norbert Elias propõe num livro hoje clássico articula estreitamente a criação do Estado absolutista, cuja forma acabada está na monarquia de Luís XIV, e o conjunto das transformações afetivas e psíquicas que levam a conter na intimidade atos que antes eram públicos. Como visa a pacificação do estado social, portanto à censura da violência selvagem; como intensifica e regulamenta as dependências que unem entre si as existências individuais; como produz uma formação social nova, a corte – diferenciada por um código de comportamentos tanto mais obrigatório quanto é progressivamente imitado pelas outras camadas sociais –, o Estado do tipo novo, desenvolvido na Europa entre o final da Idade Média e o século XVII, institui um modo inédito de ser em sociedade, caracterizado pelo controle mais severo das pulsões, pelo domínio das emoções, pelo senso mais elevado de pudor. Tais mudanças, que criam um novo *habitus*, primeiro restrito ao homem da corte e depois difundido por toda a sociedade, determinam a esfera do privado" (CHARTIER; Roger (org.). *História da vida privada*: da Renascença ao século das luzes. São Paulo: Companhia das Letras, 2009, p. 28-29).

[21] CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003, p. 116: "Sabemos, a partir dos capítulos precedentes, que a internet não é simplesmente uma tecnologia: é um meio de comunicação (como eram os pubs), e é a infra-estrutura material de uma determinada forma organizacional: a rede (como era a fábrica)".

A geografia, agora, adquire nova versão, na medida em que a atuação do indivíduo não é mais limitada ao espaço físico do Estado; atua o indivíduo com a geografia do próprio globo. Seu limite é o espaço mundial[22].

O domicílio, insistimos nesta ideia, é levado com o indivíduo e não mais se resume a um local físico para onde nos dirigimos. O domicílio hoje é levado com o indivíduo graças a essa característica da internet[23].

Evidentemente que não interessa ao Estado esta visão de ciberespaço em que há restrição ao controle exercido por ele sobre o indivíduo. Neste sentido, afirma Pierre Lévy que:

> *Os Estados ainda tem outros pontos de vista, mais ou menos vastos e compreensivos, sobre a emergência do ciberespaço. A abordagem mais limitada coloca os problemas em termos de soberania e de territorialidade. De fato, o ciberespaço é desterritorializante por natureza, enquanto o Estado Moderno baseia-se, sobretudo, na noção de território*[24].

Cumpre ressaltar que a intimidade e o domicílio estão intrinsecamente ligados e ambos estão em conexão com o princípio da dignidade da pessoa humana, sendo escolhido como princípio fundamental e, portanto, como condutor de valoração para o intérprete dos demais direitos fundamentais.

Assim sendo, quando falamos em intimidade devemos ter em mente que se trata da esfera privativa do indivíduo, de informações e fatos que se quer manter em sigilo, obstando o acesso a terceiros.

O direito à proteção da intimidade atinge não somente terceiros, mas também o Estado, e, portanto, este deverá ter ordem judicial para restringir este direito.

A ofensa a este preceito fundamental pode ser caracterizada tanto pelo acesso às informações que se quer manter só para si, como pela divulgação destas informações. E esta agressão é passível de indenização moral.

Dada esta particularidade da vida atual, em que carregamos nossos segredos conosco, é fundamental que o conceito de domicílio seja reformulado, passando a abarcar também os meios eletrônicos como aparelhos celulares e tablets, pois com o progresso tecnológico, estes aparelhos contêm inúmeras informações de fórum íntimo, nos permitindo exercer

---

[22] Novamente Castells nos ensina que "a Era da Internet foi aclamada como o fim da geografia. De fato, a Internet tem uma geografia própria, uma geografia feita de redes e nós que processam fluxos de informação gerados e administrados a partir de lugares. Como a unidade é a rede, a arquitetura e a dinâmica de múltiplas redes são as fontes de significado e função para cada lugar. O espaço de fluxos resultante é uma nova forma de espaço, característico da Era da Informação, mas não é desprovida de lugar: conecta lugares por redes de computadores telecomunicadas e sistemas de transporte computadorizados. Redefine distâncias mas não cancela a geografia. Novas configurações territoriais emergem de processos simultâneos de concentração, descentralização e conexão espaciais, incessantemente elaborados pela geometria variável dos fluxos de informação global" (CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003, p. 170).

[23] Manuel Castells identifica, nesse sentido, inclusive a grande mudança de poder havida na sociedade na era da internet, afirmando que "[…] the terrain where power relationships operate has changed in two major ways: it is primarily constructed around the articulation between the global and the local; and it is primarily organized around networks, not single units. Because networks are multiple, power relationships are specific to each network" (CASTELLS, Manuel. *Comunication power*. Nova York: Oxford University Press, 2009, p. 50).

[24] LÉVY, Pierre. *Cibercultura*. São Paulo: Ed. 34, 1999, p. 210.

atos da vida privada não mais somente em ambientes físicos fechados e privativos, mas sim em qualquer lugar, e nem por isso não devem ser tutelados constitucionalmente.

Como bem salientaram Helena Regina Lobo da Costa e Marcel Leonardi:

> *Diante de todo o exposto, se percebe mais uma vez como a tecnologia, de forma contínua, apresenta desafios aos aplicadores do direito, exigindo soluções e adaptações às novas conformações da realidade. O que não se pode admitir, em tais hipóteses, é o abandono ou a flexibilização de garantias constitucionais do processo penal, que concretizam a aplicação de direitos fundamentais, para a obtenção de prova a qualquer custo.*

Deste modo, é imprescindível um novo olhar sobre a tutela constitucional do domicílio, principalmente em face conceitual, para que este esteja coadunado com a sociedade atual. Para que esta análise seja completa, é preciso compreender que o artigo 6 da Lei 12.965/2014 positiva este entendimento.

A Lei 12.965 (Marco Civil), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, em seu artigo 6[25], estabelece que para a interpretação desta lei será levado em conta os usos e costumes particulares, bem como a natureza da internet.

E qual a importância deste referido artigo para o novo conceito de domicílio, anteriormente explanado?

Ora, dentro do contexto de uma nova conceituação de domicílio, entendemos que o domicílio é o local, físico ou não, onde se exerce o direito à vida íntima e privada. E, ao regulamentar que a interpretação da lei se dará conforme os usos e costumes da internet, o legislador permitiu que se estendesse a proteção domiciliar à internet, pois usualmente a utilizamos como local de exercício de nossa vida íntima e privada, que nada mais é do que o conceito clássico do domicílio.

Deste modo, entendemos que estamos diante de mais um fundamento (agora legal) de que é necessário analisarmos o conceito de domicílio de acordo com os avanços tecnológicos.

E, portanto, podendo ser entendido o uso costumeiro da internet como domicílio (não importando se este uso se dará por meio de computadores ou celulares), este deverá receber as mesmas proteções constitucionais dadas ao domicílio, ou seja, a sua invasão só pode ocorrer nos casos elencados na Constituição Federal.

Seguramente, trata-se de um dos mais importantes artigos de toda a Lei do Marco Civil e sua aplicação não deve ficar restrita à aplicação da própria lei. Toda e qualquer interpretação, seja no âmbito civil, criminal ou administrativo, deve ter por norte interpretativo o artigo 6 quando envolver relações baseadas na internet. Este artigo 6 representa, em verdade, verdadeira cláusula interpretativa para as relações quando nelas houver a intermediação da internet.

[25] Art. 6º. Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

O STJ tem o entendimento consolidado de que a busca e apreensão em aparelhos celulares demanda autorização judicial, ainda que se trate de flagrante. O STF está para decidir este tema.

De nossa parte, entendemos que a aproximação do celular ao regime do domicílio traz como consequência que nas mesmas hipóteses em que se pode adentrar no domicílio também se poderá pesquisar o conteúdo do celular.

Assim, diversamente do STJ, entendemos que poderá ser olhado o conteúdo do celular nas hipóteses em que haja prisão em flagrante da pessoa ou mesmo com sua concordância.

Caso contrário, ou seja, caso mantida a posição do STJ, poderemos estar diante de uma contradição: a CF autoriza que se entre na residência do indivíduo no caso de flagrante, que se faça busca por toda a residência e em todos os cômodos mas não autoriza que se faça busca no celular eventualmente encontrado dentro da residência do indivíduo.

As interpretações não podem conduzir a inconsistências como a acima, com a devida vênia das posições em contrário. Não parece que a CF tenha querido atribuir maior proteção a smartphones do que ao domicílio. Para se evitar tamanha discrepância devemos trabalhar com a ideia de que os smartphones estão submetidos ao regime do inciso XI do artigo 5 e não o do inciso X.

Conclusão

O conceito de domicílio liga-se à proteção da privacidade, embora não seja única manifestação dela. A conceituação de domicílio prevista no artigo 150, parágrafo 4, do Código Penal, não é mais suficiente para abarcar aspectos da vida moderna ligados à tecnologia.

É preciso que se reveja o conceito de domicílio para abarcar também os aparelhos eletrônicos, na medida em que levamos conosco aquilo que antes somente ficaria dentro do próprio domicílio.

No entanto, para que haja o correto equilíbrio entre a eficiência e a proteção dos direitos fundamentais, devemos tomar cuidado com a resposta ao problema para que não haja superproteção do celular sobre o domicílio.

Os aparelhos celulares são verdadeiros computadores portáteis, que armazenam dados e informações que devem ser tutelados pelos princípios constitucionais da proteção à intimidade e também da proteção ao domicílio.

Assim, entendemos que é possível acessar o celular do indivíduo nas mesmas hipóteses em que se pode entrar no domicílio. Dessa forma, caso esteja em flagrante, não haverá necessidade de autorização judicial como preconiza o STJ. Com isso, entendemos que se dará maior equilíbrio entre a eficiência e o garantismo.

Bibliografia

AMARAL, Cláudio do Prado. Inviolabilidade do domicílio e flagrante de crime permanente. *Revista Brasileira de Ciências Criminais*, v. 95, p. 165, 2012.

ANDRADE, Manuel da Costa. Domicílio, intimidade e Constituição (anotação crítica do Acórdão 364/2006 do Tribunal Constitucional). *Revista Brasileira de Ciências Criminais*, v. 21, n. 100, p. 55, 2013.

ARAUJO, Luiz Alberto David. A correspondência eletrônica do empregado (e-mail) e o poder diretivo do empregador. *Revista de Direito Constitucional e Internacional*, v. 410, n. 40, p. 96-121, 2002.

ARENDT, Hannah. *A condição humana*. 11. ed. Rio de Janeiro: Forense Universitária, 2013.

BAUMAN, Zygmunt. *Globalização*: as consequências humanas. Rio de Janeiro: Zahar, 1999.

CARVALHO, Kildare Gonçalves. *Direito Constitucional*. 10. ed. Belo Horizonte: Del Rey, 2004.

CASTELLS, Manuel. *A galáxia da internet*: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. *Communication power*. Nova York: Oxford University Press, 2009.

CASTELLS, Manuel. *Redes de indignação e esperança*: movimentos sociais na era da internet. Rio de Janeiro: Zahar, 2013.

CHARTIER; Roger (org.). *História da vida privada*: da Renascença ao século das luzes. São Paulo: Companhia das Letras, 2009. v. 3.

COSTA, Helena Regina Lobo da; LEONARDI, Marcel. Busca e apreensão e acesso remoto a dados em servidores. *Revista Brasileira de Ciências Criminais*, v. 19, n. 88, 2011.

DWORKIN, Ronald. *Levando os direitos a sério*. São Paulo: Martins Fontes, 2002.

FALLON JUNIOR, Richard H. Judicially manageable standards and constitutional meaning. *Harvard Law Review*, v. 119, n. 5, p. 1331-1332, 2006.

GIDDENS, Anthony. *A constituição da sociedade*. 3. ed. São Paulo: Martins Fontes, 2009.

GIDDENS, Anthony. *The consequences of modernity*. California: Stanford University Press, 2012.

GONÇALVES, Pedro Correia. O direito ao respeito pela vida privada e familiar dos doentes mentais à luz da jurisprudência do Tribunal Europeu de Direitos Humanos. *Revista Brasileira de Ciências Criminais*, n. 79, p. 303-322, 2009.

LÉVY, Pierre. *Cibercultura*. São Paulo: Ed. 34, 1999.

LIPOVETSKY, Gilles. *Os tempos hipermodernos*. São Paulo: Barcarolla, 2004.

LIPOVETSKY, Gilles; SERROY, Jean. *A cultura mundo*: resposta a uma sociedade desorientada. São Paulo: Companhia das Letras, 2011.

MARCONDES FILHO, Ciro. *Superciber*: a civilização místico-tecnológica do século 21. São Paulo: Paulus, 2009.

RIVERO, Jean; MOUTOUH, Hugues. *Liberdades públicas*. São Paulo: Martins Fontes, 2006.

SILVA, José Afonso da. *Curso de Direito Constitucional positivo*. 19. ed. São Paulo: Malheiros, 2009.

ZAGREBELSKY, Gustavo; MARTINI, Carlo Maria. *La exigencia de justicia*. Madrid: Miguel Carbonell, 2006.

Direito digital e legitimação passiva nas ações de remoção de conteúdo e responsabilidade civil

Fernando da Fonseca Gajardoni[1]
Juiz de Direito no Estado de São Paulo

Ricardo Maffeis Martins[2]
Advogado

Sumário: Introdução; 1. As mudanças advindas do Marco Civil da Internet; 2. A preocupação legal com o sigilo de dados; 3. Legitimação passiva nas ações de remoção de conteúdo e responsabilidade civil; Conclusões; Referências bibliográficas.

Resumo: À luz da legislação brasileira de proteção dos dados dos usuários (Marco Civil da Internet – Lei n. 12.065/2014) (Lei Geral de Proteção de Dados – Lei n. 13.709/2018), o ensaio investiga a legitimidade passiva nas ações de remoção de conteúdo e responsabilidade civil derivadas de atos ilícitos praticados pela internet.

Palavras-chave: Legitimação Passiva. Remoção de Conteúdo. Responsabilidade Civil. Direito Digital. Marco Civil da Internet. Lei Geral de Proteção de Dados.

Introdução

Sempre se considerou que, tanto quanto o remédio que é escolhido à luz da doença (e não contrário), é o processo civil que tem que se adequar às vicissitudes do direito material, competindo ao juiz, caso o legislador não tenha sido capaz de adequar o procedimento processual ao caso concreto, fazer a competente adaptação[3].

Na moderna concepção do processo civil, não prevalece mais o antigo entendimento de que os litigantes se encontram em lados opostos do processo ao passo que o juiz – equidistante – assumiria uma postura estanque e mal poderia ter contato com as partes, evitando influir senão quando chamado e expressamente autorizado, sob o risco de colocar em dúvida sua imparcialidade.

Assim, no caminho que vai entre o "demandar-contestar-conhecer-julgar", que Dinamarco define como a "estrutura funcional do processo de conhecimento"[4],

[1] Doutor e Mestre em Direito Processual pela USP (FD-USP). Professor Doutor de Direito Processual Civil e Arbitragem da USP (FDRP-USP) e do G7 Jurídico.

[2] Professor de Direito Processual Civil da Escola Paulista de Direito (EPD) Membro da Comissão de Direito Digital do Instituto dos Advogados de São Paulo (IASP). Ex-assessor de Ministros do Superior Tribunal de Justiça.

[3] Neste sentido, vide as considerações de Fernando da Fonseca Gajardoni. *Flexibilização do procedimento*: um novo enfoque para estudo do procedimento em matéria processual. São Paulo: Atlas, 2007.

[4] DINAMARCO, Cândido Rangel. *Instituições de direito processual civil*. 5. ed. São Paulo: Malheiros, 2005, v. 3, p. 31.

não é vedado que o juiz possa impor determinados provimentos de ofício em um pleito já instaurado, desde que observada a regra que proíbe a tomada das chamadas decisões-surpresa, previstas expressamente no art. 10 do novo Código de Processo Civil (CPC/2015).

Aliás, como lembra Yarshell, a doutrina brasileira admite que o poder de instrução oficial do processo possa até mesmo ser exercido diante de uma prova não solicitada pelos litigantes sem que isso venha a afastar ou mitigar a imparcialidade do julgador, na medida em que ele não sabe a quem favorecerá a prova[5].

Desta forma, a afirmação supra, de que compete ao juiz adaptar o procedimento ao caso concreto, sempre que a legislação processual não tiver condições de resolver as inevitáveis lacunas, se torna ainda mais contundente nos processos relacionados ao direito digital, especialmente quando há ato ilícito praticado pela internet por pessoa incerta; escondida atrás do anonimato constitucionalmente vedado (art. 5º, IV, da Constituição Federal – CF).

Explicamos.

O Marco Civil da Internet (Lei nº 12.965/2014 – MCI), em seus artigos 19, 22 e 23, garante aos ofendidos o direito de obter judicialmente os registros de aplicações e de conexão para fins de fazer prova em processos civis e criminais, inclusive autorizando a propositura da ação perante os Juizados Especiais Cíveis, conforme preceitua o § 3º do art. 19.

Contudo, não indica qual a via processual adequada para a postulação.

Nesse sentido, a recém-aprovada Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD, com os acréscimos trazidos pela Medida Provisória nº 869/2018), editada com nítida inspiração na sua equivalente europeia, o Regulamento Geral de Proteção de Dados[6] (*GDPR*, em sua sigla em inglês), tampouco soluciona o problema, na medida em que seu capítulo sobre a responsabilidade civil e o ressarcimento dos danos[7] disciplina os responsáveis por eventual indenização, a inversão do ônus da prova, ações coletivas e até mesmo ações de regresso, mas, tal qual o Marco Civil da Internet, não especifica as ações a serem movidas para se obter a reparação.

Em outros termos, nos casos de ilegalidade praticada por pessoa encoberta pelo signo da proteção de seus dados pessoais (uma das garantais do acesso à internet, como prevê o art. 7º, I, da Lei nº 12.965/2014, complementado pelos arts. 46 a 49 da Lei nº 13.709/2018), as providências judiciais para derrubada do conteúdo ilegal e obtenção dos dados do(s) ofensor(es) não é tarefa das mais fáceis.

Acrescente-se a necessidade de tomada de providências urgentes, em regra antes mesmo da citação dos réus, para a retirada de conteúdo da internet. Muitas vezes o material ilícito se torna *viral*, atingindo rapidamente um número enorme – às vezes até mesmo gigantesco – de pessoas e, a cada dia ou a cada hora que passa, a lesão à honra do ofendido aumenta de forma exponencial. Especialmente no atual estágio das redes sociais (Facebook, Instagram e Twitter à frente) e dos aplicativos de comunicação (cujo maior exemplo, pelo número de usuários em nosso país, é o WhatsApp), em que há verdadeiro estímulo para o compartilhamento imediato do que se recebe.

---

[5] YARSHELL, Flávio Luiz. *Curso de direito processual civil*. São Paulo: Marcial Pons, 2014, v. 1, p. 99.

[6] O *GDPR* (Regulamento UE 2016/679 do Parlamento Europeu e do Conselho) foi aprovado em abril de 2016 e entrou em vigor na União Europeia em maio de 2018. Sua íntegra, em português, pode ser conferida em: http://bit.ly/2RrnAX0. Acesso em: 20 fev. 2019.

[7] Artigos 42 a 45 da LGPD.

Válido aqui abrir um parêntese para comentar o entendimento que prevalecia no Superior Tribunal de Justiça (STJ) antes do advento do Marco Civil da Internet. Firmou-se, graças sobretudo a precedentes relatados pela Ministra Nancy Andrighi, a regra de que, caso o ofendido denunciasse (extrajudicialmente) ao provedor de aplicações a existência de conteúdo ofensivo, o provedor teria o prazo de 24 horas para removê-lo, sob pena de, ultrapassado tal interregno, ser solidariamente responsável, juntamente com o ofensor[8].

Tome-se por exemplo o Recurso Especial nº 1.338.214/MT, da Terceira Turma, relatora a Ministra Nancy Andrighi, onde se decidiu que, embora a fiscalização prévia do conteúdo postado pelos usuários não seja uma atividade intrínseca ao serviço prestado, ao ser cientificado do conteúdo ilícito o provedor teria 24 horas para "remover preventivamente" o material, fazer uma análise da alegada ilicitude e, confirmada, excluir definitivamente, para não responder de modo solidário.

Convencionou-se que este seria um prazo razoável para que os provedores tomassem as providências necessárias e removessem o conteúdo que considerassem ilegais. Todavia, como dito, embora nas situações corriqueiras a regra poderia ser eficaz, nos casos em que o conteúdo se torna viral, mesmo este prazo de 24 horas pode ser considerado longo demais, de modo que a ofensa se multiplique e atinja um número incalculável e inimaginável de pessoas.

Assim, à exceção dos casos de *revenge porn*, ou pornografia de vingança – onde a exclusão do conteúdo pode ser requerida extrajudicialmente diretamente ao provedor de aplicações (art. 21 da Lei nº 12.965/2014) –, o prejudicado deve sempre ajuizar ação judicial[9] para: a) exclusão do conteúdo tido por ilícito; b) obtenção dos dados de IP[10] do servidor de aplicações (Google, Facebook, UOL, para citar apenas os mais conhecidos no dia a dia do Judiciário); c) a partir do endereço IP fornecido no tópico acima, obtenção dos dados cadastrais, registrados em um servidor de conexão (Vivo, Claro, Oi, Net etc.); d) para só então (em sendo possível), chegar ao titular da conexão de onde foi praticada a ilegalidade, que eventualmente será acionado civil ou criminalmente por conta do ilícito praticado.

Esta – que para muitos pode ser considerada uma verdadeira *via crucis* processual[11] – tem sua razão de ser sobretudo a partir da edição do Marco Civil da Internet (MCI).

[8] Sobre o tratamento conferido pela jurisprudência à questão da responsabilidade civil dos provedores, pré e pós Marco Civil, vide GODOY, Claudio Luiz Bueno de. Uma análise da responsabilidade civil dos provedores na lei nº 12.965/14 (Marco Civil da Internet). *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*: Marco Civil da Internet (Lei n. 12.964/2014). São Paulo: Quartier Latin, 2015, t. 2, p. 307.

[9] Não se esqueça que o entendimento citado acima prevalecia previamente ao MCI, não sendo mais aplicável por expressa disposição legal.

[10] IP é a sigla para *Internet Protocol*. De acordo com o site de tecnologia TechTudo, trata-se de uma identificação única para cada computador conectado a uma rede. Podemos imaginá-lo como uma espécie de documento de identificação único. Conhecer o endereço IP de um usuário pode ser muito útil, por exemplo, para descobrir se o computador está conectado diretamente à internet ou se há alguma outra máquina fazendo o intermédio. A informação pode até mesmo ser usada para confirmar algum tipo de atividade ligada a um *Internet Protocol*, como em casos de fraudes. Disponível em: https://glo.bo/362jVEo. Acesso em: 20 fev. 2019.

[11] Os civilistas, em especial, são os maiores críticos deste longo caminho que, para eles, dificulta muito (quando não verdadeiramente priva) os ofendidos de conseguirem a reparação pelos danos sofridos.

Isso porque, nos anos que antecederam a edição do MCI, uma prática muito comum era o ajuizamento de ações com pedidos de remoção de conteúdo considerado ilícito, cumuladas com pedidos indenizatórios, apenas contra os provedores de aplicações.

Na prática, os ofendidos direcionavam as suas pretensões todas aos servidores, sob alegação de falha no serviço, por não terem monitorado e impedido que a publicação tida por ofensiva ocorresse. Além disso, era um modo mais eficaz de conseguir a indenização pecuniária, uma vez que os provedores costumam ser grandes empresas. Não era raro nem mesmo observar que, satisfeito com a remoção e a indenização recebida, o ofendido sequer se preocupasse em descobrir a pessoa responsável pela propagação da ilicitude.

1. As mudanças advindas do Marco Civil da Internet

Não há procedimento expressamente previsto na lei processual vigente (Código de Processo Civil – CPC/2015), ou mesmo nas mais importantes legislações sobre direito digital (Marco Civil da Internet e Lei de Proteção de Dados), que aparentemente suporte tantas providências distintas contra tantos responsáveis diferentes (provedor de aplicações, provedor de conexão, ofensor), o que torna um verdadeiro desafio para os processualistas e tribunais[12] indicar quais seriam as vias adequadas – ou a mais adequada – para a obtenção da tutela necessária nestes casos de direito digital.

A Lei nº 12.965/2014 trouxe uma significativa mudança na responsabilidade pelo conteúdo criado por terceiros, que logo – como não poderia deixar de ser – foi adotada pela jurisprudência pátria, embora não ficasse imune a críticas, nem a projetos de lei tendentes a alterá-la[13].

Dispõe o artigo 19 do MCI que, para "assegurar a liberdade de expressão e impedir a censura", o provedor de aplicações "somente será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para [...] tornar indisponível o conteúdo apontado como infringente".

A disciplina legal trazida pelo Marco Civil foi muito comemorada pelos defensores da liberdade de expressão e também pelos provedores de aplicações. Para estas empresas, a regra até então aplicada gerava forte insegurança jurídica, na medida em que o provedor era responsável por suspender o conteúdo preventivamente e fazer uma análise própria, privada, sobre a ilicitude ou não do material, removendo-o permanentemente em caso positivo ou o recolocando no ar, caso a ofensa não justificasse a remoção.

Sempre se alegou que, excluídas as hipóteses evidentes, não competiria a uma empresa privada decidir a respeito da ilicitude ou não do conteúdo, tarefa afeita ao Poder Judiciário, a quem compete, efetivamente, julgar.

[12] Para uma ampla análise da jurisprudência do Superior Tribunal de Justiça (STJ) a respeito de temas processuais ligados ao direito digital, conferir: MARTINS, Ricardo Maffeis, *As decisões do Superior Tribunal de Justiça sobre Direito Digital*. No prelo.

[13] Uma das tentativas mais bizarras foi a ideia de um projeto de lei do deputado Cláudio Cajado (DEM/BA) que visava acelerar a identificação e punição de pessoas que criassem páginas ofensivas a políticos. A proposta ainda responsabilizava, inclusive criminalmente, os provedores, redes sociais ou portais que hospedassem tais *sites*, tornando desnecessária a busca da via judicial. Datada de setembro de 2015, pela nossa consulta no *site* da Câmara dos Deputados, a proposta sequer foi formalizada como projeto de lei após grande polêmica de que seria uma tentativa de censura a críticas feitas a políticos.

Com a nova regra, criou-se um *safe harbor* para os provedores de aplicações, ou seja, uma proteção para que eles não sejam mais civilmente responsáveis por danos praticados por terceiros, até que sejam judicialmente chamados a remover o conteúdo.

E não só isso, pois a lei se preocupou em exigir uma "ordem judicial específica […] no âmbito e nos limites técnicos do seu serviço" e ainda com "identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material", tudo sob pena de nulidade da ordem judicial[14].

Com isso, restaram definitivamente afastadas as ordens genéricas, outrora tão comuns, do tipo *remover da internet o conteúdo ofensivo* ou *deletar todas as postagens ofensivas ao autor*. Eventual ordem nesse sentido que ainda seja proferida acaba, inevitavelmente, sendo reformada pelas instâncias superiores.

Enquanto, de um lado, a nova disciplina trouxe segurança jurídica aos provedores e, de fato, contribuiu com a defesa e proteção da liberdade de expressão[15], é inegável que tornou mais difícil a responsabilização civil dos ofensores.

Se antes o trabalho consistia, basicamente, em notificar extrajudicialmente o provedor para que o conteúdo fosse removido (ao menos temporariamente), os ofendidos passaram a ter que contratar um advogado[16] e ajuizar uma ação para conseguir tal intento.

Mais do que isso, tornou-se necessário que o pedido de tutela de urgência seja formulado de forma técnica e deferido — em ordem judicial específica e nos limites técnicos de cada serviço — para que o pleito de remoção seja efetivamente cumprido pelo provedor.

E, como visto, nem as leis específicas (Marco Civil e Lei de Proteção de Dados), nem o Código de Processo Civil, regulamentam especificamente os modos à disposição do autor para atingir seu objetivo.

2. A preocupação com o sigilo de dados

Dois pontos de especial relevo merecem ser discutidos nos casos aqui tratados, em que o réu não pode ser identificado desde o início da lide, por estar protegido pelo anonimato.

O primeiro, é a promulgação da Lei Geral de Proteção de Dados, em agosto de 2018, e o segundo é a tormentosa questão sobre o fornecimento ou não dos dados do suposto ofensor no início da lide, ainda em sede de cognição sumária (momento processual em que raras vezes é possível saber se a ofensa narrada pelo autor constitui ou não um ilícito).

Comecemos pelo primeiro tópico.

[14] Segundo o parágrafo único do artigo 19 do MCI.

[15] Especialmente quando se considera que, se o antigo entendimento da jurisprudência prevalecesse, a regra fatalmente seria a remoção em massa de conteúdo, pois poucos provedores teriam incentivo a manter no ar algo produzido por terceiro.

[16] Salvo nos casos de ingresso nos Juizados Especiais Cíveis, com todas as limitações que o sistema possui, seja quanto ao valor da causa, à impossibilidade de denunciação da lide ou de realização de perícia etc., uma vez que destinado às causas de menor complexidade. Inclusive, não é atípico encontrar na praxe dos Juizados, magistrados que não admitem ação de remoção de conteúdo e identificação/responsabilização do ofensor a pretexto de ser alta a complexidade da matéria, pese a autorização expressa do art. 19, § 3º, do MCI, de processamento destas ações nos Juizados.

A entrada em vigor do Marco Civil da Internet, em junho de 2014, trouxe, pela primeira vez, de forma consistente, a preocupação do legislador com a proteção dos dados pessoais[17], considerada um dos princípios do uso da internet no país (art. 3º, inc. III).

Na sequência, no capítulo reservado aos direitos e garantias dos internautas, o MCI assegura a inviolabilidade e o sigilo, tanto do "fluxo das "comunicações pela internet", quanto das "comunicações privadas armazenadas" (art. 7º, inc. II e III), assim como o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão e de acesso a aplicações" (art. 7º, inc. VII). Convém mencionar que essas garantias podem ser afastadas por ordem judicial, nos casos autorizados em lei.

Posteriormente, a Lei nº 13.709/2018 veio para complementar o MCI no que se refere aos dados pessoais dos usuários de internet[18]. Dentre suas previsões, destacamos, ainda na parte dos direitos dos titulares dos dados[19], a previsão expressa de o titular obter do controlador[20] dos dados "a qualquer momento", a confirmação da existência dos dados, o acesso a eles, a possibilidade de correção de equívocos, a eliminação ou anonimização[21] do que se mostrar desnecessário, a portabilidade para outras empresas e a revogação do consentimento para o tratamento dos dados por terceiros (art. 18, *caput* e incisos).

Importante previsão da LGPD está no capítulo referente à responsabilidade e ao ressarcimento dos dados (a partir do art. 42). Embora, por um lado, a previsão de que o controlador ou operador de dados que, em sua atividade, causar dano a outrem, esteja obrigado a repará-lo seja mera repetição da regra geral de responsabilização civil do Código Civil (arts. 186 e 927), a lei regula pontos bem específicos referentes ao tratamento de dados.

Tudo isso acaba sendo de fundamental importância pela obrigatoriedade de preservação do sigilo dos dados dos usuários, de forma que, efetivamente, não restará alternativa a quem precise obter os dados para identificação de outra pessoa senão se socorrer do Poder Judiciário.

Surge então o segundo ponto a ser enfrentado: deve o juiz autorizar liminarmente a entrega de dados do suposto ofensor ao autor da ação?

Entendemos que esta questão é verdadeiramente tormentosa porque, de um lado, sem o fornecimento dos dados, o autor terá real dificuldade até mesmo para corretamente

[17] Como bem pontuado por Renato Leite Monteiro, a captação e guarda de dados dos usuários é uma realidade, uma vez que sua monetização faz parte do próprio modelo de negócios sob o qual estão estruturados os provedores de internet. MONTEIRO, Renato Leite. Da proteção aos registros, aos dados pessoais e às comunicações privadas. *In*: DEL MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coord.). *Marco Civil da Internet*: lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014, p. 141.

[18] A LGPD não se limita à proteção dos dados no meio virtual, mas, para o objeto deste artigo, vamos nos limitar a eles.

[19] Esse ponto é muito importante, pois a LGPD afasta as dúvidas sobre a titularidade dos dados quando, em seu art. 17, dispõe expressamente que "toda pessoa natural tem assegurada a titularidade de seus dados pessoais", fulminando a pretensão de empresas que, por permitir o uso de programas e aplicativos, entendiam serem elas as titulares dos dados de seus usuários.

[20] Empresa ou pessoa física responsável pela coleta dos dados e que tem a obrigação de tomar as decisões sobre o tratamento destes dados, mesmo que não realize diretamente o tratamento.

[21] De acordo com a definição da própria LGPD, anonimização é a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo" (art. 5º, XI). Em outras palavras, com ela aumenta-se a privacidade dos dados colhidos, pois são substituídos ou deletados os dados que vinculam determinada informação a um certo usuário, de modo que a informação somente poderá ser utilizada em relatórios e estatísticas. A título de exemplo, uma vez anonimizados os dados de uma livraria virtual, esta continuará sabendo quantos dicionários ou quantos códigos comentados foram vendidos, mas não mais quem adquiriu cada exemplar.

identificar o sujeito passivo da demanda[22]; por outro lado, como fica a situação do réu, exposto desde o início da lide, se ao final, quando do julgamento de mérito, restar decidido que não houve delito, mas sim o exercício da liberdade de expressão?

Temos a convicção de que a questão não se resolve da forma simples como poderia parecer à primeira vista, com a mera observância do disposto no art. 5º, inc. IV, da Constituição Federal, no sentido de ser livre a manifestação do pensamento, "sendo vedado o anonimato".

Este tema foi objeto de profícuo debate no seminário "Privacidade, Sigilo e Compartilhamento"[23], onde um dos autores deste texto pôde expor os embates entre liberdade de expressão *versus* proteção da privacidade e as questões relativas ao anonimato, sigilo e uso de pseudônimos. Na oportunidade, concluiu-se[24] que o sigilo sobre a autoria de determinado conteúdo deve ser garantido quando não houver a configuração de um ilícito, sobretudo a partir do momento em que o Supremo Tribunal Federal classificou como um "sobredireito" a livre e plena manifestação do pensamento e da informação[25].

Porém, esse entendimento é válido quando o autor puder identificar alguém para inclusão no polo passivo de uma ação judicial.

Explica-se: um *site* pode publicar uma matéria sem designação da autoria ou com a utilização de um pseudônimo e alguém se sentir ofendido com a publicação. Na busca por seus direitos, o ofendido não terá problemas em ajuizar uma ação em face do responsável pela página, que poderá se defender sem identificar o autor daquela publicação específica, pelo menos até que a sentença declare que, efetivamente, ocorreu um ilícito.

Caso se conclua que não houve ilício, não há razão para prestar tal informação. Não é o caso propriamente de anonimato, na medida em que o responsável pela publicação − e não necessariamente pela matéria impugnada − estava identificado.

Por outro lado, há casos em que a identificação do autor do conteúdo combatido se mostra obrigatória para o próprio desenrolar da lide, sob pena de não se saber sequer a quem imputar a prática ilícita. Para estes casos, onde se fala efetivamente em anonimato, apontamos as seguintes saídas.

3. Legitimação passiva nas ações de remoção de conteúdo e responsabilidade civil

De nossa parte[26] já tivemos a oportunidade de apontar cinco soluções possíveis no âmbito cível para a questão de como proceder para obter a satisfação do pedido (normalmente, remoção de conteúdo e indenização por danos materiais e morais)

[22] Este tema, com as diferentes possibilidades colocadas à disposição do autor, será abordado no próximo capítulo.

[23] Ocorrido em São Paulo, em outubro de 2017, organizado pelo Observatório de Comunicação da USP e pelo Instituto Palavra Aberta.

[24] MARTINS, Ricardo Maffeis. A garantia do sigilo diante da inexistência de ilícito. *In*: COSTA, Maria Cristina Castilho (org.). *Privacidade, sigilo e compartilhamento*. São Paulo: ECA-USP, 2018. Disponível em: http://bit.ly/38rGCDV. Acesso em: 8 mar. 2019.

[25] No julgamento da Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 130. Ainda sobre a colisão de princípios constitucionais e o uso da ponderação como mais eficaz meio de solução, vide: SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil*: da erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015, p. 145.

[26] Um dos autores deste ensaio (Fernando da Fonseca Gajardoni) sustentou referido ponto de vista em seminário sobre Direito Digital realizado na Escola Paulista da Magistratura (EPM) entre agosto e outubro de 2018, em curso sob a coordenação do Desembargador Luis Soares de Mello Neto e do Juiz Fernando Antonio Tasso (http://bit.ly/2RppN5C). Posteriormente, publicou brevíssimo texto a respeito do tema: Direito digital e ações contra réus indeterminados no Novo CPC. *Jota*. São Paulo, 3 set. 2018. Disponível em: http://bit.ly/38g0N7k. Acesso em: 9 mar. 2019).

nos casos em que o violador da lei está encoberto pelo anonimato. Em todas elas, uma boa pitada de flexibilização do procedimento pelo juiz é fundamental para a adaptação do instrumental existente às particularidades do direito digital.

A maioria das alternativas que serão abaixo apontadas já foi colocada em prática perante o Judiciário, especialmente, a partir de 2018, nas Varas de Direito Empresarial e de Conflitos Relacionados à Arbitragem do Foro Central de São Paulo[27], de modo que os apontamentos feitos levam em consideração não apenas a abordagem teórica do Direito Processual e Digital, mas também a prática.

1ª opção – Esta é, provavelmente, a mais complicada para o autor, seja em termos de demora processual, seja no tocante aos custos, pois envolve o manejo de, ao menos, três ações sucessivas.

Inicia-se com uma ação de obrigação de fazer (art. 497 do CPC/2015) contra o provedor de aplicações para obtenção dos registros[28], cumulada com pedido de retirada liminar do conteúdo ilícito (art. 300 do CPC/2015).

Tome-se por exemplo uma ação movida contra o Facebook denunciando uma postagem ofensiva feita naquela rede social, ou uma ação ajuizada contra o Google, para remoção de um vídeo publicado no YouTube.

Atendido no pedido de urgência de remoção do material apontado como ofensivo e depois no fornecimento de dados por parte do provedor de aplicações – que, via de regra, não possui os dados cadastrais do usuário, mas somente seus dados de acesso e, talvez, uma conta de e-mail[29] – o autor passa à segunda etapa, que é o ajuizamento de uma segunda ação de obrigação de fazer (art. 497 do CPC/2015), desta vez movida contra o provedor de conexão, para indicação dos registros de conexão de onde proveio a prática do ato ilegal[30].

Diferente dos provedores de aplicações, os provedores de conexão têm a obrigação de obter e guardar os dados pessoais de seus usuários.

Assim, de posse dos dados de acesso já fornecidos, é possível identificar qual computador foi o responsável pelas conexões buscadas e entregar os dados de quem – pessoa física ou jurídica – é o responsável por aquela conexão. Pode-se chegar a uma residência (por exemplo, a internet de sua casa), a uma empresa (se a conexão foi feita a partir da internet do local de trabalho) ou ao titular de uma linha de telefonia celular (modalidade de uso de internet que mais cresce no Brasil e no mundo).

[27] Duas varas especializadas, instaladas no final de 2017 no Fórum João Mendes Júnior, na capital paulista.

[28] Normalmente, os pedidos mais comuns apresentados ao Judiciário são de identificação do endereço IP, mas, a depender da situação concreta, pode ser necessário o fornecimento de outros dados além do IP.

[29] Faça o leitor um exercício de memória. Tente se lembrar se precisou apresentar algum documento pessoal ao criar uma conta de e-mail, um perfil de rede social ou baixar um aplicativo em seu celular. A resposta é, invariavelmente, não. Preenche-se um questionário (onde o usuário pode criar um perfil totalmente falso), pode-se colocar uma foto (verdadeira ou não) e, na maior parte das vezes, é preciso confirmar a inscrição utilizando-se apenas uma conta de e-mail (que pode, por sua vez, também ter sido criada com dados falsos). Nenhuma outra confirmação ou comprovação dos dados fornecidos é solicitada. Por outro lado, os provedores de aplicações têm a obrigação de registrar e armazenar em segurança os dados do acesso por parte de seus usuários.

[30] Explica-se. Com o fornecimento do IP utilizado na conexão, pode-se descobrir, na maior parte das vezes sem qualquer dificuldade, quais foram os provedores de conexão utilizados para a prática do ilícito. Assim, conhecendo-se a operadora e informando a ela os registros de conexão, com data hora e local, tais empresas têm condições de identificar qual de seus usuários foi o responsável pela prática ilícita.

Partindo-se do pressuposto que tudo tenha dado certo nas duas primeiras demandas[31], o ofendido, que já obteve a remoção do conteúdo, de posse agora da identificação do ofensor, poderá finalmente ajuizar a terceira ação, com pleito de indenização contra o violador da lei, buscando a reparação civil.

Nesta terceira ação, costuma-se formular também pedido de obrigação de não fazer para que o ofensor não torne a publicar ofensas de igual ou semelhante teor. Não raras vezes, também é feito o pedido de retratação pública, pleito que – a partir de nossa experiência – tem se mostrado majoritariamente infrutífero.

Reitere-se que seriam três ações judiciais consecutivas para a solução de um único problema. Três demandas autônomas, cada qual com recolhimento de custas processuais, espera de citação e resposta dos réus – eventualmente sendo necessário defender em 2º grau a tutela de urgência concedida, quando, não raro, os provedores interpõem agravo de instrumento para não serem obrigados a cumprir a ordem judicial ou, no mínimo, para afastar eventual multa diária fixada – sem falar nos gastos com honorários advocatícios[32].

2ª opção – Ajuíza-se um pedido de tutela antecipada antecedente (art. 303 do CPC/2015) contra o provedor de aplicações para obtenção dos registros de IP de onde proveio a ofensa, com pleito de remoção do conteúdo.

Deletado o material ilícito e fornecidos os dados, procede-se ao aditamento da petição inicial (art. 303, § 1º, do CPC), agora lançando-se no polo passivo o provedor de conexão, sendo certo que o novo pedido é o de cumprimento da obrigação de fazer (art. 497 do CPC/2015) consistente na identificação dos dados cadastrais do titular da conexão de onde proveio a violação da lei.

Identificado o ofensor, tal qual na primeira hipótese, o caminho a seguir é o ajuizamento de uma segunda ação, agora com pleito indenizatório cumulado com pedido de obrigação de não fazer contra o violador da lei, para responsabilização pecuniária, inclusive para eventualmente impedir que a conduta ilícita se renove.

Aqui já se tem uma ação a menos, porém, ainda com ao menos duas ações judiciais consecutivas. A primeira delas, bastante discutível do ponto de vista processual (art. 303, § 1º, do CPC), uma vez que a propositura da tutela antecedente se dá contra uma parte (provedor de aplicações), mas a emenda será contra outra parte (provedor de conexão). Ou seja, o risco de indeferimento da petição inicial torna-se concreto por conta desta questão processual não prevista no CPC.

[31] Não vamos poder nos aprofundar no tema no âmbito deste artigo, mas uma das questões que mais atormenta o Judiciário nas demandas ligadas ao Direito Digital ocorre quando o provedor de aplicações fornece o IP e a operadora não pode identificar o usuário, por ainda utilizar a tecnologia conhecida como IPV-4, cujo número de endereços IP é limitado, de forma que um mesmo IP pode ser utilizado, simultaneamente, por um número grande de usuários daquele provedor de conexão (às vezes, centenas). Nesses casos, a operadora costuma requerer que o Juízo solicite ao provedor de aplicações a chamada *Porta Lógica de Origem*, através da qual seria possível chegar ao usuário. Na prática, porém, os provedores de aplicações informam não serem obrigados a armazenar tal dado, de modo que o autor da ação fica sem saber o que fazer. Indicamos, aos interessados no tema, a leitura dos seguintes acórdãos: TJ/SP – Agravo de Instrumento nº 2193330-35.2017.8.26.0000, 9ª Câmara de Direito Privado, Rel. Des. PIVA RODRIGUES, j. em 30.01.2018; STJ – Recurso Especial nº 1.641.133/MG, 3ª Turma, Rel. Min. NANCY ANDRIGHI, j. em 20.06.2017.

[32] Doutrina e jurisprudência majoritárias entendem ser incabível, na ação de remoção de conteúdo e identificação do ofensor, a condenação dos provedores em sucumbência. Trata-se de ação necessária, sem causalidade por parte dos provedores, considerando que não podiam, por força do MCI, fornecer os dados do ofensor mediante simples requerimento extrajudicial.

E, em caso de indeferimento da inicial, retorna-se à necessidade da propositura de três ações distintas.

3ª opção – Ajuizamento de uma ação de produção antecipada de provas (art. 381, III, do CPC/2015) contra os provedores de aplicações e de conexão (formando um litisconsórcio sucessivo) para identificar o violador da lei através do fornecimento dos dados necessários para tanto.

Apresentados os dados, em caso de sucesso na identificação do ofensor, o autor pode seguir pelo caminho já explicado, ajuizando ação autônoma com pedidos de obrigação de não fazer, eventual retratação e reparação financeira por danos morais e/ou materiais.

Novamente, temos duas ações judiciais consecutivas.

Antes de passarmos às duas últimas alternativas, importante fazer um adendo. A primeira opção não enfrenta qualquer restrição por parte do Judiciário. Seu maior problema reside nos gastos – de tempo e financeiros – relativos ao ajuizamento de três ações.

As alternativas de número dois e três, por sua vez, estão mais suscetíveis de enfrentarem resistências. A da tutela antecipada antecedente, como visto, pelo fato de o pedido principal (emenda à inicial) ser voltado a uma parte diferente daquela contra quem é formulado o pedido de urgência.

A produção antecipada de provas, por seu turno, sofreu significativa alteração com o CPC/2015, sendo possível afirmar que o Judiciário ainda não assimilou, por completo, a existência no país, de ações autônomas de produção de provas. Além disso, embora seja um procedimento sem maiores complicações, não é difícil que a parte contrária consiga, via agravo de instrumento, retardar seu andamento nos tribunais.

Há ainda outro ponto que merece ser mencionado, pela relevância.

Temos observado de nossa experiência no Judiciário e na advocacia que, como regra, quando uma pessoa ou empresa decide ajuizar uma ação para remoção de conteúdo postado na internet e identificação do responsável pelo material ilícito, normalmente há extrema urgência; necessita-se de resposta imediata da Justiça; que os provedores cumpram rapidamente a ordem judicial de remoção e fornecimento de dados.

No afã de conseguir o que se quer no menor tempo possível, muitas vezes os autores optam por requerer que a ordem seja cumprida em prazo exíguo, sob pena de altíssimas multas diárias em caso de descumprimento.

Embora os juízes costumem agir com discernimento e ponderação nestes momentos, normalmente reduzindo as *astreintes* a um valor mais razoável do que o pleiteado, o arbitramento da multa (muitas vezes de imposição prévia desnecessária, considerando que os provedores não têm interesse, como regra, na preservação do conteúdo e dos dados do usuário diante da ordem judicial), é o motivo da interposição de agravos que podem tumultuar o trâmite processual e dificultar o cumprimento da ordem.

Isso porque nem sempre a determinação judicial é específica, nos limites técnicos do serviço prestado (como preceitua o art. 19, *caput* e seu parágrafo único, da Lei nº 12.965/2014), de modo que se possa identificar de modo preciso e inequívoco o material tido por infringente.

Assim, na dúvida quanto à extensão do cumprimento da ordem judicial, o provedor, que poderia simplesmente fazer um questionamento ao Juízo quanto ao

modo de atender o comando judicial, opta por interpor o agravo de instrumento para não correr o risco de ver contra si aplicada uma pena cujo valor aumenta diuturnamente[33].

4ª opção – Uma única ação de obrigação de fazer cumulada com indenização por danos materiais e/ou morais (art. 327 do CPC/2015) contra o provedor de aplicações, para obtenção dos registros (endereços IP) e retirada liminar do conteúdo (art. 300 do CPC), em litisconsórcio facultativo eventual[34] com os seguintes corréus indeterminados (art. 319, §§ 1º e 2º, do CPC/2015[35]): (i) o provedor de conexão, para indicação dos dados cadastrais/pessoais do infrator e; (ii) o violador da lei, para responsabilização civil e comprometimento de não tornar a repetir a conduta ilícita.

Pela primeira vez, tem-se a opção de ajuizamento de uma única ação e não mais duas ou três. Porém, não será uma ação simples, na medida em que o polo passivo será constituído por – pelo menos – três réus, sem qualquer ligação entre si e que comparecerão ao processo cada qual com uma função distinta dos demais, pois os pedidos formulados contra cada um deles não têm relação com os outros (com exceção, claro, da necessidade de fornecimento consecutivo de dados, para identificação do ofensor).

5ª opção – Uma única ação de indenização contra réu(s) indeterminado(s) violador(es) da lei para fins de responsabilização civil e obrigação de não fazer, ou seja, não voltar a publicar o material ofensivo (art. 319, §§ 1º e 2º, do CPC).

Aqui, ataca-se diretamente o responsável pelo dano causado, nos termos não apenas da legislação específica (Marco Civil da Internet e Lei Geral de Proteção de Dados), mas do próprio Código Civil, em seus artigos 186 e 927[36].

O problema continua sendo o de que, no momento do ajuizamento da ação, não se sabe a identidade dos ofensores, que ainda são indeterminados.

Para chegar a eles, em vez da apresentação de outras ações antecedentes, requer-se ao juiz a expedição de ofícios sucessivos aos provedores de aplicações (identificação do IP e remoção liminar do conteúdo inadequado) e, na sequência, aos provedores de conexão (apresentação dos dados cadastrais/pessoais do violador).

Vencida esta etapa e fornecidos os dados, o autor emenda sua petição inicial para consolidação do polo passivo da demanda, uma vez que o réu, antes indeterminado, agora já é conhecido do autor da ação, graças às respostas fornecidas pelos provedores aos ofícios judiciais.

---

[33] Convém ainda não esquecer que, quando as *astreintes* atingem um valor elevado em decorrência do decurso do prazo, muitos autores passam a deixar de se preocupar com o cumprimento da ordem de remoção/fornecimento de dados, preferindo optar por torcer para que a multa aumente cada vez mais, esquecendo-se que, quando a penalidade atinge valor exagerado, costuma ser reduzida pelas instâncias superiores.

[34] Sobre a temática, ver: SANTOS, Silas Silva. *Litisconsórcio eventual, alternativo e sucessivo*. São Paulo: Atlas, 2013. Para fins deste texto, entende-se por litisconsórcio passivo eventual aquele que será formado, apenas, se eventualmente for possível a revelação dos dados do provedor de conexão e/ou do ofensor.

[35] Sobre o art. 319, §§ 1º e 2º, do CPC, conferir os comentários de André Roque. *In*: GAJARDONI, Fernando da Fonseca; DELLORE, Luiz; ROQUE, André Vasconcelos, e OLIVEIRA JR., Zulmar Duarte. *Processo de conhecimento e cumprimento de sentença*: comentários ao CPC/2015. 2. ed. São Paulo: Método, 2018.

[36] "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".
"Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

Esta última opção tem duas vantagens.

A primeira delas, cristalina, que é a sensível diminuição de gastos e de tempo com o ajuizamento de apenas uma ação.

A segunda, não tão perceptível, mas real: como os provedores deixam de figurar no polo passivo da demanda, limitando-se agora, na qualidade de terceiros, a responder ofícios judiciais, deixam de se preocupar com questões como custas processuais, eventual sucumbência, necessidade de provisionamento e gastos com advogados etc.

Tudo isso faz com que os ofícios expedidos para remoção do conteúdo, identificação do provedor de conexão e indicação do suposto ofensor sejam prontamente atendidos, restando afastado o comportamento litigioso observando quando, então, são os provedores de aplicação e conexão citados na qualidade de réus.

Todas as medidas judiciais supra indicadas, como regra, seriam possíveis à luz do interesse (e disposição) da parte prejudicada pela ofensa[37].

Conclusões

Apresentadas as medidas, cada qual com suas vantagens e problemas, entendemos que a via mais vantajosa (para as partes e para o Poder Judiciário) e adequada (do ponto de vista processual) é a última delas.

Os motivos são vários.

Primeiro, em uma interpretação pró-ativa do art. 319, §§ 1º e 2º do CPC/2015 (que não foi pensado para as situações ora cogitadas), bem se verá que compete à autoridade judiciária colaborar com o autor na própria identificação da parte requerida na demanda, e não, apenas, para a obtenção da sua qualificação completa.

A admissão da ação para remoção liminar do conteúdo ilegal e indenização contra o ofensor incerto, seguida de ofícios para os provedores de aplicações e conexão (a fim de excluir o conteúdo e informar os dados do ofensor), cumpre adequadamente tal dever processual do Estado-Juiz, pois permite a identificação do ofensor em estrito cumprimento dos ditames da Lei nº 12.965/2014, além de garantir a proteção dos dados dos usuários da internet, que, como visto, não serão divulgados caso o Judiciário não constate a ocorrência do ilícito[38].

Segundo, pois a manutenção dos provedores como terceiros no processo parece ser a solução mais adequada do ponto de vista do direito material (Lei nº 12.965/2014), já que, graças ao *safe harbor* dos artigos 18 e 19 do Marco Civil da Internet, não são eles responsáveis pelos danos decorrentes de conteúdo gerado por terceiros, de modo que as providências que lhes são requisitadas com base nos parágrafos do art. 19 e nos arts. 22 e 23, todos do MCI, devem se dar na forma do art. 403, parágrafo único, do CPC/2015 (exibição incidental contra terceiros), dispensando que figurem no polo passivo do processo.

[37] Salvo se o lesado preferir o ajuizamento da ação pelo sistema dos Juizados Especiais, como autoriza o art. 19, § 3º, da Lei nº 12.965/2014. Nestes casos, crê-se que somente as opões 1 e 3 seriam viáveis, pois o emprego da tutela antecipada antecedente (artigo 303 do CPC/2015) e a identificação da parte passiva (artigo 319, §§ 1º e 2º, do CPC/2015) – necessários para o uso das opções de nº 2, 4 e 5 –, parece incompatível com o procedimento sumaríssimo da Lei nº 9.099/1995, que regula os Juizados Especiais Cíveis e Criminais.

[38] Vide capítulo II, supra.

Terceiro, porque a solução preconizada ainda traz a reboco a vantagem de que, não resistindo à ordem de baixa do conteúdo tido por ilícito e prestando as informações requisitadas, não há sucumbência a se arbitrar em desfavor dos provedores de aplicações e de conexão (que não são partes no processo), até porque não tinham autorização legal para baixar o conteúdo (salvo no caso do art. 21 do Marco Civil) ou prestar informações (dados de conexão e cadastrais) sem requisição judicial.

A quarta vantagem vem do que temos observado no dia a dia forense. Se, há alguns anos, a adoção da quinta opção acima seria vista com desconfiança e provavelmente esbarraria em questões processuais ligadas aos requisitos da petição inicial, hoje este modelo tem sido aceito de forma mais ampla, desde que bem justificada a necessidade da expedição de ofícios para posterior identificação completa do(s) réu(s). Ademais, agora há suporte legal por aproximação para a adoção desta medida (art. 319 e §§ do CPC).

Por fim, uma última nota.

A temática dos processos envolvendo violações da lei praticadas pela via digital ainda é nova (o Marco Civil da Internet é de 2014, ao passo que a LGPD foi editada em 2018), embora tenda a se tornar cada vez mais comum com o passar dos anos. Além disso, demanda dos operadores do Direito um certo conhecimento de questões técnicas ligadas ao tema, de modo que sempre é bom ter em mente que o Judiciário, à luz do princípio da cooperação (art. 6º do CPC/2015), deve orientar as partes sobre suas escolhas processuais e respectivas vantagens e desvantagens da eleição de cada uma das opções processuais supra indicadas.

Relembramos então a lição com a qual abrimos este breve ensaio: diante de lacunas na lei, compete ao julgador, em auxílio e cooperação com os litigantes (art. 6º do CPC/2015), calibrar o procedimento ao caso concreto, fazendo as competentes adaptações de modo que nem o autor seja prejudicado na busca pela tutela jurisdicional, nem o réu no seu direito de defesa.

Referências bibliográficas

DINAMARCO, Cândido Rangel. *Instituições de direito processual civil*. 5. ed. São Paulo: Malheiros, 2005. v. 3.

GAJARDONI, Fernando da Fonseca. *Flexibilização do procedimento*: um novo enfoque para estudo do procedimento em matéria processual. São Paulo: Atlas, 2007.

GAJARDONI, Fernando da Fonseca. Direito digital e ações contra réus indeterminados no Novo CPC. *Jota*. São Paulo, 3 set. 2018. Disponível em: http://bit.ly/38g0N7k. Acesso em: 16 jan. 2020.

GAJARDONI, Fernando da Fonseca; DELLORE, Luiz; ROQUE, André Vasconcelos; OLIVEIRA JR., Zulmar Duarte. *Processo de conhecimento e cumprimento de sentença*: comentários ao CPC/2015. 2. ed. São Paulo: Método, 2018.

GODOY, Claudio Luiz Bueno de. Uma análise da responsabilidade civil dos provedores na lei nº 12.965/14 (Marco Civil da Internet). *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*: Tomo II: Marco Civil da Internet (Lei n. 12.964/2014). São Paulo: Quartier Latin, 2015.

MARTINS, Ricardo Maffeis. A garantia do sigilo diante da inexistência de ilícito. *In*: COSTA, Maria Cristina Castilho (org.). *Privacidade, sigilo e compartilhamento*. São Paulo: ECA-USP, 2018.

MARTINS, Ricardo Maffeis. As decisões do Superior Tribunal de Justiça sobre Direito Digital. No prelo.

MONTEIRO, Renato Leite. Da proteção aos registros, aos dados pessoais e às comunicações privadas. *In*: DEL MASSO, Fabiano; ABRUSIO, Juliana; FLORÊNCIO FILHO, Marco Aurélio (coord.). *Marco Civil da Internet*: Lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014.

SANTOS, Silas Silva. *Litisconsórcio eventual, alternativo e sucessivo*. São Paulo: Atlas, 2013.

SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil*: da erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

YARSHELL, Flávio Luiz. *Curso de direito processual civil*. São Paulo: Marcial Pons, 2014. v. 1.

Considerações sobre a autenticidade e a integridade da prova digital

Guilherme de Siqueira Pastore
Juiz de Direito no Estado de São Paulo

Resumo: A crescente relevância da tecnologia no meio social interfere diretamente na atividade probatória no processo jurisdicional, exigindo a adaptação do juízo de admissibilidade e da valoração dos elementos de prova, para que os existentes em meio eletrônico possam receber tratamento equivalente às informações documentadas em suporte físico, no tocante às exigências de confiabilidade. A falta de critérios adequados e suficientes a garantir a autenticidade e integridade das informações obtidas de fontes digitais, cuja importância se realça neste trabalho, compromete a sua força probante e pode levar a equívocos na apreciação dos fatos pelo julgador.

Palavras-chave: Direito Processual. Direito Probatório. Prova Digital. Documento Eletrônico. Banco de Dados Digital. Autenticidade. Integridade.

1. Introdução

O direito à prova, tal como se reconhece às partes do processo em contraditório, decorre diretamente do direito de ação (art. 5º, inc. XXXV, da Constituição da República) e da garantia da ampla defesa (art. 5º, inc. LV), porque do resultado da atividade probatória depende a delimitação das alegações que, tidas por verdadeiras, sustentarão a incidência normativa, atraindo as respectivas consequências jurídicas, e, por conseguinte, a prestação jurisdicional.

É inócuo alegar sem poder provar o que se alegou. Considerada, por isso, "um dos mais respeitados postulados inerentes à garantia política do devido processo legal" e "um dos fundamentais pilares do sistema processual contemporâneo" (DINAMARCO, 2017, p. 51), a adequada disciplina da produção e da valoração da prova é indispensável à realização de um processo justo.

Com efeito, embora já superada na ciência processual a equivocada noção da busca da chamada "verdade real", não se pode ignorar que haverá chances tanto maiores de se alcançar uma decisão justa, capaz de atender ao escopo magno da jurisdição — de pacificar com justiça —, quanto mais completa e precisa for a reprodução, no processo, dos fatos que lhe constituem o objeto. Não obstante, por uma "falsa suposição de que os fatos não necessitam da atenção dos juristas" (MARINONI; ARENHART, 2011, p. 25), o direito probatório frequentemente recebe atenção desproporcional à sua importância.

O descuido com a temática se tem observado, no cotidiano forense — não apenas no contexto brasileiro (*e.g.*, cf. FRIEDEN; MURRAY; LEIGH, 2011) —, pela crescente utilização de provas digitais sem atenção às suas peculiaridades, com prejuízo relevante à força probante dos elementos de convicção que se trazem aos autos e, em decorrência disso, à própria realização do direito por meio do processo, o que impõe urgente reflexão sobre o fenômeno.

2. Avanço da tecnologia e relevância da fonte de prova digital

A prova segue, pela sua própria natureza e finalidade, as alterações por que passam as relações jurídicas de direito material em que os litígios se originam, bem como a realidade que as envolve. É natural, portanto, que o marcante avanço das tecnologias nos últimos anos implique a alteração da forma pela qual se estabelecem essas relações e inspire o recurso a novos meios de acautelar informações para o futuro, acarretando então significativa mudança no perfil dos elementos que servem a reconstituir, no processo, os fatos pretéritos que se mostrem pertinentes ao desate de uma controvérsia.

A incorporação da tecnologia aos mais variados aspectos da vida tem modificado profundamente as interações humanas e a organização da sociedade, redesenhando desde a comunicação, com a substituição das cartas pelo correio eletrônico, dos telefonemas por mensagens instantâneas de texto, áudio ou vídeo etc.; até os registros – públicos ou privados – que se pretendem perenes, antes inscritos em papel com toda sorte de cautela, e hoje amplamente substituídos pelos sistemas de informática; passando, ainda, por toda espécie de atividade que, prescindindo do contato presencial antes necessário ou criando possibilidades inéditas, se vale da *internet*, por meio da qual se acessa e se transmite um volume imenso de informação, se celebram negócios jurídicos e também se praticam atos ilícitos.

Essa drástica mudança de paradigma reflete na atividade probatória de modo relevante, mas sutil, porque os *meios de prova* – assim entendidos os "instrumentos ou atividades por intermédio dos quais os dados probatórios (elementos de prova) são introduzidos e fixados no processo" (GOMES FILHO, 2005, p. 308) permanecem essencialmente os mesmos, ao menos nos aspectos exteriores mais facilmente perceptíveis, enquanto as *fontes de prova* – "pessoas ou coisas das quais se possam extrair informações capazes de comprovar a veracidade de uma alegação" (DINAMARCO, 2017, p. 97) se alteram e reclamam a elaboração de novos critérios para o seu adequado exame.

Isto é, o novo cenário implica que a produção da prova no processo ainda observa o rito próprio da juntada ou depósito em juízo dos documentos, da tomada de depoimentos e dos exames e vistorias periciais para esclarecimentos de ordem técnica; mas a fonte que se acessa por esses meios, que é o traço verdadeiramente distintivo do que se chama de *prova digital*, ostenta peculiaridades merecedoras de tratamento diferenciado.

A título de exemplo, é notório que "a confiabilidade da prova documental – e a importância singular que os ordenamentos processuais lhe emprestam – assenta-se, exatamente, na *estabilidade do suporte* em que a informação é registrada" (MARINONI; ARENHART, 2011, pp. 563-564).

Ocorre que o documento produzido em meio eletrônico pode, em regra, ser alterado sem esforço, em meios de armazenamento suscetíveis de regravação. Notadamente no fluxo de dados em uma rede de computadores, como a *internet*, a informação armazenada em meio eletrônico "assume caráter temporário, é fungível e de grande volatilidade" (RAMOS, 2014, cap. 2.2), em aparente contradição com a natureza e a própria utilidade da prova documental.

Paradoxalmente, porém, cada reprodução de um documento, seja no mesmo meio ou em outro meio congruente a que transportado, poderá ser idêntica e, assim, indistinta do original, inclusive para efeitos probatórios. A conservação do original com seus atributos próprios pode, assim, exceder a vida útil de um dispositivo de armazenamento, incrementando a estabilidade documental. Já a sua

transposição para meio diverso, por outro lado, como sucede com a materialização em suporte de papel, sempre resultará em cópia, com as ressalvas que a reprodução comporta, pela eventual necessidade de confronto com o original, no meio em que produzido (MARCACINI, 1999, p. 75).

Nesse contexto, em que a atividade probatória recai sobre fontes às quais inaplicáveis diversas premissas sedimentadas no direito processual, já houve alertas para o risco de obsolescência do processo, pelo descompasso com o direito material (CABRAL, 2006, p. 99), ao que atualmente se soma, em decorrência da observação da prática forense, o receio de que os sujeitos do processo – mais especificamente, os profissionais do direito – possam inadvertidamente frustrar, seja pela postulação deficiente ou pela decisão equivocada, a satisfação de direitos legítimos.

3. Confiabilidade da prova documental em meio físico

Historicamente, a estabilidade propiciada pelos documentos, como prova pré-constituída e apta a perpetuar, sem inclinações de ordem subjetiva, a memória dos atos e fatos jurídicos, lhes rendeu tratamento especial na legislação brasileira e estrangeira, que a eles têm conferido pleno crédito (MARINONI; ARENHART, 2011, pp. 548-549), inclusive como único meio idôneo para a prova de determinados fatos, como determinava o art. 401 do Código de Processo Civil instituído pela Lei n.º 5.869, de 11 de janeiro de 1973 (CPC/73)[1].

Sobre as fontes de prova pessoais – também ditas ativas –, ao revés, pesa um estigma de desconfiança, pela pouca efetividade do depoimento pessoal para a obtenção de informações relevantes e, em especial, pelo frequente comprometimento da prova testemunhal pelo esquecimento, pelas falsas memórias, pela parcialidade ou corrupção do depoente, ou mesmo pela morte ou impossibilidade de localização da testemunha.

Assim é que, sem embargo da significativa redução da tarifação legal da prova no Código de Processo Civil em vigor, no qual não se encontra disposição equivalente ao já mencionado art. 401 do CPC/73, a cultura jurídica brasileira ainda se inclina – não sem razão – ao reconhecimento de eficácia probatória superlativa aos registros documentais.

Tal singular relevância dos documentos explica o tratamento minucioso da sua produção e da sua valoração pela lei, uma vez que, embora inerentemente mais segura em comparação com outros meios, a prova documental sabidamente se expõe ao erro, à falsificação, ao perecimento e a toda ordem de utilização inescrupulosa.

Para este fim, a par das exigências de forma solene para determinados atos e das disposições sobre o teor de instrumentos particulares, o cuidado legislativo com a prova documental se observa, exemplificativamente, na disciplina dos pormenores do conteúdo e do momento da lavratura das escrituras públicas, quanto ao que deve ser declarado, como as declarações devem ser conferidas pelos subscritores, quem deve assinar o instrumento público e de que modo os presentes devem se identificar para a prática do ato (art. 215, §§ 1º, 2º e 5º, do Código Civil).

[1] "Art. 401. A prova exclusivamente testemunhal só se admite nos contratos cujo valor não exceda o décuplo do maior salário mínimo vigente no país, ao tempo em que foram celebrados."

Cautela semelhante se revela na exigência de que as certidões dos documentos produzidos ou armazenados em juízo, para que façam a mesma prova que os originais, sejam extraídas pelo próprio escrivão ou sob a sua vigilância (art. 216 do Código Civil e art. 425, inc. I, do Código de Processo Civil); bem como de que os telegramas e as cópias autenticadas por tabelião sejam conferidos com os originais na hipótese de lhes ser impugnada a autenticidade (arts. 222 e 223 do Código Civil).

No aspecto da valoração, a lei ainda cuidou de explicitar algumas noções intuitivas, que na falta de disposição normativa poderiam ser facilmente extraídas das regras de experiência comum, como a de que a declaração constante de documento apenas se presume verdadeira em relação ao signatário (art. 219 do Código Civil e art. 412 do Código de Processo Civil), ou de que, a fim de evitar o uso de documentos antedatados para prejudicar direitos, a data do documento particular não é oponível a terceiros, até que verificada, por dado externo e objetivo – a exemplo da morte de um dos subscritores ou da inscrição em registro público –, a impossibilidade de data diversa (art. 409, parágrafo único, do Código de Processo Civil).

Em síntese, as precauções adotadas pela lei em relação aos documentos permitem extrair ao menos duas premissas que interessam ao tratamento da prova digital: primeiro, que o conteúdo de um documento tem a sua força probante condicionada à sua origem e, em vista dela, à credibilidade que possa merecer o que nele se inscreveu; e, segundo, que a fidelidade das informações, quando não se tem acesso direto ao original, depende da fé de quem as transporta para a forma documental que ingressará nos autos do processo. Este último enfoque é o que, de forma mais direta, interessa à apuração da autenticidade e da integridade, no paralelo que se exporá a seguir.

4. Confiabilidade da prova digital: requisitos de autenticidade e integridade

As premissas estabelecidas a respeito da prova inscrita em suporte físico não se distanciam do que se deve almejar em relação à prova digital. Procedendo-se à adequada decomposição analítica dos documentos em seu aspecto intrínseco, correspondente ao conteúdo, e o seu suporte material, como manifestação concreta e sensível (MARINONI; ARENHART, 2011, p. 255), nota-se que a evolução tecnológica tende sempre a propiciar o uso de novos suportes, sem, contudo, desnaturar a essência nem a finalidade do registro de um fato, que caracterizam a prova em função de seu conteúdo (MARCACINI, 1999, pp. 75-76) e, portanto, inspiram igual prudência no reconhecimento da sua eficácia.

Não é dizer que o suporte do documento seja indiferente. Os seus atributos distintos ensejaram, desde o início, intenso debate a respeito da fidedignidade da prova digital e resistência à sua admissão. E tal resistência não é inédita: no curso da evolução do direito processual, a informática não é a primeira mudança de paradigma imposta pela disseminação de novas tecnologias. Em retrospectiva, os obstáculos que a prova digital enfrentou na prática forense, quanto à sua confiabilidade, foram considerados previsíveis, à vista das semelhantes ressalvas que os tribunais opuseram à fotografia, ainda no século XIX, e às gravações de conversas, já no início do século XX (GOODE, 2009, p. 4).

A resistência inicial é superada, como de fato o foi em todos os casos mencionados, pela crescente familiaridade com a tecnologia, bem como, no caso da prova digital, pelo avanço legislativo que se verificou desde as primeiras advertências sobre a obsolescência do direito processual diante da tecnologia, dispensando o esforço interpretativo antes

necessário que as informações armazenadas em meio eletrônico fossem admitidas como prova e valoradas pelo seu conteúdo.

Na ordem jurídica brasileira, trata-se, principalmente, da Medida Provisória n.º 2.200-2, de 2001, de efeitos perenizados pela Emenda à Constituição n.º 32, de 24 de agosto de 2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, outorgando expresso reconhecimento aos documentos eletrônicos produzidos naqueles moldes[2]; bem como da Lei n.º 11.419, de 19 de dezembro de 2006, que disciplinou a informatização do processo digital e, reconhecendo a assinatura digital como garantia de autenticidade das informações (art. 1º, § 2º, inc. III[3], e art. 2º, § 2º[4]), passou a admitir a conservação dos autos em meio exclusivamente eletrônico, desde que garantida a integridade dos dados[5]; e, finalmente, do Código de Processo Civil editado em 2015, que passou a tratar da prova digital, embora com ambiguidades e imprecisões.

Também a Lei n.º 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet no Brasil, ao cuidar de aspectos do tráfego de dados na *internet*, acabou por tocar questões pertinentes à informática em geral e ao direito à prova, embora, por escaparem ao âmbito declarado da sua incidência, não tenham sido objeto de regulação minuciosa, dando ensejo à crítica no sentido de que "o Marco Civil acabou por se tornar uma norma incompleta e passível de sofrer prováveis problemas interpretativos" (MARCACINI, 2015, pp. 469-470).

Na verdade, a dificuldade em relação à prova digital se inverteu: a onipresença da tecnologia, fora do restrito âmbito processual, e a crescente familiaridade dos profissionais do direito com as fontes de prova que frequentemente interessam ao processo – basta pensar nos históricos de conversas travadas por meio de aplicativos de celular, reproduzidos por imagem da tela do dispositivo –, somados à legislação lacunosa, têm resultado na prevalência da confiança individual e subjetiva em cada específica fonte de prova, muitas vezes superficial e alheia às suas características técnicas, em detrimento de análise objetiva dos riscos que a atividade probatória envolve.

O que muitas vezes se negligencia, como efeito desse crescente conforto com a prova digital, é que documentos eletrônicos em sentido estrito e outras informações armazenadas em meio eletrônico são também suscetíveis de falsidade, não apenas ideológica, mas também material. Conforme já se apontou no início, uma sequência de dados armazenada em meio eletrônico pode, desde que o meio comporte regravação ou que a informação seja transportada a outro meio que a comporte, ser alterada, o que pode ser difícil ou mesmo impossível de detectar, pelas próprias peculiaridades do suporte:

---

[2] "Art. 10. Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória."

3 "§ 2º Para o disposto nesta Lei, considera-se:
[...]
III – assinatura eletrônica as seguintes formas de identificação inequívoca do signatário:
a) assinatura digital baseada em certificado digital emitido por Autoridade Certificadora credenciada, na forma de lei específica;
b) mediante cadastro de usuário no Poder Judiciário, conforme disciplinado pelos órgãos respectivos."

[4] "§ 2º Ao credenciado será atribuído registro e meio de acesso ao sistema, de modo a preservar o sigilo, a identificação e a autenticidade de suas comunicações."

[5] "§ 1º Os autos dos processos eletrônicos deverão ser protegidos por meio de sistemas de segurança de acesso e armazenados em meio que garanta a preservação e integridade dos dados, sendo dispensada a formação de autos suplementares."

> *Não há bits falsos. Isto equivale a afirmar que, enquanto no mundo físico, a materialidade do meio em que se propagam as mensagens permite uma série de mecanismos de verificação de sua autenticidade (exame grafotécnico, análise da tinta, do papel em que impressa a mensagem, como papel-moeda, marca d'água, etc.), no meio virtual isto é impossível. (CABRAL, 2006, p. 102).*

As imagens da tela de um computador pessoal ou de um aparelho de telefonia celular, a seu turno, podem ser compostas sem qualquer especial exigência de habilidade em editores de imagens, ou mesmo em sítios eletrônicos que facilitam a criaçãointeiramente nova de uma reprodução visualmente indistinta de uma conversa autêntica. Há numerosas aplicações de *internet* para este fim, facilmente encontradas por intermédio de qualquer sistema de busca, que aqui não se listam para evitar a promoção de software não verificado, potencialmente malicioso.

A lei não passou integralmente ao largo desse risco, ao preceituar que qualquer reprodução mecânica ou eletrônica tem o valor do original, se não for impugnada (art. 225 do Código Civil[6]), e que as fotografias digitais, assim como a forma impressa das mensagens eletrônicas, fazem prova do que reproduzem até a impugnação, cabendo, neste caso, a "autenticação eletrônica" ou a realização de perícia (art. 422, §§ 1º e 3º, do Código de Processo Civil). Igualmente se admitiu o valor probatório dos documentos "produzidos eletronicamente e juntados aos processos eletrônicos com garantia da origem e de seu signatário" (art. 11, *caput*, da Lei n.º 11.419, de 2006), bem assim dos extratos digitais de bancos de dados, desde que atestada a conformidade com o original pelo emitente, sob as penas da lei (art. 425, inc. V, do CPC).

O regramento legal é longe de exaustivo, e deve ser compatibilizado, na jurisdição criminal, com a necessidade de exame pericial do corpo de delito, independentemente de impugnação (art. 158 do Código de Processo Penal[7]), mas permite entrever que, para a atribuição de força probante a documentos eletrônicos e outras informações extraídas de meios digitais, "é fundamental avaliar o grau de segurança e de certeza que se pode ter, sobretudo quanto à sua *autenticidade*, que permite identificar a sua autoria, e à sua *integridade*, que permite garantir a inalterabilidade do seu conteúdo" (DIDIER JÚNIOR; BRAGA; OLIVEIRA, 2016, p. 221-222).

Vale destacar que tais parâmetros – autenticidade e integridade – são expressamente previstos pela legislação processual para o registro de atos processuais eletrônicos (art. 195 do Código de Processo Civil[8]) e podem ser estendidos, seja por analogia, seja pela própria finalidade da prova, a todo e qualquer registro eletrônico que se pretenda utilizar com força probante no processo.

A verificação da presença desses requisitos depende estritamente do suporte em que os dados são armazenados, da forma como são produzidos, da finalidade a que se

[6] "Art. 225. As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão."

[7] "Art. 158. Quando a infração deixar vestígios, será indispensável o exame de corpo de delito, direto ou indireto, não podendo supri-lo a confissão do acusado."

[8] "Art. 195. O registro de ato processual eletrônico deverá ser feito em padrões abertos, que atenderão aos requisitos de autenticidade, integridade, temporalidade, não repúdio, conservação e, nos casos que tramitem em segredo de justiça, confidencialidade, observada a infraestrutura de chaves públicas unificada nacionalmente, nos termos da lei."

destinam e, sobretudo, do estado da técnica. O essencial, portanto, é que se tenha sempre presente a sua imprescindibilidade e, em caso de dúvida fundada, haja o recurso à prova pericial para que o exercício da jurisdição não seja induzido em erro por elementos que não tenham aptidão ou idoneidade para retratar a realidade.

Não obstante, algumas diretrizes podem, diante do cenário atual, ser traçadas visando à utilidade imediata e a fundamentar o exame de evoluções futuras, para tanto distinguindo-se entre os instrumentos, que como documentos em sentido estrito comportam a assinatura, em alguma forma, dos que concorrem para a sua formação; e os documentos em sentido amplo, que podem, com maior ou menor concurso das pessoas a que digam respeito, ser captados ou mantidos por terceiros idôneos, ou ainda gerados automaticamente por sistemas de informática.

a. A técnica aplicável aos documentos em sentido estrito e semelhantes

Entendem-se como documentos em sentido estrito os escritos que veiculam declarações, originados portanto em uma pessoa, com uma finalidade própria, que assim se ligam ao respectivo autor. São, por exemplo, os contratos, a correspondência eletrônica, peças processuais etc. Também em função da autoria, a eles se assemelham outros registros textuais que, embora não se prestem a perpetuar a memória de um ato ou fato jurídico, têm por conteúdo a produção humana em um suporte relativamente estável, a exemplo do *software*.

Essa característica comum permite que tais documentos – instrumentos negociais, correspondência, código para operação de computadores ou qualquer equivalente – sejam assinados pelos seus autores, à semelhança do que sucede com os documentos físicos, mas com os atributos próprios da tecnologia, a lhes garantir redobrada segurança quanto à autenticidade e à integridade.

A assinatura digital, tal como hoje reconhecida pela lei, é produto de sofisticada técnica elaborada a partir da criptografia assimétrica, que recebe tal denominação por não se basear em um segredo comum (do qual dois interlocutores se valem para, substituindo um signo por outro, segundo padrão uniforme, ofuscar uma mensagem), como nas raízes históricas da prática.

Em breve resumo, essa forma de criptografia atua a partir de um conjunto de chaves, compostas de uma sequência de caracteres gerada por computador, a partir de elementos aleatórios e fórmulas matemáticas avançadas que viabilizam a sua correlação. Com elas, permite-se que, a partir da chave pública (assim chamada porque passível de ampla divulgação, sem prejuízo à segurança do mecanismo), qualquer pessoa ou dispositivo possa codificar conteúdo que apenas poderá ser decifrado pela chave privada (cuja posse é reservada ao emissor do par), bem como identificar a chave pública associada ao conteúdo codificado com a chave privada, tudo sem ter acesso a ela; por conseguinte, sem poder acessar conteúdo destinado ao seu detentor de forma protegida nem simular a autoria do código cifrado, que se relaciona exclusivamente à chave pública correspondente.

Uma vez aplicada essa espécie de criptografia sobre determinado conteúdo, a alteração de qualquer mínima unidade de informação – um *bit* que seja, ainda que em metadados que não repercutam diretamente no seu teor – torna impossível que a decodificação resulte no que se assinou ou mesmo algo próximo, dada a assimetria das

chaves utilizadas no algoritmo; antes produzindo conteúdo ilegível, no caso de texto, ou inteiramente imprestável, no caso de *software*.

Mais comum, porém, é aplicar a assinatura aos chamados *hashes*, *digests* ou *checksums*, que são produtos de algoritmos capazes de reduzir grandes quantidades de dados a uma sequência menor, usualmente de tamanho determinado, alcançada de modo unidirecional. Ou seja, submetido um conjunto de dados a um determinado algoritmo, que resume fragmentos de conteúdo distintos a uma representação igual, de modo a reduzi-los, resulta uma sequência de caracteres própria para identificar o documento, que não é única, pela própria natureza, mas suficientemente distintiva para evitar confusão ou adulteração em um mesmo contexto. Com isso, vincula-se ao autor do documento o *hash* e, se o documento a conferir produzir o mesmo código, quando submetido ao mesmo algoritmo, ter-se-á a certeza da integridade do conteúdo, isento de qualquer mínima modificação.

Esta visão geral, que não se pretende exaustiva do aspecto técnico pelo próprio escopo do trabalho, permite compreender que, com elevadíssimo grau de confiabilidade, o documento assinado digitalmente, por par de chaves de criptografia assimétrica, ostenta as garantias de autenticidade (porque identificável, pelo par de chaves, o autor da assinatura) e de integridade (porque inalterável o documento sem que a assinatura fique prejudicada).

É importante ter em conta que os pares de chaves podem ser emitidos por qualquer pessoa, em qualquer dispositivo, mas a identidade do seu detentor pode ser verificada pelo próprio interessado, obtendo diretamente a chave pública de seu interlocutor, ou a partir de entidades públicas ou privadas de certificação, que se incumbem de atestar que uma determinada chave pertence a uma dada pessoa. É o que se alcançou, no Brasil, sobretudo para fins oficiais, com a criação pela Infraestrutura de Chaves Públicas Brasileira — ICP-Brasil, disciplinada pela Medida Provisória n.º 2.200-1, de 2001, já antes mencionada.

Delineado o cenário ideal, contudo, surgem ao menos quatro ordens de problemas na aplicação prática.

O primeiro é que a emissão de certificados digitais por autoridades certificadoras integrantes da ICP-Brasil ainda é um mecanismo custoso e normalmente limitado aos âmbitos de obrigatoriedade na interação com órgãos públicos, como na escrituração fiscal de empresas de porte relevante e no processo eletrônico. Não é algo corrente, que se utilize, por exemplo, no trato negocial ou nas relações de consumo, o que limita severamente a sua utilidade cotidiana — e a esse respeito não há muito de que cogitar, no estudo da técnica jurídica.

O segundo problema decorre do primeiro: são correntes outros métodos de autenticação, alguns equivalentes, outros mais singelos; alguns idôneos, outros não.

De um lado, a infraestrutura oficial não esgota as possibilidades, antes coexistindo com o emprego de mecanismos de criptografia assimétrica e de certificação fora do âmbito da ICP-Brasil. Os outros instrumentos não podem ser desprezados, porque da mesma forma propiciam a verificação de autoria (autenticidade) e de conteúdo conforme à expressão do autor (integridade), cabendo apenas ter clareza quanto à finalidade de cada aspecto do mecanismo para lhe assegurar a força probante. Se emitidos os certificados por entidade idônea, valendo-se da mesma tecnologia, ou se os litigantes prescindirem da intermediação, reconhecendo a titularidade das chaves utilizadas na assinatura, ou ainda se por outros

meios se puder provar o uso de um determinado par de chaves por uma pessoa[9], não há por que recusar eficácia probatória ao documento assinado digitalmente, ainda que fora da macroestrutura eleita pelo Estado para negócios oficiais.

De outro lado, é também frequente, para o fim de autenticação, o envio de correspondência a um endereço de correio eletrônico, ou de mensagem de texto (SMS) a uma linha de telefonia móvel, contendo um código a ser fornecido ao prestador de serviços na própria plataforma, com o escopo de provar que o usuário de um determinado sistema é o titular da linha ou o detentor do endereço de e-mail, e assim atestar a autoria do que ele venha a produzir nesse ambiente. Concorre para essa finalidade o registro da origem de um acesso a um serviço ou aplicação, pelo endereço do Protocolo de *Internet* (IP) e pela porta lógica de origem da conexão, que em tese permitiria, pela consulta aos registros do provedor de conexão à *internet*[10], identificar o autor de dado conteúdo. Mesmo no setor público, a Lei n.º 11.419, de 2006, expressamente faculta a assinatura "mediante cadastro de usuário no Poder Judiciário" (art. 1º, § 2º, inc. III, alínea "b"), sem o uso de certificado digital.

Todos esses métodos propiciam, em alguma extensão, a garantia de autenticidade dos documentos – como correspondência entre o autor indicado em uma declaração e o seu efetivo emitente –, mas não preservam, sem outras cautelas, a integridade dos dados, assim entendida a inalterabilidade do conteúdo, para oportuna prova do seu teor oponível ao próprio autor. Não se pode, só por isso, dizer que sejam inidôneos ou inadmissíveis: é apenas necessário ter consciência das suas limitações, para que a valoração da prova não pressuponha uma característica que o documento não reveste.

A conclusão é diversa a respeito de métodos que, espelhando impropriamente a lógica de documentos físicos, não oferecem segurança alguma, a exemplo da reprodução digitalizada de assinatura manuscrita em documento originalmente digital, que alguns rotulam, a nosso juízo equivocadamente, como assinatura eletrônica. Trata-se, na verdade, de mera imagem digital, que pode ser inserida em qualquer documento por quem detenha uma cópia sua, cópia que pode inclusive ser extraída de um documento no qual já aposta, para eventual reprodução em outros. Em alguns casos, com que já deparamos no exercício da jurisdição, chega-se a copiar, junto com a assinatura, o selo de autenticação da firma por notário público em outro documento[11], o que evidentemente caracteriza falsidade, da qual não se pode inferir qualquer efeito jurídico que não o sancionatório da ilegalidade, prejudicando a verificação de autenticidade a que a assinatura se presta, em qualquer meio.

No mais, o derradeiro problema que se anunciou é o emprego inadequado da assinatura digital, mesmo quando produzida por certificado digital. Merecem destaque dois exemplos do manejo equivocado: a ocultação da assinatura, substituída pela verificação em um sítio na internet presumivelmente confiável, e a materialização do documento digital em suporte físico, em especial para juntada aos autos de processo físicos, denominados pela lei de "convencionais" (art. 439 do Código de Processo Civil).

---

[9] A prova indireta é utilizada para esse fim com êxito na ordem jurídica dos Estados Unidos da América, com base na Regra 901(b)(4) da legislação alcunhada de *Federal Rules of Evidence*. A esse respeito, cf. FRIEDEN; MURRAY; LEIGH, 2011, p. 11.

[10] Os conceitos relativos à internet são aqui referidos na terminologia da Lei n.º 12.695, de 2014 (Marco Civil da Internet no Brasil), sem consideração pelo rigor técnico, de modo a evitar confusão desnecessária no âmbito da discussão, em que a lei vige como posta.

[11] TJSP, 4ª Turma Cível e Criminal do Colégio Recursal 52ª Circunscrição Judiciária – Itapecerica da Serra, Recurso Inominado Cível n.º 1003745-98.2018.8.26.0176, rel. Juiz Guilherme de Siqueira Pastore, julgado em 22/02/2019.

No primeiro caso, o documento é mantido em meio digital, mas, ao invés de se manter íntegro, é alterado para que, às suas margens, conste uma observação de que é autêntico e pode ser verificado em determinado endereço, mediante a inserção de um certo código. Isto é, rompe-se a garantia de integridade do documento pela alteração, ainda que automatizada. Em raras situações, preserva-se íntegro o documento, mas ele é exibido dentro de um enquadramento que faz menção à assinatura. Em nenhum caso, porém, o *hash* assinado é repassado ao usuário, que assim não pode conferir pelos próprios meios a validade da assinatura digital. Esse é, por exemplo, o funcionamento do portal e-SAJ, utilizado pelo Tribunal de Justiça de São Paulo, que na averbação adverte que o documento é cópia do original assinado.

Embora compreensíveis as razões de ordem prática que levam a tanto, seja pela maior facilidade proporcionada ao usuário que não tem familiaridade com a tecnologia, seja pela preservação de dados pessoais atrelados à assinatura digital no âmbito da ICP-Brasil, a solução engendrada prejudica a maior vantagem da assinatura digital, de permitir ao destinatário final a autenticação do específico e exato documento que tem consigo, assegurando que foi assinado pelo detentor da chave, e que nenhum erro de sistema possa atestar tal circunstância equivocadamente. Nesse caso, não é a assinatura, mas a confiança no próprio sistema que sustenta a força probante do documento.

Mais perigoso, porém, é o segundo caso, no qual o equívoco consiste em tomar como prova a materialização do documento digital, que, como já se advertiu no início deste texto, é mera cópia, que não se deve preferir ao original, pela possibilidade de adulteração ou perda acidental das suas características. A própria lei contribui para a aplicação errônea da técnica, ao dispor que a utilização do documento depende da sua conversão à forma impressa e determinar a verificação da sua autenticidade.[12]

À vista de todo o exposto até aqui, é elementar que "o valor probante do documento eletrônico deve ser sempre aferido no ambiente em que ele foi gerado" (RINALDI, 2016, p. 638). Desta forma, a única interpretação possível da disposição normativa, que não anula os benefícios da tecnologia na garantia de autenticidade e integridade da prova, é a de que, *ainda que* integrado aos autos físicos, para melhor compreensão do acervo probatório e garantia do contraditório, o documento digital deve ter a sua autenticidade verificada *no meio digital* e assim certificada pelo escrivão, sem prejuízo de permanecer disponível, *no original*, para verificação independente das partes e, se o caso, exame pericial.

Adotadas estas cautelas, o documento digital oferece segurança superior ao seu semelhante físico, não merecendo, portanto, a resistência que inicialmente se lhe opôs. Caso se tomem pelo valor de face, contudo, soluções tecnicamente insustentáveis, o documento digital não conferirá segurança quanto à sua autenticidade e integridade, não merecendo, então, admissão para fins probatórios.

[12] "Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei."

b. Outras informações armazenadas em meio eletrônico

Além dos documentos digitais em sentido estrito, já tratados no tópico anterior, existe um grande volume de outras informações armazenadas eletronicamente[13], de potencial interesse para fins probatórios. Na legislação brasileira, o fundamento normativo que melhor se ajusta ao seu tratamento é o extrato digital de banco de dados, que tem previsão lacônica e pouco utilizada desde a edição do art. 11, § 1º, da Lei n.º 11.419, de 2006[14], e teve sua força probante reiterada pelo art. 425, inc. V, do Código de Processo Civil atualmente em vigor[15].

O banco de dados, no âmbito jurídico, tem sido tratado como uma "compilação de dados, obras e outros materiais organizados de uma maneira sistemática e ordenada, em função de determinados critérios e para finalidades específicas, em condições de serem acessados individualmente por meio eletrônico ou não" (SANTOS, 2005, pp. 321-322), com especial enfoque na proteção de direitos de autor, em conformidade com a Diretiva n.º 96/9/CE, do Parlamento Europeu e do Conselho da União Europeia, e, mais recentemente, sob o ponto de vista da proteção de dados pessoais.

O conceito, porém, é abrangente e alcança também os registros informatizados da Administração Pública, bem como de empresas privadas, com ênfase, pela utilidade, nos dados mantidos por concessionárias de serviços públicos – ou de caráter público, como os "cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres" (art. 43, § 4º, do Código de Proteção e Defesa do Consumidor) –, instituições financeiras e provedores de conexão à *internet* e de aplicação na *internet*, que frequentemente são necessários para o esclarecimento de diversas situações. A corroborar essa percepção, a doutrina destaca a inclusão, no dispositivo legal, do banco de dados privado, sem exigência da presença de autoridade pública na extração da cópia (NEVES, 2016, p. 628).

A manutenção de um banco de dados é complexa e encerra múltiplas funções, de que depende a adequada compreensão do seu valor de prova: primeiro, a produção da informação que dele constará; depois, a efetiva inserção da informação no banco; em seguida, a guarda da informação (o que envolve pessoas físicas ou jurídicas, *software* e *hardware* utilizados no armazenamento dos registros digitais); e, por fim, a extração do conteúdo do banco de dados para qualquer finalidade.

De início, então, sobressai a importância da origem da informação. Caso se trate de reprodução, para fins internos, de conteúdo extraído de outra fonte de prova – como a transcrição do registro em áudio de uma ligação telefônica, ou o resumo de um relatório

[13] Nos Estados Unidos da América, a terminologia empregada é *electronically-stored information (ESI)*, que nos parece adequada para retratar a multiplicidade de formas e meios que a tecnologia propicia, sem prejuízo da sua subsunção à categoria de documentos, em sentido amplo.

[14] "Art. 11. […]
§ 1º Os extratos digitais e os documentos digitalizados e juntados aos autos pelos órgãos da Justiça e seus auxiliares, pelo Ministério Público e seus auxiliares, pelas procuradorias, pelas autoridades policiais, pelas repartições públicas em geral e por advogados públicos e privados têm a mesma força probante dos originais, ressalvada a alegação motivada e fundamentada de adulteração antes ou durante o processo de digitalização."

[15] "Art. 425. Fazem a mesma prova que os originais:
[…]
V – os extratos digitais de bancos de dados públicos e privados, desde que atestado pelo seu emitente, sob as penas da lei, que as informações conferem com o que consta na origem".

elaborado em meio físico –, o extrato digital do banco de dados não poderá suprir a fonte de prova direta, porque de tal modo violada a própria garantia de autenticidade da informação, uma vez rompida a sua vinculação ao seu autor. Ressalva-se, neste particular, a presunção de legitimidade dos atos administrativos, que pode, porém, ser desconstituída diante de prova em contrário, e não desobriga a Administração, em caso de impugnação fundada, de apresentar o suporte documental do que inscreveu nos seus assentos.

Caso, todavia, se trate de informações produzidas em meio exclusivamente eletrônico, assim as inseridas pelo preenchimento de um formulário digital, que têm possibilidade de vinculação ao seu autor, como aquelas resultantes de escrituração eletrônica de transações financeiras, ou mesmo geradas automaticamente por sistemas informatizados, para registro da sua utilização ou em função dela – desde ligações telefônicas, troca de mensagens, acesso a aplicações na *internet*, até dados de localização obtidos de dispositivos móveis utilizados no acesso etc. –, não haverá outro meio de prova possível e a informação deverá ser necessariamente extraída do banco de dados digital.

Em tal situação, pode haver dúvida fundada a respeito da fidelidade da informação contida no banco de dados, sendo então necessário o esclarecimento pelo responsável pela base de dados quanto ao seu funcionamento e, assim, quanto ao crédito que possam merecer os dados por meio dele obtidos.

Essa premissa é aplicável aos históricos de utilização de sistemas informáticos, denominados *logs*, que já foram considerados "registros digitais potencialmente adulteráveis, passíveis de erros gerados pelo sistema que os produz, como ocorre com qualquer sistema informático" (MARCACINI, 2015, p. 471). De fato, o Marco Civil da Internet no Brasil, embora tenha disciplinado a requisição de dados aos provedores de conexão e aplicação, não cuidou da confiabilidade desses dados e, *potencialmente*, as assertivas que embasam a crítica doutrinária são verdadeiras, como também em relação a qualquer documento eletrônico, sem que implementadas formas de garantia do seu conteúdo. Nada impede, porém, que na produção da prova se previnam tais riscos, seja com a declaração do emitente, expressamente prevista no art. 425, inc. V, do Código de Processo Civil, seja por meio de prova pericial, a persistir a dúvida.

No direito estrangeiro, a título exemplificativo e sem pretensão comparatística, encontra-se a prestigiada solução adotada no caso *Lorraine v. Markel American Insurance Co.* em respeitada decisão singular de juiz de instrução (*magistrate judge*), de se exigir prova testemunhal, a respeito da criação, aquisição, manutenção, preservação e extração da informação armazenada em meio digital, inclusive, se o caso, quanto ao funcionamento específico de *software* e *hardware*, a fim de garantir que o sistema tenha adequados mecanismos de segurança; sem prejuízo do exame de metadados, do procedimento adequado para extração dos dados e do reconhecimento do extrato pela testemunha (FRIEDEN; MURRAY; LEIGH, 2011).

O precedente estrangeiro também reforça, em linha com o que se afirmou a respeito das funções relacionadas ao banco de dados, que a fidedignidade da informação original não garante que o seu transporte para o processo conserve os mesmos atributos. É disso que se trata quando a lei exige o atestado, pelo emitente, que as informações conferem com o que consta na origem (art. 425, inc. V, do Código de Processo Civil), sujeitando-o assim a responsabilidade penal e civil, sem prejuízo da impugnação do documento em arguição de falsidade (NERY JÚNIOR; NERY, 2018, p. 1209).

Tão relevante é a responsabilidade pela extração dos dados digitais que o tema recebeu, em outras ordens jurídicas, tratamento mais minucioso, a exemplo da alteração, em 2008, da legislação italiana, na esteira da Convenção sobre o Cibercrime, firmada em Budapeste (CONSELHO DA EUROPA, 2001), a fim de que o *codice di procedura penale* (ITÁLIA, 1988) passasse a exigir a conformidade dos dados extraídos aos respectivos originais e também a sua inalterabilidade[16].

A extração do banco de dados, em suma, é um processo: implica o acesso a um sistema de informática, com controles de permissões, e o adequado manejo de ferramentas previamente instaladas para que se possa chegar a determinado conteúdo, que deve então ser transportado para suporte adequado, com a garantia do responsável pela extração quanto à conformidade com o original, que é a própria base de dados digital.

A prática forense, no entanto, tem se mostrado aquém até mesmo dos rasos parâmetros traçados pela legislação brasileira. São frequentemente juntadas aos autos, como documento ou mesmo em reprodução de baixa qualidade no corpo dos arrazoados, imagens de telas de computador, em que aparentemente se contém um registro informatizado, mas sem nenhum esclarecimento sobre a criação e guarda dos dados, sobre o método de acesso ao banco de dados nem a responsabilidade por essa atividade.

Fica inteiramente prejudicada, dessa forma, a eficácia probatória do banco de dados digital, porque não se pode garantir que a informação é confiável na origem, tampouco que o que foi reproduzido nos autos corresponde ao que consta na origem (autenticidade), sem possibilidade de alteração desde a extração (integridade).

A produção adequada dessa prova pode se dar, por expressa previsão legal, mediante atestado do responsável pela extração dos dados, que pressupõe também a devida justificação sobre os meios utilizados para tanto; ou, por cautela, pela extração dos dados acompanhada por notário e descrita em ata notarial. Pode ainda, na pendência de controvérsia fundada, ensejar exame pericial, a que não se poderão opor restrições de acesso, irrelevante a qualidade dos dados armazenados e o vulto dos sistemas envolvidos, se necessário ao esclarecimento a respeito dos meios de criação e guarda das informações.

c. O caso especial da obtenção forçosa das informações

Um último registro é pertinente, a respeito das informações armazenadas em meio eletrônico que podem, além das hipóteses de oferecimento de extratos digitais com certificação de autenticidade, ser obtidas forçosamente, sobretudo em procedimentos criminais, a partir de dispositivos apreendidos no curso de uma investigação penal, ou do recolhimento de conjuntos de informações obtidas por meio de provedores de aplicação.

Também neste particular a prática forense frequentemente se situa aquém do necessário a atender à natureza e da finalidade da prova digital, podendo-se observar, não raro, a juntada aos autos de meras fotografias de dispositivos eletrônicos, a fim de

[16] "Art. 254-bis. Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. 1. L'autorita' giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, puo' stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformita' dei dati acquisiti a quelli originali e la loro immodificabilita'. In questo caso e', comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali."

retratar conteúdo ilícito em si mesmo (a exemplo de pornografia infantil) ou reproduzir outras imagens armazenadas, que documentem fatos pertinentes à prática criminosa; além de históricos de comunicação (com tratativas entre criminosos a respeito dos delitos investigados).

Ocorre que a reprodução fotográfica, como já anotado, constitui prova do objeto reproduzido, mesmo no âmbito civil, apenas até que haja impugnação (art. 225 do Código Civil), considerando que a mediação pode implicar prejuízo à sua conformidade com o original (autenticidade); e, por considerações semelhantes, não pode ser tida, em princípio, como prova suficiente no âmbito criminal, sem que se proceda ao exame pericial do corpo de delito, tal como preceituado pelo art. 158 do Código de Processo Penal.

Essa abordagem, ademais, subestima gravemente a riquíssima gama de informações que o exame pericial bem realizado pode fornecer, relativas à utilização do dispositivo, à sua geolocalização etc., além das vicissitudes originadas na complexidade da microinformática atual, que permite a eliminação remota do conteúdo de dispositivos eletrônicos sem nenhum preparo especial, desde que conectados à *internet*, ou ativar criptografia capaz de torná-los indevassáveis às autoridades públicas, mesmo tendo à sua disposição técnicas avançadas e vasto poder computacional.

Essas situações são mencionadas apenas exemplificativamente, porque as possibilidades e dificuldades relacionadas à atividade pericial são muitas e cabem a estudo de maior profundidade técnica, no âmbito da informática, excedentes da proposta deste artigo; mas dos exemplos já é possível inferir que a produção da prova digital "não se compraz com os velhos métodos de busca que se realizavam (e continuam a realizar) na descoberta de provas de outros tipos de criminalidade" (RAMOS, 2014, cap. 2.3), podendo o descuido com a técnica inviabilizar a confirmação da autenticidade e da integridade das informações com repercussão probatória.

Esta a questão central: não há técnica única ou estanque para o exame pericial de uma infinidade de dispositivos com características próprias, mas, a despeito do concurso de técnico para a realização do exame, é sempre possível ao julgador e às partes do processo zelar pela garantia de autenticidade e integridade das informações submetidas ao exame do perito, controlando os métodos empregados para tal fim.

A modificabilidade inerente aos meios de armazenamento digitais, se não devidamente acautelada por meios justificadamente suficientes, expõe o conteúdo de interesse probatório, em tese, ao acréscimo, à supressão e à alteração, com aptidão para conduzir à conclusão de que o material apreendido não se relaciona ao detentor do equipamento ou do titular da conta em determinado serviço *online* (falta de autenticidade), ou mesmo de que o material, conquanto original, possa ter sofrido alteração proposital, seja de grande extensão, em prejuízo do contexto, ou pontual, com a inclusão em um acervo aparentemente autêntico de informações inverídicas, anulando assim a sua força probante, por falta de integridade.

Independentemente da solução técnica a ser adotada em cada caso, tal precaução somente tem valor se a posse do material for restrita a pessoas idôneas e desinteressadas no resultado da investigação, demonstrando-se tal circunstância por fiel registro documental, complementado por testemunhas, se necessário, anotando-se o uso de lacres, transporte e acondicionamento. É o que se chama, no direito estrangeiro, de cadeia de custódia (*chain of custody*), também identificada na célebre decisão do já citado caso

Lorraine v. Markel American Insurance Co. como pressuposto elementar da admissibilidade da prova digital (RASHBAUM; KNOUFF; MURRAY, 2012, p. 4).

A prova pericial não subtrai, portanto, ao julgador o conhecimento dos meios de investigação e da validade da prova, cabendo às partes e ao juiz zelar diretamente, sem embargo do concurso de auxiliar eventual, pela validade da prova digital, que depende de que sejam garantidos, desde a colheita até valoração, os atributos da autenticidade e da integridade.

5. Conclusão

Pela exposição contida nos tópicos precedentes, pretendeu-se demonstrar que a tecnologia abriu caminho, antes mesmo da disciplina legislativa, para a atividade probatória em meio eletrônico, considerando que a prova é um dos grandes pontos de contato entre o processo e a realidade exterior, cuja evolução necessariamente acompanha. Essa antecipação foi possível porque, a despeito das peculiaridades do suporte digital, as informações armazenadas em meio eletrônico guardam com os documentos, em sentido amplo, identidade de conteúdos e finalidades.

O suporte digital, por si só, permite a alteração irrestrita e indetectável das informações nele armazenadas, mas, paradoxalmente, oferece, na presença de determinadas cautelas, garantias de autenticidade e integridade superiores às que o suporte físico jamais foi capaz de propiciar. Essa contradição enseja a oscilação da doutrina e da prática forense entre extremos, desde a absoluta desconfiança e prevenção em relação ao meio, até a confiança excessiva, desatenta aos atributos de cada específica fonte de prova.

A proposição que se extrai dessas premissas é de que a produção de prova digital depende, quando indisponíveis os direitos em litígio, inclusive no processo criminal, ou quando impugnada a reprodução, de escorreita demonstração de autenticidade e integridade, a ser assegurada por meios técnicos adequados, sob pena de o elemento de prova obtido de fonte digital não carregar eficácia probatória.

Tais meios não se restringem à previsão legal de assinatura digital de documentos eletrônicos, com o uso de certificado emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, mas alcançam também quaisquer outros mecanismos que, pelo uso adequado da tecnologia, possam garantir, ainda que parcialmente, os mesmos atributos; excluídos, porém, os esforços que nada garantem quanto à autenticidade e integridade e se relacionam ao desconhecimento da prova digital, como a reprodução digitalizada de assinaturas manuscritas em documentos eletrônicos.

No específico caso dos extratos digitais de bancos de dados, além da atenção à formação do seu conteúdo na origem, a garantia de autenticidade e integridade depende de procedimento documentado de extração, que pode ser atestado pelo emitente, sob pena de responsabilidade civil e criminal, ou fiscalizado por delegado do serviço notarial, em ata própria; não se admitindo, contudo, imagens digitais coligidas sem nenhuma explicação, cuidado ou segurança, como tem sido recorrente na prática forense.

Por fim, em relação à fonte de prova que não escape à necessidade da técnica pericial para a sua produção, de que se destacam os materiais apreendidos no curso de investigação, é inafastável o controle jurisdicional da atividade do perito, de modo a garantir a autenticidade e a integridade, pela supervisão da técnica empregada e pela

observação da cadeia de custódia, a fim de que o manejo do material com fins probatórios seja reservado a pessoas idôneas e desinteressadas no resultado da prova.

Referências

BRASIL. *Decreto-Lei n.º 3.689, de 3 de outubro de 1941*. Código de Processo Penal. Brasília, DF: 1941. Disponível em: http://bit.ly/30xq6z6. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 5.869, de 11 de janeiro de 1973*. Institui o Código de Processo Civil. Brasília, DF: 1973. Disponível em: http://bit.ly/2RpgtP7. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 8.078, de 11 de setembro de 1990*. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: 1990. Disponível em: http://bit.ly/2R70Vkd. Acesso em: 27 set. 2019.

BRASIL. *Emenda constitucional n.º 32, de 11 de setembro de 2001*. Altera dispositivos dos arts. 48, 57, 61, 62, 64, 66, 84, 88 e 246 da Constituição Federal, e dá outras providências. Brasília, DF: 2001. Disponível em: http://bit.ly/2ud8LPS. Acesso em: 27 set. 2019.

BRASIL. *Medida provisória n.º 2.200-2, de 24 de agosto de 2001*. Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Brasília, DF: 2001. Disponível em: http://bit.ly/2RuS5eG. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 10.406, de 10 de janeiro de 2002*. Institui o Código Civil. Brasília, DF: 2002. Disponível em: http://bit.ly/389l1jk. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 11.419, de 19 de dezembro de 2006*. Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências. Brasília, DF: 2006. Disponível em: http://bit.ly/38lABIN. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: 2014. Disponível em: http://bit.ly/2Nz5KAA. Acesso em: 27 set. 2019.

BRASIL. *Lei n.º 13.105, de 16 de março de 2015*. Código de Processo Civil. Brasília, DF: 2015. Disponível em: http://bit.ly/3738LR7. Acesso em: 27 set. 2019.

CABRAL, Antonio do Passo. A eficácia probatória das mensagens eletrônicas. *Revista de Processo*, São Paulo, v. 31, n. 135, p. 97-131, 2006.

CONSELHO DA EUROPA. *Convention on cybercrime*: ETS no. 185. Estrasburgo: Council of Europe, 2001. Disponível em: http://bit.ly/38iC7eF. Acesso em: 27 set. 2019.

CONSELHO DA UNIÃO EUROPEIA. Parlamento Europeu. *Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de março de 1996, relativa à protecção jurídica das bases de dados*. Disponível em: http://bit.ly/2uUBJ7C. Acesso em: 27 set. 2019.

DIDIER JÚNIOR, Fredie; BRAGA, Paula Sarno; OLIVEIRA, Rafael Alexandria de. *Curso de direito processual civil*. 11. ed. Salvador: Jus Podivm, 2016. v. 2.

DINAMARCO, Cândido Rangel. *Instituições de direito processual civil*. 7. ed. São Paulo: Malheiros, 2017. v. 3.

FRIEDEN, Jonathan D.; MURRAY, LEIGH M. The admissibility of electronic evidence under the Federal Rules of Evidence. *Richmond Journal of Law and Technology*, Richmond, v. 17, n. 2, p. 1-40, 2011.

GOMES FILHO, Antonio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). *In*: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (coord.). *Estudos em homenagem à professora Ada Pellegrini Grinover*. São Paulo: DPJ, 2005.

GOODE, Steven. The admissibility of electronic evidence. *The Review of Litigation*, Austin, v. 29, n. 1, p. 1-64, 2009.

ITÁLIA. *Decreto del Presidente dela Repubblica 22 settembre 1988, n. 447*. Approvazione del codice di procedura penale. Roma: 1988. Disponível em: http://bit.ly/30xJz32. Acesso em: 27 set. 2019.

MARCACINI, Augusto Tavares Rosa. O documento eletrônico como meio de prova. *Revista de Direito Imobiliário*, São Paulo, v. 22, n. 47, p. 70-101, 1999.

MARCACINI. Provas digitais: limites constitucionais e o Marco Civil da Internet. *In*: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & internet III*. São Paulo: Quartier Latin, 2015. t. 2.

MARINONI, Luiz Guilherme; ARENHART, Sérgio Cruz. *Prova*. 2. ed. São Paulo: Revista dos Tribunais, 2011.

NEVES, Daniel Amorim Assumpção. Da produção da prova documental (arts. 434 a 438). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). *Comentários ao novo Código de Processo Civil*. 2. ed. Rio de Janeiro: Forense, 2016.

RAMOS, Armando Dias. *A prova digital em processo penal*: o correio eletrônico. Lisboa: Chiado, 2014.

RASHBAUM, Kenneth N.; KNOUFF, Matthew F.; MURRAY, Dominique. Admissibility of non-U.S. electronic evidence. *Richmond Journal of Law and Technology*, Richmond, v. 18, n. 3, p. 1-76, 2012.

RINALDI, Luciano. Dos documentos eletrônicos (arts. 439 a 441). *In*: CABRAL, Antonio do Passo; CRAMER, Ronaldo (coord.). *Comentários ao novo Código de Processo Civil*. 2. ed. Rio de Janeiro: Forense, 2016.

SANTOS, Manoel J. Pereira dos. Considerações iniciais sobre a proteção jurídica das bases de dados. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito & internet*: aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005. v. 1.

Como as plataformas digitais podem promover a desjudicialização: o caso do consumidor.gov

Isabela Maiolino[1]
Assessora técnica do secretário nacional do consumidor

Luciano Benetti Timm[2]
Secretário nacional do consumidor no Ministério da Justiça e Segurança Pública

Resumo: A estabilização política e monetária dos últimos 30 anos foi responsável por promover uma intensificação nas relações de consumo, o que ocasionou, adicionado a outros fatores, também, um aumento dos litígios consumeristas. Tendo em vista o alto grau de judicialização no Brasil, faz-se necessário encontrar novas formas de diminuir o número de ações que ingressam no judiciário, sem com isso precarizar o acesso à justiça, fazendo uso da tecnologia como aliada nesse movimento. Assim, este artigo expõe um panorama de como as plataformas digitais podem promover a desjudicialização, tratando, com ênfase, do caso da justiça brasileira e da plataforma digital governamental "consumidor.gov.br".

Palavras-chave: plataformas digitais. direito do consumidor. desjudicialização.

Abstract: Political and monetary stabilization over the last 30 years is responsible for intensifying consumer relations, which caused, among other factors, an increase in consumer disputes. In view of the high degree of use of judicial actions in Brazil, it is necessary to find new ways to reduce the number of actions that enter the judicial system, making use of technology as an ally in this movement. Therefore, this paper presents an overview of how digital platforms can promote dejudicialization, dealing, specifically, with the case of Brazilian justice and the governmental digital platform "consumer.gov.br".

Keywords: digital platforms. consumer law. dejudicialization.

[1] Mestranda na Faculdade de Direito da Universidade de Brasília (UnB). Bacharela em Direito pelo Instituto Brasiliense de Direito Público.

[2] Doutor em Direito pela Universidade Federal do Rio Grande do Sul (2004). Mestre (1997) e Bacharel (1994) em Direito pela PUC-RS. Cursou Master of Laws (LL.M.) na Universidade de Warwick (Inglaterra) e realizou pesquisa de Pós-Doutorado na Universidade da Califórnia, Berkeley (Estados Unidos). É professor da UNISINOS, da FGV-SP e do CEDES, professor convidado da AJURIS e da EMAGIS, e professor visitante do PPGD da USP.

1. Introdução

No contexto na indústria 4.0[3], as empresas mais valiosas do mundo são aquelas que atuam com tecnologia[4], o que demonstra uma clara mudança de tendência do mercado, agora ainda mais sensível às inovações tecnológicas (ditas "disruptivas"). Exemplo disso é que a maior empresa de transporte de passageiros (Uber) não possui carros, as mídias digitais mais utilizadas (Facebook e Twitter) não criam conteúdo, a empresa varejista mais valiosa do mundo (Alibaba) não tem estoque, e um dos grandes provedores de acomodações do mundo (Airbnb) não possui propriedades[5]. Nesse cenário de concorrência mais acirrada, criam-se incentivos para que empresas passem a buscar resolver litígios dentro de plataformas próprias digitais de solução de disputas (sendo a da eBbay a mais conhecida).

Essa nova realidade promove a globalização da informação e a potencialização de formas diversas de consumo (sobretudo por meios digitais), devendo o Estado acompanhar essa evolução tecnológica a fim de garantir o bom funcionamento do mercado e a segurança e transparência nas relações consumeristas (FERNANDES; SIMÃO FILHO; 2015).

Tendo em vista o alto grau de judicialização em que o Brasil se encontra e o alto custo de manutenção do sistema judiciário nacional, conforme dados do Conselho Nacional de Justiça (CNJ), é primordial que se busquem novos modelos que promovam a desjudicialização e métodos alternativos de resolução de conflitos[6], priorizando o uso de ferramentas digitais.

O presente artigo mostrará como essa nova realidade altera os cenários da nossa sociedade atual, especificamente no que diz respeito ao tratamento dado aos litígios no Brasil. No caso, será demonstrado como as plataformas digitais podem promover a desjudicialização das lides consumeristas por meio do "consumidor.gov.br", garantindo um "acesso à ordem jurídica justa"[7].

O primeiro tópico tratará das plataformas digitais, do contexto judicial brasileiro e do nível de judicialização no qual nos encontramos. Subsequentemente, tratar-se-á de como as plataformas digitais podem alterar o mundo jurídico, passando-se, em seguida, para um tópico específico sobre o caso da plataforma brasileira "consumidor.gov.br". Por fim, serão apresentadas as conclusões do trabalho.

2. Plataformas digitais de solução de disputas ("ODR")

Muito embora não exista consenso em relação ao conceito de plataformas digitais, é possível encontrar pontos e aspectos em comum elencados pela doutrina. Tais aspectos

[3] Costuma-se chamar de "indústria 4.0" a quarta revolução industrial, caracterizada por um conjunto de tecnologias que permitem a fusão do mundo físico, digital e biológico. As principais tecnologias que permitem essa fusão são a manufatura aditiva, a inteligência artificial, a internet das coisas, a biologia sintética e os sistemas ciber-físicos (SCHWAB, 2016).

[4] De acordo com a Brand Finance Global 500, as cinco empresas mais valiosas são: 1 – Amazon; 2 – Apple; 3 – Google; 4 – Microsoft; 5-Samsung (BRAND FINANCE, 2019).

[5] Essa declaração tem sido incluída em diversas publicações sobre plataformas digitais, mas sem indicação de autoria específica.

[6] Conforme explica Marcelo Cabral (2012), "Meios alternativos de resolução de conflitos – MARC – é a denominação mais utilizada no tratamento dos mecanismos que permitem a obtenção da resolução de um conflito à margem da via jurisdiciona1, expressão que decorre da tradução do termo mais recorrente na doutrina internacional para seu tratamento: ADR – Alternative Dispute Resolution".

[7] Richard Ross (2002, p. 637-684) explica de forma teórica como as plataformas podem promover a desjudicialização.

incluem o uso da informação e da tecnologia de comunicação com o objetivo de facilitar a interação entre os seus usuários, o armazenamento e o uso de informações sobre essas interações e o efeito de rede, além de promover a inovação (ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, 2019).

Não há, ao menos no Brasil, regulação específica para esse tipo de plataforma – o que não é, necessariamente, um problema, já que a legislação poderia tornar-se obsoleta em razão das rápidas mudanças tecnológicas. Nesse sentido, explica David Friedman (2001, p. 71) que a lei é afetada pela mudança tecnológica de pelo menos três maneiras. Primeiro, há uma alteração no custo de violação ou imposição de normas. Segundo, ocorrem alterações dos fatos que justificam essas mesmas regras. E terceiro, há uma mudança dos fatos assumidos pela lei, o que pode tornar obsoletas as categorias legais existentes, ou até mesmo sem sentido. Uma alternativa nesse cenário é a alteração legislativa seletiva, ou então interpretação judicial[8].

Os meios alternativos de solução de disputas não poderiam ficar alheios a essa transformação promovida pelas tecnologias no que se refere às plataformas (LIMA, 2019, p. 76), surgindo, assim, o modelo de *online dispute resolution* (ODR) (LIMA; FEITOSA, 2016, p. 54), que "podem ser definidos como a transposição de métodos adequados para plataformas" (LIMA, 2019, p. 77). Esse modelo pode abranger várias técnicas de modelos alternativos de solução de disputas, ao mesmo tempo que se utiliza de uma rede como local virtual para resolver disputas (BECKER; LAMEIRÃO, 2017, p. 1).

De acordo com a doutrina, existem quatro modalidades de ODR: (i) sistema de reivindicação financeira; (ii) sistema de arbitragem online; (iii) serviços de Ombudsman; e (iv) sistema de mediação online, seja ela automatizada ou assistida (NASCIMENTO JUNIOR, 2017, p. 274). Trataremos desta última modalidade nos próximos tópicos, especificamente da plataforma governamental "consumidor.gov.br" e sobre como ela pode promover a desjudicialização na resolução de conflitos. Conforme explica Richard Ross (2002, p. 641-642, tradução nossa):

> *As culturas jurídicas eletrônicas gravitarão para a resolução alternativa de disputas, com seu compromisso de considerar uma ampla gama de informações sobre o contexto. Além disso, a tendência da impressão estável em direção ao conhecimento eletrônico mutável prejudicará a valorização cultural da lei e, portanto, do tribunal, como meio de resolver disputas*[9].

Antes de adentrar na plataforma brasileira, veremos, no tópico subsequente, o atual cenário da justiça brasileira.

[8] No original: "Technological change affects the law in at least three ways: (1) by altering the cost of violating and enforcing existing legal rules; (2) by altering the underlying facts that justify legal rules; and (3) by changing the underlying facts implicitly assumed by the law, making existing legal concepts and categories obsolete, even meaningless. The legal system can choose to ignore such changes. Alternatively, it may selectively alter its rules legislatively or via judicial interpretation". (FRIEDMAN, 2001, p. 71).

[9] No original: "Electronic legal cultures will gravitate toward alternative dispute resolution, with its commitment to considering a broad range of information about context. In addition, the drift from stable print toward mutable electronic knowledge will undermine the cultural valorization of law, and therefore of the court, as a means of resolving disputes" (ROSS; 2002, p. 641-642).

3. Contexto da justiça brasileira

De acordo com o CNJ, o ano de 2017 terminou com 80,1 milhões de processos judiciais em tramitação, ou seja, aguardando solução definitiva, com uma taxa de congestionamento (percentual de processos que ficaram represados sem solução, comparativamente ao total tramitado no período de um ano) de 70% (CNJ, 2018, p. 197). Isso significa que, a cada dez ações judiciais que tramitaram, sete continuaram tramitando sem decisão final.

Além disso, os dados do CNJ demonstram que a quantidade de novas ações tem aumentado gradativamente ano após ano. Enquanto em 2009 houve o ajuizamento de 24,6 milhões, em 2016 foram ajuizados 29,4 milhões de novos processos. De 2009 a 2016 também houve o aumento do número de casos pendentes de decisão final – ou seja, não só a quantidade de novos conflitos judicializados, mas há um incremento, também, do estoque de processos judiciais pendentes de julgamento (LIMA, 2019, p. 19).

Várias causas são apontadas como motivadoras do aumento do número de processos no Brasil. Daniel Lima (2019, p. 20) condensou os diversos argumentos em cinco grandes grupos:

> *Diversos são os motivos apontados como causas que contribuem para o aumento exponencial do número de processos judiciais no Brasil. Embora pesquisadores do Direito possam apontar inúmeros deles, diretos e indiretos, não há dúvidas de que contribuem para esse crescimento (1) a dificuldade de efetivação dos direitos e garantias constantes da Constituição, (2) a atual pluralidade e complexidade das relações sociais, 3) determinadas facilidades no acesso à jurisdição e a (4) crescente prática de judicialização da política. Uma das principais causas, todavia, é (5) o modo de agir dos operadores do Direito e jurisdicionados, os quais acreditam que o processo judicial é o único caminho para resolução das contendas.*

No que se refere a despesas, o judiciário teve um custo total de 90,8 bilhões de reais, chegando a R$ 437,47 (quatrocentos e trinta e sete reais e setenta e quarenta e sete centavos) por habitante, R$ 15,20 (quinze reais e vinte centavos) a mais do que no ano anterior. Nesse sentido, o Brasil está em primeiro lugar, dentre diversos países, no que diz respeito ao custo da justiça, que alcança 1,4% do Produto Interno Bruto (PIB), ou 2,6% dos gastos totais da União, dos estados, do Distrito Federal e dos municípios (CNJ, 2018).

Além disso, o custo médio de um processo no Brasil, por ano, é de R$ 1.899,32 (um mil, oitocentos e noventa e nove reais e trinta e dois centavos) em caso de processos estaduais, e de R$ 2.755,24 (dois mil, setecentos e cinquenta e cinco reais e vinte e quatro centavos) em caso de processos que tramitam na Justiça Federal (CNJ, 2018).

Ademais, a média de duração de processos costuma ser de três a quatro anos, para os juizados especiais, e de cerca de quatro a cinco anos para a Justiça Comum, sendo a fase de execução da sentença no âmbito da Justiça Federal o maior gargalo, com uma média de sete anos e onze meses para finalização do processo (CNJ, 2018).

Especificamente sobre ações consumeristas, o assunto mais demandado no juizado especial, em 2017, foi o da "responsabilidade do fornecedor e direito a indenização por dano moral", representando 15,15% das ações, atingindo o número de 1.234.983

(um milhão, duzentos e trinta e quatro mil, novecentos e oitenta e três) de processos somente em 2017, sem contar a fase recursal ou de execução.

Nota-se que parte considerável desses processos envolve ações referentes a direitos do consumidor. Assim, podemos concluir, sem prejuízo de análises mais profundas e detalhadas, que os direitos dos consumidores não estão sendo nem adequadamente garantidos pelos reguladores nem respeitados de modo sistemático no mercado – caso contrário, não haveria um alto número de ações judiciais a respeito de danos morais.

Adicionalmente, pode-se concluir que o custo para garantir o cumprimento de uma lei não espontaneamente respeitada no mercado, quando se vai ao Poder Judiciário, é substancial para contribuintes e consumidores (sem contar que, certamente, alguns litigantes estratégicos fazem um uso predatório da Justiça).

Nesse sentido, cabe mencionar o posicionamento de Hofmann, Katzenbach e Gollatz (2017, p. 1406-1423, tradução nossa), que mostram que os modelos de comando-controle, aqui entendidos como os processos judiciais, tendem a se tornar ultrapassados:

> *O conceito de governança reflete um amplo entendimento dos processos de ordenação que transcendem as ações dos governos (Rosenau e Czempiel, 1992). Modelos de comando-e-controle centrados no Estado têm sido considerados ultrapassados e incapazes de explicar as complexas interações entre o Estado e a sociedade (Mayntz, 2003; Jessop, 2003). A perspectiva de governança tem destacado regimes e racionalidades pluricêntricas, cooperação e competição, novos sites e ferramentas de ordenação. O estado não é mais entendido como o "centro de controle da sociedade" (Mayntz, 2003: 29), mas como um ator entre outros. Como resultado, as fronteiras entre legisladores e tomadores de regras estão se tornando embaçadas. Leis brandas, como acordos informais, memorandos de entendimento, códigos de conduta, mas também padrões técnicos e outras formas de especialização, tornaram-se proeminentes na literatura de governança (Feick e Werle, 2010: 525)*[10].

Surge, aí, a importância de mecanismos que promovam a desjudicialização através de plataformas digitais, pois é necessário pensar "em ferramentas que garantam um cumprimento espontâneo maior dos direitos do consumidor e que, em caso de eventuais disputas, existam ferramentas mais baratas para resolvê-las em tempo e modo devido" (TIMM, 2019).

Os tópicos subsequentes tratarão do assunto, após uma breve introdução acerca do Sistema Nacional de Defesa do Consumidor.

[10] No original: "The concept of governance reflects a broad understanding of ordering processes transcending the actions of governments (Rosenau and Czempiel, 1992). State-centric models of command-and-control have been deemed outdated and incapable of accounting for the complex interactions between state and society (Mayntz, 2003; Jessop, 2003). The governance perspective has highlighted pluricentric regimes and rationalities, cooperation and competition, new sites and tools of ordering. The state is no longer understood as the 'control centre of society' (Mayntz, 2003: 29) but as one actor among others. As a result, the boundaries between rule-makers and rule-takers are becoming blurry. Soft laws such as informal agreements, memorandum of understandings, codes of conducts but also technical standards and other forms of expertise have become prominent in the governance literature (Feick and Werle, 2010: 525)" (HOFMANN; KATZENBACH; GOLLATZ, 2017, p. 1406-1423).

4. O Sistema Nacional de Defesa do Consumidor

A defesa do consumidor está prevista como direito fundamental na Constituição Federal de 1988[11], sendo a principal legislação de defesa do consumidor brasileira o Código de Defesa do Consumidor (Lei nº 8.078/1990).

Para as políticas públicas de defesa do consumidor, podem-se destacar dois instrumentos: a política nacional das relações de consumo, que estabelece diretrizes para a defesa do consumidor e cria instrumentos para sua execução – em especial órgãos oficiais e incentivos à criação e desenvolvimento de associações civis – e o Sistema Nacional de Defesa do Consumidor (SNDC). Para fins de estudo, focaremos apenas no SNDC.

O SNDC está regulamentado pelo Decreto Presidencial nº 2.181, de 20 de março de 1997, e congrega Procons, Ministério Público, Defensoria Pública, Delegacias de Defesa do Consumidor, Juizados Especiais Cíveis e Organizações Civis de defesa do consumidor, que atuam de forma articulada e integrada com a Secretaria Nacional do Consumidor (Senacon).

Os órgãos do SNDC têm competência concorrente e atuam de forma complementar para receber denúncias, apurar irregularidades e promover proteção e defesa dos consumidores.

A Senacon, por sua vez, tem por atribuição legal a coordenação do SNDC e está voltada à análise de questões que tenham repercussão nacional e interesse geral, além do planejamento, elaboração, coordenação e execução da Política Nacional de Defesa do Consumidor. Além disso, a Senacon é o órgão responsável pelo "consumidor.gov.br" e também gerencia o sistema "Sindec" de coleta de dados dos Procons estaduais e municipais e publica anualmente o relatório "consumidor em números" nele baseados.

5. Como as plataformas digitais podem promover mudanças nesse cenário: o caso do consumidor.gov.br

A solução de problemas de consumo de maneira individual e presencial é, em regra, de competência dos órgãos de defesa do consumidor estaduais e municipais – os Procons. Esses órgãos também são responsáveis pela política estadual de defesa do consumidor e por fiscalizar as relações de consumo. Ou seja, têm competência para atuar em nível tático e operacional. A Senacon, por sua vez, é responsável pelo desenho das políticas públicas nacionais e por ações que envolvam o território nacional.

Com as redes sociais e a massificação da conexão móvel, as pessoas passaram a viver conectadas, e essa realidade fez surgir um novo consumidor, que tem mais autonomia, pois tem acesso a uma grande diversidade de informações; que é engajado, pois sabe que essa atitude lhe dá poder; que é social, porque pensa no impacto coletivo e tem as redes sociais como principal plataforma de interação; que precisa da troca, pois acredita que um mundo melhor é um mundo onde as relações são uma via de mão dupla; e que quer a verdade, porque a transparência é um dos seus maiores valores.

Esse cenário fez com que parte dos consumidores não quisessem mais participar do modelo que, até então, era o tradicional de atendimento. Assim, ao não procurar os

[11] Constituição Federal de 1988, art. 5º, inciso XXXII – o Estado promoverá, na forma da lei, a defesa do consumidor.

meios formais de reclamação, tais consumidores demonstravam um descontentamento com o serviço público prestado.

Tendo em vista a atual situação da justiça brasileira e a insustentabilidade do modelo vigente para o tratamento de conflitos de consumo que são levados aos órgãos do Estado, o novo Código de Processo Civil incentiva o uso de meios autocompositivos para solução de conflitos[12]. Além disso, o próprio CNJ possui resolução sobre a política judiciária nacional de tratamento adequado dos conflitos (CNJ, 2010)[13] e do crescimento das plataformas digitais. Diante desse cenário, surge um serviço como uma alternativa sustentável para tratamento em escala de conflitos de consumo: o "consumidor.gov.br".

Conforme explica Sousa (2014, p. 14), o "consumidor.gov.br" consiste em:

> *[…] uma política pública para a defesa do consumidor que auxilia no subsídio de informações para o processo decisório da defesa do consumidor, atende o cidadão e auxilia na mitigação e resolução de problemas de consumo. Para tanto, este trabalho busca compreender como se desenvolveu a política pública em questão para o enfrentamento dos desafios impostos à defesa e ao direito do consumidor.*

Trata-se de uma plataforma de Estado, sob responsabilidade da Senacon, estabelecida pelo Decreto nº 8.573/2015[14], para conciliação entre consumidores e fornecedores na internet, com foco na solução e prevenção de conflitos de consumo. Por meio dessa plataforma, o consumidor se manifesta, a empresa responde, o consumidor avalia e todos podem monitorar o desenvolvimento da resolução.

Conforme explica João Sousa (2014, p. 30), a plataforma tem como base as seguintes premissas:

> *[…] transparência e controle social; importância estratégica das informações prestadas pelos consumidores; e acesso a informação como potencializadora do poder de escolha dos cidadãos. Assim, tem-se a expectativa de que o consumidor assuma um papel ativo, ao acompanhar e avaliar o desempenho dos fornecedores – disponível na própria plataforma.*

A plataforma é pública, gratuita e transparente, e funciona da seguinte forma. As empresas preenchem um "formulário de proposta de adesão" (contendo seus dados) e concordam

[12] O novo Código de Processo Civil prevê, em diversos artigos, a promoção da autocomposição de conflitos, como: art. 3º, § 3º; art. 6º; art. 139, inc. V; art. 313, inc. III; art. 334 e parágrafos; art. 359; art. 515, incisos II, III e VII; e art. 565, § 1º. Nesse sentido, ver Grinover (2015).

[13] A Resolução nº 125/2010 do CNJ dispõe sobre a política judiciária nacional de tratamento adequado dos conflitos de interesse no âmbito do Poder Judiciário, trata a conciliação, a mediação e outros métodos consensuais como instrumentos efetivos de pacificação social, solução e prevenção de demandas, visto serem aptos a reduzir a judicialização, a interposição de recursos e a execução de sentenças.

[14] A base normativa para o funcionamento do consumidor.gov é: **Lei nº 8.078/90**, Art. 4º, caput III e V, Harmonização das Relações de Consumo; **Decreto nº 7.963/2013**, Art. 3º I e VI Art. 4º I, Proteção e Defesa do Consumidor como Política de Estado, Harmonização das relações de consumo, Mecanismos alternativos para resolução de conflitos de consumo; **Decreto n 8.573/2015**, Institui o sistema alternativo de solução de conflitos de consumo – Consumidor.gov.br; **Comitê Gestor – Consumidor.gov.br**, Instituído pelo Decreto nº 8.573 e regimento interno – Deliberação nº 1, de 5 de maio de 2016.

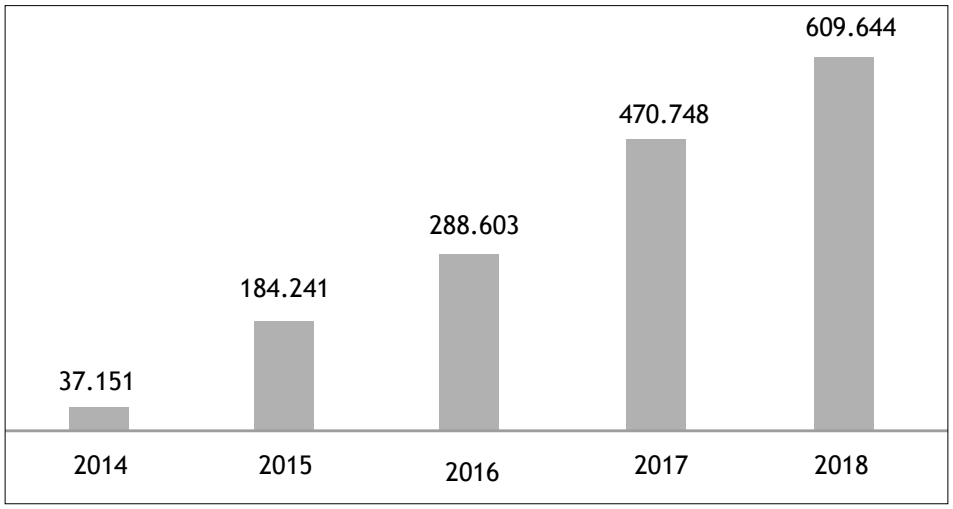
com um "termo de adesão" e um "termo de uso". O termo de adesão, assinado entre fornecedor e Senacon, permite: o acesso para receber e responder às reclamações registradas pelos consumidores; a interação com o consumidor na plataforma; o acompanhamento das demandas registradas em nome da empresa; e o requerimento da recusa da reclamação, "exclusivamente nos casos em que for comprovado que o serviço ou produto reclamado foi produzido, ofertado e/ou comercializado por outro fornecedor e que não há qualquer indício de solidariedade na relação de consumo mencionada". O fornecedor se compromete, dentre outros pontos, a responder às demandas em até 10 dias e a informar à Senacon os dados do responsável direto pelo tratamento do sistema dentro da empresa.

O consumidor, por sua vez, realiza o seu cadastro, assumindo os termos de uso, e fica habilitado a registrar reclamações contra qualquer uma das empresas participantes do serviço. Durante o prazo de resposta, o consumidor pode acompanhar sua demanda, bem como se relacionar com o fornecedor. Ao receber a resposta final da empresa, o consumidor pode avaliar a reclamação e participar de pesquisas em andamento na Senacon caso tenha interesse.

Até o momento, a plataforma teve mais de 1,9 milhão de reclamações recebidas pelas 531 empresas credenciadas[15]; cerca de 99% de reclamações respondidas pelas empresas dentro de um prazo médio de respostas de sete dias (menor do que o prazo determinado de dez dias que as empresas têm para responder as reclamações dos consumidores), com 81% de resolutividade avaliado pelos consumidores, que dão 3,3 sobre 5 às empresas.

A Senacon tem atuado para ampliar o uso da plataforma, podendo-se verificar que houve um aumento de 29,51% no número de reclamações em 2018 quando comparado com o ano de 2017, conforme demonstra o Gráfico 1.

Gráfico 1 — Total de reclamações por ano



Fonte: Martins (2019).

[15] Informações de junho de 2014 a 31 de dezembro de 2018. Informações obtidas do SINDEC, do Ministério da Justiça e Segurança Pública.

Ressalta-se, inclusive, o apoio do Conselho da Justiça Federal (CJF, 2016), que, na I Jornada de "Prevenção e solução extrajudicial de litígios", aprovou o enunciado 50:

> *O Poder Público, os fornecedores e a sociedade deverão estimular a utilização de mecanismos como a plataforma CONSUMIDOR.GOV.BR, política pública criada pela Secretaria Nacional do Consumidor – Senacon e pelos Procons, com vistas a possibilitar o acesso, bem como a solução dos conflitos de consumo de forma extrajudicial, de maneira rápida e eficiente.*

Atualmente, a Senacon realiza projetos de cooperação do Tribunais de Justiça com o objetivo de incentivar a redução e a prevenção de litígios por meio da plataforma[16]. Além disso, a Senacon firmou, recentemente, convênio com o Conselho Nacional de Justiça para integração do "consumidor.gov.br" ao processo judicial eletrônico (PJe)[17], fazendo com que as partes que ingressam com ações no poder judiciário tenham a opção de utilizar a plataforma antes de dar prosseguimento ao processo.

Um dos pontos mais interessantes da plataforma, além da promoção da desjudicialização, é a possibilidade de acesso a uma base de dados com o perfil dos consumidores que utilizam a plataforma, podendo-se, inclusive, fornecer subsídios à elaboração de políticas públicas[18], conforme explica o site do Ministério da Justiça e Segurança Pública:

> *"Os registros realizados pelos consumidores geram uma base de dados pública que disponibiliza à sociedade informações relevantes sobre empresas, assuntos, e problemas demandados na plataforma. Tais informações alimentam indicadores que são divulgados no site, bem como estão à disposição de qualquer interessado, independentemente de solicitação, em formato aberto, em conformidade com diretrizes de acesso à informação e transparência ativa. Acreditamos que o acesso a esses dados apoia a produção de conhecimento pela própria sociedade, pelo meio acadêmico, bem como serve ao próprio mercado. Além disso, oferece condições ao Estado para fiscalizar o comportamento das empresas, especialmente no que tange à lesão a direitos coletivos" (O QUE…, 2018)*[19].

Exemplo do mapeamento dessas informações pode ser encontrado em pesquisa realizada por Martins (2019), na qual foi possível identificar o perfil das reclamações, dos usuários e das empresas que fazem uso da plataforma, podendo-se chegar às seguintes conclusões.

Por exemplo, dos consumidores que submeteram reclamações, cercaX de 58,44% comprou os produtos ou adquiriu os serviços de forma não presencial (35,73% pela internet,

[16] No momento, são conveniados: Tribunal de Justiça do Estado do Acre; Tribunal de Justiça da Bahia; Poder Judiciário do Ceará; Tribunal de Justiça de Rondônia, Tribunal de Justiça de Sergipe, dentre outros.

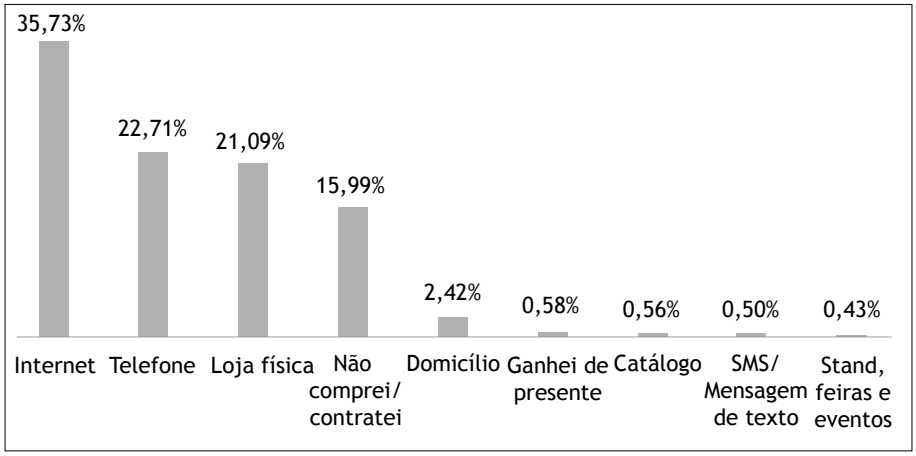
[17] BRASIL. **Acordo de Cooperação Técnica nº 016/2019**. Acordo de cooperação técnica entre o Conselho Nacional de Justiça e o Ministério da Justiça e Segurança Pública, por meio da Secretaria Nacional do Consumidor (SENACON), para incremento de métodos autocompositivos, mediante plataformas on-line, para solução de controvérsias consumeristas. 2019.

[18] Cabe destacar recente pesquisa realizada pela Senacon através da plataforma para mapear a situação das ligações indesejadas recebidas por consumidores, conforme explica reportagem do portal valor econômico (PERON, 2019).

[19] Informação disponível em: https://www.justica.gov.br/seus-direitos/consumidor/consumidor-gov.br.

e 22,71% pelo telefone), enquanto 0,43% comprou em *stands*, feiras e eventos e 21,09% adquiriu seus produtos em lojas físicas.

Gráfico 2 — Canais de compra



Fonte: Martins (2019).

Além disso, os dados elencados por Martins nos permitem ver que praticamente todas as operadoras de telefonia constam da relação de empresas com maior número de reclamações. Vivo, Oi, TIM e Claro totalizam, juntas, 54,36% de todas as reclamações dos consumidores.

Já os cinco principais problemas que os consumidores enfrentam são: dados pessoais usados sem autorização (23,18%); venda e publicidade enganosos (23,01%); cobrança indevida ou abusiva (22,07%); cobrança por serviço não contratado (20,32%); dificuldade na devolução de valores pagos (11,22%).

Por meio da análise dos dados elencados, originados da plataforma, é possível que o SNDC elabore políticas públicas que, de um lado, promovam uma maior proteção do consumidor e, de outro, evitem que novas ações consumeristas cheguem ao judiciário, sem que isso signifique uma precarização dos direitos dos consumidores.

6. Conclusão

A indústria 4.0 impõe mudanças nas relações sociais, na maneira que nós como sociedade adquirimos bens e serviços e, consequentemente, nas relações de consumo. Exemplo disso são as plataformas digitais que são amplamente utilizadas no dia a dia, como Uber, Facebook, Airbnb, dentre outras.

O número de ações em tramitação no judiciário, os custos envolvidos para sua manutenção e o tempo de espera para uma efetiva prestação jurisdicional nos mostram que é necessário investir em sistemas de tecnologia, como plataformas digitais, que promovam a desjudicialização. No caso, se as partes envolvidas em um litígio conseguem resolver os problemas da disputa sem que isso resulte em um processo judicial, eventualmente será possível transformar isso em um modelo a ser replicado como política pública, como foi o caso do "consumidor.gov.br". Nesse sentido, Grimmelmann (2004, p. 1.719, tradução nossa) explica que:

> *Esse deslocamento funciona porque a lei não é automatizada nem imediata. Como a lei não é automatizada, se as partes de uma disputa potencial estiverem satisfeitas com sua resolução, a lei as deixará em paz. E como a lei não é imediata, é bom esperar até que uma das partes compareça com uma queixa. Deixa tempo para eles fazerem acordos informais uns com os outros, ou para normas comunitárias internalizadas que evitam o surgimento de uma disputa*[20].

Nesse sentido, é necessário investir no empoderamento do consumidor e, sobretudo, na congregação de consumidores capazes de negociar coletivamente (conforme previsão do artigo 107 do CDC[21]). É também o momento, diante da indústria 4.0, de aproveitarmos plataformas digitais que promovam soluções alternativas de conflitos, como negociação, mediação e até mesmo arbitragens em disputas coletivas, como já ocorre em diversos países.

Além disso, essas plataformas permitem a realização de estudos com o fim de classificar empresas de acordo com o nível de conformidade em relação ao cumprimento dos direitos do consumidor e de acordo com a satisfação dos consumidores mensurada pela sua responsividade em plataformas como o "consumidor.gov.br". Da mesma forma que consumidores são avaliados, a plataforma também permite a avaliação das empresas, podendo-se pensar, no futuro, em punição para empresas que não são bem avaliadas.

Ademais, é necessário sermos mais eficientes na regulação do mercado, ensejando uma maior coordenação entre os integrantes do SNDC e, ainda, destes com as agências reguladoras.

É, portanto, a hora de o SNDC estabelecer uma política nacional de defesa do consumidor, prevista no CDC, baseada em evidências hoje disponíveis nas plataformas digitais, levando em consideração a Análise de Impacto Regulatório (AIR) e investindo em uma regulação que funcione e que crie para as empresas o receio de que não vale a pena descumprir a lei.

Essa política, se bem desenhada, poderá fazer com que, no futuro, casos de descumprimento da legislação consumerista cheguem ao Poder Judiciário apenas residualmente, o que deve ser pensado, também, dentro de uma lógica sistêmica que não incentive o descumprimento da lei.

7. Bibliografia

ALMEIDA, João Batista de. *Manual de direito do consumidor*. São Paulo: Saraiva, 2015.

BECKER, Daniel; LAMEIRÃO, Pedro. Online Dispute Resolution (ODR) e a ruptura no ecossistema da resolução de disputas. *AB2L*, Rio de Janeiro, 27 ago. 2017. Disponível em: https://bit.ly/2MSGqGb. Acesso em: 9 ago. 2019.

[20] No original: "This displacement works because law is neither automated nor immediate. Because law is not automated, if the parties to a potential dispute are satisfied with its resolution, the law will leave them alone. And because law is not immediate, it is content to wait until one of the parties comes before it with a complaint. It leaves time for them to strike an informal deal with each other, or for internalized community norms to keep a dispute from arising" (GRIMMELMANN, 2004, p. 1.739).

[21] Art. 107. As entidades civis de consumidores e as associações de fornecedores ou sindicatos de categoria econômica podem regular, por convenção escrita, relações de consumo que tenham por objeto estabelecer condições relativas ao preço, à qualidade, à quantidade, à garantia e características de produtos e serviços, bem como à reclamação e composição do conflito de consumo.

BRAND FINANCE. *Global 500 2019*: the annual report on the world's most valuable and strongest brands. [*S. l.*]: Brand Finance, 2019. Disponível em: https://bit.ly/2R6Vsdb. Acesso em: 24 jun. 2019.

BRASIL. Presidência da República. *Resolução nº 125, de 29 de novembro de 2010*. Dispõe sobre a Política Judiciária Nacional de tratamento adequado dos conflitos de interesses no âmbito do Poder Judiciário e dá outras providências. Brasília, DF: Presidência da República, 2010. Disponível em: https://bit.ly/30ukoy0. Acesso em: 23 jun. 2019.

BRASIL. *Acordo de Cooperação Técnica nº 016/2019*. Dispõe sobre a cooperação técnica entre o CNJ e o MJSP/SENACON para incremento de métodos autocompositivos de resolução de controvérsias na seara consumerista, o que alcança a integração da plataforma "consumidor.gov.br" ao Processo Judicial Eletrônico – PJe. Conselho Nacional de Justiça, Brasília, DF, 7 jun. 2019. Disponível em: https://bit.ly/2G1VVXG. Acesso em: 17 jan. 2020.

CABRAL, Marcelo Malizia. *Os meios alternativos de resolução de conflitos*: instrumentos de ampliação do acesso à justiça. 2012. Dissertação (Mestrado Profissional em Poder Judiciário) – Fundação Getúlio Vargas, Rio de Janeiro, 2012. Disponível em: https://bit.ly/2Y9D7wN. Acesso em: 23 jun. 2019.

CONSELHO DA JUSTIÇA FEDERAL. *I Jornada "Prevenção e Solução Extrajudicial de Litígios"*. Brasília, DF: CJF, ago. 2016.

CONSELHO NACIONAL DE JUSTIÇA. *Justiça em números 2018 (ano-base 2017)*. Brasília, DF: CNJ, 2018.

FERNANDES, Cassiane Melo; SIMÃO FILHO, Adalberto. A proteção do consumidor na sociedade da informação: uma análise da plataforma consumidor.gov.br. *In*: CONGRESSO BRASILEIRO DE PROCESSO COLETIVO E CIDADANIA, 3., 2015, Ribeirão Preto. *Anais* […]. Ribeirão Preto: Universidade de Ribeirão Preto, ago. 2015. Disponível em: https://bit.ly/2xc23bh. Acesso em: 24 jun. 2019.

FILISTRUCCHI, Lapo; GERADIN, Damien; VAN DAMME, Eric. *Identifying two-sided markets*. Tilburg: TILEC, 2012. (TILEC Discussion Paper n. 2012-008).

FRIEDMAN, David. Does technology require new law. *Harvard Journal of Law & Public Policy*, Cambridge, v. 25, p. 71-85, 2001. Disponível em: https://bit.ly/2ZON3fY. Acesso em: 21 jun. 2019.

GRIMMELMANN, James. Regulation by software. *Yale Law Journal*, New Haven, v. 114, p. 1.719, 2004. Disponível em: https://bit.ly/2X69VKH. Acesso em: 21 jun. 2019.

GRINOVER, Ada Pellegrini. Os métodos consensuais de solução de conflitos no novo CPC. *In*: BONATO, Giovanni. *O novo Código de Processo Civil*: questões controvertidas. São Paulo: Atlas, 2015.

HOFMANN, Jeanette; KATZENBACH, Christian; GOLLATZ, Kirsten. Between coordination and regulation: finding the governance in Internet Governance. *New Media & Society*, [*S. l.*], v. 19, n. 9, p. 1406-1423, 2017. Disponível em: https://bit.ly/2ZK3mKO. Acesso em: 22 jun. 2019.

LIMA, Daniel Henrique Sprotte. *Da cultura do litígio à do consenso*: o uso de *online dispute resolution* na Comarca de Araquari (SC). 2019. Dissertação (Mestrado em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2019.

MARTINS, Marcos. Análise Exploratória de Dados (AED) – As reclamações do consumidor em 2018. *Jota*, São Paulo, 14 jun. 2019. Disponível em: https://bit.ly/2RAGqLm. Acesso em: 24 jun. 2019.

NASCIMENTO JUNIOR, Vanderlei de Freitas. A evolução dos métodos alternativos de resolução de conflitos em ambiente virtual: online dispute resolution. *Revista Eletrônica da Faculdade de Direito de Franca*, Franca, v. 12, n. 1, p. 265-281, 2017.

O QUE é o Consumidor.gov.br. *Justiça e Segurança Pública*, Brasília, DF, 11 jul. 2018. Disponível em: https://bit.ly/2RyMfcz. Acesso em: 20 jan. 2020.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *Policy roundtables*: two-sided markets. Paris: OECD, 17 Dec. 2009. DAF/COMP(2009)20.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. *An introduction to online platforms and their role in the digital transformation*. Paris: OECD Publishing, 2019. Disponível em: https://bit.ly/2Y8BOhM. Acesso em: 23 jun. 2019.

PERON, Isadora. 92,5% das pessoas recebem ligações indesejadas de telemarketing. *Valor Econômico*, Brasília, DF, 21 maio 2019. Disponível em: https://bit.ly/31Qjg8g. Acesso em: 24 jun. 2019.

ROSS, Richard J. Communications Revolutions and Legal Culture: An Elusive Relationship. *Law & Social Inquiry*, [*S. l.*], v. 27, n. 3, p. 637-684, 2002. Disponível: https://bit.ly/2J6reSb. Acesso em: 23 jun. 2019.

SCHWAB, Klaus. *A quarta revolução industrial*. São Paulo: Edipro, 2016.

SOUSA, João Paulo Alexandre de. *Defesa do consumidor e políticas públicas*: um estudo sobre o consumidor.gov.br. 2014. Monografia (Bacharelado em Gestão de Políticas Públicas) – Universidade de Brasília, Brasília, DF, 2014.

TIMM, Luciano Benetti. Ainda sobre a função social do direito contratual no Código Civil brasileiro: justiça distributiva versus eficiência econômica. *Revista da AMDE*, Belo Horizonte, v. 2, 2009. Disponível em: https://bit.ly/2X6R7uR. Acesso em: 23 jun. 2019.

TIMM, Luciano Benetti. Por um plano nacional de defesa dos direitos do consumidor. *Consultor Jurídico*, São Paulo, 22 jan. 2019. Disponível em: https://bit.ly/2WX7Bko. Acesso em: 23 jun. 2019.

II
Proteção de dados pessoais

A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor

Fernando Antonio Tasso[1]
Juiz de Direito no Estado de São Paulo

Sumário: Introdução; 1. Os novos desafios da responsabilidade civil diante da evolução tecnológica; 2. O regime jurídico da proteção de dados na Lei 13.709/2018; 2.1. O sistema de responsabilidade civil na Lei Geral de Proteção de Dados; 2.2. A dupla inserção da responsabilidade civil na Lei Geral de Proteção de Dados; 2.2.1. Quando o controlador é um ente público; 2.2.2. Quando o controlador é uma pessoa natural ou pessoa jurídica de direito privado; 2.3. A violação de um dever como ensejador da responsabilidade civil; 2.4. Interpretação sistemática; 2.5. Interpretação teleológica; 2.6. Interpretação histórica; 3. A interface da Lei Geral de Proteção de Dados com o Código Civil; 4. A interface da Lei Geral de Proteção de Dados com o Código de Defesa do Consumidor; Conclusão; Bibliografia.

Introdução

A Constituição Federal contempla em seu artigo 5º um extenso rol de direitos e garantias fundamentais, dentre os quais a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, assegurando ao lesado o direito a indenização pelo dano material ou moral decorrente de sua violação[2]. Tais direitos assumem inquestionável importância quando se está a tratar da sociedade inserida na era da informação.

O Direito, assim como todas as demais ciências, evolui em ciclos à medida que o conhecimento da humanidade e a tecnologia avança. A própria percepção da evolução do tempo, mudou com o tempo, segundo o conceito lapidar de Marc Halévi[3].

A Internet teve inquestionável influência em questões como a liberdade de expressão, a comunicação interpessoal e a própria comunicação social, repercutindo diretamente na dimensão do conceito de privacidade.

Se no contexto norte-americano, a privacidade era enfrentada sob a perspectiva do plano horizontal e, portanto, interindividual, como sendo o direito de ser deixado só, na postulação de Warren e Brandeis[4], em solo europeu, o era no plano vertical, uma vez que direcionado contra o Estado, impedindo-o de proceder ao tratamento não autorizado ou não consentido dos dados pessoais. Este, contrariamente ao primeiro, possui a característica de uma liberdade negativa, consagrada no conceito de autodeterminação informativa.

---

[1] Juiz de Direito Titular I da 15ª Vara Cível Central. Coordenador de TI e Direito Digital da Escola Paulista da Magistratura e Coordenador do Núcleo de Estudos em Direito Digital da Escola Paulista da Magistratura.

[2] Artigo 5º, inciso X da Constituição Federal.

[3] HALÉVI, Marc. A era do conhecimento: princípios e reflexões sobre a revolução noética no século XXI. São Paulo: Editora Unesp, 2010.

[4] WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, 15 dez. 1890.

Em ambos os enfoques, na ensinança de Stefano Rodotá, a preservação da privacidade é precondição da cidadania na era eletrônica[5].

Sob o epíteto de ser o novo petróleo[6], os dados pessoais são o insumo da indústria denominada 4.0, porquanto inserida no contexto da Quarta Revolução Industrial[7]. Com efeito, tecnologias como *big data*, Internet das Coisas (IoT), Inteligência Artificial (AI), *Blockchain*, entre outras relacionadas ao impulsionamento da atividade econômica, geram o ganho em eficiência e escala de determinada atividade econômica devido à operação denominada tratamento de dados pessoais[8].

Já se alertou que dados pessoais estão à venda[9] e que no universo de aplicações da Internet[10] não há serviço gratuito, a resultar que se o produto ou serviço é aparentemente gratuito, o produto é o próprio consumidor, ou seja, seus dados pessoais.

Hoje, diferentemente do que ocorria há duas décadas, as pessoas não mais "entram" na Internet, porquanto já estão absolutamente imersas no ambiente virtual. Perfis fantasma[11], existentes no ambiente das plataformas digitais de redes sociais; o monitoramento de atividade e do próprio sono do usuário por meio de dispositivos vestíveis, como *smart watches* ou *smart bands*, ou portáveis, como *smartphones* ou *tablets*, são tecnologias que ancoram a existência humana no ambiente virtual, ainda que sem sua ciência ou de acordo com sua plena concordância.

Nesse contexto, em que é impossível se desconectar de modo absoluto da rede mundial de computadores, a Internet, normas reguladoras em todo o globo têm a pretensão de traçar regras que, ao invés de inibirem ou vedarem o tratamento de dados pessoais, no dizer de Helen Nissembaum[12], buscam permitir um adequado fluxo informacional, preservada a autodeterminação informativa, que foi consagrada como um dos fundamentos da Lei Geral de Proteção de Dados[13], ao lado do respeito à privacidade[14], à inviolabilidade da intimidade, da honra e da imagem[15].

Conquanto a elevação do direito à proteção de dados ao patamar constitucional seja uma tendência mundial a exemplo da previsão na Constituição Portuguesa desde 1976, bem assim como se encontra previsto nas constituições de países como Áustria, Espanha,

---

[5] RODOTÁ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 129.

[6] THE WORLD'S most valuable resource is no longer oil, but data. *The Economist*, London, 6 maio 2017. Disponível em: https://econ.st/37geKlQ. Acesso em: 21 jan. 2020.

[7] BARBOSA, Marcos T. J.; BAISSO, Marcos; ALMEIDA, Marcos T. Surge uma nova sociedade. *In*: SILVA, Elcio B.; SCOTON, Maria L. R. P. D.; PEREIRA, Sérgio L.; DIAS, Eduardo M. *Automação & sociedade*: Quarta Revolução Industrial, um olhar para o Brasil. São Paulo: Brasport, 2018.

[8] Lei 13.709/2018 – Art. 5º, X: – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[9] YOUR Data for sale. *Time*. New York: Time Inc, v. 177, n. 11, 21 mar. 2011.

[10] Lei 12.965/2014 – Art. 5º, VII: aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet;

[11] Perfis fantasma são os existentes no âmbito interno das redes sociais e se referem a pessoas que a despeito de não terem voluntariamente se inscrito em determinada plataforma e inserido seus dados pessoais, tem seu perfil formado a partir da reunião de informações coletadas a partir de referências em perfis de pessoas a ela relacionadas.

[12] NISSENBAUM, Helen. *Privacy in Context*: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law books, 2010.

[13] Art. 2º, II da Lei 13.709 de 14 de agosto de 2018.

[14] Art. 2º, I da Lei 13.709 de 14 de agosto de 2018.

[15] Art. 2º, IV da Lei 13.709 de 14 de agosto de 2018.

Estônia e Polônia, no Brasil igual tratamento é veiculado pela PEC 17/2019[16] que propõe a inserção da proteção de dados no rol dos direitos fundamentais inserindo-o no artigo 5º, inciso XII da carta magna.

A proteção de dados como direito autônomo advém da constatação de que novas situações de fato ensejam proteção legal, por decorrerem do puro e simples tratamento de dados pessoais, como o perfilamento racial, as listas negras de trabalhadores que ingressam na Justiça Obreira contra seus patrões, testes genéticos pré-admissionais e identificações biométricas em gravações de vídeo de espaços públicos.

Tais fatos, isoladamente considerados, não violam honra, intimidade ou vida privada. Porém, no contexto do tratamento e utilização massiva de dados pessoais, passam a ser geradores de novos valores passíveis de garantia legal, conforme já preconizado pela teoria nomogênica do direito tridimensional de Miguel Reale[17], uma vez que repercutem em direitos e garantias fundamentais como a igualdade, do livre exercício profissional, da dignidade da pessoa humana e da liberdade de reunião e locomoção.

O estudo da responsabilidade civil se vê face aos desafios de um novo contexto de relações interpessoais e, por vezes, entre pessoas e máquinas, que instigam doutrina e jurisprudência a tratar dessa nova espécie de risco[18].

A responsabilidade civil tem por desafios novas relações jurídicas decorrentes de novas espécies contratuais, como contratos de transporte celebrados por intermédio de plataformas digitais, ou prestados por veículos autônomos, contratos de transporte de coisas por *drones* e contratos coligados de serviços prestados pela Internet, assim como de novas condutas como espionagem industrial realizada por *softwares* invasores. São esses apenas alguns exemplos que desafiarão a jurisprudência, tal como hoje já o fazem as questões, antes impensáveis, como a da responsabilidade civil por *links* patrocinados[19], das plataformas de pagamento[20] ou do *marketplace*[21].

1. Os novos desafios da responsabilidade civil diante da evolução tecnológica

A evolução tecnológica resulta na sensível alteração na forma de tratamento dos fatos jurídicos pelo direito.

Se é fato que, segundo Klaus Schwab[22], estamos vivendo a Quarta Revolução Industrial, a notável evolução dos institutos de direito a permear as novas relações jurídicas e suas peculiaridades não é algo novo.

---

[16] BRASIL. Senado Federal. *Proposta de Emenda à Constituição nº 17, de 2019*. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2019. Disponível em: https://bit.ly/2RgVmzz. Acesso em: 4 dez. 2019.

[17] REALE, Miguel. *Lições preliminares de Direito*. 27. ed. São Paulo: Saraiva, 2013.

[18] GODOY, Cláudio Luiz Bueno. A responsabilidade civil na era digital. *In*: III CONGRESSO INTERNACIONAL DE RESPONSABILIDADE CIVIL DO IBERC, 3., 2019, São Paulo. *Palestras* […]. [*S. l.*]: Iberc, 2019.

[19] TJSP; Apelação Cível 1011391-95.2015.8.26.0005; Relator (a): Francisco Loureiro; Órgão Julgador: 1ª Câmara de Direito Privado; Foro Regional V – São Miguel Paulista – 4ª Vara Cível; Data do Julgamento: 07/06/2016; Data de Registro: 07/06/2016.

[20] TJSP; Apelação 0012751-40.2012.8.26.0344; Relator (a): Alfredo Attié; Órgão Julgador: 26ª Câmara de Direito Privado; Foro de Marília – 1ª. Vara Cível; Data do Julgamento: 14/09/2017; Data de Registro: 15/09/2017.

[21] TJSP; Apelação Cível 1004338-89.2017.8.26.0297; Relator (a): Cesar Luiz de Almeida; Órgão Julgador: 28ª Câmara de Direito Privado; Foro de Jales – 5ª Vara; Data do Julgamento: 22/06/2018; Data de Registro: 22/06/2018.

[22] SCHWAB, Klaus. *Aplicando a Quarta Revolução Industrial*. São Paulo: Edipro, 2018

Foi assim com a invenção da máquina a vapor na década de 1760 que, acompanhada pelo pensamento liberal de Adam Smith, conduziu a humanidade à denominada Primeira Revolução Industrial.

No Brasil, a entrada em vigor do Decreto nº 2.681/1912 trouxe a responsabilidade objetiva imputada às estradas de ferro, pública ou privada, pela perda total ou parcial, furto ou avaria das mercadorias que recebiam para transportar.

A invenção da eletricidade proveu os alicerces das linhas de montagem e do Taylorismo[23] dando ensejo à Segunda Revolução Industrial na década de 1870.

O crescimento em escala das relações de trabalho e a demanda social por preservação da segurança, proteção e incolumidade do trabalhador, pessoa física e sujeito de direitos, resultou na legislação trabalhista garantidora da responsabilidade objetiva do empregador em caso de sinistro vitimando o fâmulo[24].

No âmbito das relações privadas, o Código Civil de 1916 inaugurou, dentre as hipóteses de responsabilidade objetiva, a do detentor dos meios de produção, qual seja, o patrão, amo ou comitente, por atos de seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou por ocasião dele[25]. Disposição análoga foi repetida pelo Código Civil em seu artigo 932, inciso III[26].

O desenvolvimento da tecnologia computacional com a germinação das ideias de robotização e automação de processos de trabalho foi o fator chave propulsor do Plano Marshall liderado pelos Estados Unidos da América ao final da Segunda Guerra Mundial, identificando-se esse contexto como sendo a Terceira Revolução Industrial na década de 1960.

Ainda que tardiamente, o Código de Defesa do Consumidor (1990) previu a responsabilidade objetiva por fato do produto ou serviço[27] e, posteriormente, o Código Civil consagrou cláusula geral de responsabilização civil daquele que desenvolve atividade de risco, no parágrafo único do artigo 927.

Diferentemente das anteriores, em que a constatação de sua ocorrência e identificação de seus fatores determinantes foi feita mediante análise de fatos pretéritos, a Quarta Revolução Industrial foi cunhada a partir do vislumbre de seu alvorecer pelo engenheiro e economista Klaus Schwab, fundador do Fórum Econômico Mundial, que a elegeu como tema da edição de 2016. Tem por pressupostos a eliminação dos limites entre os mundos físico, digital e biológico em decorrência do desenvolvimento das novas tecnologias em cada uma dessas áreas.

Nesse contexto se estabelecem as novas perspectivas da responsabilidade civil, em tempos que Anderson Schreiber reputa caracterizado pela erosão dos filtros da responsabilidade civil que, ao lado da crescente ampliação das hipóteses de

[23] Modelo de administração desenvolvido pelo engenheiro Frederick Taylor, caracterizado pela ênfase nas tarefas, objetivando o aumento da eficiência no nível operacional.

[24] Decreto-Lei nº 5.452/1943.

[25] Art. 1.521, inciso III do Código Civil de 1916.

[26] Art. 932. São também responsáveis pela reparação civil: [...] III – o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele.

[27] Arts. 12 e 14 da Lei 8.078/1990.

responsabilidade objetiva, a jurisprudência tem amalgamado na ampliação das hipóteses de indenização pelo dano presumido[28].

Claudio Luiz Bueno de Godoy[29] pontua que novas tecnologias trazem novos riscos e propõe que estes devem ser analisados à luz da revisitação dos institutos tradicionais da responsabilidade civil, buscando recompreendê-los, cabendo às novas leis estabelecer regras de conduta no espaço virtual, deveres imputados aos agentes dessa nova relação jurídica, prevendo critérios de escolha daquele que ressarcirá o dano provocado.

A Lei Geral de Proteção de Dados, segundo ele, cumpre esse papel inovando o critério binário de imputação consistente na culpa e no risco, identificado por Alvino Lima, para prever novos deveres aos agentes de tratamento, quais sejam o de prevenção, vigilância e segurança.

Atendendo à demanda global pela positivação de um regime jurídico de proteção de dados pessoais, fruto do estabelecimento de um *standard* jurídico com a aprovação do Regime Geral de Proteção de Dados[30] europeu, que passou a vigorar em sua plenitude no ano de 2018, o legislador brasileiro editou em tempo recorde a Lei 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD).

Como assinala Walter Aranha Capanema[31], já existiam em nosso ordenamento jurídico outras leis que tratavam, de alguma forma, do tema, como o Código de Defesa do Consumidor (Lei 8.078/1990), o Marco Civil da Internet (Lei 12.965/2014), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei do Cadastro Positivo (Lei 12.414/2011), dentre outras.

A Lei Geral de Proteção de Dados surgiu no ordenamento jurídico com a função de ser o referencial normativo do sistema de proteção de dados pessoais que, no cenário então vigente, era regulamentado por leis e decretos setoriais ou temáticos[32].

Assim sendo, este trabalho se propõe a analisar a inserção da Lei Geral de Proteção de Dados no sistema jurídico nacional sob o recorte da responsabilidade civil de entes privados que procedem ao tratamento de dados pessoais, analisando sua convivência e interface com as duas maiores instituições normativas do direito privado, o Código Civil e o Código de Defesa do Consumidor.

2. O regime jurídico da proteção de dados na Lei 13.709/2018

A Lei Geral de Proteção de Dados tem por âmbito de incidência material o tratamento de dados pessoais em meio digital ou analógico, realizado por pessoa natural ou pessoa jurídica de direito público ou privado, visando à proteção dos direitos fundamentais da liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[28] SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil*. A erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

[29] GODOY, Cláudio Luiz Bueno. A responsabilidade civil na era digital. *In*: CONGRESSO INTERNACIONAL DE RESPONSABILIDADE CIVIL DO IBERC, 3., 2019, São Paulo. *Palestras* […]. [*S. l.*]: Iberc, 2019.

[30] UNIÃO EUROPEIA. *Regulamento (EU) 2016/679 do Parlamento Europeu e do conselho*. Bruxelas: UE, 2016. Disponível em: https://bit.ly/38wxTzZ. Acesso em: 4 dez. 2019.

[31] CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. *Cadernos Jurídicos*, [2020]. No prelo.

[32] TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019b, p. 263.

Sua estrutura normativa, segundo Laura Schertel Mendes[33], divide-se em três grandes frentes. Tem na base de sua estrutura, as condições de legitimidade para o tratamento de dados pessoais, ao contemplar sua base principiológica e as bases legais autorizadoras do tratamento de dados pessoais.

A seguir, prevê os procedimentos para o tratamento lícito de dados pessoais, declarando os direitos do titular dos dados, as obrigações dos agentes de tratamento, bem assim, as regras de governança de dados e códigos de conduta.

Ao final, trata das consequências do descumprimento das normas de proteção de dados ao prever sanções administrativas e regras de responsabilidade civil dos agentes de tratamento. Este último aspecto é o que nos interessa neste estudo.

Em sintonia com a mais moderna corrente do tratamento de dados pessoais, estabelece diferença conceitual entre dados pessoais[34] e dados sensíveis[35] e exclui de sua incidência os dados anonimizados[36].

Estabelece como sendo o indivíduo, denominado titular[37], o destinatário último das normas de proteção, no âmbito de relações jurídicas que envolvam o tratamento de dados[38], que consiste em todas as operações de interação de terceiros com os dados pessoais do indivíduo. Elimina, portanto, qualquer espectro de dúvida quanto à propriedade dos dados pessoais[39].

Identifica como integrantes do polo adverso da relação jurídica de direito material os agentes de tratamento de dados[40], quais sejam, aquele a quem compete as decisões referentes ao tratamento de dados pessoais, o controlador[41], e aquele que efetivamente realiza as operações de tratamento de dados pessoais em nome daquele, o operador[42]. Sob a ótica civilista, o controlador seria o mandante, enquanto o operador, seu mandatário[43].

A norma prevê ainda a figura do encarregado[44] que exerce função consultiva e de interface entre o controlador e os titulares dos dados ou a Autoridade Nacional de Proteção

[33] MENDES, Laura Schertel. *Contexto internacional e economia de dados pessoais; histórico da implementação da regulamentação europeia de proteção de dados (GPDR); Marco Civil da Internet, Código de Defesa do Consumidor e Cadastro Positivo; Lei Geral de Proteção de Dados (LGPD) e Medida Provisória 869/2018.* São Paulo: Escola da Defensoria Pública, 13 jun. 2019. Palestra proferida no Curso sobre a Lei Geral de Proteção de Dados.

[34] Art. 5º, I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;

[35] Art.5º, II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

[36] Art. 5º, III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

[37] Art. 5º, V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

[38] Art. 5º, X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[39] Art. 17 – Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

[40] Art. 5º, IX – agentes de tratamento: o controlador e o operador.

[41] Art. 5º, VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[42] Art. 5º, VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

[43] CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. *Cadernos Jurídicos*, [2020]. No prelo.

[44] Art. 5º, VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)

de Dados, sendo este o órgão ocupante do mais alto posto na rede de governança de proteção de dados.[45]

Declara como fundamentos da norma, dentre outros, o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais[46].

A autodeterminação informativa é, de fato, o vetor hermenêutico de primeira ordem, porquanto, nas palavras de Danilo Doneda, consiste no direito individual de escolher quais dados pessoais serão usados, bem como os limites e o prazo de sua utilização[47].

A garantia de observância dos fundamentos da lei se vê materializada pela declaração do plexo de direitos do titular seu Capítulo III, abrangendo desde o mais elementar direito à confirmação da própria existência de tratamento[48] à potestade de eliminação de seus dados em poder do controlador[49].

A par das garantias de direitos do titular, a Lei Geral de Proteção de Dados prevê em extensa gama de dispositivos legais normas que impõem deveres de prevenção e segurança aos operadores com a finalidade de evitar acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito[50].

O sistema prescritivo de proteção de dados também encontra em diversos dispositivos do Capítulo VII "Da Segurança e das boas práticas", a imposição aos operadores da adoção de normas de segurança da informação e governança de dados baseada em evidências, de modo a dar concretude à sua função bifronte de proteção do titular e prestação de contas pelo operador.

O desatendimento aos direitos do titular, bem como a não conformidade das operações de tratamento de dados às normas de segurança da informação dão azo à imposição de sanções administrativas, bem como a ações judiciais fundamentadas na responsabilidade civil.

---

[45] Art. 5., XIX – autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

[46] Art. 2º – A disciplina da proteção de dados pessoais tem como fundamentos:
I – o respeito à privacidade;
II – a autodeterminação informativa;
III – a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
V – o desenvolvimento econômico e tecnológico e a inovação;
VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

[47] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006, p. 196.

[48] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I – confirmação da existência de tratamento.

[49] Art. 18, VI – eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei.

[50] Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

2.1 O sistema de responsabilidade civil na Lei Geral de Proteção de Dados

Inserida no Capítulo VI "Dos agentes de tratamento de dados pessoais" está a Seção III que trata da responsabilidade e do ressarcimento de danos imputados aos agentes de tratamento.

O artigo 42 "caput" da Lei Geral de Proteção de Dados prevê o dever de reparação civil por dano patrimonial, moral, individual ou coletivo, imposto aos agentes de tratamento, controlador ou operador, quando executarem operação de tratamento de dados em violação à legislação de proteção de dados.

Sobressai de sua leitura que, se por um lado não prevê o elemento culpa, por outro não o exclui expressamente. Ainda, traz como requisito da obrigação de reparar a circunstância de ter sido a operação de tratamento lesiva realizada em violação à legislação de proteção de dados.

É legítimo concluir, conforme aponta Gisela Sampaio da Cruz[51], que são utilizados apenas dois critérios objetivos para fundamentar a responsabilidade, quais sejam, o exercício da atividade de tratamento de dados e a violação da legislação de proteção de dados.

Com a finalidade de atribuir maior garantia de reparação do dano, o inciso I, do §1º do referido artigo estabelece hipótese de responsabilidade solidária do operador quando descumpre a Lei ou atua em contrariedade com as ordens lícitas do controlador.

Os controladores podem ser solidariamente responsáveis, na dicção do inciso II do §1º do artigo 42, uma vez demonstrado estarem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados. Tal previsão se mostra alinhada à complexa realidade das operações de tratamento compartilhado de dados, por vezes envolvendo o compartilhamento entre entes públicos e privados.

2.2 A dupla inserção da responsabilidade civil na Lei Geral de Proteção de Dados

O tratamento da responsabilidade civil no âmbito da proteção de dados pessoais tem sido tema de atenção da moderna doutrina, porquanto estando a lei em período de *vacatio legis*, não exprimirá, até o seu término, sua aplicabilidade concreta em julgados ou decisões administrativas de cunho normativo a balizar o debate sobre a responsabilidade civil dos agentes de tratamento.

Deve-se o fato à aparente imprecisão normativa quanto ao sistema de responsabilidade civil adotado pela lei protetiva. O embate doutrinário é travado entre posições que afirmam ter a lei estabelecido um sistema baseado na responsabilidade objetiva ou subjetiva, sendo respeitáveis os posicionamentos em ambos os sentidos.

Marcos Gomes da Silva Bruno[52] afirma que a Lei Geral de Proteção de Dados não é exatamente clara quanto à aplicabilidade da responsabilidade subjetiva ou da responsabilidade objetiva.

[51] CRUZ, Gisela Sampaio da. Responsabilidade civil da Lei de Proteção de Dados Pessoais. *In*: CONGRESSO INTERNACIONAL DE RESPONSABILIDADE CIVIL DO IBERC, 3., 2019, São Paulo. *Palestras* […]. [*S. l.*]: Iberc, 2019.

[52] BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. *In:* MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019, p. 323.

A inexatidão terminológica da Lei, como se verá, confere ao intérprete e ao aplicador da lei a possibilidade de uma primeira distinção clara na aplicação do sistema de responsabilidade civil conforme o agente de tratamento, se pessoa física ou jurídica de direito privado ou, em outra abordagem, se se estiver tratando de pessoa jurídica de direito público.

2.2.1 Quando o controlador é um ente público

É necessário se proceder a um primeiro corte do tema sob análise, excluindo, não sem antes abordar, o sistema de responsabilidade civil do tratamento de dados operacionalizado pelo ente público.

Ao ente público, a Lei Geral de Proteção de Dados dedicou o Capítulo IV "Do tratamento de dados pessoais pelo Poder Público"[53], com inegáveis reflexos em seu sistema de responsabilidade civil. Dispensou a ele um conjunto de deveres específicos em decorrência do tratamento de dados pessoais e traçou normas reguladoras do uso compartilhado de suas bases de dados entre órgãos da administração pública e entre este e um ou mais entes privados.

A despeito de louvável a preocupação do legislador em tratar do tema de forma sistematizada, é notável a dificuldade interpretativa dos dispositivos correlatos, conforme já tivemos a oportunidade de tratar[54].

Contrariamente, ao não tratar especificamente da responsabilidade civil dos entes públicos quando da verificação de danos decorrentes de tratamento de dados pessoais, a Lei deixou ao intérprete a tarefa de proceder à integração do sistema protetivo.

Não parece haver dúvidas que, nesta hipótese, a responsabilidade civil do ente público se dá com fundamento na teoria do risco administrativo.

Conforme a previsão maior vazada no artigo 37, §6º da Constituição Federal[55], nenhum particular deve suportar o dano decorrente de atividades voltadas para o interesse social da coletividade. O tema adquire especial relevância nos tempos atuais em que se espera do poder público um planejamento de políticas públicas baseado em dados a garantir a eficiência em sua implementação, desde que leve em consideração o risco decorrente.

Dessa forma, segundo o entendimento do Supremo Tribunal Federal[56], a responsabilidade estatal no espectro das atividades de tratamento de dados pessoais é analisada segundo os critérios da responsabilidade objetiva para os atos comissivos, aqui exemplificados como o tratamento e o compartilhamento irregular de dados e, por outro lado, segundo os pressupostos da responsabilidade subjetiva em se tratando de ato omissivo, como, por exemplo, a não observância das normas de prevenção e de segurança da informação a oportunizar o vazamento de dados pessoais dos cidadãos.

---

[53] TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019b, p. 263.

[54] TASSO, Fernando Antonio. Compartilhamento de dados entre o setor público e privado – possibilidades e limites. *Revista do Advogado*, São Paulo, n. 144, nov. 2019a.

[55] Art. 37, § 6º da Constituição Federal – As pessoas jurídicas de direito público e as de direito privado prestadoras de serviços públicos responderão pelos danos que seus agentes, nessa qualidade, causarem a terceiros, assegurado o direito de regresso contra o responsável nos casos de dolo ou culpa.

[56] RDA 137/233 – RTJ 55/50 – RTJ 163/1170-1109.

2.2.2 Quando o controlador é uma pessoa natural ou pessoa jurídica de direito privado

Em frente diversa, quando o controlador for pessoa física ou pessoa jurídica de direito privado, há que se analisar o sistema de configuração da responsabilidade civil não somente observando o critério pessoal, mas da relação jurídica subjacente, de acordo com uma visão dialógica das fontes.

Nesse âmbito, já nos estritos limites do direito privado, é cabível analisar os dispositivos pertinentes à responsabilidade civil dos agentes de tratamento na Lei Geral de Proteção de Dados conforme três critérios hermenêuticos, com o fito de identificar qual o sistema de responsabilidade civil adotado.

Antes da análise dos dispositivos legais sob a ótica dos critérios hermenêuticos, há que se estabelecer o fundamento da responsabilidade civil como dever sucessivo ao descumprimento de um dever originário.

A seguir, a interpretação sistemática permitirá identificar nos diplomas jurídicos existentes em nosso ordenamento jurídico e no estrangeiro, ambos já extensamente tratados pela doutrina e jurisprudência, qual o critério adotado e a técnica legislativa respectiva.

A interpretação teleológica buscará dar o respaldo finalístico à forma e à lógica de proteção ao bem jurídico tutelado.

Finalmente, buscar-se-á nos anais do processo legislativo a possível intenção do legislador ao atribuir aos artigos pertinentes à responsabilidade civil quanto ao tema a dicção legal que foi objeto de promulgação pela Casa Legislativa.

Trata-se, naturalmente, da abordagem de um tema em início de construção de modo que, longe da pretensão de exauri-lo, cumprirá à presente análise, lançar luzes sobre a questão.

2.3 A violação de um dever como ensejador da responsabilidade civil

A identificação do sistema de responsabilidade civil no âmbito da Lei Geral de Proteção de Dados, em um contexto em que não há expressa eleição do sistema da responsabilidade objetiva, fundada no risco, nem, por outro lado, da responsabilidade subjetiva decorrente da culpa, há que se proceder a uma análise do instituto do dever jurídico originário e sucessivo.

Nas palavras de Carlos Roberto Gonçalves, "A responsabilidade civil tem, pois, como um de seus pressupostos a violação do dever jurídico e o dano. Há um dever jurídico originário, cuja violação gera um dever jurídico sucessivo ou secundário, que é o de indenizar o prejuízo"[57].

Em suma, a responsabilidade subjetiva, que consiste no dever jurídico de reparar o dano, decorre da violação de um dever jurídico antecedente, qual seja o *neminem laedere*.

Portanto, conforme já assinalado por Cláudio Luiz Bueno de Godoy[58], a Lei Geral de Proteção de Dados cumpre o papel inovador do critério binário de imputação consistente na culpa ou no risco, ao prever que, no contexto do tratamento de dados pessoais, há deveres antes não enunciados explicitamente, mas agora tratados de forma categóri-

[57] GONÇALVES, Carlos Roberto. *Responsabilidade civil*. 10. ed. São Paulo: Revista dos Tribunais, 2007.

[58] Vide nota 28.

ca pela Lei a impor aos agentes de tratamento, os deveres de prevenção de incidentes, vigilância e segurança nas operações de tratamento de dados pessoais.

Assim sendo, a ressignificação e o alargamento do plexo dos deveres impostos aos indivíduos que ostentam a especial condição de agentes de tratamento resulta na leitura do sistema de responsabilidade civil na Lei Protetiva sob os pressupostos da responsabilidade subjetiva.

2.4 Interpretação sistemática

Em todas as situações jurídicas em que o legislador excepcionou a regra da responsabilidade subjetiva no direito privado, o fez de modo expresso e inequívoco, a exemplo do emprego da expressão "independentemente da existência de culpa" nos artigos 12 e 14 do Código de Defesa do Consumidor ou singelamente se referindo à obrigação de reparar o dado "independentemente de culpa", como na cláusula geral do artigo 927, parágrafo único do Código Civil.

Não há na Lei Geral de Proteção de Dados qualquer artigo que se valha da expressão "independentemente de culpa" ou "independentemente da existência de culpa", a indicar de modo inequívoco que o regime jurídico adotado fora o da responsabilidade objetiva.

Outro argumento eloquente a indicar a escolha da regra da responsabilidade subjetiva consiste no fato de que a Lei é pródiga na imposição de uma série de deveres de ação e de abstenção aos agentes de tratamento.

Esses deveres estão presentes em todos os segmentos da lei e vão desde a observância cumulativa e incondicional de todos os princípios de proteção de dados[59]; a disponibilização de forma clara, adequada e ostensiva das características do tratamento de dados[60]; a publicização acerca dos tipos de dados coletados[61]; a abstenção de coleta de dados desnecessários[62], a disponibilização de informações claras no tratamento de dados de crianças e adolescentes[63]; a manutenção de dados em formato interoperável e estruturado[64]; a comunicação de convênios de uso compartilhados de dados à Autoridade Nacional[65]; a divulgação ostensiva da identidade e das informações de contato do encarregado[66]; a adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito[67] desde a concepção do produto ou serviço (*privacy by design*)[68]; passando pela adoção das melhores práticas de segurança da informação[69]; pelo dever de comunicação

[59] Art. 6º da Lei 13.709/2018.
[60] Art. 9º da Lei 13.709/2018.
[61] Art. 14, §2º da Lei 13.709/2018.
[62] Art. 14, §4º da Lei 13.709/2018.
[63] Art. 14, §6º da Lei 13.709/2018.
[64] Art. 25 da Lei 13.709/2018.
[65] Art. 26, §2º da Lei 13.709/2018.
[66] Art. 41, §1º da Lei 13.709/2018.
[67] Art. 46 da Lei 13.709/2018.
[68] Art. 46, §2º da Lei 13.709/2018.
[69] Art. 47 da Lei 13.709/2018.

de incidente à Autoridade Nacional e ao titular dos dados[70]; e, finalmente, pela publicação das regras e boas práticas de governança[71].

À evidência, tais regras não consistem em meras recomendações tendentes a evitar incidentes de segurança. Antes, o legislador estabeleceu um *standard* de conduta e cobra o cumprimento desses deveres. O tratamento regular de dados[72] consiste em uma obrigação de resultado e não de meio.

Assim sendo, caso o sistema de responsabilidade civil fosse da modalidade objetiva, a prescrição exaustiva e detalhada dos deveres seria algo absolutamente inócuo, sobretudo porque redundaria na conclusão de que de nada adiantaria o cumprimento dos deveres se, qualquer que fosse o incidente, a responsabilidade pela reparação estivesse configurada, o que é um contrassenso.

Ao contrário, o artigo 42 prescreve a reparação do dano "em razão do exercício de atividade de tratamento de dados pessoais" causado "em violação à legislação de proteção de dados pessoais". A noção do condicionamento da reparação à violação da legislação de dados pessoais decorre de exegese elementar.

Em reforço a essa concepção, o artigo 43 da Lei prevê hipóteses excludentes de responsabilidade utilizando a expressão "só não serão responsabilizados quando provarem: II – que embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados". Ou seja, se não houve violação da legislação de proteção de dados, não há em princípio o dever de indenizar.

Um aspecto a ser tratado em outra seara consiste em identificar a subsistência, nessa hipótese, dos deveres anexos da boa-fé objetiva, tratada no artigo 6º "caput" da Lei, como os deveres de assistência e de mitigação do dano.

A mesma lógica condicionante da responsabilidade civil encontra-se presente no artigo 44 ao prever que o tratamento de dados será irregular somente quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar. Contrariamente, não pode ser tido como irregular o tratamento que observou a lei e que, concomitantemente, proveja a segurança que dele se espera.

Desse modo, a reparabilidade pelos danos advindos de ato lícito somente se dá por expressa disposição legal, a adotar de modo inequívoco a responsabilidade objetiva cuja caracterização, conforme o ensinamento de Maria Cecília Bodin de Moraes[73], "independe, completamente de negligência, imprudência, imperícia ou mesmo da violação de qualquer dever jurídico por parte do agente. São danos (injustos) causados por atos lícitos, mas que, segundo o legislador, devem ser indenizados.". Evidentemente, não é essa a hipótese do precitado artigo.

Na mesma linha é a dicção do parágrafo único do artigo 44 ao prever que somente responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no artigo 46,

[70] Art. 48 da Lei 13.709/2018.

[71] Art. 50, §3º da Lei 13.709/2018.

[72] Art. 44 da Lei 13.709/2018, *a contrario sensu*.

[73] MORAES, Maria Celina Bodin de. Risco, solidariedade e responsabilidade objetiva. *Revista dos Tribunais*, São Paulo, v. 854, dez. 2006, p. 25.

der causa ao dano. Mais uma vez, o dever sucessivo da responsabilidade civil decorre da infringência a um dever originário, o de adotar as medidas de segurança previstas na Lei.

É cediço ser todo o sistema de responsabilidade civil na Lei Geral de Proteção de Dados intrinsecamente vinculado ao elemento culpa.

De remate, é pertinente uma análise comparativa entre as causas excludentes da responsabilidade civil constantes do artigo 43 da Lei e do artigo 12, §3º do Código de Defesa do Consumidor, que sabidamente adotou a responsabilidade objetiva como regra.

Enquanto as hipóteses dos incisos I e III de ambos os artigos se equivalem, este coloca como excludente a não colocação do produto no mercado, o que consiste num fato de objetividade binária, enquanto a Lei Geral de Proteção de Dados prevê mais um dever ao agente de tratamento de dados, qual seja a observância de uma conduta diligente que, em sendo observada é causa de elisão da responsabilidade civil.

2.5 Interpretação teleológica

A sociedade da informação é marcada por frequentes e reiterados vazamentos de dados, bastando que se faça uma busca pela expressão "vazamento de dados" em mecanismos de busca na Internet para se ter acesso a incontáveis relatos de incidentes envolvendo dados pessoais distribuídos por todo o globo.

Colocações como "*another day, another breach*"[74] e que o vazamento de dados é mais uma questão de "quando" e menos uma questão de "se" demonstram que incidentes de segurança envolvendo dados pessoais são uma realidade inafastável, cabendo à regulamentação temática prover meios de mitigar seus efeitos pela imposição aos agentes de tratamento de deveres de prevenção e segurança.

Foi justamente com a finalidade de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural que a própria Lei Geral de Proteção de Dados enunciou em seu artigo 1º ser este o objetivo de sua existência.

Nem mesmo o intérprete mais aguerrido identificará na Lei entraves injustificáveis à atividade de tratamento de dados por entes privados e entes públicos, sobretudo porque ao lado de tutelar direitos e garantias individuais como a autodeterminação informativa, o respeito à privacidade e a defesa do consumidor, a Lei fundamenta-se no desenvolvimento econômico e tecnológico, na inovação, na livre iniciativa, na livre concorrência.

De tal sorte, a adoção como regra do sistema de responsabilidade civil objetiva resultaria em autêntico desincentivo à observância dos deveres específicos de proteção, prevenção e segurança impostos aos agentes de tratamento, desprestigiando, igualmente, a ideia de um adequado fluxo informacional como solução para uma economia global baseada em dados.

[74] Em tradução livre: "Outro dia, outro vazamento".

2.6 Interpretação histórica

À medida que questões como a ora colocada vão sendo desafiadas pela doutrina e jurisprudência, conclusões extraídas da interpretação histórica se tornam irrelevantes.

No entanto, encontrando-se a Lei Geral de Proteção de Dados em período de *vacatio legis*, é pertinente trazer à luz um argumento dessa natureza como forma de sedimentar a conclusão de que o sistema de responsabilidade civil adotado pela Lei foi o da responsabilidade subjetiva, pela constatação de que o legislador suprimiu deliberadamente qualquer expressão que pudesse ser relacionada à responsabilidade objetiva.

O Projeto de Lei 5.276/2016, que resultou na redação final da Lei 13.709/2018, previa no artigo 35, inserido no Capítulo V, que tratava sobre "Transferência internacional de dados" que "O cedente e o cessionário respondem, solidária e objetivamente pelo tratamento de dados, independentemente do local onde estes se localizarem, em qualquer hipótese". Tal disposição, que consistia na única referência à responsabilidade objetiva, foi extirpada do texto final e não replicada em qualquer outro dispositivo.

Bem assim, a redação original do artigo 42, inserido no Capítulo VI "Dos agentes de tratamento", Seção II, era nos seguintes termos: "Todo aquele que, em razão do tratamento de dados, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo" não havendo, portanto, qualquer menção à violação da Lei como condição do dever de indenizar, como ficou sacramentada na redação aprovada. Ao contemplar na redação final o condicionamento a um dever, o fez em prestígio ao sistema de responsabilidade subjetiva.

Conclui-se que, se por um lado qualquer referência à responsabilidade objetiva foi suprimida no texto promulgado, por outro e, em reforço à tese da responsabilidade subjetiva, diversos são os argumentos a demonstrar a adoção desta sistemática.

3. A interface da Lei Geral de Proteção de Dados com o Código Civil

A noção de culpa a legitimar a reparação do dano decorrente do descumprimento de um dever já representava uma evolução em relação à ideia de vingança privada a nortear as relações interpessoais na sociedade antiga.

A este período marcado pela autotutela, sucedeu-se o período da composição, em que a substituição da vindita pela compensação econômica decorreu da identificação pelo indivíduo de sua vantajosidade, ainda que não se cogitasse a ideia de culpa.

Somente com a evolução histórica que redundou na ascensão de uma autoridade soberana, o aspecto reparatório, que era facultativo e a critério da vítima, passou a ser obrigatório e, inicialmente, tarifado como bem se identifica no Código de Ur-Nammu, no Código de Manu e na Lei das XII Tábuas[75].

Nos tempos dos romanos, a diferenciação entre pena e reparação deu ensejo à diferenciação entre delitos públicos, hoje conhecido como o ilícitos penais, e delitos privados ou ilícitos civis. Enquanto naquela a indenização era recolhida aos cofres públicos, nesta, o dinheiro cabia à vítima.

[75] GONÇALVES, Carlos Roberto. *Responsabilidade civil*. 10. ed. São Paulo: Revista dos Tribunais, 2007.

A assunção pelo Estado do monopólio da punição e repressão dos ilícitos públicos, a responsabilidade penal surgiu ao lado da responsabilidade civil.

Nesse contexto, a Lei Aquilia era a referência da jurisprudência clássica com relação à injúria e fonte direta da moderna concepção de culpa, por esse motivo chama de aquiliana.

O direito francês foi o primeiro a estabelecer, paulatinamente, princípios que exerceram influência em outros povos generalizando o princípio aquiliano, pelo qual a culpa, ainda que levíssima, obrigava a indenizar.

O Código Napoleão previu em seu corpo normativo a noção de culpa em abstrato, bem como a distinção da culpa delitual e culpa contratual.

A concepção de que a responsabilidade civil se funda na culpa e sua reafirmação nos diplomas legais subsequentes e na jurisprudência francesa, foram fatores que irradiaram efeitos na produção legislativa dos povos ocidentais, inclusive na brasileira.

No direito brasileiro, o Código Civil de 1916 filiou-se à teoria subjetiva exigindo, portanto, prova de culpa ou dolo do causador do dano como pressuposto para sua reparação, sendo esta presumida em casos excepcionais.

Com a evolução tecnológica e o impacto nas relações pessoais e negociais, a concepção tradicional da reparação que pressupunha a existência de culpa passou a não mais atender ao reclamo social pela proteção da vítima, dando ensejo ao desenvolvimento da teoria do risco.

O reflexo imediato da garantia constitucional da privacidade, enquanto direito personalíssimo, vem gizado nos artigos 11[76] e 21[77] do Código Civil que vedam a limitação voluntária dos direitos da personalidade e reafirmam a inviolabilidade da vida privada, prevendo a reparação por perdas e danos, sem prejuízo de outras sanções previstas em lei.

A lei material adotou por regra a responsabilidade civil subjetiva em seu artigo 186 ao prever que todo aquele que violar direito e causar dano a outrem comete ato ilícito. Essa prescrição é complementada pelo artigo 927 do Código Civil que preconiza: "Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo".

Excepciona a regra a hipótese do exercício de atividade de risco, através da cláusula geral de responsabilidade do artigo 927, parágrafo único[78], bem como em outras disposições legais em que a reponsabilidade civil se verifica independentemente de culpa (artigo 931[79]), inclusive em se tratando de ato de terceiro (artigo 932[80]).

[76] Artigo 11 do Código Civil.

[77] Artigo 12 do Código Civil.

[78] Código Civil – Art. 927, parágrafo único: Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

[79] Código Civil – Art. 931 – Ressalvados outros casos previstos em lei especial, os empresários individuais e as empresas respondem independentemente de culpa pelos danos causados pelos produtos postos em circulação.

[80] Código Civil – Art. 932 – São também responsáveis pela reparação civil:
I – os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;
II – o tutor e o curador, pelos pupilos e curatelados, que se acharem nas mesmas condições;
III – o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele;
IV – os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos;
V – os que gratuitamente houverem participado nos produtos do crime, até a concorrente quantia.

No contexto das relações privadas regidas pelo Código Civil, portanto, em que a regra do sistema de responsabilidade civil baseia-se nos requisitos da responsabilidade subjetiva, excepcionando hipóteses específicas, bem como o exercício de atividade de risco por uma cláusula geral, denota-se que o sistema adotado pela Lei Geral de Proteção de Dados tem perfeita consonância com a matriz legal.

As relações jurídicas de tratamento de dados pessoais celebradas no âmbito do direito privado são fundadas, portanto e em regra, no sistema de responsabilidade civil subjetiva, somente verificável pela demonstração da culpa do agente de tratamento, identificável pelo descumprimento de um dever legal enunciado na própria Lei Geral de Proteção de Dados.

Consequentemente, as excludentes de responsabilidade civil aplicáveis à hipótese seguem a regra do sistema civilista.

Excepcionam a regra as atividades de tratamento de dados pessoais que sejam essencialmente, não apenas reflexamente, consideradas atividades de risco, hipótese em que a elas se aplica o sistema da reponsabilidade objetiva por incidência da regra do artigo 927, parágrafo único do Código Civil, sob o fundamento da teoria do risco do negócio ou da atividade.

A interpretação dialógica entre as fontes deve ser feita com cautela, na medida em que não se pode admitir como risco toda e qualquer situação, sob pena de banalização do instituto, como adverte Marcos Gomes da Silva Bruno[81].

A interface da Lei Geral de Proteção de Dados com o Código de Defesa do Consumidor

A Lei 13.709/2018 positivou em seu artigo 45 a interligação entre o microssistema de proteção e defesa do consumidor e o microssistema de proteção de dados, especificamente no que diz respeito às regras da responsabilidade civil.

No microssistema das relações de consumo, a regra da responsabilidade civil é objetiva quando se trata de fato do produto ou serviço, por força dos artigos 12 e 14 do Código de Defesa do Consumidor.

Questão que se coloca é se a violação de direito do titular de dados em toda e qualquer relação de consumo atribui ao fato jurídico o tratamento dispensado pelo Código de Defesa do Consumidor, que adota o sistema de responsabilidade objetiva.

A resposta deve ser afirmativa, na medida em que a Constituição Federal alçou a defesa do consumidor ao patamar de garantia fundamental[82], enquanto o direito fundamental à proteção de dados ainda busca sua colocação Constitucional pela Proposta de Emenda Constitucional nº 17/2019.

Conclui-se que, pela relevância apriorística da defesa do consumidor hoje desenhada pelo mosaico de direitos e garantias fundamentais que integram o artigo 5º da Constituição Federal, em havendo o elemento de conexão resultante da relação de consumo, ainda que não tivesse sido expressamente previsto no artigo 45 da Lei, haveria que se dispensar à violação do direito do titular de dados na relação de consumo,

[81] BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019, p. 325.

[82] Art. 5º, XXXII da Constituição Federal.

o tratamento jurídico da responsabilidade objetiva previsto no microssistema do Código de Defesa do Consumidor.

Identifica-se que, no atual panorama Constitucional e infralegal, a relação entre os microssistemas não é de mera intersecção, mas de continência, na medida em que a toda e qualquer violação de direito do consumidor deve-se atribuir, dentre os regimes jurídicos elegíveis, o que melhor atenda à defesa do consumidor.

Uma vez tendo se estabelecido que a Lei Geral de Proteção de Dados adotou, como regra, a responsabilidade civil subjetiva, a melhor interpretação parece ser no sentido da derrogação legal em favor da responsabilidade objetiva, nas hipóteses previstas no Código de Defesa do Consumidor.

No que concerne às hipóteses excludentes de responsabilidade, contudo, o sistema a ser seguido deve ser, necessariamente, o do artigo 43 da Lei Geral de Proteção de Dados em detrimento daquele previsto no artigo 12, §3º do Código De defesa do Consumidor.

Conforme já explicitamos, as hipóteses dos incisos I e III de ambos os artigos se equivalem, enquanto a hipótese do inciso II desenha uma clara diferenciação entre os sistemas que, se por um lado indica ser subjetiva a regra da responsabilidade civil na Lei Geral de Proteção de Dados, por outro, positiva a existência de um regime próprio às relações jurídicas que envolvem tratamento de dados.

Enquanto o inciso II do referido artigo do Código de Defesa do Consumidor prevê como excludente de responsabilidade civil a não colocação do produto no mercado, o que consiste num fato de objetividade binária, o da Lei Geral de Proteção de Dados prevê mais um dever ao agente de tratamento de dados, qual seja a observância de uma conduta diligente que, em sendo observada é causa de exclusão da responsabilidade civil.

Conclusão

O avanço tecnológico é elemento propulsor da evolução do direito como instrumento de garantia dos direitos fundamentais, que neste momento histórico se depara com a identificação de novos riscos.

A releitura dos institutos clássicos do direito alinhada à regulamentação de novos deveres dos sujeitos de direitos permite uma compreensão do direito como um sistema harmônico e completo, cabendo às leis que regulamentarão essas novas hipóteses de responsabilidade civil, prever de forma clara os deveres dos partícipes das novas relações jurídicas, imputando a cada qual as hipóteses de responsabilidade civil.

A Lei Geral de Proteção de Dados criou um sistema de responsabilidade civil compatível com o Código Civil e o Código de Defesa do Consumidor para regular as relações jurídicas de direito privado baseadas no tratamento de dados pessoais.

A despeito dos embates doutrinários, verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva em perfeito alinhamento com o Código Civil, inserindo-se de forma harmoniosa no mosaico legislativo, o mesmo ocorrendo em relação ao Código de Defesa do Consumidor que, dado o tratamento Constitucional da defesa do consumidor, atrai para seu sistema de responsabilidade objetiva os fatos jurídicos dessa natureza.

Bibliografia

BARBOSA, Marcos T. J.; BAISSO, Marcos; ALMEIDA, Marcos T. Surge uma nova sociedade. *In*: SILVA, Elcio B.; SCOTON, Maria L. R. P. D.; PEREIRA, Sérgio L.; DIAS, Eduardo M. *Automação & sociedade*: Quarta Revolução Industrial, um olhar para o Brasil. São Paulo: Brasport, 2018.

BRASIL. Senado Federal. *Proposta de Emenda à Constituição nº 17, de 2019*. Acrescenta o inciso XII-A, ao art. 5º, e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria. Brasília, DF: Senado Federal, 2019. Disponível em: https://bit.ly/2RgVmzz. Acesso em: 4 dez. 2019.

BRUNO, Marcos Gomes da Silva. Dos agentes de tratamento de dados pessoais. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. *Cadernos Jurídicos*, [2020]. No prelo.

CRUZ, Gisela Sampaio da. Responsabilidade civil da Lei de Proteção de Dados Pessoais. *In*: CONGRESSO INTERNACIONAL DE RESPONSABILIDADE CIVIL DO IBERC, 3., 2019, São Paulo. *Palestras* […]. [*S. l.*]: Iberc, 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

GODOY, Cláudio Luiz Bueno. A responsabilidade civil na era digital. *In*: CONGRESSO INTERNACIONAL DE RESPONSABILIDADE CIVIL DO IBERC, 3., 2019, São Paulo. *Palestras* […]. [*S. l.*]: Iberc, 2019.

GONÇALVES, Carlos Roberto. *Responsabilidade civil*. 10. ed. São Paulo: Revista dos Tribunais, 2007.

HALÉVI, Marc. *A era do conhecimento*: princípios e reflexões sobre a revolução noética no século XXI. São Paulo: Editora Unesp, 2010.

MENDES, Laura Schertel. *Contexto internacional e economia de dados pessoais; histórico da implementação da regulamentação europeia de proteção de dados (GPDR); Marco Civil da Internet, Código de Defesa do Consumidor e Cadastro Positivo; Lei Geral de Proteção de Dados (LGPD) e Medida Provisória 869/2018*. São Paulo: Escola da Defensoria Pública, 13 jun. 2019. Palestra proferida no curso sobre a Lei Geral de Proteção de Dados.

MORAES, Maria Celina Bodin de. Risco, solidariedade e responsabilidade objetiva. *Revista dos Tribunais*, São Paulo, v. 854, dez. 2006.

NISSENBAUM, Helen. *Privacy in Context*: Technology, Policy, and the Integrity of Social Life. Stanford: Stanford Law Books, 2010.

REALE, Miguel. *Lições preliminares de Direito*. 27. ed. São Paulo: Saraiva, 2013.

RODOTÁ, Stefano. *A vida na sociedade de vigilância*: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SCHREIBER, Anderson. *Novos paradigmas da responsabilidade civil*. A erosão dos filtros da reparação à diluição dos danos. 6. ed. São Paulo: Atlas, 2015.

SCHWAB, Klaus. *Aplicando a Quarta Revolução Industrial*. São Paulo: Edipro, 2018.

TASSO, Fernando Antonio. Compartilhamento de dados entre o setor público e privado – possibilidades e limites. *Revista do Advogado*, São Paulo, n. 144, nov. 2019a.

TASSO, Fernando Antonio. Do tratamento de dados pessoais pelo Poder Público. *In*: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. *LGPD*: Lei Geral de Proteção de Dados comentada. São Paulo: Revista dos Tribunais, 2019b.

THE WORLD'S most valuable resource is no longer oil, but data. *The Economist*, London, 6 maio 2017. Disponível em: https://econ.st/37geKlQ. Acesso em: 21 jan. 2020.

WARREN, Samuel D.; BRANDEIS, Louis D. The right to privacy. *Harvard Law Review*, Cambridge, v. 4, n. 5, 15 dez. 1890.

YOUR Data for sale. *Time*. New York: Time Inc, v. 177, n. 11, 21 mar. 2011.

A autoridade nacional de proteção de dados: evolução legislativa, composição e atuação

Rubens Rihl
Desembargador do Tribunal de Justiça de São Paulo

Sumário: Um fato político; A lei brasileira; Papel da autoridade nacional; Composição da ANPD; Autonomia e independência; Bibliografia.

Resumo: O texto analisa a evolução legislativa sobre a proteção de dados pessoais, pela perspectiva da Autoridade Nacional de Proteção de Dados, criada pela Lei 13.853/2019. Traça um panorama sobre a composição da ANPD e a respectiva atuação, além de comentários sobre seu grau de autonomia.

Palavras-chave: Proteção de Dados Pessoais. Autoridade Nacional de Proteção de Dados. Conselho Diretor. Evolução Legislativa. Composição. Atuação. Lei 13.709/2018. Medida Provisória 869/2018. Lei 13.853/2019. Lei Geral de Proteção de Dados. Autonomia. Independência. Independência Orçamentária.

Um fato político

A legislação brasileira que cuidou da proteção de dados pessoais até o momento não é sistematizada ou mesmo consolidada. Alguns poucos dispositivos esparsos em vários diplomas legais eram encontrados. Código Civil, Código do Consumidor, Código Eleitoral, dentre outros, contemplavam acidentalmente tal cobertura.

Não poucas vezes, o tema não era tratado pelo valor que tinha e sua visibilidade no mundo jurídico era de baixa importância.

Analisando sua evolução, pelo ponto de vista histórico, entendemos um pouco mais porque galgou patamares mais elevados.

Em 13 de agosto de 1961, como é sabido, um muro foi construído separando fisicamente a Alemanha e, em especial, a cidade de Berlim. Da noite para o dia, literalmente, famílias e amigos foram separados. Em novembro de 1989, vinte e seis (26) anos depois, tal divisor foi derrubado (*Berliner Mauer*) e os alemães buscaram reunificar seu país e reencontrar seus entes queridos.

Surgiu assim a República Federal da Alemanha (*Bundesrepublik Deutschland*). A euforia tomou conta de todos os cidadãos e comemorações enormes foram feitas, homenageando a libertação de Berlim. Tal acontecimento irradiou seus efeitos para outros países da Europa. O movimento de eliminação de fronteiras se fortaleceu. Até que, em **1993** nasceu a **União Europeia**, fortemente influenciada pelos fatos acontecidos em 1989.

No entanto, junto com a onda evolutiva e a formação do bloco europeu, aflorou também a necessidade de **revisão de diversos procedimentos nas relações** que existiam

entre os países, muitos dos quais com diferenças sensíveis. Dentre esses ajustes, a troca de informações no mercado, entre as pessoas, órgãos de segurança pública e de Estado encontrava dissintonias patentes. Tal demanda levou a União Europeia a padronizar procedimentos e criar protocolos comuns. A Diretiva 95[1] foi a primeira norma em matéria de proteção de dados que envolveu todo o bloco. Cuidava de viabilizar as transações comerciais e bancárias, dentre outras áreas, de forma ágil e eficiente. Sua base levava em conta especialmente a proteção de dados pessoais.

Mais tarde essa norma evoluiu para outra, muito mais abrangente e precisa. Ela trouxe o ajuste fino necessário e corrigiu alguns dispositivos da antiga regra. As primeiras discussões ocorreram no Parlamento Europeu e no Conselho da União Europeia em 2014 até que, em 18 de maio de 2018, já formalizado, o Regulamento Geral sobre a Proteção de Dados[2] (RGPD) ou ***General Data Protection Regulation*** (GPDR) entrou em vigor.

Revolucionário, esse novo regulamento influenciou a criação de leis em outros países e praticamente tornou-se um padrão internacional no tratamento de dados pessoais. Cito exemplos: Estados Unidos, o ***California Consumer Privacy Act***, de 2018; México, a **Ley General de Protección de Datos Personales (LGPDP)**, de 2017; e o Brasil, com a **Lei de Proteção de Dados**, de 2018.

A Lei Brasileira

Entre 28 e 30 de maio de 2012, no WTC-SP, as vinte (20) maiores agências de publicidade, junto com as principais redes de TV e de rádio e as grandes editoras, reuniram-se no **V Congresso Brasileiro da Indústria da Comunicação** para discutir os ataques, agravos, ofensas, que o setor sofria nas redes sociais e que chamaram de ***bullying digital***. Eram reações causadas pela intolerância e pelo discurso politicamente correto. Para tanto, se fazia necessário agir para proteção (expressão comercial, propaganda, publicidade com ética e isenção, independência). Um sistema de autorregulamentação, nos moldes do Conselho Nacional de Autorregulamentação Publicitária (Conar). No caso do Brasil, a premissa era diversa da União Europeia. Aqui, **buscava-se a proteção do mercado publicitário e de comunicação**. Esse esforço resultou em projetos de lei voltados para essa proteção.

Os mais atentos acompanhavam as discussões na Europa e noticiaram no Congresso a existência de uma **norma melhorada** e que atendia, de certa forma, o anseio original dos empresários, embora com foco voltado às pessoas físicas. Nossos legisladores resolveram aglutinar todos os projetos em tramitação, depurar tudo e aproximar o texto ao máximo da regra europeia. Havia um temor também do mercado brasileiro se distanciar da União Europeia no comércio.

[1] Relativa à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Foi publicada em 24 de outubro de 1995 e possuía 72 justificativas e 34 artigos. Disponível em: https://bit.ly/2RpASUa. Acesso em: 5 ago. 2019.

[2] O Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho foi publicado em 27 de abril de 2016 com uma Vacatio Legis de dois anos, entrando em vigor em 18 de maio de 2018. Disponível em: https://bit.ly/2NAs24R. Acesso em: 5 ago. 2019.

Enquanto isso, o bloco europeu já discutia uma atualização daquela Diretiva de 1995. Em 2014 a redação do novo regulamento ganhou corpo, acompanhada de grandes discussões desde 2012.

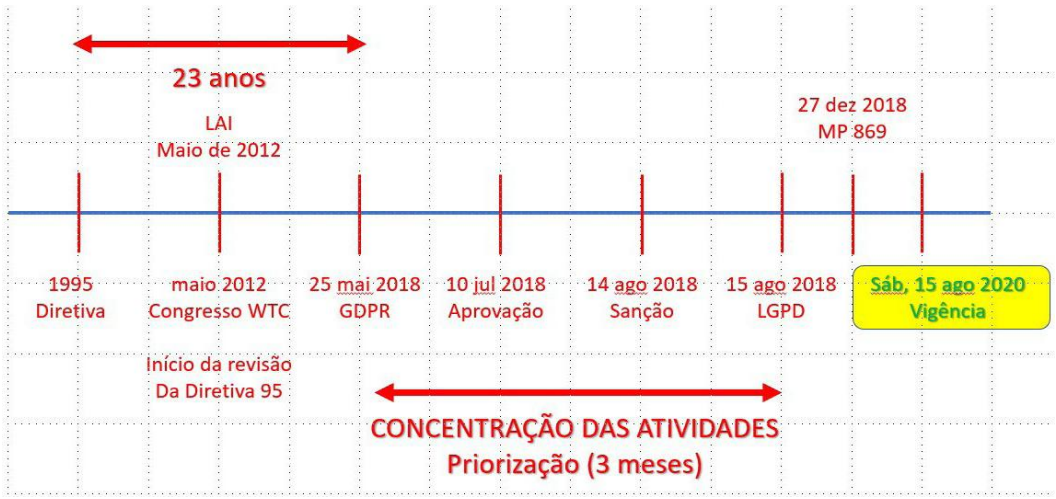
Diferentemente da discussão e do amadurecimento da regra europeia, que consumiu **vinte e três (23) anos**, no nosso caso, os debates no Legislativo Brasileiro não ultrapassaram **três (3) meses**, entre a criação do texto legal e a sua publicação. A Lei 13.709/2018 foi aprovada em agosto de 2018, fortemente influenciada pelo regramento europeu.

Como o projeto iniciou na Câmara dos Deputado e foi endossado pelo Senado, o novo parâmetro legal avançou em área que não lhe competia, isto é, definiu a Autoridade Nacional de Proteção de Dados (ANPD), sua composição, ganhos e a que órgão do Poder Executivo estaria vinculada, em clara inconstitucionalidade. Por isso, a Presidência da República vetou alguns de seus artigos, em razão desse vício formal.

Posteriormente, o Chefe do Poder Executivo editou a Medida Provisória 869/2018 para corrigir esse desvio com mais algumas alterações. Após discussão no Congresso Nacional, a Medida Provisória transformou-se na Lei 13.853/2019, alterando mais uma vez a configuração da ANPD.

Em síntese, nossa Lei de Proteção de Dados Pessoais teve um desenvolvimento um tanto tormentoso. Nasce por propósitos eminentemente de mercado, muda radicalmente de foco, agora voltado à proteção de dado das pessoas naturais, chega como lei (13.709/2018), é parcialmente vetada e reorganizada por uma Medida Provisória (869/2018) e novamente alterada por outra lei (13.853/2019) num período de dez meses, ainda durante a ***Vacatio Legis***.

Figura 1 — Concentração das atividades



Papel da Autoridade Nacional

Antes de cuidarmos de sua composição, é preciso compreender por que essa Autoridade foi criada.

Como se observa na simples leitura da lei, se fazia necessário que alguém zelasse pela proteção dos dados pessoais, pelos segredos comerciais e industriais, pela proteção da pessoa física, do sigilo das informações e que estabelecesse quais providências poderiam ser tomadas no caso de quebra do sigilo por violação da lei.

De suma importância, também se buscava algum ente que elaborasse as diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, além de fiscalizar e aplicar, quando o caso, as sanções e, em caso de violação, ser intermediador das reclamações que surgirem, destinando-as ao órgão competente, dentre outros (elaboração de convênios nacionais e internacionais, definição de padrões de serviço etc.)[3].

Justifica-se, portanto, a criação desse ente público.

Composição da ANPD

Fica patente que a Autoridade Nacional não está restrita a uma única pessoa ou órgão. Em sua redação original, era composta por vinte e seis (26) membros, desconsiderando-se os setores de apoio.

Posteriormente, com a Medida Provisória, notou-se um aumento em sua composição, para vinte e oito (28) membros. Finalmente, já na versão final (Lei 13.853/2019), manteve o mesmo número de integrantes.

Observa-se que a Medida Provisória trouxe uma estrutura melhor para a ANPD. Primeiro, porque deixou de se subordinar ao **Ministério da Justiça**, passando às mãos da **Presidência da República**, numa clara sinalização de sua importância pelo ponto de vista do Governo Federal. Em segundo lugar, porque recebeu uma Corregedoria, uma Ouvidoria e uma Assessoria Jurídica Especializada, antes inexistentes. Em terceiro lugar, porque teve um reforço no Conselho Diretor, passando de três (3) para cinco (5) membros.

Já em sua versão final, manteve seus integrantes em vinte e oito (28) membros, mantendo-se no mais as melhorias alcançadas pela Medida Provisória.

[3] Vide artigo 55-J e ss.

Figura 2 — Lei 13.709/2018

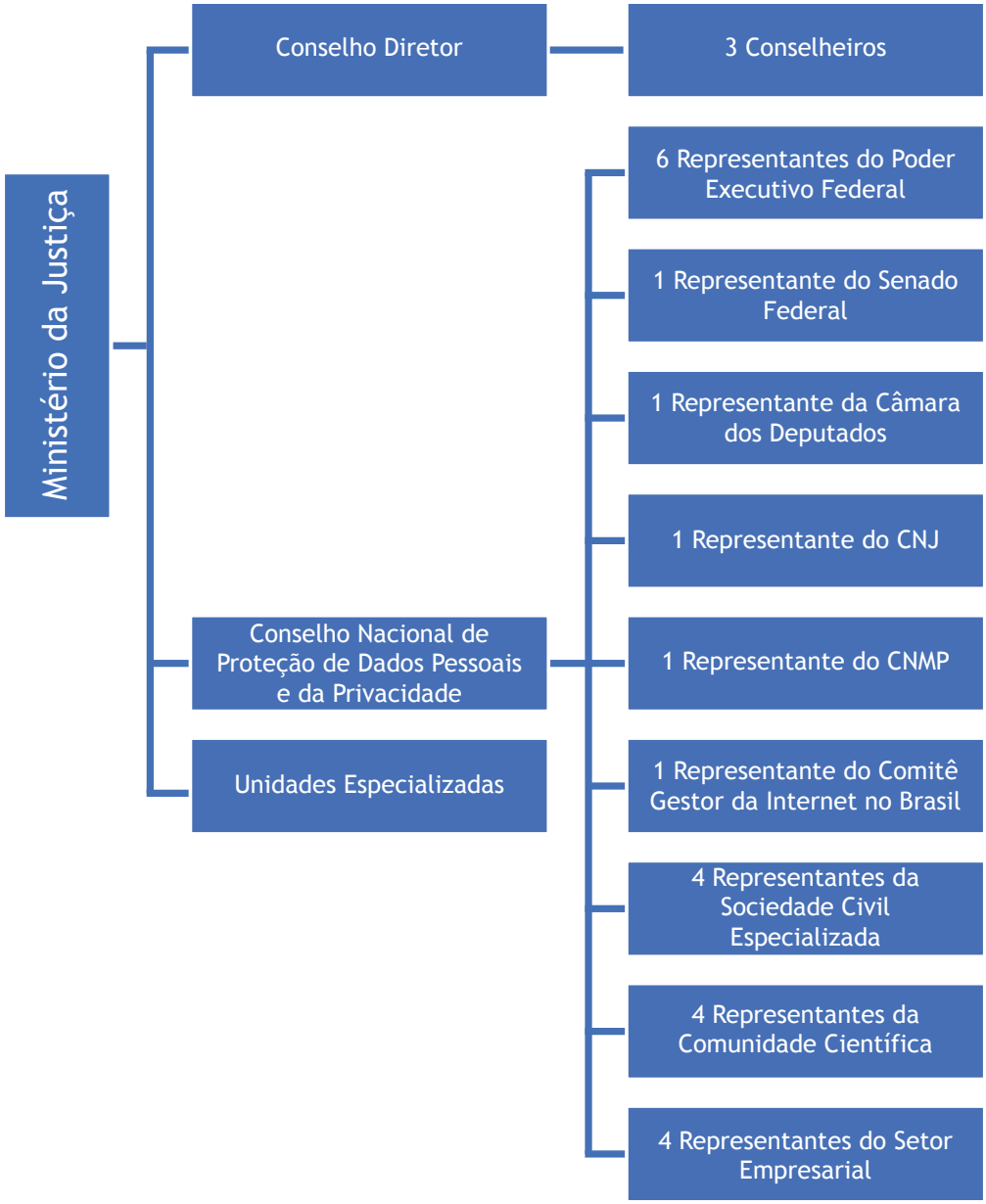


Figura 3 — Medida Provisória 869/2018

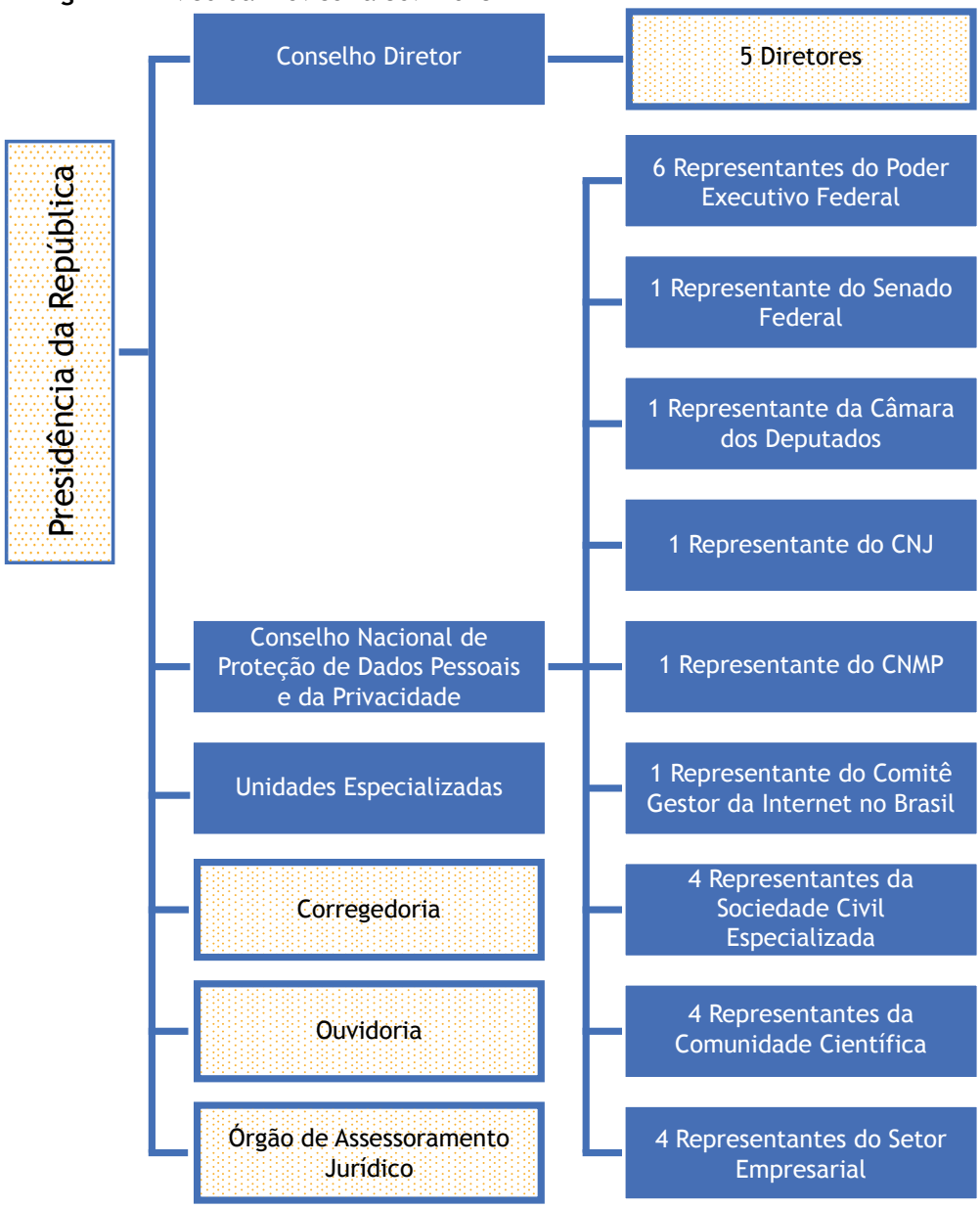
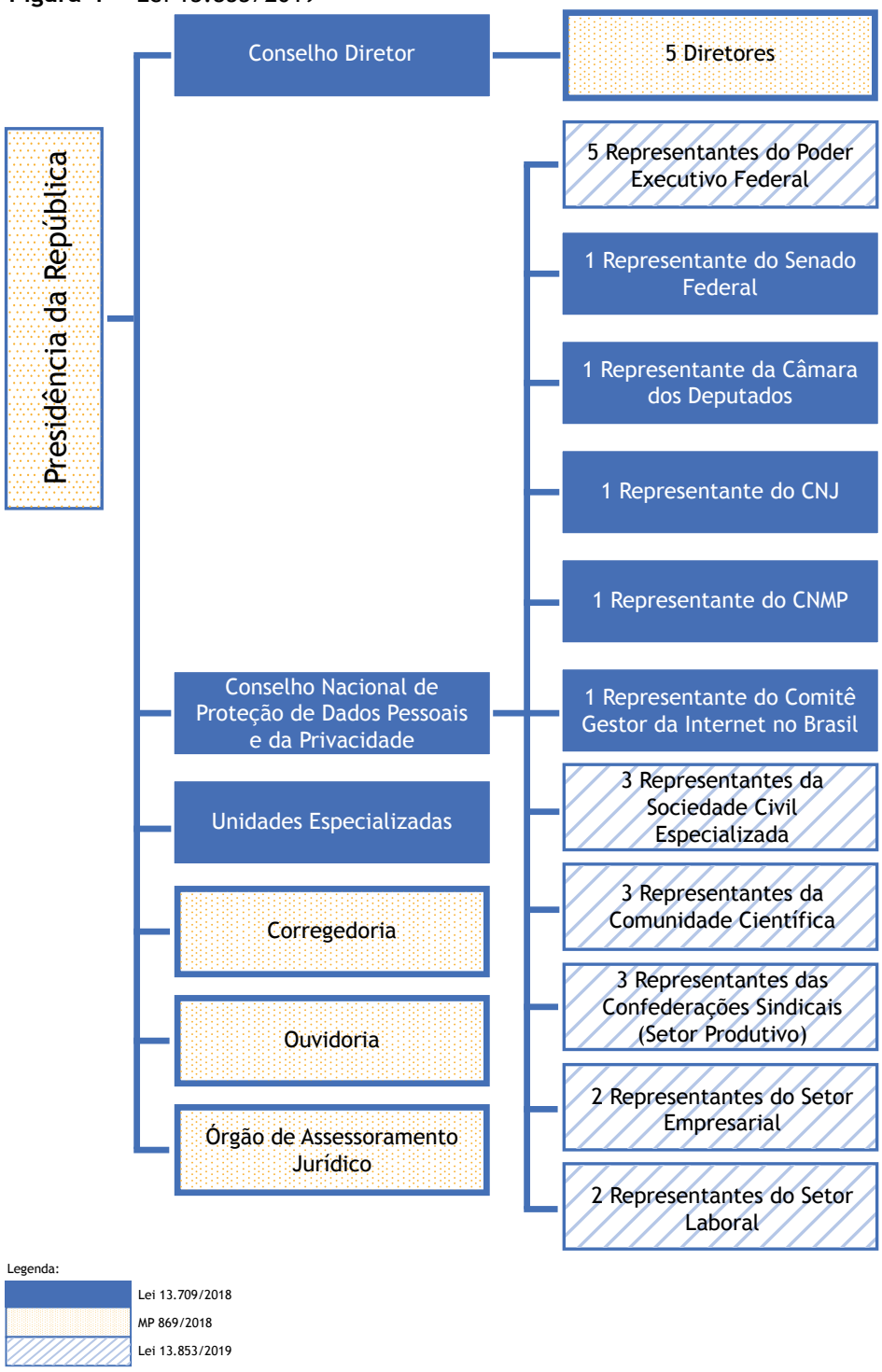


Figura 4 — Lei 13.853/2019



Autonomia e Independência

Talvez esse tópico seja o mais polêmico em nossa legislação especial. Um órgão que tem por dever a proteção dos dados pessoais e subordinado à Presidência da República poderia ser considerado autônomo e independente?

O artigo 55-B na lei deixa expresso que "Art. 55-B. É assegurada autonomia técnica e decisória à ANPD".

O governo federal manteve a ANPD sob seu domínio, ainda que tenha tentado relativizar esse vínculo com a redação dada ao artigo 55-A, parágrafo 1º.:

> *Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República.*
> *§ 1º **A natureza jurídica da ANPD é transitória e poderá ser transformada** pelo Poder Executivo **em entidade da administração pública federal indireta, submetida a regime autárquico especial** e vinculada à Presidência da República. (Grifo nosso)*

Como é dito, a ANPD é constituída por vários órgãos. Dois deles têm especial destaque o Conselho Diretor (CD) e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDPP).

Cabe ao Conselho Diretor as atribuições previstas no artigo 55-F da Lei de Proteção de Dados Pessoais. Já o Conselho Nacional de Proteção de Dados tem sua competência estabelecida no artigo 58-J do referido diploma legal. Fazemos essas referências apenas para pontuar o tema, cujo assunto exige um estudo específico e que, por ora, não atinge os objetivos da presente análise.

Nota-se que somente **um órgão** possui poder deliberativo sobre determinadas questões e, portanto, influencia nas políticas públicas relacionadas ao tema. Basta analisar alguns dos dispositivos da lei[4]. É de se destacar a proporção que cada Poder de Estado tem sobre cada um desses órgãos.

Quanto aos demais órgãos, a Corregedoria que atua na fiscalização das atividades e o restante assessoram os dois mais importantes e não possuem poder deliberativo algum.

Pelo ponto de vista do Conselho Diretor, temos a seguinte proporção:

Tabela 1 — Conselho diretor

Conselho Diretor									
Normas	**Integrantes**	**Executivo**	**%**	**Legislativo**	**%**	**Judiciário**	**%**	**Sociedade Civil**	**%**
Lei 13.709/2018	3	3	100	0	0	0	0	0	0
MP 869/2018	5	5	100	0	0	0	0	0	0
Lei 13.853/2019	5	5	100	0	0	0	0	0	0

[4] Lei 13.853/2019, artigos 55-J, III, IV, X, XI, XIII, XV, XVI, XVII, XVIII, XX, XXI, XXII, XXIV, dentre outros.

Em outros termos, o Poder Executivo domina integralmente este órgão.

Se analisarmos sob a perspectiva do Conselho Nacional de Proteção de Dados, a proporção é de:

Tabela 2 — Conselho Nacional de Proteção de Dados e da Privacidade

Conselho Nacional de Proteção de Dados e da Privacidade									
Normas	**Integrantes**	**Executivo**	**%**	**Legislativo**	**%**	**Judiciário**	**%**	**Sociedade civil**	**%**
Lei 13.709/2018	23	6	26,1	2	8,7	1	4,3	14	60,9
MP 869/2018	23	6	26,1	2	8,7	1	4,3	14	60,9
Lei 13.853/2019	23	5	21,7	2	8,7	1	4,3	15	60,9

Observamos que aqui o Poder Executivo possui pouco mais da quinta parte de sua influência.

O que chama a atenção é a forte influência do Poder Executivo na Autoridade Nacional de Proteção de Dados:

Tabela 3 — Autoridade Nacional de Proteção de Dados

Autoridade Nacional de Proteção de Dados									
Normas	**Integrantes**	**Executivo**	**%**	**Legislativo**	**%**	**Judiciário**	**%**	**Sociedade civil**	**%**
Lei 13.709/2018	26	9	34,6	2	7,7	1	3,8	14	53,8
MP 869/2018	28	11	39,3	2	7,1	1	3,6	14	50
Lei 13.853/2019	28	10	35,7	2	7,1	1	3,6	15	53,6

É de fácil constatação a influência do Executivo sobre a Autoridade Nacional verificando-se a evolução legislativa no curso do tempo.

A última alteração trouxe uma influência significativa desse Poder, em que supera um terço dos votos de todos os seus integrantes. O que se busca demonstrar aqui é a relativa autonomia e independência que essa Autoridade tem em relação aos Poderes de Estado, em especial ao Executivo.

Ganha destaque o aspecto financeiro e orçamentário. Não há independência plena, conforme notamos no dispositivo abaixo transcrito:

> *Art. 55-A. Fica criada, **sem aumento de despesa**, a Autoridade Nacional de Proteção de Dados (ANPD), **órgão da administração pública federal, integrante da Presidência da República**.*
>
> *[...]*
>
> *§ 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD **está condicionado à expressa autorização física e financeira na lei orçamentária** anual e à permissão na lei de diretrizes orçamentárias. (Grifo nosso)*

A questão ganha peso quando, por exemplo, ocorrer um incidente de segurança em prejuízo de uma pessoa física e, em razão disso, favorecer interesses governamentais. Neste caso, a ANPD teria liberdade de ação em face de eventual prejuízo do Poder Executivo Federal?

Outra hipótese surge numa suposta investigação relacionada a "lavagem de dinheiro" e envolvendo autoridades de Estado, cujo interesse público salta aos olhos, mas que pode ser comprometida por restrições impostas a ANPD ou mesmo por ela? Podemos considerar o uso desses dados como controle político do Estado quando temos um órgão que se subordina à Presidência da República? A ANPD poderia editar regras determinando a eliminação de registros processuais depois de determinado período ao Poder Judiciário?

Esses exemplos ocorreram recentemente em Portugal[5] e estão próximos de uma judicialização perante a Suprema Corte.

O modelo da União Europeia, de fato, possui essa independência e autonomia. O artigo 52 é claro nesse contexto:

> *Artigo 52 – Independência* [6]
>
> *1. As autoridades de controle agem com total independência na prossecução das suas atribuições e no exercício dos poderes que lhe são atribuídos nos termos do presente regulamento.*
> *2. **Os membros das autoridades de controle não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem.***
> *3. Os membros da autoridade de controle abstêm-se de qualquer ato incompatível com as suas funções e, durante o seu mandato, não podem desempenhar nenhuma atividade, remunerada ou não, que com elas seja incompatível.*
> *4. Os Estados-Membros asseguram que cada autoridade de controle disponha dos recursos humanos, técnicos e financeiros, instalações e infraestruturas necessários à prossecução eficaz das suas atribuições e ao exercício dos seus poderes, incluindo as executadas no contexto da assistência mútua, da cooperação e da participação no Comitê.*
> *5. Os Estados-Membros asseguram que cada autoridade de controle selecione e disponha do seu próprio pessoal, que ficará sob a direção exclusiva dos membros da autoridade de controle interessada.*
> *6. Os Estados-Membros asseguram que cada autoridade de controle fique sujeita a um controle financeiro que não afeta a sua independência e que disponha de orçamentos anuais separados e públicos, que poderão estar integrados no orçamento geral do Estado ou nacional. (Grifo nosso)*

O texto reproduzido anteriormente revela a **grande preocupação do Parlamento Europeu em garantir efetivamente a independência e autonomia da Autoridade de Proteção de Dados**. Precisamos avançar para este patamar também no Brasil.

[5] Disponível em: https://bit.ly/38gbAOZ; https://bit.ly/2NDAXCq. Acesso em: 6 ago. 2019.

[6] Vide Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Disponível em https://bit.ly/38iJhzz. Acesso em: 6 ago. 2019.

Já há mobilização no Congresso Nacional para aumentar ainda mais a importância da referida proteção. O Senado apresentou uma PEC (17/2019)[7] em que acrescenta o inciso XII-A ao artigo 5º da Constituição Federal. Inclui nos **direitos fundamentais do cidadão** a proteção de dados pessoais e fixa a competência legislativa privativamente para a União. Talvez, a partir dessa inclusão, a preocupação com estrutura da ANPD aumente e traga o aperfeiçoamento esperado.

Por outro lado, a publicação de uma lei brasileira tão moderna e inspirada em fonte qualificada já é por si só um precioso avanço. Precisamos apenas aperfeiçoar esse instrumento. Que mais a frente tenhamos uma ANPD plenamente autônoma e independente.

Bibliografia

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLUM, Renato Opice *et al*. *LGPD*: Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters, 2019.

[7] O texto da proposta está disponível em https://bit.ly/2SBfwoG. Acesso em: 6 ago. 2019.

A extraterritorialidade das decisões judiciais no universo digital

Viviane Nóbrega Maldonado[1]
Juíza aposentada e professora

Sumário: 1. Introdução; 2. Background; 3. O desafio; 4. Conclusão.

Resumo: A *Internet* não tem fronteiras e os fatos que decorrem da utilização da rede frequentemente ensejam repercussões em ambientes territoriais distintos. Tal peculiar circunstância produz reflexos imediatos na questão atinente à clássica delimitação da jurisdição, não sendo incomum que, em algumas hipóteses, uma determinada decisão judicial venha a expandir-se para além do restrito e formal limite de incidência. Esse artigo propõe-se a discutir o tema sob essa ótica.

Palavras-chave: Poder Judiciário. jurisdição. territorialidade. extraterritorialidade. competência. soberania. *Internet*.

1. Introdução

A *Internet* não é apenas uma ferramenta útil para um mundo sem fronteiras. A *Internet*, em si própria, é um universo sem quaisquer barreiras, circunstância da qual decorre a dificuldade de harmonização das particularidades de cada uma das jurisdições nacionais, haja vista a notória diversidade de modelos regulatórios à qual se acrescentam as peculiaridades de ordem cultural.

Outro aspecto que emerge do caráter transfronteiriço da rede diz respeito às hipóteses em que, para atingir efetividade, uma determinada decisão de cunho jurisdicional deve alcançar outras jurisdições, sob pena do reconhecimento da própria inutilidade do provimento se houver limitação espacial sob os moldes do clássico modelo das regras atinentes à territorialidade.

O assunto é sabidamente controverso. Alguns argumentam com sólidos fundamentos legais no sentido de que tais decisões esbarram em noções básicas de jurisdição e soberania. Por outro lado, é inafastável o entendimento de que toda e qualquer decisão judicial em concreto deve mostrar-se eficaz. Com efeito, sem a plena eficácia, não há nem mesmo razão para a sua existência. E, em última instância, se uma dada decisão

[1] Juíza de Direito TJSP (1993-2018), Data Protection Expert (CIPP/E); Data Protection Officer (DPO) Professional (Maastricht University, Países Baixos); Mestre em Direito Comparado (Samford University, Estados Unidos), MBA em Relações Internacionais (FGV-SP) e Pós-Graduação em Direito Civil à luz da Constituição pela Escola Paulista da Magistratura; Docente em Proteção de Dados em nível de Pós-Graduação e Educação Executiva; Autora dos livros *Direito ao Esquecimento*, *Comentários ao GDPR*, *LGPD Comentada*, *Advocacia 4.0*, *LGPD: Manual de Implementação*, além de diversos artigos acadêmicos publicados no Brasil e no exterior. Membro do Training Advisory Board (IAPP e ITechLaw); Partner do Instituto de Inovação Legal (Portugal); Fundadora na Nextlaw Academy.

judicial é reconhecidamente inútil, todo o processo em si acha-se igualmente desprovido de utilidade, a comprometer a lógica do sistema judicial.

Essa nova perspectiva põe em xeque o modelo clássico de jurisdição. É claro que, formalmente, seriam esperados os prévios ajustes e a colaboração entre diferentes atores para validar-se uma determinada decisão judicial, seja por meio da implementação de acordos internacionais, seja pela via diplomática direta, quando se tratar de questão de cunho internacional.

Entretanto, o que se constata é que, com o surgimento de novas demandas em virtude do desenfreado avanço tecnológico, muitas vezes não é possível aguardar-se o anterior estabelecimento de tais parâmetros, tampouco a implementação de específicos ajustes, mormente quando há perigo na demora quanto ao cumprimento da decisão, potencialmente a acarretar graves prejuízos muitas vezes irreversíveis e, principalmente, quando se constata circunstância capaz de, com a delonga, malferir o princípio da dignidade humana.

Esse paradigma não é regra e constitui exceção. Sendo assim, se não for encontrada a indispensabilidade da extraterritorialidade para a eficácia de uma determinada decisão, deve ela, de fato, ser limitada, no espaço e por padrão, aos limites da própria jurisdição. Por outro lado, se houver perigo decorrente da urgência do provimento e se não houver outro caminho apto a alcançar o resultado desejado que não alargar os limites formais da delimitação jurisdicional, deve o juiz agir de forma ampla e, se necessário, em caráter universal.

Espera-se, pois, o amadurecimento de tal compreensão de modo a, com vistas às exigências do mundo moderno, prestigiar-se de forma inarredável a completa eficácia das decisões judiciais, para que, com isso, possa avançar-se rumo aos próximos estágios de desenvolvimento do tema.

2. Background

Há alguns anos, li um interessante artigo ("A lei em um mundo sem fronteiras") do atual presidente executivo do Grupo Globo[2], em que se destacava:

> *Misturar o conceito de liberdade no ambiente da internet, incluindo o de liberdade de expressão, com a ideia de fim das fronteiras, sem incluir a lei, é sugerir que a pós-modernidade é anárquica, e, intencionalmente, levar à conclusão de que a lei não pode ou não deve regulá-la. A quem interessa esse movimento?*[3]

O texto imediatamente chamou minha atenção.

Nessa época, eu já estudava aspectos relacionados ao ainda pouco conhecido Direito ao Esquecimento, que começava a difundir-se no meio acadêmico europeu à vista da reclamação formulada pelo cidadão Mario Costeja González junto à Agência Espanhola de Proteção de Dados (AEPD). A Agência, em 30 de setembro de 2010, e acolhendo parcialmente a pretensão, determinara que o Google removesse da *Internet* dados ou *links*

[2] https://glo.bo/2topLD3.

[3] NÓBREGA, Jorge. https://glo.bo/2RzWrBp.

que conduzissem à figuração da informação questionada pelo interessado. A subsidiária espanhola do Google, bem como a própria matriz, interpuseram apelo à Suprema Corte Espanhola, a qual, após suspensão da instância, remeteu o processo ao Tribunal de Justiça da União Europeia, que, em 13 de maio de 2014, reconheceu expressamente ao cidadão o direito quanto à remoção de informações. E, com isso, afirmou-se o Direito ao Esquecimento naquele contexto[4].

Neste interregno de quase quatro anos entre a reclamação e o julgamento definitivo, já se discutia, nos bastidores, a questão afeta à concreta utilidade de uma potencial decisão que viesse a acolher o pedido de remoção. De um lado, alguns sustentavam que o acolhimento da pretensão seria inócuo, na medida em que, em tese, a informação poderia vir a ser buscada e encontrada por meio de plataforma diversa que não aquele específico buscador. E, de outra parte, havia quem defendesse que a remoção no âmbito de atuação do Google espanhol (google.es), dentro dos limites territoriais da Espanha, não impediria que, efetuada a busca por meio do Google a partir de outro ponto geográfico, a informação seria igualmente encontrada.

Não obstante a existência de tais argumentos que apontavam para a inconveniência ou desimportância de uma decisão judicial que determinasse a remoção da informação na forma do pedido, o fato é que o parâmetro estabeleceu-se em definitivo, reconhecendo-se a possibilidade de deleção ou desindexação nas hipóteses elencadas na decisão. Por essa razão, aliás, e até porque inexistia instância recursal, o Google veio a acatar referida decisão e, ainda no mesmo mês de maio de 2014, inaugurou ferramenta em sua própria plataforma para que os cidadãos europeus pudessem, doravante, efetuar, direta e pessoalmente, requerimentos de remoção[5].

Pouco tempo depois, especificamente no ano de 2015, a autoridade francesa de proteção de dados, *Commission Nationale de l'Informatique et Des Libertés* (CNIL), determinou que o Google procedesse à desindexação de informações em termos universais, porquanto entendido que não seria suficiente que a ação se limitasse à jurisdição francesa (google.fr). Sem o cumprimento dessa determinação, a autoridade francesa impôs multa de 100 mil euros à plataforma[6].

O Google recorreu sob o argumento de que houve ampliação da compreensão tirada do caso espanhol e que a aplicação universal quanto ao cumprimento da determinação traria implicações atinentes à jurisdição e à soberania. Além disso, ao que sustentou, a decisão teria desconsiderado o balanceamento dos aspectos do direito à privacidade sob o enfoque dos parâmetros legislativos de cada país.

Em setembro de 2018, ocorreu audiência[7] para que as partes interessadas pudessem expor seus argumentos quanto à possibilidade de extensão de uma determinada decisão a outras jurisdições.

O caso será ainda julgado pelo Tribunal de Justiça da União Europeia, inexistindo data agendada para tanto. Estima-se, porém, que a decisão advirá ainda no ano de 2019, quando então o Tribunal de Justiça da União Europeia definirá com exatidão qual

[4] https://bit.ly/2NGe2Xq.

[5] https://bit.ly/38s6783.

[6] https://reut.rs/2TEgbqg.

[7] https://bit.ly/2TIzeQe.

a abrangência da decisão em termos territoriais e, o que releva, se é possível atuação que desborde da restrita jurisdição[8].

Tal futura decisão representará inequívoco marco histórico sobre a possibilidade, ou não, de aplicação universal do Direito ao Esquecimento por força de ordem proveniente da jurisdição europeia. Independentemente, entretanto, do que vier a ser decidido em futuro próximo, o fato é que as críticas de lado a lado e o debate já estão profundamente estabelecidos no que concerne ao ponto fulcral do tema.

Qualquer acadêmico de direito conhece, ou pelo menos deveria conhecer, o Princípio da Territorialidade, que, no Brasil, é expressamente reconhecido no art. 16 do Código de Processo Civil e no art. 1º do Código de Processo Penal, além de previsto em nosso sistema jurídico no art. 5º do Código Penal, e em relação também a matéria trabalhista e tributária. Este princípio contempla poucas e predefinidas exceções de caráter legal e pode ser entendido como mecanismo que permite estabelecer e delimitar a área geográfica em que o Estado exercerá a sua soberania por meio da jurisdição.

Esse modelo clássico encontra-se desafiado pela inexistência de fronteiras físicas em ambiente digital, de sorte que, a depender do específico caso concreto, bem possível é que a decisão judicial não revele qualquer efetividade se for limitada ao espaço territorial de atuação do órgão jurisdicional. De outro lado, como já exposto, o surgimento de novas demandas por força do crescente avanço tecnológico muitas vezes não permite, de fato, o prévio estabelecimento do parâmetro legislativo e, muito menos, da concretização de acordos internacionais, que, a rigor, constituiriam exigência normativa na doutrina tradicional.

Trata-se de um intrincado desafio a conciliação de tais temas. De todo modo, ao contrário do que preconizava o articulista referido ao início desse tópico, tal caráter universal de uma concreta decisão não representa, em absoluto, o estabelecimento de um padrão anárquico, na medida em que, reconhecidamente, os conceitos formais da lei devem ser revistos frente às novas realidades e demandas, sem que tal fato signifique o comprometimento da organização dos Estados e a sobrevivência da civilização. De fato, no tema em concreto, trata-se de mera adequação necessária ao intercâmbio e à interconexão, agora também de dados, que o mundo convencionou chamar de globalização.

No mais, princípios relativos a direitos individuais devem ser observados e prestigiados de modo a conferir-lhes amplitude e efetividade para que possam, concretamente, estar sempre assegurados e garantidos.

3. O desafio

Reconhecendo esta tendência e esta necessidade, foi fundada, no ano de 2012, a *Internet & Jurisdiction Policy Network*[9], também conhecida simplesmente como "*I & J*", que consiste em rede global de políticas multissetoriais com a finalidade de abordar as complexas questões concernentes à *Internet* transfronteiriça frente às jurisdições nacionais.

A entidade visa a facilitar o processo de política mundial para permitir a cooperação transnacional e para preservar o caráter global da *Internet*. Desde sua criação,

[8] https://bit.ly/2G3wvJc.

[9] https://www.internetjurisdiction.net/.

tomaram parte da "*I & J*" mais de duzentas entidades-chave de diferentes grupos de todo o mundo, incluídos governos, empresas de *Internet*, comunidade técnica, sociedade civil, academia e organizações internacionais.

Em seu *site* oficial, encontra-se ampla base de dados na qual podem ser encontradas diversas ocorrências ao redor do mundo em que houve a necessidade de atuação extraterritorial. Um dos mais emblemáticos casos ali listados diz respeito à decisão emanada da Suprema Corte do Canadá que, afastando o apelo do Google, manteve a decisão da Corte da Colúmbia Britânica e autorizou a aplicação universal da ordem como necessária ao atingimento de seu objetivo[10].

Eis o caso: a *Equustek Solutions Inc.*, a *Clarma Enterprises Inc.* e *Robert Angus*, distribuidores de *hardware*, ajuizaram ação contra a *Datalink*, seu concorrente direto. Na ação, a parte autora alegou que a *Datalink* teria violado seus segredos industriais de forma a induzir os consumidores em erro. A *Equustek* obteve várias ordens do Poder Judiciário canadense contra a *Datalink*, as quais foram desconsideradas pela empresa.

A gigante Google, no âmbito da ação e por ordem judicial, bloqueou centenas de *sites* da *Datalink* que apareciam em seus resultados de pesquisa no Canadá. No entanto, não removeu *links* de resultados de pesquisa realizados por usuários fora daquela jurisdição. E, por essa razão, a *Equustek* obteve junto à Corte da Colúmbia Britânica e à Suprema Corte do Canadá uma decisão determinando a remoção dos resultados da pesquisa em nível global.

Em razão dos claros efeitos extraterritoriais, o Google ingressou com uma ação na Califórnia buscando a declaração judicial de que a ordem proveniente do Canadá não haveria de ser aplicada dentro dos Estados Unidos, na forma do artigo 230 do *Communications Decency Act*[11]. E a moção do Google, para tal medida liminar, foi concedida.

Dentre outros dispositivos relevantes, consta do texto de lei: "*Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property*". E, ainda: "*Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section*".

Em referida Decisão, o Juiz Edward J. Davila entendeu que o Google atendia aos requisitos da imunidade da Seção 230 que protege os provedores de serviços de computação interativa contra responsabilidade decorrente de conteúdo criado por terceiros. Com efeito, a Seção 230 declara: "*no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider*".

O Google, sob a acepção americana, é considerado como mero provedor de serviço de computador interativo, sendo certo que as informações em questão (*Datalink websites*) teriam sido disponibilizadas pela própria *Datalink*. Assim, não seria a plataforma de busca a pessoa jurídica responsável pela remoção pretendida. Diferentemente dos Estados Unidos, no Canadá o Google é tratado como editor, ou publicador, de modo a autorizar-se que ele próprio possa remover conteúdos disponibilizados por terceiros.

Trata-se esse caso, pois, de emblemático exemplo relativo às dificuldades relacionadas à diversidade de entendimento e de modelos regulatórios, aliadas aos entraves

[10] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do.

[11] https://transition.fcc.gov/Reports/tcom1996.txt.

que decorrem do não acatamento de um determinado provimento judicial estrangeiro por força dos argumentos atinentes à soberania.

Barry Sookman, um proeminente advogado canadense, assim pronunciou-se sobre a específica demanda:

> *The decision sets an unfortunate precedent. Google and other major online providers operate global platforms. While their businesses are global, they often seek, as in this case, to have only the laws of the U.S. apply to their businesses. They want all the benefits of carrying on business in Canada and around the world, but want to insulate themselves from local liability – in this case arguing that their foreign responsibilities to abide by a Canadian court order are trumped by a U.S. law (the CDA) that does not apply in Canada. This type of immunity is especially troubling because injunctions against these intermediaries to de-index illegal content or to take down web sites that disseminate illegal materials are becoming more and more common and represent an essential enforcement tool online*[12].

A objeção do Google pode, à primeira vista, mostrar-se pertinente. De todo modo, nesse específico caso, a natureza da causa não permitia o aguardo de ratificação de instrumento internacional, o que se revela, como já dito, um processo complexo. Ademais, como pontuou o advogado Sookman, questiona-se se é plausível, de fato, o argumento da imunidade por parte das empresas que atuam de forma global. Por essa razão, há campo para a aceitação da atuação extraterritorial como forma mesmo de garantir eficácia àquela decisão.

O "Tallinn Manual" (originalmente intitulado Manual de Tallinn sobre o Direito Internacional Aplicável à Guerra Cibernética) é um estudo acadêmico, de caráter não vinculativo, sobre a atuação do direito internacional, em particular no que se refere ao *jus ad bellum* e ao direito internacional humanitário. O "Manual de Tallinn" foi escrito entre 2009 e 2012 a convite da OTAN[13] em Tallinn, capital da Estônia[14].

Eis a história. No final de 2009, considerando-se as novas questões que emergiam do campo cibernético, o Centro de Excelência em Defesa Cibernética Cooperativa da OTAN reuniu um grupo internacional de juristas e profissionais para redigir um manual abordando a questão de como interpretar o direito internacional no contexto de operações cibernéticas e guerra cibernética. Como tal, essa força-tarefa pode ser entendida como o primeiro esforço destinado a analisar este tópico de forma abrangente e oficial para trazer algum grau de clareza para as complexas questões jurídicas que emergem de tais aspectos.

O foco primário do "Manual de Tallinn" estava centrado nas operações cibernéticas mais severas, tais sejam aquelas que violam a proibição do uso da força nas relações internacionais, as que autorizam os Estados a exercerem o direito de autodefesa e as

[12] https://bit.ly/2RtqlHm/.

[13] https://ccdcoe.org/.

[14] http://csef.ru/media/articles/3990/3990.pdf.

que possam ocorrer durante conflitos armados. Encerrada essa primeira fase, o Manual foi publicado em 2013 pela *Cambridge University Press*[15].

O "Tallinn Manual 2.0", lançado em 2017, e que representa a segunda geração do documento, acrescenta análise legal dos incidentes cibernéticos mais comuns que os Estados enfrentam no dia a dia, elencando-se hipóteses em patamar de gravidade inferior a aquelas que dizem respeito a limites do uso de força ou conflitos armados, tal como analisadas na primeira edição.

Esta segunda versão cobre um espectro completo de leis internacionais aplicáveis a operações cibernéticas que vão desde regimes jurídicos em tempo de paz até a própria lei de conflitos armados, abrangendo, portanto, ampla gama de princípios e regimes de leis internacionais que regulam praticamente todos os eventos no ciberespaço.

Algumas hipóteses pertencem ao ramo do direito internacional geral, como o princípio da soberania e as várias bases legais para o exercício da jurisdição. A questão da responsabilidade do Estado, por exemplo, e que inclui normas legais de atribuição, é também examinada em detalhes. Mas o trabalho não se esgota nesses temas, haja vista que aborda igualmente direitos humanos, direito aéreo e espacial, direito do mar e direito diplomático e consular, os quais são examinados no contexto das operações cibernéticas.

A menção do estudo a outros temas não necessariamente relacionados a questões relevantes do Estado demonstra, de forma evidente, a preocupação do meio acadêmico com a temática em questão, notadamente porque reconhecido que, em muitas situações, não é possível a negativa da ordem sob a alegação de infração formal da jurisdição. Expandiu-se, pois, o escopo do primeiro trabalho para alcançar inúmeras outras hipóteses concernentes ao ambiente da *Internet* que não as relativas às questões de Estado.

O tema em si não é tão novo quanto parece. No âmbito dos Estados Unidos, por exemplo, encontram-se inúmeras decisões judiciais em que se discute a possibilidade de que uma ordem possa ter aplicabilidade sobre um *website* situado fora dos limites da jurisdição estadual, em caráter extraterritorial.

Tal ocorrência mostrou-se tão relevante que ensejou até mesmo a criação de um paradigma, denominado "*Zippo Test*", que decorreu de ação judicial proposta na Pensilvânia pela fabricante de isqueiros contra empresa *web* que se utilizava de sua marca identificadora e que se localizava no Estado da Califórnia (*Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997)[16]. A partir de tal decisão, criou-se, em termos jurisprudenciais, um critério lógico relacionado a uma "escala móvel" que se atrela ao concreto nível de atividade e de interação da empresa em face de quem recebeu a demanda.

Não se extrai dessa decisão critério suficientemente objetivo. De toda forma, possui ela relevância no contexto das discussões referentes ao tema, que, a cada dia, tornam-se mais corriqueiras. E, se antes a questão era discutida à luz das jurisdições estaduais dentro de um mesmo País, hoje o debate é deslocado para a extraterritorialidade em nível global.

Em 6 de fevereiro de 2018, quatro senadores dos Estados Unidos anunciaram a introdução da "*Clarifying Lawful Overseas Use of Data Act*"[17] (CLOUD Act), que modificaria

[15] http://csef.ru/media/articles/3990/3990.pdf.

[16] https://bit.ly/2ujdgIK/.

[17] https://bit.ly/3apw35U.

profundamente as regras para o acesso transfronteiriço aos dados para fins de aplicação da lei. O projeto de lei alterou o "*Stored Communications Act*" (SCA) e o "*Electronic Communications Privacy Act*" (ECPA), que estabelecem as regras para divulgação de dados de comunicações armazenadas e que estão no centro do chamado caso "Microsoft Irlanda".

O *background* para a sanção da lei decorreu de dificuldades que o *Federal Bureau of Investigations* (FBI)[18] experimentou em obter dados de provedores de serviços por meio de mandados expedidos. Em 2013, por ocasião de investigações relativas ao tráfico de drogas, foi expedido mandado para informações relativas a *e-mails* de cidadãos americanos que estavam armazenados em servidores remotos da Microsoft, localizados em Dublin, na Irlanda. A empresa recusou-se à entrega de tais informações, o que ensejou o processo "Microsoft Corp. v. United States"[19].

Argumentou o FBI que a Microsoft detinha total controle dos dados, de modo que deveria cumprir a ordem. Por seu turno, a empresa sustentou que a ordem emitida com base no "*Stored Communications Act*" (SCA) não abrangia os dados armazenados fora dos Estados Unidos. No mais, muito embora fosse verdade que o FBI poderia requisitar um MLAT (*Mutual Legal Assistance Treaty*)[20], esse processo seria inquestionavelmente lento de modo a impedir a eficácia.

O Cloud Act, pois, nasce nesse contexto, e como decorrência das legislações anteriores, e estabelece que as empresas devem fornecer dados de cidadãos americanos que estejam sob sua custódia, sendo irrelevante o local em que se encontrem armazenados. Para equacionar objeções normalmente apresentadas, a Lei provê mecanismos às companhias e às cortes para rejeitarem ou desafiarem a requisição se há violação de direitos da privacidade no país no qual estejam alocados os dados. Por fim, prevê igualmente como alternativa o estabelecimento de "acordos executivos" nas circunstâncias descritas no texto.

Além disso, a Lei permite que governos estrangeiros solicitem dados de provedores de serviços com sede nos Estados Unidos. E, para esses fins, o procurador-geral e o secretário de Estado dos EUA precisam determinar os níveis de respeito dos direitos humanos, das normas do Estado de Direito e dos requisitos processuais do país do governo estrangeiro, suficientes para que este se qualifique para a celebração de acordo executivo.

As empresas de tecnologia Apple, Facebook, Google, Microsoft e Oath assinaram carta em 6 de fevereiro de 2018, apoiando o CLOUD Act e descrevendo-a como "um passo importante para melhorar e proteger os direitos individuais de privacidade, reduzindo conflitos de leis internacionais e mantendo todos nós mais seguros[21].

No mais, no esforço de encontrar soluções para as questões afetas à extraterritorialidade, a "I & J", em fevereiro de 2018, organizou evento com mais de duzentos participantes de governos, grandes empresas de *Internet*, operadores técnicos, sociedade civil, academia e organizações internacionais de mais de 40 países, que se reuniram em Ottawa, Canadá, para a segunda Conferência Global da *Internet* e Rede de Políticas Jurisdicionais.

[18] https://www.fbi.gov/.

[19] https://www.supremecourt.gov/opinions/17pdf/17-2_1824.pdf.

[20] https://www.mlat.info/.

[21] https://bit.ly/2SHumKp

Desse encontro, emergiu o documento final desta segunda Conferência Global, dele constando planos de trabalho concretos para os três Programas da Rede de Políticas: Dados e Jurisdição, Conteúdo e Jurisdição e Domínios e Jurisdição[22]. Tal trabalho tem por objetivo auxiliar o desenvolvimento de políticas de participação múltipla e é o resultado de evento do qual tomou parte o Governo do Canadá, com apoio institucional da OCDE, Conselho da Europa, Unesco, Comissão Europeia e Icann[23].

Tópicos como "os perigos da incerteza jurídica no ciberespaço", "o futuro da sociedade digital está em jogo", bem como a "necessidade de estruturas" e "coerência política", foram temas com os quais foi enfrentada a questão que emerge da colisão entre a contenção jurisdicional e a necessidade de responder adequadamente a reclamações envolvendo direitos relevantes.

4. Conclusão

As novas necessidades de um mundo globalizado e sem fronteiras clamam por novas soluções e tal fator impacta e desafia as noções clássicas que embasam os tradicionais princípios relativos à territorialidade e à delimitação geográfica de uma determinada jurisdição.

Não se sustenta, por evidente, que tal posicionamento seja acolhido de forma indistinta. O que parece relevante, porém, é que, em específicas circunstâncias, uma determinada decisão poderá expandir-se a outro território para conferir efetividade.

Formalmente, seria exigido, dentro da clássica doutrina do direito internacional, o estabelecimento de ajustes prévios entre os diferentes Estados. Ocorre que, em muitas hipóteses, há premência quanto à atuação jurisdicional, que não pode esvaziar-se em termos de concretos efeitos ante a inexistência de adoção de parâmetros formais.

A propósito, vislumbram-se situações em que a demora enseja grave risco de prejuízos à parte, muitas vezes irreversíveis, e, em algumas ocorrências, a delonga pode, concretamente, malferir o princípio da dignidade humana.

Tal entendimento, por evidente, não significa dotar os juízes com superpoderes. Para este tipo de desempenho excepcional, deve haver causa plenamente justificada concernente à plausibilidade de que a ineficácia da decisão possa dar origem a consequências potencialmente irreparáveis. E a lógica para chegar-se a essa conclusão é proceder-se ao balanceamento correto da equação com base na avaliação dos princípios e valores de direito envolvidos.

Em síntese, considerando-se que o caráter extraterritorial de uma concreta decisão judicial não se atrele a situações de premência ou relevância, deve ela permanecer limitada ao espaço da jurisdição até que satisfeitas as exigências legais que dizem respeito aos ajustes entre os Estados na forma das normas de direito internacional público.

Por outro lado, se houver perigo na demora e se não existir outro caminho para alcançar o resultado desejado, o juiz, prescindindo da formalidade em questão, deve desde logo agir universalmente.

[22] https://bit.ly/39IaIU7

[23] https://www.icann.org/

Temas contemporâneos de direito à educação: a utilização de sistema de vigilância por câmeras nas escolas e o direito à privacidade

Nina Beatriz Stocco Ranieri[1]
Professora de Direito

Letícia Antunes Tavares[2]
Juíza de Direito no Estado de São Paulo

Sumário: Considerações iniciais; 1. Breves comentários sobre o direito à privacidade no contexto escolar; 2. Privacidade x Segurança na escola; 2.1. Tratamento do tema no plano jurisprudencial; 2.2. Tratamento do assunto no plano legislativo; Considerações finais; Referências bibliográficas.

Resumo: O artigo aborda o tratamento jurisprudencial e legislativo a respeito do uso do sistema de vigilância por câmeras nas escolas, com enfoque nos seguintes direitos fundamentais e constitucionalmente garantidos: a privacidade, a segurança e a liberdade. Para tanto, parte-se da análise do direito à privacidade no contexto escolar e, ao final, expõem-se as conclusões a respeito do tema, tendo em vista os possíveis conflitos entre os direitos fundamentais citados.

Palavras-chave: Educação. câmeras. sala de aula. vigilância. era informacional. privacidade. liberdade. segurança.

Considerações iniciais

Tendo em vista a evolução dos conflitos envolvendo o direito à educação, importante trazer ao debate-tema conexo à liberdade de ensinar e de aprender o direito à privacidade nas escolas, que ganha especial relevância na era informacional.

Trata-se de assunto que, como veremos, corrobora a mudança de rumo da jurisprudência, que não mais se centra exclusivamente na garantia de prestações estatais positivas, mas também passa a assegurar liberdades negativas, ou seja, direitos na educação.

Importante salientar que o direito à educação é considerado um *cross-sectoral right*, pois ao mesmo tempo seria um direito civil e político, bem como econômico, social e

[1] Professora Associada da Faculdade de Direito da Universidade de São Paulo. Coordenadora de Cátedra Unesco de Direito à Educação da Faculdade de Direito da Universidade de São Paulo. Sócia efetiva do Movimento Todos pela Educação. Conselheira consultiva do Conselho Nacional de Justiça.

[2] Juíza de Direito do Estado de São Paulo. Doutoranda em Direito do Estado pela Faculdade de Direito da Universidade de São Paulo. Cursou "Master in Comparative Law" pela Samford University/EUA. Especialista em Direito Público pela Escola Paulista de Magistratura.

cultural (MEHEDI, 1998), mantendo direta relação com os princípios fundamentais da República Federativa do Brasil, em especial com o princípio da dignidade humana, pois a educação é responsável pelo desenvolvimento da personalidade do indivíduo e da cidadania, contribuindo para a construção da identidade social.

Ainda, o acesso à educação propicia o desenvolvimento de uma sociedade livre, justa e solidária, já que o indivíduo formalmente educado passa a ter consciência de sua individualidade, atrelado a forte sentimento de solidariedade social.

O Superior Tribunal de Justiça, salientando o caráter prioritário do direito à educação e a importância deste para a convivência dos indivíduos, decidiu que

> *a consciência de que é da essência do ser humano, inclusive sendo o seu traço característico, o relacionamento com os demais em um espaço público – onde todos são, in abstrato, iguais, e cuja diferenciação se dá mais em razão da capacidade para a ação e o discurso do que em virtude de atributos biológicos – é que torna a educação um valor ímpar. (REsp 1185474/SC, Rel. Ministro HUMBERTO MARTINS, SEGUNDA TURMA, julgado em 20/04/2010, DJe 29/04/2010).*

De acordo com Anísio Teixeira, a educação escolar se faz necessária, constituindo-se num problema público, num interesse público, num direito de cada indivíduo e num dever da sociedade politicamente organizada. Não se trata de vantagem, nem de sucesso individual, mas de condição de funcionamento da própria sociedade (TEIXEIRA, 2009, p. 44-48).

Não é demais lembrar que a escola, como um local privilegiado para a formação integral do indivíduo, é ambiente fecundo para a discussão fundamentada no respeito pelo outro e na diversidade.

E, por todo o exposto, com vistas à manutenção de um ambiente escolar saudável, abordar tema relativo ao direito à privacidade nas escolas, na era informacional, é de suma importância, tendo em vista a sua relação com a liberdade de ensinar e aprender. Além disso, deve-se ter em mente que a privacidade, assim como a educação, também tem grande relevância para o desenvolvimento pessoal do indivíduo, pois possibilita a reflexão crítica sobre as relações sociais. E a sua inexistência poderia causar a destruição do convívio íntimo das pessoas, com a banalização da confiança e do respeito das relações individuais (COSTA JUNIOR, 1970, p. 23).

1. Breves comentários sobre o direito à privacidade no contexto escolar

Nas palavras de J. J. Calmon de Passos

> *A privacidade é hoje o reduto último da resistência do individuo às forças que operam no sentido de seu aniquilamento – econômicas, políticas, culturais […]. Quando tanto se fala de direitos humanos fundamentais e se batalha tanto para defini-los e garanti-los, nenhum se me afigura mais fundamental que a proteção da privacidade, da intimidade. Protegê-la é a forma mais segura de preservar a liberdade. E a liberdade é o essencial do homem, porque sem ela*

> *a humanização do animal homem se frustra, aprisionada no mundo da necessidade, nele se aniquilando. (PASSOS, 1989, p. 63)*[3]

Não à toa, o direito à privacidade foi expressamente reconhecido na Declaração Universal dos Direitos Humanos, de 1948[4], considerada o grande marco na história dos direitos fundamentais, o que sacramenta sua importância para o indivíduo. E, nesta linha, a Constituição de 1988, inovando, garantiu à privacidade o caráter de direito fundamental, nos seguintes termos: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (artigo 5º, inciso X, da Constituição Federal).

Nossa Lei Maior adotou um conceito amplo de privacidade abrangendo a proteção à vida privada, intimidade, honra e imagem das pessoas. Segundo Tércio Sampaio Ferraz Junior, há certa gradação entre os direitos da privacidade, partindo-se da intimidade (o mais exclusivo dos seus direitos, cujo atributo básico é o estar-só), passando pela ideia de vida privada (envolve a proteção de formas exclusivas de convivência) e, enfim, chegando àqueles objetos que pressupõem comunicação e envolvem situações personalíssimas, mas perante terceiros, sendo, portanto, menos exclusivos: a honra e a imagem (FERRAZ JUNIOR, 1993, p. 442-443). Esta distinção é bastante importante para tratarmos do tema proposto neste capítulo, em relação à utilização de câmeras de vigilância nas escolas, como explicaremos mais detalhadamente adiante.

Feitas estas considerações, uma conclusão inarredável merece nota: proteger a privacidade, que é também um direito da personalidade, é garantir a liberdade, inclusive a liberdade de ensinar e aprender. Além disso, assegurar-se a privacidade é de suma importância para o desenvolvimento pessoal dos alunos, em vista ser a escola um local privilegiado para a formação do cidadão.

A verdadeira escola tem como missão precípua formar para a autonomia, sendo a liberdade de aprender e ensinar o princípio fecundador do processo de aprendizagem, que supõe processos contínuos de interação, com o envolvimento de componentes afetivos, cognitivos, éticos, morais etc. A liberdade em sala de aula pressupõe formas flexíveis de construção do dinamismo do cotidiano escolar (CARNEIRO, 2015, p. 62-63).

Por essa razão, a defesa da privacidade de alunos e professores é medida que se impõe. Contudo, muito embora a questão, *prima facie*, pareça isenta de qualquer discussão, na prática, pensar-se na privacidade com um direito intangível, seria fazer vistas grossas à realidade que nos cerca. Não por outra razão, recentemente, casos envolvendo o direito à privacidade nas escolas foram submetidos à apreciação do Poder Judiciário. E, para os fins deste estudo, nos interessam aqueles relativos à implantação de câmeras em salas de aula.

[3] Esta estreita relação entre privacidade e liberdade tem inspiração nas lições de Immanuel Kant, no sentido de que liberdade, para além de uma determinação negativa, equivaleria a uma faculdade (positiva), ou seja, à autonomia da vontade. "À ideia da liberdade está inseparavelmente ligado o conceito de autonomia, e a este o princípio universal da moralidade, o qual na ideia está na base de todas as acções de seres racionais como a lei natural está na base de todos os fenômenos" (KANT, 2011, p. 102).

[4] Disponível em: https://bit.ly/2O1ziHl. Acesso em: 9 set. 2018.

2. Privacidade × segurança nas escolas

Sobreleva anotar que nenhum direito fundamental é absoluto, comportando restrições, em caso de colisão, pela via do sopesamento, com a aplicação da regra da proporcionalidade, em sua tríplice manifestação: adequação, necessidade e proporcionalidade em sentido estrito (GUERRA FILHO, 2000, p. 81-85). Destaque-se que tais restrições não têm qualquer influência no conteúdo do direito, podendo apenas, no caso concreto, restringir seu exercício. Em outras palavras, numa colisão entre direitos fundamentais, o direito que tem que ceder em favor de outro não tem afetadas sua validade e, em especial, sua extensão.

Nesse sentido dispõe o Enunciado nº 139 da III Jornada de Direito Civil: "os direitos da personalidade podem sofrer limitações, ainda que não especificamente previstas em lei, não podendo ser exercidos com abuso de direito de seu titular, contrariamente à boa-fé objetiva e aos bons costumes".

O uso de câmeras nas salas de aula, necessariamente, gera um conflito entre direitos fundamentais, pois, se de um lado está o direito à privacidade e, indiretamente, a liberdade de ensinar e aprender; de outro, se encontra um direito não menos fundamental, qual seja, o direito à segurança, previsto no artigo 5º, *caput*, artigo 6º, e no artigo 144, todos da Constituição Federal. Este último dispositivo inaugura um capítulo específico em nossa Lei Maior para tratamento do assunto, prevendo que "a segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio".

Segundo Silva (2014, p. 74), o direito à segurança aparelha situações, limitações e procedimentos destinados a assegurar o exercício e o gozo de direitos fundamentais. E, considerando que uma das facetas da garantia da segurança é a redução de riscos, é dever do Estado assegurar a incolumidade das pessoas e do patrimônio por meio de prevenção, vigilância e repressão de condutas delituosas (SOUZA NETO, 2013, p. 231).

Portanto, diante da colisão entre direitos tão relevantes, a solução se daria por meio do sopesamento, o que implicaria a restrição do exercício de direitos fundamentais, tarefa esta que é sempre complexa, de forma que é difícil encontrar unanimidade a respeito do assunto. E, para os fins deste estudo, trataremos de alguns casos submetidos ao Judiciário e também de atos tratados pelo Legislativo para tentarmos exemplificar a divergência que circunda o assunto. Iniciemos, pois, com a análise da jurisprudência.

2.1. Tratamento tema no plano jurisprudencial

Em 2018, o Prefeito do Município de São José do Rio Preto propôs em face do Presidente da Câmara deste Município a Ação Direta de Inconstitucionalidade nº 2113734-65.2018.8.26.0000, julgada pelo Órgão Especial do Tribunal de Justiça do Estado de São Paulo[5], que, por maioria de votos, declarou a validade de uma lei municipal que dispõe sobre a instalação de câmeras de monitoramento de segurança em creches e

[5] Vale destacar que, em 29 de setembro de 2016, no julgamento do ARE nº 878911, sob o regime de repercussão geral, o Supremo Tribunal Federal decidiu que a aprovação de leis de iniciativa Parlamentar dispondo sobre a instalação de câmeras de monitoramento em escolas e cercanias não é de competência privativa do Poder Executivo municipal, pois, "embora crie despesa para a Administração Pública, não trata da sua estrutura ou da atribuição de seus órgãos nem do regime jurídico de servidores públicos".

escolas públicas municipais, inclusive dentro de salas de aula. De acordo com o Tribunal, o monitoramento e armazenamento das imagens para consulta eventual, em razão de um caso específico, não ofende a intimidade dos alunos e professores, nem se consubstancia em fator inibidor do aprendizado, sendo possível a restrição de direitos fundamentais face à necessidade de garantia da segurança. O Desembargador Relator baseou seu entendimento em quatro premissas, que merecem ser destacadas: a) em sendo a escola um espaço público, não se poderia falar em prática de atos privados e particulares, de formar que o monitoramento por câmeras de segurança não afetaria a intimidade ou vida privada de alunos e professores; b) a coleta das imagens, por si só, não ofende o direito à imagem dos indivíduos, sem que haja indícios de uso indevido; c) o monitoramento por câmeras não interfere na liberdade de ensinar e aprender, já que a conduta de alunos e professores deve obrigatoriamente se pautar pelo princípio da legalidade; e d) é possível a relativização de direitos fundamentais em razão da necessidade de fiscalização e garantia de segurança na escola.

Como salientado, tratando-se de colisão de direitos fundamentais, a tarefa do sopesamento é complexa, o que gera uma pluralidade de opiniões sobre o tema. Não por outra razão, o julgamento da citada ação se deu por maioria, ante a divergência instalada. Vale destacar os dois principais argumentos dissonantes da maioria: a) a instalação de câmeras de vigilância no interior das salas de aula viola as normas do Estatuto da Criança e do Adolescente, da Constituição Federal, gerando efeitos negativos ao aprendizado e convivência entre professores e alunos; e b) o monitoramento viola a liberdade de ensinar, impactando na autonomia do professor para o exercício de suas funções.

Tema semelhante também foi objeto de discussão no Tribunal Regional do Trabalho da 4ª Região, quando do julgamento do Recurso Ordinário nº 0020494-38.2014.5.04.0007. O recurso foi interposto pela Escola Maternal e Jardim de Infância Castelinho S/S Ltda. em face da sentença do juízo trabalhista que acolheu o pedido do Sindicato dos Professores do Estado do Rio Grande do Sul, condenando a reclamada na obrigação de se abster de manter câmeras de vídeo nas suas salas de aula, bem como na obrigação de pagar indenização referente a dano moral coletivo, na monta de R$ 75.000,00, porquanto o monitoramento de alunos e professores transmite desconfiança e ofende a privacidade. O citado Tribunal, por maioria, acolheu o pedido da reclamada, reformando integralmente o julgado. E o voto vencedor funda-se basicamente em dois argumentos: a) a instalação de câmeras de vigilância em salas de aula não comprometeria a liberdade de ensinar e aprender, sendo que a presença de câmeras já faz parte da rotina dos brasileiros; e b) há necessidade de se garantir a segurança de alunos e professores, diante da realidade fática.

Por sua vez, o voto da Desembargadora relatora do Acórdão, que restou vencido, se baseou em dois principais argumentos: a) as câmeras instaladas no interior das salas de aula não servem para garantir a segurança aos alunos e professores contra agressores externos, não se podendo presumir que alunos e professores atuem contra a lei; b) há violação do princípio da liberdade de cátedra, gerando um ambiente de desconfiança, não só nos alunos, mas também nos professores; c) há ofensa à intimidade e à imagem de alunos e professores.

O caso submetido à Justiça Trabalhista já transitou em julgado, enquanto que aquele submetido ao Tribunal de Justiça de São Paulo aguarda apreciação do Supremo Tribunal Federal.

Em casos semelhantes, os Tribunais Regionais do Trabalho das 1ª e 6ª regiões decidiram que a colocação de câmeras em salas de aula não gera violação da privacidade ou assédio moral contra professores (Recurso Ordinário n. 00222007120055010034, j. 20/04/06 e n. 0000069-74.2012.5.06.0016, j. 29/01/14, respectivamente).

2.2. Tratamento do assunto no plano legislativo

No plano legislativo, é importante destacar que tramitou no Senado Federal o Projeto de Lei nº 88, de 2014[6], que visava a alterar a Lei nº 9.394/1996 (Lei de Diretrizes e Bases da Educação Nacional) para prever a obrigação das escolas públicas ou privadas instalarem sistema de segurança baseado em monitoramento por câmeras de vídeo. O projeto, todavia, foi arquivado, após receber voto contrário da Comissão de Constituição, Justiça e Cidadania, sob o argumento de que seria inconstitucional. De acordo com o relator, muito embora se trate de matéria atinente à segurança pública, com vistas à proteção da criança e do adolescente, a proposição interferiria em assunto de interesse local, não se tratando, portanto de diretriz educacional, mas de medida concreta para assegurar a segurança das escolas. Além disso, segundo o relator, o projeto poderia se consubstanciar em controle excessivo sobre as atividades dos docentes, em especial se instaladas câmeras nas salas de aula, bem como em fator opressor de mobilizações estudantis.

No Estado de São Paulo, o Projeto de Lei nº 1135/2011[7], que dispunha sobre a instalação de câmeras de monitoramento em asilos, creches e pré-escolas, também teve voto contrário da Comissão de Constituição e Justiça, o que gerou seu arquivamento.

Por sua vez, o Estado do Mato Grosso do Sul promulgou a Lei nº 3.946/2010[8], autorizando a instalação de sistema de segurança baseado em monitoramento por câmeras de vídeo nas escolas públicas e privadas daquele ente da federação, com o objetivo de prevenir e apurar a autoria de atos criminosos ou nocivos à segurança da comunidade escolar e de preservar o patrimônio da escola. A lei permite a instalação de câmeras em locais de circulação interna ou externa das escolas, excepcionando, todavia, vestiários, banheiros, salas de professores e salas de aula.

Veja-se que a questão envolvendo o monitoramento em salas de aula não é nova, mas invariavelmente retorna ao debate público, justamente por não encontrar unanimidade, nem na jurisprudência, nem no plano legislativo.

Mas não é somente no âmbito do Judiciário e do Legislativo que o assunto encontra divergência. Também dentre os profissionais da educação esta uniformidade de entendimentos está longe de ser alcançada. Em 28 de setembro 2012, a revista *Isto É* publicou uma reportagem ("Câmera na sala de aula: isso é bom?"[9]) a respeito da instalação de câmeras em um conhecido colégio da Capital paulista. Na matéria foram ouvidas educadoras com posições contrapostas, expondo os pontos positivos e negativos elencados. Assim, quem se manifesta favoravelmente à vigilância eletrônica elenca os seguintes fundamentos: a) trata-se de ferramenta para auxiliar na segurança do ambiente escolar; b) ajuda a manter a disciplina durante as aulas; c) colabora na solução

[6] Disponível em: https://bit.ly/36cNWlb. Acesso em: 21 jan. 2019.

[7] Disponível em: https://bit.ly/36h1vQq. Acesso em: 12 ago. 2019.

[8] Disponível em: https://bit.ly/2uiXgGP. Acesso em: 12 ago. 2019.

[9] Disponível em: https://bit.ly/2RAc8Zy. Acesso em: 12 ago. 2019.

de conflitos; e d) pode ser utilizado como instrumento de aprimoramento profissional. Por outro lado, são argumentos contrários à vigilância por câmeras: a) prejudica a espontaneidade da relação professor e aluno; b) inibe os estudantes na discussão de temas polêmicos; c) traz prejuízo à formação dos alunos, pois atrapalha o desenvolvimento da autonomia e da responsabilidade dos adolescentes; e d) diminui a autoridade do professor ao colocar outro árbitro na sala de aula.

Apesar destas críticas, no Estado de São Paulo[10], como parte do "Sistema de Proteção Escolar", que visa à prevenção de conflitos na escola, foram disponibilizadas câmeras de vigilância a diversas escolas públicas, sendo que, em relação a uma parte delas, a instalação seria pré-definida pela Secretaria de Educação (salas de informática e secretaria) e, quanto à outra parte, caberia ao diretor da unidade escolar definir o local de instalação, conforme as necessidades da escola.

Além disso, cumpre anotar que não são raras as escolas privadas que fazem uso deste mecanismo de segurança, inclusive ofertando o monitoramento por câmeras como um diferencial de seus serviços.

Este fenômeno não é exclusividade brasileira. Nos Estados Unidos da América, por exemplo, as escolas têm crescentemente utilizado câmeras de segurança como uma ferramenta para monitorar e melhorar a segurança dos alunos. As imagens gravadas, inclusive, podem ser compartilhadas com os pais dos estudantes expostos nas imagens, bem como com as autoridades competentes[11].

Trazendo o debate para a esfera jurídica, cabe refletirmos a respeito dos principais pontos abordados nos citados acórdãos e também no parecer da Comissão de Constituição e Justiça do Senado Federal, que se centram basicamente na dicotomia que abarca, de um lado, a privacidade e a liberdade e, de outro, a segurança.

Considerações finais

Diante do contexto exposto, é de se indagar se, de fato, há colisão entre privacidade e segurança na sala de aula. Para responder a esta pergunta, faz-se necessário um esclarecimento conceitual. Como salientado, nossa Constituição prefere utilizar a expressão direito à privacidade, "num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional em exame consagrou" (SILVA, 2017, p. 208). Destarte o termo privacidade abarca o direito à vida privada, à intimidade, à honra e à imagem, nesta ordem de exclusividade.

Pensando na escola como um espaço público, jamais se poderia falar que a colocação de câmeras em salas de aula violaria a vida privada e intimidade, pois estes são direitos que abarcam os mais exclusivos fatos da vida do ser humano, normalmente decorrentes de reserva mental ou compartilhados com um pequeno número de pessoas confiáveis, em ambientes privados. E não se poderia incluir a sala de aula neste conceito, pois, tratando-se de espaço público, necessariamente pressupõe o compartilhamento de experiências pedagógicas, destinando-se ainda ao convívio entre alunos. De outro lado, é imprescindível a preservação da intimidade nos espaços privativos, como é o caso, e.g.,

[10] Disponível em: https://bit.ly/2Rbz2qW. Acesso em: 12 ago. 2019.

[11] Disponível em: https://bit.ly/2TKMpQA. Acesso em: 12 ago. 2019.

dos vestiários ou banheiros das escolas, como citados nos julgados e atos legislativos anteriormente abordados.

Também não se cogitaria ofensa à honra ou imagem em decorrência da mera instalação de câmeras de vigilância em sala de aula. Todavia, como salientado no caso julgado pelo Tribunal de Justiça de São Paulo, deve-se assegurar o tratamento adequado das imagens captadas de modo a coibir eventual abuso na sua utilização.

Isto denota, inclusive, a ressignificação do conceito de privacidade, antes centrado no trinômio pessoa-informação-sigilo, mas que hoje se funda no seguinte quadrinômio: pessoa-informação-circulação-controle. Cabe, assim, ao titular do direito à privacidade exigir formas de circulação controlada, mas não interromper o fluxo de informações que lhe digam respeito (RODOTÁ, 2008, p. 93).

A sociedade da vigilância parece se desenvolver num caminho sem volta. A preocupação, portanto, deveria se centrar em temas envolvendo circulação e controle desta informação captada pelas câmeras de segurança e não na alegação de violação da intimidade, do que não se poderia cogitar, em se tratando de sala de aula, um espaço público. Ademais, quando tais imagens são obtidas por órgãos públicos, seria possível até a aplicação dos dispositivos da Lei de Acesso à Informação, em especial seu artigo 31, de forma que o cidadão não estaria desamparado.

Este verdadeiro *Big Brother* de Orwell se justifica, normalmente, com base em uma alegação: necessidade de garantir segurança. E não sem razão. A violência em sala de aula, infelizmente, é uma realidade, até o momento sem solução adequada.

De acordo com a Pesquisa Internacional sobre Ensino e Aprendizagem (Talis)[12] divulgada pela Organização para a Cooperação e o Desenvolvimento Econômico (OCDE), em 2014, o Brasil, dentre os países participantes, é aquele que apresenta os maiores índices de violência contra professores, por meio de ofensas e intimidação e uso ou posse de drogas ou bebidas alcóolicas.

Corroborando estas informações, o Sindicato dos Professores do Ensino Oficial do Estado de São Paulo (Apeoesp), em 2013, divulgou o estudo "Violência nas escolas: o olhar dos professores"[13], em que se apontou que 44% dos professores entrevistados já sofreram algum tipo de violência em suas escolas.

De acordo a pesquisa, a violência nas escolas implica um problema de segurança tanto para professores quanto para os alunos, impactando severamente no processo de aprendizagem.

No mais, conforme decidiu o Superior Tribunal de Justiça, a garantia da segurança dentro do estabelecimento de ensino é dever do Estado. No caso que envolveu ato de violência praticado contra professora no ambiente escolar, a Corte manteve Acórdão do Tribunal de Justiça do Distrito Federal, condenando o ente a pagar indenização por danos morais à docente, em razão da negligência:

> *Destacou-se, à vista de provas colacionadas aos autos, que houve negligência quando da prestação do serviço público, já que se mostrava razoável, ao tempo dos fatos, um incremento na segurança dentro do estabelecimento escolar, diante de ameaças perpetradas*

[12] Disponível em: https://bit.ly/37fpiS7. Acesso em: 10 ago. 2019.

[13] Disponível em: https://bit.ly/38qhiOs. Acesso em: 10 ago. 2019.

pelo aluno, no dia anterior à agressão física. (REsp 1142245/DF, Rel. Ministro CASTRO MEIRA, SEGUNDA TURMA, julgado em 05/10/2010, DJe 19/10/2010)

Tratar da segurança pelo o prisma da prevenção de riscos é, portanto, fundamental para que se avalie a possibilidade de colocação de sistema de monitoramento por câmeras nas escolas, inclusive nas salas de aula. E, em sendo a segurança um dever do Estado, bem como um direito fundamental e essencial para garantia do processo educativo das crianças e adolescentes, assegurá-la é, por outra via, garantir o direito à educação e o princípio da proteção integral previsto no Estatuto da Criança e do Adolescente.

Enfim, encerramos este estudo, tratando do terceiro e último ponto, imprescindível para análise adequada do problema posto: a liberdade de ensinar e aprender. Prevista no artigo 206, inciso II, da Constituição Federal, se consubstancia numa das formas de manifestação do pensamento, mas específica para o exercício do magistério, dentro de uma visão de pluralista de ideias[14]. O enunciado constitucional engloba uma dimensão objetiva e outra subjetiva. Esta diz respeito aos sujeitos do conhecimento; aquela se relaciona à liberdade do professor escolher o objeto do ensino a transmitir, liberdade esta condicionada aos currículos escolares e aos programas oficiais de ensino (SILVA, 2014, p. 802).

Pontes de Miranda já nos alertava de que não se pode confundir a liberdade de ensinar, que resulta da objetividade, da investigação da verdade, com o direito fundamental do indivíduo quanto à opinião. Para o autor, o Estado contemporâneo tem de ser educativo e a liberdade de ensinar assume a característica de verdadeira garantia institucional (PONTES DE MIRANDA, 1947, p. 113).

E por esta razão, tendo em conta a objetividade desta garantia, que é a liberdade de ensinar e aprender, não se pode encará-la como um direito absoluto, até porque está necessariamente vinculada aos objetivos e programas da educação nacional.

Indaga-se, todavia – e isto foi motivo de intensos debates jurisprudenciais e legislativos – se a colocação de câmeras de segurança em sala de aula poderia gerar lesão à garantia institucional e fundamental.

Não restam dúvidas de que vigilância constante é fator que dificulta a espontaneidade, podendo gerar artificialidade e o desestímulo ao debate. Trata-se de uma espécie de liberdade monitorada, que, de certo modo, se assemelha àquela abordada por Foucault ao tratar do Pan-óptico de Bentham, que se destinava a induzir à sensação de vigilância constante e à modificação de comportamentos, com vistas a assegurar o funcionamento do poder (FOUCAULT, 2010, p. 191-194).

Mas falar-se em restrição da liberdade de ensinar e aprender em razão da implementação deste mecanismo de segurança parece exagero. Não há evidência de lesão à liberdade de ensinar e aprender. Como salientado pelo Tribunal de Justiça de São Paulo no julgamento do caso citado, não se poderia falar em constrangimento ou censura à liberdade do professor ou aluno se estes praticam suas atividades de acordo com a legalidade.

[14] José Afonso da Silva critica a expressão "liberdade de cátedra", pois era mais restritiva ao se vincular à ideia de catedrático, relativa à titularidade de determinados cargos de magistério. A fórmula empregada atualmente é mais compreensiva abrangendo qualquer exercente do magistério (SILVA, 2014, p. 802).

Além disso, não se pode deixar de mencionar que, hoje, o cidadão está exposto ao monitoramento por câmeras em diversos ambientes, e.g., nas ruas, no trabalho, em elevadores, restaurantes etc. Segundo a Associação Brasileira das Empresas de Sistemas Eletrônicos de Segurança (Abese), em 2011[15], a cidade de São Paulo chegou a registrar mais de um milhão de câmeras, numa média de um aparelho para cada dez habitantes. De acordo com a associação, o paulistano no seu trajeto da casa ao trabalho passa por no mínimo dez câmeras de monitoramento. Todavia, este tipo de vigilância quase que onipresente, fundada na ideia de insegurança pública, por si só, não implica restrição à liberdade do indivíduo.

Aliás, é justamente esta questão da segurança um dos principais argumentos utilizados para manutenção das câmeras em salas de aula, quando do julgamento dos casos mencionados anteriormente, o que nos leva a afirmar que, no sopesamento entre os direitos fundamentais de privacidade, liberdade e segurança, este tem sido considerado o elemento prevalente.

Assim sendo, toda a discussão muda de foco para se centrar na ideia de controle e tratamento adequado das imagens coletadas por tais sistemas de vigilância.

Afinal, na aldeia global, a defesa do direito à privacidade se converte em instrumento para tornar mais transparente e controlável o tratamento de informações pessoais (RODOTÁ, 2008, p. 93).

As questões tratadas neste artigo nos indicam não só a necessidade de se adotar esta visão, mas em especial, a imprescindibilidade da criação e aprimoramento dos mecanismos legais e regulatórios que verdadeiramente amparem alunos e professores e que garantam a adequada proteção às imagens coletadas no ambiente escolar.

Referências bibliográficas

CARNEIRO, Moacir Alves. *LDB fácil*: leitura crítico-compreensiva artigo a artigo. 23. ed. Petrópolis: Vozes, 2015.

COSTA JÚNIOR., Paulo José da. *O direito de estar só*: tutela penal da intimidade. São Paulo: Revista dos Tribunais, 1970.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista da Faculdade de Direito, Universidade de São Paulo*, São Paulo, v. 88, p. 439-459, jan. 1993. ISSN 2318-8235. Disponível em: https://bit.ly/2NHWf1Q. Acesso em: 12 ago. 2019.

FOUCAULT, Michel. *Vigiar e punir*. 38. ed. Tradução Raquel Ramalhete. Petrópolis: Vozes, 2010.

GUERRA FILHO, Willis Santiago. Teoria processual da Constituição. 2. ed. Celso Bastos editor, 2000.

KANT, Immanuel. *Fundamentação da metafísica dos costumes*. Tradução Paulo Quintela. Lisboa: Edições 70, 2011.

MALISKA, Marcos Augusto. In: SARLET, Ingo Wolfgang et al. *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 2013.

[15] Disponível em: http://www.abese.org.br/clipping/2012/08/294.htm. Acesso em: 12 ago. 2019.

MEHEDI, M. The realization of economic, social and cultural rights. *UN Sub-Commission on the Promotion and Protection of Human Rights*, 2 jun. 1998. Disponível em: https://bit.ly/2sJypvn. Acesso em: 12 ago. 2019.

PASSOS, J. J. Calmon de. A imprensa, a proteção da intimidade e o processo penal. *Revista Forense*, v. 324, p. 61-67, 1989. ISSN 0102-8413.

PONTES DE MIRANDA, Francisco Cavalcanti. *Comentários à Constituição de 1946*. Rio de Janeiro: Henrique Cahen Editor, 1947. v. 4.

RAMOS, André de Carvalho. *Curso de Direitos Humanos*. São Paulo: Saraiva, 2016.

RANIERI, Nina Beatriz Stocco. O novo cenário jurisprudencial do direito à educação no Brasil: o ensino domiciliar e outros casos no Supremo Tribunal Federal. *Pro-Posições*, Campinas, v. 28, n. 2, p. 141-171, ago. 2017. Disponível em: https://bit.ly/2tCx5uM. Acesso em: 12 ago. 2019.

RODOTÁ, Stefano. *A vida na sociedade da vigilância: a privacidade hoje*. Tradução Danilo Doneda, Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SILVA, José Afonso. *Curso de direito constitucional positivo*. 40. ed. São Paulo: Malheiros, 2017.

SILVA, José Afonso. *Comentário contextual à Constituição*. 9. ed. São Paulo: Malheiros, 2014.

SOUZA NETO, Claudio Pereira de. In: SARLET, Ingo Wolfgang *et al*. *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 2013.

TAVARES, Letícia Antunes; ALVAREZ, Bruna Acosta. Da proteção dos dados pessoais: uma análise comparada dos modelos de regulação da Europa, dos Estados Unidos da América e do Brasil. *In*: BALDANI, Thiago Gomes de Fillipo; ONODERA, Marcus Vinicius Kiyoshi (coord.). *Brasil e EUA: temas de direito comparado*. São Paulo: Escola Paulista da Magistratura, 2017.

TEIXEIRA, Anísio. *Educação é um direito*. Rio de Janeiro: Editora UFRJ, 2009.

Lei Geral de Proteção de Dados, direito ao apagamento, correção dos dados e blockchain: análise da pertinência tecnológica

Renata Barros Souto Maior Baião
Juíza de Direito no Estado de São Paulo

Sumário: 1. Introdução; 2. Lei Geral de Proteção de Dados – Lei n. 13.709, de 14 de agosto de 2018 – breves considerações; 3. Blockchain; 3.1. Qual problema a blockchain resolve?; 3.2. Classificação das redes blockchain; a) grau de centralização; b) grau de transparência; c) grau de autonomia; 3.3. Conteúdo do bloco; 4. Análise da pertinência tecnológica entre a blockchain e a Lei Geral de Proteção de Dados; 5. Sugestões para compatibilização tecnológica; 6. Considerações finais; 7. Referências bibliográficas.

Resumo: A Lei Geral de Proteção de Dados, a exemplo da *General Data Protection Regulation*, estabeleceu direitos ao titular de dados, tais como o de apagamento e correção. Paralelamente, desenvolve-se a tecnologia blockchain que, para além de viabilizar a individualização de ativos digitais como o bitcoin, registra transações de forma imutável, transparente, segura e auditável, características, em tese, incompatíveis com direitos franqueados ao titular de dados. Todavia, a depender da natureza da rede e das transações realizadas, é possível compatibilizar o exercício pleno dos direitos do titular de dados e a tecnologia blockchain.

Palavras-chave: Proteção de Dados. Tecnologia. Proteção. Apagamento. Correção. Blockchain. Compatibilidade.

1. Introdução

Dentro do universo da internet da informação, nunca foram registrados, publicados, armazenados e tratados tantos dados quanto atualmente[1].

Este universo criou um cenário no qual os indivíduos, a pretexto de uma "melhor experiência do usuário" são monitorados ao longo de seus dias e tais informações são retidas e utilizadas por empresas privadas que, com base nelas, disponibiliza publicidade direcionada ou, até mesmo, realiza experiências de cunho psicológico com seus usuários, tal como a que o Facebook fez (KRAMER; GUILLORY; HANCOCK, 2014).

Os usuários são estimulados a passar cada vez mais tempo conectados, e os dispositivos e aplicativos são especialmente desenhados para reter a atenção de cada indivíduo por longos períodos, viciando-o (ALTER, 2018, posição 157).

[1] Por exemplo, são carregadas, no Youtube, mais de 500 horas de vídeo por minuto (OSMAN, 2019).

Aos poucos, a internet da informação virou um modelo de negócio e seus usuários foram transformados em "ratinhos de laboratório", explorados para a obtenção de lucro, por meio de publicidade direcionada[2], dentre outros.

Entretanto, diversamente de um suporte físico impresso, tal como um livro, localizar informações na internet tornou-se ação simples, que possibilita a obtenção de resultados de forma instantânea e automatizada.

Com o aumento de informações disponibilizadas e da eficiência dos mecanismos de busca, identificar e acessar conteúdo de divulgação indesejada pelo particular tornou-se ação não só fácil como rápida. Além disso, em tempos de *big data*, qualquer dado é relevante, pois conversível em informação valiosa[3] para encetar os novos modelos de negócios.

Em razão disso, passou-se a questionar o universo de informações constantes na internet, o uso que poderia ser dado a ele, bem como os rastros digitais e o impacto que sua existência poderia causar na vida das pessoas.

Diante desse cenário, a teoria do direito ao esquecimento ganhou corpo e não foi ignorada pela legislação específica.

A Lei Geral de Proteção de Dados, apesar de não a referir expressamente, estabeleceu, em seu art. 18, IV e VI, o direito do titular de dados de ter seus dados eliminados por aqueles que, eventualmente, os tenham captado para tratamento, mediante o atendimento de certos requisitos.

Paralelamente e, fundado na liberdade de expressão, na liberdade financeira e no exercício do direito à privacidade, em plena crise econômica de 2008[4], Satoshi Nakamoto[5] publicou um *whitepaper* criando o bitcoin, um sistema de dinheiro eletrônico ponto a ponto (NAKAMOTO, 2008).

Satoshi Nakamoto estabeleceu, em seu *whitepaper*, os parâmetros iniciais de uma estrutura de dados organizada sob a forma de contabilidade de tripla entrada[6] que possibilitaria, a partir de 3 de janeiro de 2009[7], a transferência de um ativo digital individualizado, sem intermediação.

O *whitepaper* evidenciou ainda que os parâmetros criptográficos da rede do bitcoin, bem como a forma de realização de encadeamento das transações, tornaria seus registros imutáveis, transparentes, auditáveis, seguros, confiáveis, na medida em que são propagados para uma rede de computadores distribuída.

Os debates não tardaram a surgir, questionando a possibilidade de compatibilizar a tecnologia blockchain com alguns direitos atribuídos ao titular de dados pessoais,

[2] "Essa capacidade de identificar os mais diversos padrões de comportamentos e prever a sua recorrência no futuro é uma verdadeira 'mina de ouro' para a abordagem publicitária" (BIONI, 2018, posição 914).

[3] "Dados são simplesmente fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação" (BIONI, 2018, posição 813).

[4] Em 2008, a crise financeira mundial "queimou as pontes de confiança" entre os "titãs" da indústria financeira e o público (BURNISKE; TATAR, 2018, p. 3).

[5] A identidade de Satoshi Nakamoto não é conhecida (EHA, 2017, p. 11). Apesar de pessoas se autoproclamarem Satoshi Nakamoto, nenhuma delas movimentou os bitcoins do criador do criptoativos, não sendo possível esclarecer a veracidade das informações daqueles que dizem ser Satoshi Nakamoto.

[6] Na contabilidade de tripla entrada, cada saída corresponde a uma entrada, assegurada por uma camada de validação.

[7] BLOCO gênese do Bitcoin. Disponível em: https://bit.ly/2R68Kqi. Acesso em: 7 ago. 2019.

notadamente o direito ao apagamento e o direito à correção de dados estabelecido na Lei Geral de Proteção de Dados.

É o que será enfrentado neste artigo.

2. Lei Geral de Proteção de Dados, Lei nº 13.709, de 14 de agosto de 2018: breves considerações

O desenvolvimento de modelos de negócio voltados para a captação de dados e monitoramento de indivíduos, a fim de possibilitar uma propaganda direcionada e uma "melhor experiência do usuário", aliado às notícias de situações de monitoramento e vigilância determinaram uma maior urgência no exame do direito à privacidade e à proteção de dados e, em consequência, na elaboração da General Data Protection Regulation europeia e, no Brasil, da Lei Geral de Proteção de Dados (LGPD).

A LGPD foi claramente inspirada na legislação europeia (COTS; OLIVEIRA, 2019, p. 9), alinhando-se a um dos principais regramentos mundiais sobre o tema.

Houve um grande avanço legislativo, pois a LGPD modificou o viés interpretativo quanto à coleta de dados, concentrando na figura do titular os atos de disposição, atribuindo-lhes o caráter de irrenunciabilidade (COTS; OLIVEIRA, 2019, p. 154).

Salienta-se que, sob uma perspectiva tecnológica, a legislação é neutra. Entretanto, ao analisar-se os agentes de tratamento (art. 5º, IX, da Lei nº 13.709/2018), verifica-se que a LGPD foi elaborada considerando a centralização da operação de tratamento de dados em pessoa física ou jurídica e, em consequência, possibilitando a responsabilização na hipótese de afronta.

A tecnologia blockchain, por sua vez, é alicerçada em conceitos de distribuição e descentralização das informações como uma das formas de tornar as redes resilientes, o que, em última análise, permite que os registros nelas constantes sejam transparentes, imutáveis e auditáveis.

Tais atributos, por sua vez, levam a uma conclusão inicial — e, diga-se, precipitada — de que a tecnologia blockchain está inviabilizada pela Lei Geral de Proteção de Dados. Todavia, respeitadas as opiniões em sentido contrário, a tecnologia blockchain, observadas algumas cautelas, é sim compatível com a legislação protetiva.

3. Blockchain

Blockchain é tecnologia de propósito amplo, podendo compreender tanto o armazenamento de informações como a execução de protocolos.

Primavera de Filippi e Aaron Wright definem blockchain como banco de dados descentralizados, mantidos por uma rede distribuída de computadores, salientando a reunião de diferentes tecnologias (redes ponto a ponto, criptografia assimétrica e mecanismos de consenso) para tanto (2018, posição 234).

Michael Talbot conceitua blockchain como um banco de dados digital distribuído que utiliza tecnologia ponto a ponto, encadeada, combinada com chaves criptográficas para permitir o registro de um livro-razão de transações de forma segura, imutável, irretratável, confiável e transparente, sem ponto central de controle (2018, posição 450).

Malekan expõe uma visão sintética de blockchain, definindo-a como uma tecnologia que permite a existência de algo digital em apenas um lugar (2018, p. 2).

Paul Vigna e Michael Casey conceituam blockchain como um livro-razão digital compartilhado em uma rede descentralizada de computadores independentes, que o mantém atualizado de forma a permitir a comprovação de que os registros nele contidos são completos e incorruptíveis (2018, p. 12).

Kravchenko, Skriabin e Dubinina esclarecem tratar-se de um banco de dados que contém transações comuns entre todos os nós envolvidos na rede bitcoin, com a peculiaridade de que cada bloco confirma a integridade do bloco anterior, assegurando, em consequência, a integridade do histórico de todas as transações realizadas (2018, posição 2822).

Davis e Le Merle estabelecem que blockchains são livros-razão abertos, distribuídos e que podem registrar transações entre duas partes de forma eficiente, verificável e permanente (2019, p. 97).

Ressalve-se, entretanto, que a arquitetura peculiar da blockchain e seu estágio inicial de desenvolvimento tecnológico muitas vezes podem trazer alguma confusão entre seus conceitos e seus atributos.

Assim, a partir dos conceitos acima elencados, elabora-se uma definição mínima de blockchain[8]: conjunto de tecnologias que compõe uma estrutura de dados organizados sob a forma de contabilidade de tripla entrada[9]. Isso significa, essencialmente, que os registros desses dados são compostos pelos seguintes elementos mínimos: a) uma entrada que corresponde a uma saída; b) uma saída; c) uma camada de validação criada pela rede, que assegura a saída.

A denominação "blockchain" se originou justamente do fato de as transações serem agrupadas em blocos que, por sua vez, são encadeados de forma criptografada aos blocos anteriores. Esse recurso confere segurança às transações e imutabilidade aos registros.

Em razão de tais elementos, aliados a critérios criptográficos de encadeamento das operações, as informações registradas por meio da aplicação da tecnologia blockchain vêm revestidas de uma série de atributos, consistentes em imutabilidade, transparência, segurança e auditabilidade.

A partir de tais atributos, alcança-se o propósito da tecnologia: criar valor a partir da descentralização da criação, verificação, validação e armazenamento seguro de transações (CAMPBELL-VERDUYN, 2018, posição 1375), permitindo a individualização dos ativos digitais.

Trata-se de tecnologia em crescimento, tanto no desenvolvimento de novas soluções, como em adoção pelos mais diversos modelos de negócio, os quais, por sua vez, customizam aplicações.

Assim, diante do objeto deste estudo, é necessário ingressar também na natureza da informação armazenada na blockchain, salientando-se que há várias redes distintas, com objetivos peculiares.

[8] Frise-se: a conceituação apresentada é mínima, a fim de que possa ser aplicada nas distintas espécies de redes existentes. A tecnologia blockchain, para ser identificada como tal, deve ainda observar algumas estruturas tecnológicas que vão além do necessário para este estudo e que, por isso, não serão analisadas.

[9] Na contabilidade de dupla entrada, cada transação é representada por dois lançamentos, um a crédito, outro a débito (ETWARU, 2017, p. 41).

3.1. Qual problema a blockchain resolve?

Blockchain resolve o problema do gasto duplo no meio digital. Ou seja, desde a criação do bitcoin, é possível "gastar" um ativo digital, sem duplicá-lo. Assim, quando bitcoins são remetidos de um endereço para o outro, eles efetivamente saem da esfera de disposição do remetente, ou, em outras palavras, são "gastos".

Embora, como dito, trate-se de tecnologia ainda embrionária, os efeitos e possibilidades já se descortinam no horizonte, todas elas envolvendo um reposicionamento do intermediário.

Em comparação à transferência de bitcoins exemplificada acima – concretizada sem a interferência de intermediários –, uma transferência de quantia no sistema bancário seria realizada necessariamente mediante intervenção da instituição financeira, que verificaria a existência de saldos, regularidade documental etc.

O confrontamento das duas situações traz à luz um dos efeitos da adoção da blockchain: o reposicionamento do intermediário que, a depender do grau de centralização da rede, sequer será necessário.

3.2. Classificação das redes blockchain

Para este estudo, como não é possível analisar individualmente todas as redes existentes, será proposta classificação de redes ampla, permitindo o exame das principais questões por meio de grupos maiores, divididos conforme a seguinte classificação: a) o grau de centralização; b) o grau de transparência; c) o grau de autonomia.

a) grau de centralização:

Redes centralizadas: concentram a informação em um local, tais como aquelas que operam no sistema cliente-servidor, e, por isso, criam um ponto central de vulnerabilidade (WERBACH, 2018, posição 2472). O intermediário é mantido.

Redes descentralizadas[10]: as redes descentralizadas possuem pontos de concentração ou controle de informação. O intermediário é mantido, mas pode ser deslocado para ponta da cadeia, avaliando a informação recebida.

Redes distribuídas: as redes distribuídas não possuem pontos de concentração de informação ou centros de poder. Todos os nós da rede estão conectados entre si e atuam em conjunto, porém de forma independente e, na blockchain, possuem uma cópia do livro-razão atualizada com todas as transações (NORMAN, 2017, p. 32). O intermediário é excluído.

A distinção é relevante porque, apesar de amplamente propagado que blockchain é tecnologia que elimina o intermediário, isso não se verifica em todas as espécies de rede (WERBACH, 2018, posição 2399).

Embora exista uma clara proposta de valor na existência do intermediário para verificar a veracidade de uma informação, no caso de uma rede blockchain distribuída,

[10] Há autores que não diferenciam os termos descentralização e distribuição. Em uma perspectiva classificatória, a distribuição é a descentralização absoluta, com a remoção de todos os pontos de concentração da rede.

o intermediário será o *ledger*[11], não o criador do protocolo. Na rede blockchain distribuída, o intermediário como conhecemos é eliminado.

Já nas redes descentralizadas há pontos de controle e centralização que representam não só um intermediário como também pontos de fragilidade da rede.

Além disso, é muito comum encontrar, na literatura técnica, classificações que incluem, nas características de redes públicas, a possibilidade de qualquer pessoa delas participar, desempenhando qualquer atividade[12], elementos distintivos das redes não permissionadas. Isso ocorre porque para desempenhar todas as atribuições existentes em uma rede não permissionada é necessário ter acesso à integralidade do conteúdo do *ledger*, fazendo da rede não permissionada, assim, uma rede pública. Portanto, se qualquer pessoa pode ter conhecimento do conteúdo do *ledger* em uma rede não permissionada, a rede não permissionada é, também, pública.

b) Grau de transparência:

Redes públicas: redes cujo conteúdo pode ser acessado por qualquer pessoa.

Redes privadas: redes cujo conteúdo é restrito a usuários participantes da rede ou cujo acesso é de alguma forma controlado.

c) Grau de autonomia:

Redes permissionadas: apenas usuários autorizados podem participar da rede e é possível configurar o tipo de perfil que cada usuário terá (SWAN, 2015, p. 8). Nesta espécie, os participantes da rede já são conhecidos e "confiáveis" (BASHIR, 2018, p. 34), possibilitando-se inclusive a configuração de perfis distintos para cada um deles.

Redes não permissionadas: qualquer pessoa pode participar da rede, executar o protocolo, validar transações etc.

Tomando-se como exemplo a rede bitcoin, trata-se de rede pública, distribuída e não permissionada.

3.3. Conteúdo dos blocos

A rede blockchain é formada por blocos, que nada mais são que arquivos que registram transações realizadas em um intervalo de tempo, reunindo em sua estrutura outras informações (JUN, 2018, posição 543). Estes blocos são encadeados entre si criptograficamente, e as transações neles registradas podem variar de acordo com a destinação da rede.

Tendo em vista o estudo referente à proteção de dados, é necessário compreender o conteúdo dos blocos que compõem as redes.

Segundo Antonopoulos, o bloco do bitcoin[13] contém metadados (versão do protocolo, referência ao *hash* do bloco anterior, grau de dificuldade, *timestamp*, *nonce*, *merkle tree root*) e as transações, até o limite do tamanho do bloco (2017, p. 197).

Metadados são "marcos ou pontos de referência que permitem circunscrever a informação sob todas as formas" (WIKIPEDIA, 2019).

[11] *Ledger* pode ser compreendido como a consolidação de todos os registros de transações realizadas na blockchain.

[12] Confira-se Laurence (2017, p. 21).

[13] Primeira e mais conhecida rede blockchain e, por isso, aqui utilizada como exemplo.

As transações indicam os endereços de onde será remetido determinado saldo de bitcoins e qual endereço receberá tal saldo.

Como se vê, nenhum dos elementos do bloco corresponde objetivamente a um dado pessoal ou sensível.

Além disso, cada detentor de bitcoins poderá ter um ou mais endereços, sem que precise revelar sua titularidade, a não ser quando realize alguma transação. Frise-se: para movimentar o saldo de bitcoins constante em um determinado endereço, o detentor da chave privada correspondente – e, em consequência, do saldo de bitcoins – deverá solicitar a transação para a rede que, constatando a suficiência de saldo, validará a operação e a registrará em um bloco.

Os blocos das redes possuem capacidade de armazenamento limitada e, no caso da rede bitcoin, um bloco é minerado[14] a cada dez minutos[15], aproximadamente.

Com a mineração, os blocos são encadeados na rede e as transações neles constantes estarão permanentemente registradas.

4. Análise da pertinência tecnológica entre a blockchain e a Lei Geral de Proteção de Dados

Pode-se estabelecer, desde logo, que, em razão de sua arquitetura e características, a tecnologia blockchain não traz vantagens imediatamente perceptíveis para o armazenamento de dados pessoais ou sensíveis de forma pública e direta.

Entretanto, mediante a utilização de alguns recursos tecnológicos já existentes, é possível observar rigorosamente a legislação e, ainda, valer-se de todas as propriedades da blockchain.

Tomando-se a rede bitcoin como exemplo, rede pública, distribuída e não permissionada, a realização de transação depende da divulgação das chaves pública e privada.

Embora, em primeira análise, as chaves pública e privada não configurem dados pessoais, se for possível atrelá-las a uma pessoa física, haverá essa identificação. De outro lado, pela própria forma de funcionamento da criptografia assimétrica, elemento essencial para a realização da transação, se não forem fornecidas as chaves pública e privada, tal não será possível.

E, uma vez inseridas tais informações na rede, a transação será imutável.

Portanto, diante de uma rede distribuída, pública, não permissionada, na qual a transação seja feita diretamente pelo titular dos dados, caso haja rompimento da criptografia ou por outro modo o detentor das chaves pública e privada venha a ser conhecido, nada poderá ser feito.

Ademais, a correção do dado, quando envolver a correção da própria transação (se houver sido feita por engano, por exemplo), dependerá exclusivamente daquele que recebeu dito ativo, se este decidir realizar transação no sentido inverso, revertendo-a.

[14] A mineração é o ato de criação de um novo bloco na rede. Ela consiste em uma competição entre os nós da rede na solução de um problema matemático. Aquele que solucionar o problema matemático primeiro criará o bloco e receberá, em troca, bitcoins.

[15] Este tempo é o grau de dificuldade da rede do problema matemático a ser solucionado pelos mineradores no cumprimento da prova de trabalho, a fim de serem remunerados com créditos em bitcoin.

Acrescente-se, ademais, que se a transação for realizada com pessoa desconhecida, ou se forem remetidos ativos para um endereço equivocado, é possível que sequer se descubra quem os recebeu.

Esse cenário, entretanto, não impossibilita o uso das redes públicas, não permissionadas e distribuídas com a Lei Geral de Proteção de Dados.

Como os blocos da rede bitcoin possuem tamanho limitado, nem sempre é possível inserir, por exemplo, um arquivo de imagem. Todavia, nada impede que tal arquivo venha a ser convertido em uma *hash*[16] e que a própria *hash* conste no bloco. Uma vez que, a depender do padrão criptográfico utilizado, não é possível reverter a *hash* obtida no arquivo convertido, ao menos não de acordo com os recursos tecnológicos disponíveis na data da elaboração deste estudo, a anonimização da informação desta forma atenderia aos ditames legais.

Entretanto, tendo em vista a existência de redes que interagem com a rede distribuída ou, ainda, a possibilidade de anonimização desses dados (para que conste apenas a *hash* resultante na blockchain), as redes distribuídas não são de todo incompatíveis com a LGPD.

Além disso, como nas redes não permissionadas não há óbices à participação de quem quer que seja, nada impede que qualquer pessoa obtenha cópia integral de todas as transações realizadas e, a partir dela, realize mineração de dados, caso em que, a depender da natureza destes, poderá se submeter à legislação protetiva.

Todavia, reconhece-se desde já a dificuldade de monitoramento de tais condutas, já que não há nada, ao menos até o encerramento da elaboração do presente texto, que possa impedi-las.

Com relação às redes descentralizadas e às permissionadas, as soluções são distintas. Há claros pontos de centralização e, por consequência, de controle, inclusive de quem são os membros da rede. Estabelecidos tais núcleos, é possível delimitar quais informações são registradas ou, ao menos, por qual meio tal ocorreu.

Ainda que eventualmente isso não seja possível, diante do ponto de centralização vislumbra-se uma via para imposição da obrigação de informar o usuário final acerca do funcionamento da blockchain e das cautelas que devem por ele ser tomadas na realização de operações.

Dito isso, os registros realizados em blockchain são imutáveis, não importando exatamente a classificação da rede. Porém, quando há intermediação, há a possibilidade de maior controle do conteúdo que constará em um registro em blockchain.

A correção de dados na blockchain também não é imune a peculiaridades.

Nesse particular, o atendimento ao direito do titular de dados de correção ou atualização de informações a seu respeito ocorrerá somente a partir do momento em que tal correção ou atualização for inserida na cadeia de blocos, pois não é tecnicamente possível a alteração de informações já registradas na blockchain.

Entretanto, nesse ponto, destaca-se que pode ser, inclusive, forma de atender à seguinte recomendação:

[16] Nesse ponto, destaca-se que a função *hash* converte dados de comprimento variável, apresentando um resultado com comprimento fixo (WIKIPEDIA, 2019). Assim, quando o número de caracteres convertido em hash for maior que aquele do resultado da função, haverá economia de espaço.

> *Evidentemente, é de todo aconselhável o registro do histórico dos apontamentos, sem que necessariamente ocorra a deleção da informação desatualizada, a qual poderá vir a ter utilidade para variados fins, seja para o controlador, seja para o titular (MALDONADO; BLUM, 2019, posição 7037).*

Quanto ao direito ao apagamento, "o qual pressupõe a completa eliminação dos dados quando há o requerimento do titular e quando, de fato, inexista base legal para a subsistência do tratamento" (MALDONADO; BLUM, 2019, posição 7037), surgem as maiores arestas com a tecnologia blockchain.

Embora a LGPD tenha feito menção à eliminação do dado e respeitáveis autores salientem que ela deve ser realizada de forma completa, trata-se de medida que, tecnicamente, não é tão simples de ser tomada, a depender da forma como mantido o dado em questão.

Quando arquivos são excluídos da mídia de armazenamento do computador, na verdade há uma desindexação, de sorte que eles não são mais localizados e, após, eles são sobrescritos com informação nova (ZARAMELA, [20--?]). Isso significa que, na prática, os dados não serão completamente apagados, mas, sim, indisponibilizados.

Em outras palavras, em mídias de armazenamento, quando um dado é excluído, o espaço por ele ocupado é lido pela máquina como disponível para gravação de novos arquivos, que sobrescreverão os dados cuja deleção se pretendia.

Assim, ainda que o legislador tenha estabelecido que a exclusão dos dados é direito do titular, respeitadas as opiniões em contrário, parece ser possível considerar que a indisponibilidade dos dados ou sua corrupção — hábil a impedir o acesso ao seu conteúdo — atende ao quanto pretendido pela norma.

5. Sugestões para compatibilização tecnológica

Observadas as ressalvas feitas ao longo deste texto, no sentido de que não é recomendável a inserção do dado pessoal em rede blockchain, sem nenhuma cautela ou recurso para obscurecer seu acesso, apresentam-se algumas sugestões.

Assim, a primeira medida sugerida é a de anonimização de dados, prevista na própria LGPD, em seu art. 5º, XI, definida como a "utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

A utilização da anonimização de dados pode ser interessante por alguns motivos. O mais evidente, aquele que envolve a proteção dos dados do titular. Em um segundo momento, considerando a eficiência da rede que, como regra, possui recursos limitados de armazenamento, a anonimização de dados poderá redundar em economia de espaço[17].

A própria rede bitcoin se vale de pseudônimos (os endereços) e da possibilidade da criação de mais de um deles por pessoa, notadamente porque a identidade daqueles que realizam transações não interfere na regularidade delas.

[17] Uma das formas de promover a anonimização de dados é converter a informação em uma *hash*. Se a *hash* for menor que o arquivo convertido, haverá melhor aproveitamento do espaço no bloco.

Ademais, é possível a utilização de redes paralelas (*sidechains*) ou separadas (*off-chains*), objetivando o resguardo das informações. Por exemplo: a transação pode ser realizada em uma rede paralela e apenas seu resultado constar na rede principal. Ou, ainda, os dados pessoais ou sensíveis podem constar em meio independente e ser apenas indexado na rede prioritária.

Sem prejuízo do quanto já analisado, vale ressaltar que, até em virtude da limitação do tamanho dos blocos existentes nas diversas blockchains, não há motivos para não usar indexação da informação.

Se não houver necessidade de o dado constar, ele próprio, na rede blockchain – e, diga-se, em uma análise superficial e objetiva isso não se verifica –, é possível lançar mão de sua indexação, por meio do uso de criptografia.

Melhor explicando, bastará que o dado cuja existência se pretende aferir mediante o uso dos atributos da rede blockchain seja convertido em uma *hash* e a *hash* seja transposta para a rede.

Aquele que eventualmente alcançar a informação na rede blockchain estará diante de um código intransponível mas que, confrontado com o dado original, terá sua existência comprovada na data e horário de criação do bloco.

Caso o titular do dado não pretenda mais se valer de tal recurso, bastará que ele próprio não mais disponibilize a informação entregue para conversão em *hash*.

Haverá, nesse ponto, controle integral da informação pelo titular do dado, em pleno atendimento aos objetivos delineados na Lei Geral de Proteção de Dados.

6. Considerações finais

Conquanto blockchain seja uma ferramenta de inegável potencial para o exercício da liberdade de expressão (TAPSCOTT; TAPSCOTT, 2018, p. 245), tecnologias são meios, não fins em si mesmas, e seu uso deve ser avaliado de forma crítica e ponderada.

Ademais, para além de um óbice à incidência da LGPD, blockchains poderão se tornar forma de resguardar a privacidade do titular dos dados.

Nesse sentido, Mougayar:

> *Veja o blockchain e as aplicações descentralizadas baseadas nele. Seu advento traz possíveis soluções para a segurança de dados porque a criptografia se torna uma parte padrão de aplicações blockchain, especialmente as que pertencem às partes de dados. Por padrão, tudo é criptografado. Pelo mérito de descentralizar a arquitetura dos elementos da informação, cada usuário pode ser proprietário de seus dados privados, e repositórios centrais são menos vulneráveis a perdas de dados ou violações, porque eles apenas armazenam informações criptografadas e apontadores codificados para locais de armazenamento distribuídos que estão espalhados por redes de computadores também distribuídas. Assim, hackers não conseguem reconstruir ou entender quaisquer informações parciais que podem ter em mãos. Pelo menos, essa é a teoria por trás dessa visão, e há trabalho a ser realizado para trazer isso para a realidade (2017, p. 53).*

A sociedade da informação fomentou modelos de negócios construídos sobre a captação irrestrita de dados dos particulares e um estado de monitoramento permanente.

Tal situação nutriu um terreno fértil para abusos que, conforme vêm à tona, causam notória situação de desconforto naqueles que percebem a violação de sua privacidade. Em contrapartida, daí emergem instrumentos jurídicos e tecnológicas hábeis a limitar tais condutas e a permitir o exercício racional de direitos por todos os envolvidos.

Diante do exposto, percebe-se que, após análise acurada da natureza da blockchain e das informações nela envolvidas, não há óbices ao seu uso de forma plenamente compatível com a Lei Geral de Proteção de Dados, ao menos quanto aos direitos de apagamento e correção de dados.

Com pouca reflexão, qualquer meio, até mesmo um pedaço de papel, pode afrontar os termos da LGPD.

7. Referências bibliográficas

ALTER, Adam. *Irresistible*: the rise of addictive technology and the business of keeping us hooked. Nova Iorque: Penguin Books, 2018. *E-book*.

ANTONOPOULOS, Andreas. *Mastering bitcoin*: programming the open blockchain. 2. ed. California: O'Reilly, 2017.

BASHIR, Imran. *Mastering Blockchain*. 2. ed., Birmingham: Packt, 2018. *E-book*.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018. *E-book*.

BLOCO gênese do Bitcoin. Disponível em: https://bit.ly/2R68Kqi. Acesso em: 7 ago. 2019.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://bit.ly/2Tx6Ro4. Acesso em: 7 ago. 2019.

BRASIL. *Lei nº 13.853, de 8 de julho de 2019*. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, DF: Presidência da República, 2019. Disponível em: https://bit.ly/365Hc8s. Acesso em: 7 ago. 2019.

CAMPBELL-VERDUYN, Malcolm (ed.). *Bitcoin and beyond*: cryptocurrencies, blockchain and global governance. Nova Iorque: Routledge, 2018. *E-book*.

CASEY, Michael J.; VIGNA, Paul. *The truth machine*: the blockchain and the future of everything. New York: St. Martin's Press, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei geral de proteção de dados pessoais comentada*. São Paulo: Revista dos Tribunais, 2019.

DAVIS, Alison; LE MERLE, Matthew C. *Blockchain competitive advantage*. Tiburon: Fifth Era Media, 2019. *E-book*.

EHA, Brian Patrick. *How money got free*. Londres: Oneworld Book, 2017.

ETWARU, Richie. *Blockchain trust companies*: "Every company is at risk of being disrupted by a trusted version of itself". Indianapolis: Dog Ear Publishing, 2017.

FILIPPI, Primavera de; WRIGHT, Aaron. *Blockchain and the law*: the rule of code. Massachussets: Harvard University Press, 2018. *E-book*.FUNÇÃO Hash. *In*: WIKIPEDIA:

the free encyclopedia. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: https://bit.ly/3al5YEW. Acesso em: 16 ago. 2019.

JUN, Myungsan. *Blockchain government*: a next form of infrastructure for the twenty-first century. Scotts Valley: CreateSpace, 2018. *E-book*.

KRAMER, Adam D. I.; GUILLORY, Jamie E.; HANCOCK, Jeffrey T. Experimental evidence of massive scale emotional contagion through social networks. *In:* PNAS, 2014, [*s. l.*]. *Proceedings* […]. [*s. l.*]: National Academy of Sciences of the United States of America, 2014. p. 1-5. Disponível em: https://bit.ly/30vwUgR. Acesso em: 6 ago. 2019.

KRAVCHENKO, Pavel; SKRIABIN, Bohdan; DUBININA, Oksana. *Blockchain and decentralized systems*. v. 1. Kharkiv: Distributed Lab, 2018. *E-book*.

LAURENCE, Tiana. *Blockchain for dummies*. Hoboken: John Wiley & Sons, 2017.

MALEKAN, Omid. *The story of blockchain*: a begginer's guide to the technology that nobody understands. New York: Triple Smoke Stack, 2018. *E-book*. METADADOS. *In*: WIKIPEDIA: the free encyclopedia. [São Francisco, CA: Wikimedia Foundation, [s. d.]. Disponível em: https://bit.ly/3asqLGR. Acesso em: 25 ago. 2019.

MOUGAYAR, William. *Blockchain para negócios*: promessa, prática e aplicação da nova tecnologia da internet. Rio de Janeiro: Alta books, 2017.

NAKAMOTO, Satoshi. *Bitcoin*: a peer-to-peer electronic cash system. [*S. l.*: *s. n.*], 2008. Disponível em: https://bit.ly/374U53Z. Acesso em: 7 ago. 2019.

NORMAN, Allan T. *Blockchain technology explained*: the ultimate beginner's guide about blockchain wallet, mining, bitcoin, ethereum, litecoin, zcash, monero, ripple, dash, IOTA and smart contracts. Scotts Valley: CreateSpace, 2017.

OSMAN, Maddy. *Estatísticas e fatos surpreendentes do Youtube* (2º Site mais visitado). Kinsta, [*s. l.*], 20 jun. 2019. Disponível em: https://bit.ly/38eMWOM. Acesso em: 6 ago. 2019.

SWAN, Melanie. *Blockchain*: blueprint for a new economy. California: O'Reilly, 2015.

TALBOT, Michael. *A brief description of blockchain*: why it matters in the real world. [*S. l.*]: Veracity Tech Academy, 2018. *E-book*.

TAPSCOTT, Don; TAPSCOTT, Alex. *Blockchain Revolution*: how the technology behind bitcoins is changing money, business, and the world. 2. ed. Toronto: Penguin Canada, 2018.

UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, Estrasburgo, 4 maio 2016. Disponível em: https://bit.ly/2NDhNwJ. Acesso em: 19 ago. 2019.

WERBACH, Kevin. *The blockchain and the new architecture of trust*. Cambridge: MIT Press, 2018. *E-book*.

ZARAMELA, Luciana. *Apague definitivamente os dados de seu disco rígido*. Canaltech, [*s. l.*], [20--?]. Disponível em: https://bit.ly/2TI697q. Acesso em: 20 ago. 2019.

A responsabilidade civil na Lei Geral de Proteção de Dados

Walter Aranha Capanema[1]
Advogado e professor

Sumário: Introdução. 1. A responsabilidade civil na LGPD. 2. Exclusão da responsabilidade civil. 2.1. Hipóteses de exclusão. 2.2. Vulnerabilidades e *0 days*. 3. Critérios para a definição do *quantum* indenizatório. 4. Exemplos pontuais de responsabilidade civil na LGPD. 4.2. O não-atendimento dos direitos do titular. 4.3. O *spam* e o tratamento ilegal. Conclusão. Bibliografia.

Resumo: Este artigo pretende traçar um panorama sobre as normas relativas à proteção de dados na Lei 13.709/2018 (Lei Geral de Proteção de Dados – LGDP), buscando, também, sugerir formas de aplicação.

Palavras-chave: Responsabilidade Civil. Proteção de Dados. Dados Pessoais. Privacidade. Intimidade. LGPD.

Introdução

O legislador brasileiro, com o seu costumeiro atraso em acompanhar os avanços da sociedade e da tecnologia, somente em 2018 se preocupou em regular com efetividade a proteção de dados pessoais, o que ocorreu com a edição da Lei 13.709/2018, a denominada Lei Geral de Proteção de Dados (LGPD).

É verdade que já existiam outras leis que tratavam, de alguma forma, sobre o tema, como o Código de Defesa do Consumidor, o Marco Civil da Internet (Lei 12.965/2014), a Lei de Acesso à Informação (Lei 12.527/2011), a Lei do Cadastro Positivo (Lei 12.414/2011), dentre outras.

A LGPD coloca o indivíduo (a quem denomina de "titular"[2]), como protagonista das relações jurídicas que envolvam o tratamento de dados[3], não só porque regula a proteção de dados **pessoais**, mas, principalmente, elege como fundamento em seu

[1] Coordenador da Pós-Graduação em Direito Digital do Instituto de Ensino e Pesquisa do Ministério Público do Estado do Rio de Janeiro (IEP-MPRJ). Coordenador do Curso de Extensão em Direito Eletrônico da Escola da Magistratura do Estado do Rio de Janeiro (EMERJ). Coordenador de Prerrogativas de Processo Eletrônico e Inteligência Artificial da OAB-RJ. Membro da Comissão de Proteção de Dados da OAB-RJ. Diretor de Inovação e Ensino da Smart3. Professor Convidado da Escola Paulista da Magistratura, da Escola Superior da Advocacia do Rio de Janeiro, da Escola Judiciária Eleitoral do Tribunal Superior Eleitoral, da Escola da Magistratura da Regional Federal da 2ª Região e da Fundação Getúlio Vargas.

[2] Art. 5º: "V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento".

[3] Art. 5º: "X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

art. 2º, II, a **"autodeterminação informativa"**, que consiste no direito de escolher quais dados serão usados, bem como os limites e o prazo dessa utilização[4].

A autodeterminação, portanto, é garantida pela previsão de vários direitos no Capítulo III, especialmente no art. 18, como o de informação (I), de acesso (II), de correção (III), de portabilidade (V), de eliminação (VI), dentre outros.

Por sua vez, esses direitos correspondem a um rol de deveres voltados a quem exerce a atividade de tratamento de dados. A LGPD diferencia esses deveres conforme a relação destes com o tratamento, denominando aquele que exerce a decisão sobre o tratamento de **controlador**[5], enquanto aquele que executa o tratamento, sob as ordens do controlador, de **operador**[6]. Juntos, eles são os **"agentes de tratamento"**[7].

Sob uma visão civilista, o controlador seria o **mandante**, e o operador, o **mandatário**. Talvez possa se aventar a hipótese de que a relação controlador-operador constitua modalidade especial de mandato, própria das relações que envolvam tratamento de dados pessoais.

Há ainda nessa relação jurídica um outro ator: o encarregado[8], pessoa natural ou jurídica, integrante ou não dos quadros do controlador ou do operador, que exerça, dentre outras funções, a intermediação entre os demais atores, especialmente a Autoridade Nacional de Proteção de Dados (ANPD) e, ainda, orienta a aplicação das normas de proteção de dados[9].

Essa complexa relação de múltiplos atores e deveres aqui relatada em resumo evidencia o desafio que as empresas privadas e órgãos públicos encontrarão para estar em conformidade com a LGPD. Os efeitos do não-atendimento passam não só pelas sanções administrativas que podem ser eventualmente impostas pela ANPD, mas em maior escala, por ações de responsabilidade civil.

A questão da responsabilidade civil, por estar relacionada necessariamente a ações judiciais, é talvez o aspecto da LGPD que mais interessa ao Poder Judiciário e, portanto, será analisada neste artigo.

1. A responsabilidade civil na LGPD

A responsabilidade civil está regulamentada na Seção III do Capítulo VI da LGPD, intitulada de "Da Responsabilidade e do Ressarcimento de Danos". É importante ressaltar que tais normas não serão aplicáveis em todos os casos envolvendo responsabilidade civil, podendo, dependendo da relação jurídica, ceder espaço a normas específicas, como o

[4] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 196.

[5] Art. 5º: "VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

[6] Art. 5º: "VII – operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

[7] Art. 5º: "IX – agentes de tratamento: o controlador e o operador. Numa aparente contradição, as normas relativas ao encarregado estão na Seção II do Capítulo VI, intitulado 'Dos Agentes de tratamento de dados pessoais'".

[8] Art. 5º: "VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)".

[9] Art. 41: "§ 2º As atividades do encarregado consistem em: [...] III – orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais".

Código de Defesa do Consumidor, o que, inclusive, é expressamente reconhecido pela LGPD em seu art. 45[10].

A responsabilidade surge do exercício da atividade de proteção de dados que viole a **"legislação de proteção de dados"**. Por essa expressão, o legislador reconhece que a proteção de dados é um microssistema, com normas previstas em diversas leis, sendo a LGPD a sua base estrutural. Deve-se aqui fazer uma analogia com o conceito de "legislação tributária" do art. 96 do CTN[11], para incluir não apenas as leis que versem sobre a proteção de dados, mas as normas administrativas regulamentares que serão expedidas pela Autoridade Nacional de Proteção de Dados ou por outras entidades[12].

Mas a responsabilidade civil na LGPD não surge apenas da violação do microssistema jurídico de proteção de dados. É preciso interpretar o art. 42, *caput* em conjunto com o art. 44, parágrafo único, que assim dispõe:

> *Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.*

O art. 46, por sua vez, estabelece que os agentes de tratamento deverão adotar medidas de segurança, técnicas e administrativas visando a proteção de dados pessoais[13]. Tais normas podem ser editadas, inclusive, pela ANPD[14].

Pela complexidade da atividade de segurança da informação, devem ser consideradas apenas aquelas medidas previstas em padrões devidamente reconhecidos, como as denominadas normas ISO[15].

Dessa forma, é possível identificar duas situações de responsabilidade civil na LGPD:

a) violação de normas **jurídicas**, do microssistema de proteção de dados;
b) violação de normas **técnicas**, voltadas à segurança e proteção de dados pessoais.

E, evidentemente, só caracterizará a responsabilidade civil, se a violação de norma jurídica ou técnica ocasionar dano material ou moral a um titular ou a uma coletividade.

---

[10] "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente".

[11] "Art. 96. A expressão "legislação tributária" compreende as leis, os tratados e as convenções internacionais, os decretos e as normas complementares que versem, no todo ou em parte, sobre tributos e relações jurídicas a eles pertinentes".

[12] BANCO CENTRAL DO BRASIL. *Resolução nº 4.658, de 26 de abril de 2018*. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://bit.ly/369JHql. Acesso em: 27 set. 2019.

[13] "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

[14] Art. 46: "§ 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei".

[15] ISO é o acrônimo de International Organization for Standardization, uma entidade internacional que estabelece normas e padrões. O padrão ISO 27001, por exemplo, é destinado à segurança da Informação. Seu sítio está disponível em: https://bit.ly/2G75cO2. Acesso em: 21 jan. 2020.

O art. 42 restringe a responsabilidade civil ao controlador **ou** ao operador. A presença da conjunção alternativa "ou" estabelece a alternância entre um (controlador) ou o outro (operador). Obviamente, se a relação jurídica do titular com o controlador e o operador for de natureza consumerista, serão aplicadas as normas de responsabilidade solidária dos arts. 12 e 18 do CDC.

O § 1º excepciona a regra de alternância do *caput*, permitindo a solidariedade em dois casos específicos, com vistas a "assegurar a efetiva indenização ao titular dos dados".

No inciso I, o operador responderá solidariamente em duas situações: caso descumpra a legislação de proteção de dados ou se não seguir "as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador". É muito semelhante, nesse caso, na situação do mandatário que descumpre as instruções do mandante, conforme o art. 679, CC[16].

Já no inciso II, ocorrerá a solidariedade entre "os controladores que estiverem diretamente envolvidos no tratamento", ou seja, aqueles que estabelecerem, em conjunto, decisões que violem o microssistema da proteção de dados ou às normas técnicas cabíveis.

Tais hipóteses de solidariedade estarão afastadas caso presentes as hipóteses de exclusão de responsabilidade, previstas no art. 43.

A LGPD não fala na responsabilidade civil do encarregado, contudo ela poderá surgir, por exemplo, quando essa função for exercida por uma pessoa natural ou jurídica destacada do controlador e do operador em uma relação consumerista. Por se estar diante de alguém que está na cadeia de produção, poderá ser responsabilizado de forma solidária pelo dano causado.

O § 2º admite a inversão do ônus da prova, a critério do juiz, a favor do titular de dados, desde que verossímil a alegação, haja hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular for excessivamente onerosa. Há normas sobre a redistribuição/inversão do ônus da prova em outras leis: uma muito semelhante no art. 373, § 1º do CPC[17] e outra no art. 6º, VIII do CDC[18], aplicável nas ações de natureza consumerista, exigindo menos requisitos.

Além da inversão do ônus probatório, o reconhecimento da hipossuficiência do titular também se verifica no fato de que a responsabilidade civil da LGPD ser da modalidade objetiva, onde não há discussão sobre a culpa do agente.

[16] Art. 679: "Ainda que o mandatário contrarie as instruções do mandante, se não exceder os limites do mandato, ficará o mandante obrigado para com aqueles com quem o seu procurador contratou; mas terá contra este ação pelas perdas e danos resultantes da inobservância das instruções".

[17] Art. 373: "§ 1º Nos casos previstos em lei ou diante de peculiaridades da causa relacionadas à impossibilidade ou à excessiva dificuldade de cumprir o encargo nos termos do caput ou à maior facilidade de obtenção da prova do fato contrário, poderá o juiz atribuir o ônus da prova de modo diverso, desde que o faça por decisão fundamentada, caso em que deverá dar à parte a oportunidade de se desincumbir do ônus que lhe foi atribuído".

[18] Art. 6º: "VIII – a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências".

2. Exclusão da responsabilidade civil

2.1. Hipóteses de exclusão

As hipóteses de exclusão da responsabilidade civil estão previstas no art. 43 da LGPD.

O inciso I trata da situação em que o agente não realizou o tratamento de dados a que lhe foi atribuído. Ou seja, houve um tratamento de dados, mas o réu não tem qualquer vínculo com ele. Aproxima-se muito da figura da ilegitimidade passiva, que a LGPD trata como matéria de mérito.

Já o inciso II exclui a responsabilidade na situação em que o agente realizou o tratamento, mas "não houve violação à legislação de proteção de dados". Aqui, o dano ocorreu por um ato lícito.

Seria o caso, por exemplo, de uma decisão automatizada, baseada em critérios transparentes, informados (presentes em termos de uso) e sem viés, que negue um empréstimo a um possível consumidor. O presente inciso prevê expressamente apenas a situação em que não houve violação à proteção de dados. Deve-se interpretar este artigo em conjunto com os arts. 42, 44, 46 e parágrafo único, conforme as razões já apresentadas, de modo a admitir, também a alegação de ausência de violação de **norma técnica**.

A alegação de culpa exclusiva do titular ou de terceiro está prevista no inciso III do art. 43. Serão os casos em que o dano for causado por exclusiva ingerência do titular, por terceiro, ou por uma atuação conjunta do titular com o terceiro.

Mas, ainda assim, caberão alguns questionamentos.

Imagine a situação em que houve a invasão da conta de e-mail de um usuário, com a destruição de todas as suas mensagens. Tal fato só ocorreu porque a senha utilizada pelo titular era fraca, com apenas quatro caracteres, e foi facilmente descoberta. Poder-se-ia aqui falar em culpa exclusiva do titular? Caberia aos agentes de tratamento verificar a segurança da senha criada pelo usuário e impedir o uso daquelas que fossem frágeis? Existe norma técnica estabelecendo essa obrigação?

2.2. Vulnerabilidades e *0-day*

Vale a pena trazer para a discussão um tema relacionado à segurança da informação e que certamente repercutirá na aplicação da lei: a vulnerabilidade, um conceito da tecnologia, entendido como a "condição que, quando explorada por um atacante, pode resultar em uma violação de segurança"[19].

As vulnerabilidades, quando eventualmente descobertas, são documentadas e catalogadas em sites como o *Common Vulnerabilities and Exposures* – CVE[20], permitindo que os responsáveis pela segurança da informação das empresas e órgãos públicos adotem medidas técnicas para prevenir tais incidentes.

[19] HOEPERS, Cristine; STEDING-JESSEN, Klaus. *Fundamentos de Segurança da Informação*. [*S. l.*]: Escola de Governança da Internet no Brasil. Disponível em: https://bit.ly/2unOasd. Acesso em: 27 set. 2019.

[20] Disponível em: https://bit.ly/30KTguP. Acesso em: 21 jan. 2020.

Dessa forma, se houve um dano a dados pessoais decorrentes do não-atendimento de uma norma técnica, relativa a uma vulnerabilidade já conhecida e documentada, fica, assim, evidenciada a negligência do agente de tratamento.

Contudo, é possível que o dano seja causado pelo emprego das chamadas "vulnerabilidades não-documentadas", também conhecidas como *0-day*[21]. Nesse caso, seria incabível a responsabilização civil, afinal, se não se sabe ainda da sua existência, não tem como exigir o dever de segurança.

Logo, não é possível se atribuir aos agentes de tratamento o dever de segurança/proteção dos dados pessoais em toda e qualquer hipótese, mas apenas no estado da arte/técnica existente à época.

E, mais, deve-se entender que a obrigação de segurança é de meio, e não de resultado. É impossível ao agente de tratamento garantir, com 100% de certeza, que os dados dos titulares estarão seguros contra qualquer incidente. É preciso, portanto, razoabilidade.

3. Critérios para a definição do *quantum* indenizatório

O art. 944 do Código Civil dispõe que "A indenização mede-se pela extensão do dano". E a extensão de um dano relativo à proteção de dados poderá levar em consideração os seguintes critérios:

a) a quantidade de dados pessoais afetados;
b) a natureza dos dados pessoais afetados: o vazamento de dados pessoais sensíveis[22], por exemplo, determinará uma indenização maior, especialmente se se tratar de dados biométricos, que não podem ser substituídos;
c) a reincidência da conduta;
d) a omissão em tomar medidas de segurança e técnicas para minorar o dano ou em colaborar com a Autoridade Nacional de Proteção de Dados;
e) a ausência de notificação dos usuários da ocorrência do incidente[23];
f) a comprovada utilização dos dados pessoais vazados de titulares por terceiros.

4. Exemplos pontuais de responsabilidade civil na LGPD

Embora a LGPD ainda não esteja em vigor, é possível pensar em alguns exemplos de responsabilidade civil.

[21] "A zero-day vulnerability is a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw. It has the potential to be exploited by cybercriminals". ZERO-DAY vulnerability: what it is, and how it works. *Norton*, [*s. l.*], [s. d.]. Disponível em: https://nr.tn/2G7038G. Acesso em: 27 set. 2019.

[22] Art. 5º: "II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

[23] "Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".

4.1. Vazamentos/*data leaks*

Um dos maiores pesadelos da modernidade consiste no vazamento de dados, normalmente por falhas de segurança. São relatados, todos os dias, diversos casos, desde abrangendo dados bancários[24], *logins* e senhas do Netflix[25], redes sociais[26] e biométricos[27].

O dano poderá ser potencializado com o posterior uso dos dados pessoais por criminosos, para a criação de identidades falsas, exploração de *logins* e acesso aos dados das vítimas.

4.2. O não-atendimento dos direitos do titular

O Capítulo III, como já foi dito, estabelece um rol de direitos para o titular. O não-atendimento a esses direitos poderá ensejar, a princípio, a configuração de um dano moral, sendo possível, inclusive, cumulá-lo com um dano patrimonial, caso a impossibilidade de exercício do direito tenha trazido lucro cessante ou dano emergente.

4.3. O *spam* e o tratamento ilegal

O spam, entendido como o envio de publicidade ou propaganda eletrônica não autorizada, não era expressamente vedado pela legislação. O Superior Tribunal de Justiça, em precedente de 2009, entendeu que não se constitui ilícito, "por ausência de previsão legal", e que há métodos de evitá-lo[28].

---

[24] TOZZATO, Luiza. Vazam quase 250 GB de dados bancários: saiba como se proteger. *Olhar Digital*, [*s. l.*], 22 jul. 2019, 18:20. Disponível em: https://bit.ly/37dCruV. Acesso em: 27 set. 2019.

[25] VAZAMENTO de senhas do Netflix: saiba o que fazer para se proteger. *O Globo*, [*s. l.*], 12 dez. 2017, 07:42. Disponível em: https://glo.bo/38sSw0c. Acesso em: 27 set. 2019. dez.

[26] POZZEBOM, Rafaela. Arquivo com 2,2 bilhões de logins e senhas vaza na internet. *Oficina da Net*, [*s. l.*], 5 fev. 2019. Disponível em: https://bit.ly/2NlmBRm. Acesso em: 27 set. 2019.

[27] LIMA, Bruna. *Falha de segurança expõe dados biométricos de 1 milhão de pessoas*. Olhar Digital, [*s. l.*], [s. d.]. Disponível em: https://bit.ly/2NND8nf. Acesso em: 27 set. 2019.

[28] "Trata-se de ação de obrigação de fazer cumulada com pedido de indenização por danos morais em que o autor alega receber e-mails (spam com mulheres de biquíni) de restaurante que tem show de streaptease e, mesmo tendo solicitado, por duas vezes, que seu endereço eletrônico fosse retirado da lista de e-mail do réu (recorrido), eles continuaram a ser enviados. Entre os usuários de internet, é denominada spam ou spammers mensagem eletrônica comercial com propaganda não solicitada de fornecedor de produto ou serviço. A sentença julgou procedente o pedido e deferiu tutela antecipada para que o restaurante se abstivesse do envio da propaganda comercial sob pena de multa diária, condenando-o a pagar, a título de danos morais, o valor de R$ 5 mil corrigidos pelo IPC a partir da data do julgamento, acrescidos de juros de mora, contados a partir do evento lesivo. Entretanto, o TJ proveu apelação do estabelecimento e reformou a sentença, considerando que o simples envio de e-mails não solicitados, ainda que dotados de conotação comercial, não configuraria propaganda enganosa ou abusiva para incidir o CDC e não haveria dano moral a ressarcir, porquanto não demonstrada a violação da intimidade, da vida privada, da honra e da imagem. Para o Min. Relator, que ficou vencido, o envio de mensagens com propaganda, quando não autorizada expressamente pelo consumidor, constitui atividade nociva que pode, além de outras consequências, gerar um colapso no próprio sistema de internet, tendo em vista um grande número de informações transmitidas na rede, além de que o spam teria um custo elevado para sociedade. Observou que não há legislação específica para o caso de abusos, embora existam projetos de lei em tramitação no Congresso. Daí se aplicar por analogia o CDC. Após várias reflexões sobre o tema, reconheceu a ocorrência do dano e a obrigação de o restaurante retirar o autor de sua lista de envio de propaganda, e a invasão à privacidade do autor, por isso restabeleceu a sentença. Para a tese vencedora, inaugurada pelo Min. Honildo de Mello Castro, não há o dever de indenizar, porque existem meios de o remetente bloquear o spam indesejado, aliados às ferramentas disponibilizadas pelos serviços de e-mail da internet e softwares específicos, assim manteve a decisão do Tribunal *a quo*. Diante do exposto, a Turma por maioria não conheceu do recurso" Resp. 844.736-DF, Rel. originário Min. Luis Felipe Salomão, Rel. para acórdão Min. Honildo Amaral de Mello Castro (Desembargador convocado do TJ-AP), julgado em 27/10/2009.

Com a vigência da LGPD, tal entendimento necessitará ser revisto.

O envio de mensagem, portanto, constitui hipótese de tratamento de dados, pois precisa de dados pessoais para ser efetivado (normalmente, endereço de e-mail ou número telefônico, no caso do WhatsApp).

E, assim, necessitará do consentimento do titular-destinatário, ou alguma outra base legal.

Logo, o tratamento de dados pessoais sem o consentimento do titular ou fora das previsões legais poderá configurar dano moral.

Conclusão

É fundamental que os operadores do Direito conheçam as regras da LGPD. A complexidade dessas normas é um desafio, mas é necessária a sua compreensão da parte do titular, para defender seus direitos em juízo e, por parte dos agentes, para a prevenção e minimização dos riscos de eventuais ações judiciais.

É preciso, portanto, conjugar a adequação à lei com uma mudança de cultura nas empresas e órgãos públicos. Os titulares e os seus dados merecem respeito.

Bibliografia

BANCO CENTRAL DO BRASIL. *Resolução nº 4.658, de 26 de abril de 2018*. Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. Disponível em: https://bit.ly/369JHql. Acesso em: 27 set. 2019.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

HOEPERS, Cristine; STEDING-JESSEN, Klaus. *Fundamentos de Segurança da Informação*. [*S. l.*]: Escola de Governança da Internet no Brasil. Disponível em: https://bit.ly/2unOasd. Acesso em: 27 set. 2019.

LIMA, Bruna. *Falha de segurança expõe dados biométricos de 1 milhão de pessoas*. Olhar Digital, [*s. l.*], [s. d.]. Disponível em: https://bit.ly/2NND8nf. Acesso em: 27 set. 2019.

ZERO-DAY vulnerability: what it is, and how it works. *Norton*, [*s. l.*], [s. d.]. Disponível em: https://nr.tn/2G7038G. Acesso em: 27 set. 2019.

VAZAMENTO de senhas do Netflix: saiba o que fazer para se proteger. *O Globo*, [*s. l.*], 12 dez. 2017, 07:42. Disponível em: https://glo.bo/38sSw0c. Acesso em: 27 set. 2019. dez.

POZZEBOM, Rafaela. Arquivo com 2,2 bilhões de logins e senhas vaza na internet. *Oficina da Net*, [*s. l.*], 5 fev. 2019. Disponível em: https://bit.ly/2NImBRm. Acesso em: 27 set. 2019.

TOZZATO, Luiza. Vazam quase 250 GB de dados bancários: saiba como se proteger. *Olhar Digital*, [*s. l.*], 22 jul. 2019, 18:20. Disponível em: https://bit.ly/37dCruV. Acesso em: 27 set. 2019.

Lei Geral de Proteção de Dados no setor público: transparência e fortalecimento do Estado Democrático de Direito

Renato Opice Blum[1]
Advogado

Nuria López[2]
Advogada

Sumário: 1. A construção normativa da proteção de dados no setor público; 2. A nova Lei Geral de Proteção de Dados; 3. Bases legais para o tratamento de dados pessoais; 4. Transparência e fortalecimento das relações democráticas; 5. Novos direitos; 6. Indicação de encarregado pelo tratamento de dados pessoais e outras obrigações; 7. Sanções; Conclusão; Referências.

Resumo: Trata-se da necessária análise dogmática da aplicação ao setor público da nova Lei Geral de Proteção de Dados dentro do contexto de desenvolvimento democrático. A partir da matriz de responsabilidade constitucional, pôde-se traçar uma trajetória crescente de transparência positiva do Poder Público em relação aos dados dos cidadãos, notadamente com a Lei do *Habeas Data* e a Lei de Acesso à Informação. As prestações decorrentes da Lei Geral de Proteção de Dados analisadas somam-se àquelas que as precedem, em uma perspectiva de fortalecimento cada vez maior das relações democráticas de Direito.

Palavras-chave: Lei Geral de Proteção de Dados. Setor Público. Lei de Acesso à Informação.

1. A construção normativa da proteção de dados no setor público

Há um ano da vigência da Lei Geral de Proteção de Dados, a iniciativa privada está tomada por projetos de adequação, palestras, cursos e ferramentas de segurança. Nem poderia ser diferente. No Brasil, apesar de termos trazido nossa matriz normativa do Regulamento Geral sobre Proteção de Dados europeu, desenvolvemos o conteúdo semântico de proteção de dados atrelado fortemente ao direito do consumidor. Muitos dos direitos dos titulares de dados, previstos no artigo 18, Lei Geral de Proteção de Dados, já estavam contidos no Código de Defesa do Consumidor; o nosso precedente explícito sobre acesso

[1] Mestre pela Florida Christian University; Advogado; Economista; Professor coordenador dos cursos de Proteção de Dados e Direito Digital do Insper e do curso Direito 4.0 da Faap; Juiz do Inclusive Innovation Challenge do MIT (Massachusetts Institute of Technology); Presidente da Associação Brasileira de Proteção de Dados (ABPDados); Diretor da Technology Law Association. @renatoopicelum

[2] Doutora em Teoria e Filosofia do Direito pela PUC-SP. Advogada em Direito Digital e DPO no Opice Blum, Bruno, Abrusio, Vainzof Advogados Associados. Professora convidada no Insper, Faap e FGV.

a dados em decisão automatizada é também nessa seara, no caso do *score* de crédito; e todos os casos levantados pelo Ministério Público (alguns, inclusive, judicializados) até o momento referem-se ao direito do consumidor. De fato, trata-se de um viés presente em todo o continente, desde o California Consumer Privacy Act (CCPA) nos Estados Unidos até o serviço No Llame, na Argentina.

O volume do esperado debate na iniciativa privada abafa uma narrativa mais discreta, mas crucial: o desenvolvimento da proteção de dados no Poder Público. Para os europeus, em particular os alemães, trata-se da principal linha de desenvolvimento da proteção de dados. Desde a Lei de Proteção de Dados de Hesse (*Hessisches Datenschutzgesetz*) em 1970, e de forma muito incipiente, o intuito era evitar quaisquer excessos no uso de dados pessoais pelo Poder Público. As leis que vieram posteriormente delimitariam, cada vez mais, um espaço de liberdade individual. É o fundamento da *autodeterminação informativa ou informacional*, que chegou à nossa Lei Geral de Proteção de Dados (art. 2º, II), vinda de um conhecido julgado da Corte Constitucional alemã[3], que garante a extensão do direito geral de personalidade aos dados pessoais, para que o indivíduo possa se determinar sobre eles. A Diretiva 95/46/EC, que antecedeu o Regulamento Geral (GDPR), no mesmo sentido, estabelecia como objetivo "a proteção das liberdades e dos direitos fundamentais das pessoas singulares, notadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais" (artigo 1º, 1). O Regulamento estabelece a relação explicitamente ao colocar que "defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais" (artigo 1º, 2).

A Europa deu, pouco a pouco, o salto de declarar o direito à privacidade como direito humano (artigo 12, Declaração Universal dos Direitos Humanos[4]), em 1948, para considerar a proteção dos dados pessoais a partir dos anos 1970. No Brasil, foi o recente período democrático a inaugurar a previsão legal de inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação (artigo 5º, X, Constituição). O salto para a proteção de dados ainda está por vir, na Proposta de Emenda à Constituição nº 17/2019, que "inclui a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar a matéria"[5]. Ensejada especialmente pelo pragmatismo de evitar a profusão de leis estaduais e municipais, que já estavam sendo aprovadas país afora, e concentrar a proteção de dados como tema da União, a proposta tem um significado mais profundo em termos de desenvolvimento democrático.

É também a redação constituinte que traz o *habeas data* para "assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público ou para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo" (artigo 5º, LXXII). A Lei viria apenas em 1997 (Lei do *Habeas Data* – Lei nº 9.507/1997), incluindo ainda a possibilidade de "anotação, nos assentamentos do interessado,

[3] Inteiro teor da decisão disponível em: https://bit.ly/36e9uO6. Acesso em: 20 jan. 2020.

[4] "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

[5] Disponível em: https://bit.ly/2G6BQiG. Acesso em: 20 jan. 2020.

de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável" (artigo 7º, III).

Os dados pessoais vêm, em 2011, protegidos, como exceção à transparência intrínseca às democracias, na Lei de Acesso à Informação (Lei nº 12.527/2011). Ela chega a definir "informação pessoal" nos mesmos termos que definimos hoje com a Lei Geral de Proteção de Dados, "dados pessoais", "aquela relacionada à pessoa natural identificada ou identificável" (artigo 4º, Lei de Acesso à Informação). Sem prejuízo de notarmos a distinção entre *dado* e a *informação* que dele pode ser extraída, é digno de nota a introdução normativa do conceito.

Há, além disso, a responsabilização do Poder Público, que retira sua validade da matriz estabelecida pelo artigo 37, 6º, Constituição. A Lei de Acesso à Informação replica a regra constitucional ao estabelecer que "os órgãos e entidades públicas respondem diretamente pelos danos causados em decorrência da divulgação não autorizada ou utilização indevida de informações sigilosas ou informações pessoais, cabendo a apuração de responsabilidade funcional nos casos de dolo ou culpa, assegurado o respectivo direito de regresso" (artigo 34, *caput*, Lei de Acesso à Informação).

Na Lei de Acesso à Informação incumbe ao Poder Público a proteção da informação pessoal, "observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso" (artigo 6º, III, Lei de Acesso à Informação). A proteção à informação pessoal garante acesso restrito a agentes públicos legalmente autorizados e à **pessoa a quem as informações se referirem**, independentemente da classificação de sigilo, sendo que terceiros poderão ter acesso autorizado pela lei ou em razão de consentimento expresso do titular dos dados (artigo 31, §1º, Lei de Acesso à Informação). O consentimento só é dispensado em caso de prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusiva para o tratamento médico; em caso de realização de estatísticas e pesquisas científicas de evidente interesse público ou geral previstos em lei, sendo vedada a identificação da pessoa titular das informações; de cumprimento de ordem judicial; de defesa de direitos humanos ou de proteção do interesse público e geral preponderante (artigo 31, §3º, Lei de Acesso à Informação).

Ela ainda caracteriza como condutas ilícitas divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido a informação sigilosa ou informação pessoal ou impor sigilo a informação para obter proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem (artigo 32, IV e V, Lei de Acesso à Informação).

2. A nova Lei Geral de Proteção de Dados

É nesse contexto que chega a nova Lei Geral de Proteção de Dados — como uma nova etapa da relação entre o Poder Público e o cidadão. Tanto que mesmo em casos de aparente não incidência da Lei, ela exige determinados requisitos (portanto, claro, incide). É o caso do artigo 4º, III, Lei Geral de Proteção de Dados, que estabelece que a Lei "não se aplica ao tratamento de dados pessoais realizado para fins exclusivos de: a) segurança pública; b) defesa nacional; c) segurança do Estado; ou d) atividades de investigação e repressão de infrações penais", para logo em seguida, em seu parágrafo terceiro, afirmar que a Autoridade Nacional emitirá opiniões técnicas ou recomendações sobre essas exceções e poderá solicitar relatório de impacto à proteção de dados pessoais (artigo 4º, §3º, Lei Geral de Proteção de Dados).

Apesar do paradoxo, a cautela é justificada. Trata-se de relatório descritivo das atividades de tratamento de dados pessoais que podem gerar risco às liberdades civis e aos direitos fundamentais, e das medidas, salvaguardas e mecanismos para mitigação de riscos (na definição legal do artigo 5º, XVII, Lei Geral de Proteção de Dados, e previsto no artigo 38, parágrafo único), importante para realizar uma ponderação sobre a utilização de dados pessoais, notadamente em casos de tecnologias de grande entropia, seus ganhos sociais e seus impactos nas liberdades individuais, com vistas a mitigá-los tanto quanto possível.

O que a Lei Geral de Proteção de Dados aponta ao determinar que "não se aplica" para essas finalidades, não é exatamente sua não incidência, senão incorreria nesse evidente paradoxo, mas sim que não se aplicam todas as suas disposições. Talvez a mais importante delas seja a não fundamentação dessas hipóteses de tratamento de dados em uma das bases legais previstas na Lei. Um dos principais pontos da Lei Geral de Proteção de Dados é a exigência de fundamentar cada atividade de tratamento de dados pessoais em uma base legal autorizadora do tratamento (nos termos do artigo 7º, *caput*, "o tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses").

3. Bases legais para o tratamento de dados pessoais

Para as demais hipóteses de atuação do Poder Público, um primeiro ponto é o de saber qual a base legal (fundamento de legalidade) para tratar dados pessoais. Se os artigos 6º, III, e 31, §1º, Lei de Acesso à Informação, estabelecem que, em regra, há necessidade de previsão legal ou consentimento do titular dos dados (a quem o dado se refere), a Lei Geral de Proteção de Dados acrescenta cores a essa disposição.

Evidentemente, em razão do princípio da legalidade (artigo 37, *caput*, Constituição), qualquer órgão do Poder Público acaba por sempre estar amparado em uma disposição legal em suas ações, incluindo a de tratar dados pessoais. O artigo 23, *caput*, Lei Geral de Proteção de Dados, afirma precisamente que todo tratamento de dados pessoais pelo Poder Público "deverá ser realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público". É dizer, sempre haverá, no caso do Poder Público, alguma norma legal que fundamente, em algum nível, o tratamento de dados pessoais. Todavia, isso não significa dizer que todo tratamento de dados pelo Poder Público será em *cumprimento de obrigação legal ou regulatória* (artigo 7º, II, Lei Geral de Proteção de Dados). A depender do caso, as demais bases legais poderão ser utilizadas também.

Por exemplo, o artigo 7º, III, Lei Geral de Proteção de Dados, criou uma base legal, não para todo Poder Público, mas especificamente para a Administração Pública, "para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres". Uma interpretação restritiva da expressão "Administração Pública" leva à compreensão de que apenas o Poder Executivo pode utilizar essa base legal. Contudo, há que se notar que a expressão "Administração Pública" tomada em sentido lato autoriza qualquer órgão do Poder Público na execução de políticas públicas a encontrar fundamento legal no artigo 7º, III, Lei Geral de Proteção de Dados. De certo, coaduna-se melhor com a complexidade do Poder Público que cada vez mais atua sob a ótica de suas funções públicas, independentemente de estar inserido no Executivo, Legislativo ou Judiciário.

Sem dúvidas, as demais hipóteses de bases legais são também possíveis para o Poder Público, em casos mais pontuais: a realização de estudos por órgãos de pesquisa, sendo estes sem fins lucrativos (artigo 7º, IV); contrato ou diligência contratual de que é parte um titular de dados pessoais (artigo 7º, V); exercício regular de direitos em processos judicial, administrativo ou arbitral (artigo 7º, VI); proteção da vida ou da incolumidade física de terceiros (artigo 7º, VII); tutela da saúde (artigo 7º, VIII); interesse legítimo do controlador ou de terceiro (artigo 7º, IX) ou mesmo proteção ao crédito (artigo 7º, X).

Na iniciativa privada, de acordo com levantamento realizado em agosto de 2019, 33% das atividades de tratamento de dados pessoais encontram fundamento no legítimo interesse, 32% em execução de contrato, 18% em cumprimento de obrigação legal ou regulatória e 8% no consentimento do titular[6]. Evidentemente, pode-se esperar que a distribuição de bases legais seja diferente no Poder Público, privilegiando, por exemplo, o cumprimento de obrigação legal ou regulatória e a execução de políticas públicas.

4. Transparência e fortalecimento das relações democráticas

Em quaisquer das bases legais utilizadas, é necessário observar: os princípios da proteção de dados (artigo 6º, Lei Geral de Proteção de Dados), como o de minimização dos dados, é dizer, tratar apenas os dados necessários e adequados para a finalidade pretendida; garantia de livre acesso aos titulares dos dados; a qualidade dos dados, isto é, a exatidão, clareza, relevância e atualização; transparência, garantia de informações claras sobre o tratamento, precisas e facilmente acessíveis; segurança e prevenção, que em matéria de dados devem ser lidos conjuntamente; não discriminação; e responsabilização e prestação de contas sobre as atividades. Nessa perspectiva, tem destaque o princípio da transparência para o titular dos dados, sem a qual não é possível que ele exerça a autodeterminação informativa. A GDPR, vale a menção, ainda coaduna a transparência com o princípio da lealdade com o titular de dados. A lealdade não veio expressamente para a Lei Geral de Proteção de Dados, mas representa bem o passo que a nossa lei dá no tratamento de dados pessoais.

No Poder Público, transparência ganha uma dimensão nova, de fortalecimento das relações democráticas com os cidadãos. Se em uma sociedade de informação, como a nossa, *saber é poder*, a transparência sobre os dados pessoais sobre os quais se sabe implica o compartilhamento do poder detido, haja vista que comprova pela clareza a legalidade de suas ações. Por essa razão, o artigo 23, I, Lei Geral de Proteção de Dados, estabelece critérios específicos de transparência para o Poder Público, que deve informar, preferencialmente em seus sítios eletrônicos, as hipóteses em que no exercício de suas competências tratam dados pessoais com informações claras sobre previsão legal, finalidade, procedimento e práticas adotadas. Há ainda a previsão de que a Autoridade Nacional de Proteção de Dados disponha mais detidamente sobre essa forma de publicidade (artigo 23, 1º).

5. Novos direitos

É na relação com o cidadão (titular dos dados) que se dá o desenvolvimento democrático. Se a Constituição previu o *habeas data*, para o acesso aos próprios dados pessoais, a Lei de

[6] Dados disponíveis em: https://www.portaldaprivacidade.com.br. Acesso em: 20 jan. 2020.

Acesso à Informação, anos mais tarde, tornou o caminho para esses dados institucional. Hoje, a Lei Geral de Proteção de Dados solidifica e amplia os direitos do cidadão, que vão muito além do mero acesso. O artigo 18 estabelece os direitos à confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade; portabilidade; eliminação dos dados pessoais; informação das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e revogação do consentimento.

A interpretação conjunta, indicando a evolução democrática aqui apontada, pode ser confirmada a partir da disposição do §3º, artigo 23, Lei Geral de Proteção de Dados, de que os prazos e procedimentos para o exercício desses direitos perante o Poder Público observarão a legislação específica, em especial à Lei do *Habeas Data*, a Lei Geral do Processo Administrativo e a Lei de Acesso à Informação. É dizer que a Lei Geral de Proteção de Dados adentra o ordenamento jurídico como um passo adiante na relação de transparência democrática com os cidadãos.

São, de fato, diversas as referências expressas da Lei Geral de Proteção de Dados a essas outras importantes leis que a precederam, apontando um acréscimo de *prestações positivas* aos cidadãos. Outro exemplo é a instituição de autoridades responsáveis pelo cumprimento das obrigações da Lei de Acesso à Informação, já realizadas pelos órgãos públicos, e a atual necessidade de indicação de um encarregado pelo tratamento de dados pessoais da Lei Geral de Proteção de Dados. Antes que houvesse confusão entre as referidas figuras e seus papéis, o artigo 23, §2º, Lei Geral de Proteção de Dados, faz a distinção e exige ambas as indicações.

6. Indicação de encarregado pelo tratamento de dados pessoais e outras obrigações

Aliás, a Lei é ainda mais rigorosa com o Poder Público. Em regra, a obrigatoriedade da indicação de um encarregado é apenas para os controladores de dados (artigo 41, Lei Geral de Proteção de Dados). Contudo, quando se tratar de Poder Público, mesmo que este esteja no papel de operador (artigo 39, Lei Geral de Proteção de Dados), haverá necessidade da indicação, nos termos do inciso II, artigo 23. Portanto, em quaisquer dos papéis de agente de tratamento de dados, o Poder Público deverá indicar seu encarregado. Como ponto de contato entre o órgão público e os cidadãos, titulares de dados, vê-se que haverá uma forte intersecção entre as autoridades da Lei de Acesso à Informação e da Lei de Proteção Geral de Dados. Ainda que tenham atuação conjunta para alguns pontos coincidentes, existirão como autoridades distintas, com focos e preocupações autônomas, que devem se fortalecer mutuamente.

Da mesma forma, existirão obrigações similares, como a de elaborar relatório anual de cumprimento dessas legislações. O relatório da Lei de Acesso à Informação, previsto no artigo 67, II, Decreto 7.724/2012, e o registro das operações de tratamento de dados pessoais, prevista no artigo 37, Lei Geral de Proteção de Dados, cumulado com o relatório de impacto à proteção de dados pessoais, ademais da hipótese já mencionada do artigo 4º, III, também nos casos de legítimo interesse e de tratamento de dados pessoais sensíveis; e com o monitoramento contínuo e avaliações periódicas da adequação, previstos no artigo 50, §2º, I, "h".

7. Sanções

Também no que concerne às sanções, a Lei Geral de Proteção de Dados é explícita ao somar com demais leis pertinentes. O parágrafo 3º do artigo 52, Lei Geral de Proteção de Dados, que fora vetado pelo Presidente da República e retornou ao ordenamento jurídico com a rejeição legislativa do referido veto, aplica ao Poder Público as sanções da lei (exceto as de multas simples ou diária), expressamente sem prejuízo das sanções do Estatuto do Servidor Público Federal, da Lei de Improbidade Administrativa e da Lei de Acesso à Informação. Dessa forma, é possível *a priori* que um mesmo incidente cumule as sanções dessas legislações específicas, dentro da matriz constitucional de responsabilidade do artigo 37, §6º.

Conclusão

Para qualquer agente de tratamento de dados pessoais, seja ele público ou privado, a proximidade da vigência da Lei Geral de Proteção de Dados representa a oportunidade de ingresso em um novo paradigma de proteção de dados. As exigências da adequação passam necessariamente pela reflexão sobre as atividades cotidianas nas quais se tratam os dados pessoais, a saber se eles são necessários e adequados às finalidades que atendem; e sobre a transparência e a segurança com a qual os tratamos.

Para o Poder Público, particularmente, essa oportunidade insere-se em um contexto macropolítico de relevância. A Lei Geral de Proteção de Dados surge no ordenamento jurídico brasileiro dentro da perspectiva de fortalecimento das relações democráticas com os cidadãos, construídas a partir da Constituição Federal, notadamente com a Lei do *Habeas Corpus* e a Lei do Acesso à Informação. Em uma sociedade de informação, saber é poder. A transparência sobre o tratamento dos dados pessoais sobre os quais se sabe implica necessariamente o compartilhamento do poder detido, pois comprova pela clareza a legalidade das ações realizadas pelo Poder Público. Nessa perspectiva, a Lei Geral de Proteção de Dados é um passo à frente em nossas relações democráticas.

Referências

BRASIL. *Projeto de Emenda Constitucional nº 17/2019*. Disponível em:https://bit.ly/2tArLYP. Acesso em: 20 jan. 2020.

[*Precedente sobre a autodeterminação informativa*]. Disponível em: https://bit.ly/37cJeFn. Acesso em: 20 jan. 2020.

O tratamento de dados de crianças e adolescentes no âmbito da Lei Geral de Proteção de Dados brasileira

Alessandra Borelli[1]
Advogada

Sumário: Introdução; 1. A especial proteção da criança e do adolescente; 2. LGPD e o tratamento de dados pessoais de crianças e adolescentes; 3. A responsabilidade além e em decorrência da LGPD; 4. Conclusão; 5. Referências.

Resumo: a exposição de crianças e adolescentes a sites, redes sociais, jogos on-line, entre outros tantos serviços oferecidos pelas novas tecnologias, é crescente. Na sociedade da informação, essa exposição tem o condão de captar dados pessoais, os quais, por um lado, podem expor a privacidade do seu titular, por outro, são capazes de gerar rentáveis negócios aos controladores. Ocorre que não se pode ignorar o poder de perpetuidade e de disseminação da internet, além da sua capacidade de comprometer fases importantes do desenvolvimento de uma criança ou adolescente com a exposição de seus dados pessoais. Apesar de serem habilidosos com as ferramentas tecnológicas, eles não dispõem de maturidade suficiente para compreender o valor de sua privacidade e, menos ainda, a melhor forma de protegê-la. Diante desta ampla e indiscutível preocupação, a Lei Geral de Proteção de Dados (LGPD) regulou a matéria, trazendo seção específica ao tratamento de dados pessoais de crianças e adolescentes, em suporte físico ou digital, cuidando-se de importante marco nacional em defesa dos direitos da criança e do adolescente, sobre o qual se debruça esse capítulo.

Palavras-chave: Lei Geral de Proteção de Dados. Criança e Adolescente. Dados Pessoais.

Introdução

As novas tecnologias da informação proporcionam uma fantástica globalização, permitindo o compartilhamento de momentos importantes com amigos e familiares independentemente da distância, permitindo amplo acesso à informação, dando voz

[1] Alessandra Borelli é advogada especialista em Direito Digital, pós-graduada em Direito Bancário e Mercado de Valores Mobiliários pela FGV/SP, com extensão em Direito Digital pela Escola Paulista de Magistratura, mãe de dois , uma com 10 e outro com 14 anos, diretora executiva da Nethics Educação Digital e da Opice Blum Academy, professora convidada dos cursos de Proteção de Dados e Direito Digital do Insper, membro efetivo da Comissão Permanente de Estudos de Tecnologia e Informação do IASP, colaboradora do *Manual de orientação da Sociedade Brasileira de Pediatria: saúde de crianças e adolescentes na era digital*, coautora do livro *Educação digital* (Editora RT, 2015), coordenadora e autora do *Manual de boas práticas para uso seguro das redes sociais*, da OAB/SP, autora da primeira *Coleção de educação para cidadania digital do Brasil* (Editora FTD, 2016), coautora do livro *Comentários ao GDPR – Regulamento Geral de Proteção de Dados da UE* (Editora RT, 2018), coautora dos livros *Lei Geral de Proteção de Dados comentada* e *Direito Digital: debates contemporâneos*, ambos da Editora RT (2019), e de diversos artigos e cartilhas relacionados ao tema. Palestrante no Brasil e exterior, tendo participado da Bett Show, do LearnIT – London/2019 e do International Society for Technology in Education (ISTE) – Philadelphia/2019.

às minorias, entre outras conquistas da sociedade conectada. Contudo, como adverte Jessica Baron, todas essas interações estão sendo datificadas, isto é, transformadas em dados computadorizados, situação que causa preocupação diante da iminência de uma geração datificada antes mesmo de nascer – com a exposição do pré-natal ou ainda em tenra idade, expondo-as a estranhos, que poderão usar seus dados contra elas[2].

Acontece que, como a revista londrina *The Economist* afirmou, "o recurso mais valioso do mundo já não é o petróleo, mas os dados"[3]. Nesse ínterim, o legislador brasileiro, atento às iniciativas globais e ao cenário nacional, publicou a Lei 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), que entrará em vigor em agosto/2020, trazendo seção específica para regular o tratamento de dados de crianças e adolescentes, em homenagem à Doutrina da Proteção Integral.

Cabe lembrar que por força da Constituição Federal, da Convenção da ONU sobre os Direitos das Crianças e do Estatuto da Criança e do Adolescente, a proteção do menor é dever de todos, especialmente do Estado, família e sociedade. Desta maneira, não só em razão da possibilidade das sanções previstas na LGPD (bastante significativas, diga-se), mas, especialmente, em razão do melhor interesse das crianças e adolescentes, pais, escolas, professores, governo e todos os que integram empresas que tratam dados pessoais devem ter em mente o seu papel fundamental nessa rede de proteção. A respeito, provocamos, desde logo, alguns pontos, que serão discutidos ao longo deste artigo:

1) Relatório publicado pelo Fundo das Nações Unidas para a Infância (Unicef), em 2018, revelou que a cada segundo, duas crianças entram na internet pela primeira vez, o que representa uma média de 175 mil novos usuários por dia[4]. Será que os termos de uso e política de privacidade dos sites e aplicativos que essas crianças estão acessando são suficientemente claros e acessíveis a elas? E se não forem, há alguma implicação?
2) Crianças e adolescentes frequentam uma série de locais que coletam seus dados pessoais, pessoal ou digitalmente, como escolas, hotéis, clubes e faculdades. Mas, em quais situações esse tratamento é permitido e em quais ele é abusivo? Será sempre necessário o consentimento dos pais ou responsáveis?
3) Seja por descumprirem os Termos de Uso e Políticas de Privacidade, seja por obterem do usuário seu expresso consentimento para tratar os dados coletados, a depender da forma como se dá, sites, aplicativos, jogos etc. não somente violam a privacidade como também, e em muitos casos, colocam em risco a segurança do usuário, monitorando suas pegadas digitais. Difícil crer que estes consentimentos possam ser considerados livres, expressos e informados, a começar pelo entrave de negociação dos referidos termos, os quais aliás, são, em sua maioria, complexos, longos e abastados de terminologias incompreensíveis.

[2] BARON, Jessica. *Nossas crianças estão sendo "datificadas", e isso pode colocá-las em perigo*. Tradução de Daniel Salgado. Disponível em: https://bit.ly/2NMymGx. Acesso em: 21 jan. 2020.

[3] BELLI, Luca. Seus dados são o novo petróleo: mas serão verdadeiramente seus? *O Globo*, 1º jun. 2017. Disponível em: https://glo.bo/2NK7Ddt. Acesso em: 21 jan. 2020.

[4] A cada segundo, 2 crianças entram na internet pela 1ª vez, diz Unicef. *Nações Unidas*, 8 fev. 2018. Disponível em: https://bit.ly/2ul4ES2. Acesso em: 21 jan. 2020.

Esses pontos demonstram que o estado atual ainda é desafiador. Porém, podemos, desde logo, e a cada novo aplicativo ou nova atualização, fazer um recomeço, repensar a proteção e segurança, a transparência, a informação, o direito de as crianças terem, no futuro, ingerência sobre seus dados e, desde agora, receberem a especial proteção que sua condição reclama, para o que a LGPD promete ser mais do que uma aliada, mas um marco divisor e propulsor no que diz respeito à proteção de dados de crianças e adolescentes.

1. A especial proteção da criança e do adolescente

Ao falar sobre o tratamento de dados pessoais das crianças é imprescindível ter em mente, além da LGPD, ao menos, três outras bases: Constituição da República Federativa do Brasil de 1988 (CF/88)[5], Convenção sobre os Direitos da Criança[6] e Estatuto da Criança e do Adolescente[7].

A CF/88 consagra a Doutrina da Proteção Integral à Criança e ao Adolescente, ao dispor, em seu artigo 127, que é dever da família, da sociedade e do Estado assegurar à criança e ao adolescente, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão. Tal doutrina promove três premissas a respeito das crianças e adolescentes: I) são sujeitos de direito[8]; II) destinatárias de absoluta prioridade; III) é devido respeito à sua condição peculiar de pessoa em desenvolvimento.

Por meio do Decreto nº 99.710/1990[9], publicado em 22/11/1990, sem ressalvas, o Brasil promulgou a Convenção sobre os Direitos da Criança, da Unicef, a qual, no âmbito internacional, entrou em vigor em 02/09/1990. Desta maneira, segundo a doutrina tradicional, a Convenção tem status de norma supralegal no ordenamento pátrio, isto é, abaixo da Constituição Federal, mas acima das leis, impondo o controle de convencionalidade – o que, em linhas gerais, significa que a legislação nacional não deve contrariar as diretrizes e princípios da Convenção. Tal como a CF/88, referida Convenção também acolhe a concepção do desenvolvimento integral da criança, reconhecendo-a como verdadeiro sujeito de direito, que exige proteção especial e absoluta prioridade.

Nos termos da Convenção, destacada como o tratado internacional de proteção de direitos humanos com o mais elevado número de ratificações, a criança é definida como "todo ser humano com menos de 18 anos de idade, a não ser que, pela legislação aplicável,

[5] BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: https://bit.ly/30FEupc. Acesso em: 21 jan. 2020.

[6] UNICEF. *Convenção sobre os Direitos da Criança*. Disponível em: https://uni.cf/38rvTJn. Acesso em: 21 jan. 2020.

[7] Lei 8.069/1990. Estatuto da Criança e do Adolescente. Disponível em: https://bit.ly/30RRGrn. Acesso em: 21 jan. 2020.

[8] A respeito da condição de sujeito de direitos, tem-se que, com tal proteção, "as crianças e os adolescentes ganham um novo "status", como sujeitos de direitos e não mais como menores objetos de compaixão e repressão, em situação irregular, abandonados ou delinquentes", como ocorria no Código de Menores (FERREIRA, Luiz Antonio Miguel; DÓI, Cristina Teranise. *A proteção integral das crianças e dos adolescentes vítimas (Comentários ao art. 143 do ECA)*. Disponível em: https://bit.ly/2GdOtZn. Acesso em: 21 jan. 2020).

[9] BRASIL. *Decreto nº 99.710/1990*. Disponível em: https://bit.ly/2TNWdt9. Acesso em: 21 jan. 2020.

a maioridade seja atingida mais cedo"[10]. O Estatuto da Criança e do Adolescente, por sua vez, considera criança a pessoa até doze anos de idade incompletos e adolescente aquela entre doze e dezoito anos de idade.

Isso significa dizer que à criança e ao adolescente são asseguradas todas as garantias e direitos fundamentais, inclusive o direito à intimidade, vida privada, imagem, nome, lazer e informação, assegurados pela CF/88, em seu artigo 5º, X e XIV, e na Convenção, nos artigos 16 e 17.

Desta maneira, ao dispor sobre o tratamento de dados de crianças e adolescentes, a Lei Geral de Proteção de Dados tem como plano de fundo a Doutrina da Proteção Integral à Criança e ao Adolescente, de tal modo que a interpretação da norma deverá sempre levar em consideração o especial interesse do menor, colocando a salvo, especialmente, sua segurança e direito à autodeterminação informativa, assim compreendida como o direito de escolher quais informações pessoais deseja expor e compartilhar. Com efeito:

> *a questão de fundo é, na essência, o problema do chamado "impulso à autoexposição" […], não apenas porque a pessoa participa de uma vida comum com os demais, compartilhando experiência tecnológica e informações próprias a seu tempo, mas, fundamentalmente, porque também o indivíduo deseja aparecer e, em determinada medida, fazer-se visto, "por feitos e palavras" […], pelos demais. A ação e reação sistemática ao avanço da ciência, especialmente em áreas de maior desenvolvimento tecnológico – como a da Tecnologia da Informação –, revela a tendência do homem contemporâneo de aprender a lidar com a sua individualidade sem necessariamente abdicar de um benefício tecnológico que lhe facilita o contato com uma esfera pública de relacionamento*[11].

Portanto, longe de impedir, em absoluto, a exposição e tratamento de dados pessoais de crianças e adolescentes, o que lhes negaria o direito de participação na sociedade da informação; mas seus dados devem ser tratados somente quando necessário, de forma granularizada (inclusive, a LGPD determina que as crianças não deverão ter sua participação em jogos, aplicações de internet ou outras atividades condicionada ao fornecimento de informações pessoais, além das estritamente necessárias à atividade – art. 14, §4º), considerando, especialmente, seu direito – e vontade – de integração, sua peculiar condição de vulnerabilidade e ser em desenvolvimento, assim como a máxima de que conteúdo na internet não tem devolução, de tal sorte que os dados e informações coletados, publicados e compartilhados, no atual estágio da técnica, poderão, em eventuais ataques e vazamentos, fugir do controle do menor, dos seus responsáveis e do próprio controlador.

[10] CUNHA, Rogério Sanches; ROSSATO, Luciano Alves; LÉPORE, Paulo Eduardo. *Estatuto da criança e do adolescente*: comentado artigo por artigo. 7. ed. São Paulo: Saraiva, 2015.

[11] CACHAPUZ, Maria Cláudia Mércio; CARELLO, Clarissa Pereira. Tratamento à informação, dados nominativos e a interpretação possível à Lei de Acesso à Informação. *In*: ANDRADE, Francisco António Carneiro Pacheco de; CELLA, José Renato Gaziero; FREITAS, Pedro Miguel Fernandes (org.). *Direito, governança e novas tecnologias*. Florianópolis: Conpedi, 2017, p. 7. Disponível em: https://bit.ly/36a58aU. Acesso em: 21 jan. 2020.

2. LGPD e o tratamento de dados pessoais de crianças e adolescentes

A Lei Geral de Proteção de Dados define em seu artigo 5º, I, que dado pessoal é toda "informação relacionada a pessoa natural identificada ou identificável". Assim, se bem pensarmos, a depender do contexto, até a cor da blusa pode ser dado pessoal. No inciso X, define que tratamento é toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Acerca do tratamento de dados pessoais, a Lei previu expressamente uma série de direitos e deveres, determinando em seu artigo 7º que ele somente deve ocorrer nas hipóteses previstas em lei. Ou seja, se não tiver base legal, o tratamento será ilícito e, portanto, sujeito a sanções. Entre as possibilidades, destacamos três: I) cumprimento de obrigação legal (nesse sentido, os provedores de internet devem armazenar os registros eletrônicos e cadastrais dos seus usuários, por força do Marco Civil da Internet); II) quando necessário para a execução de contrato (é o caso da escola, que precisa ter dados relacionados à identificação do aluno e histórico escolar, por ex.); III) mediante o consentimento do titular.

Cuidando especialmente dos menores, em seu artigo 14, a LGPD determina que o "tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse". A respeito desse melhor interesse e especial proteção aos dados de crianças e adolescentes, fazemos menção à Doutrina da Proteção Integral, bem como ao Considerando 38 do Regulamento Geral de Proteção de Dados europeu, no qual se espelhou a legislação nacional, que bem explica tal amparo, afirmando que: "merecem proteção especial quanto a seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão, assim como dos direitos relacionados ao tratamento de seus dados pessoais"[12].

Alinhados com a diretriz europeia, os princípios que regem a Lei Geral de Proteção de Dados objetivam, prioritariamente, proteger os interesses individuais, sobretudo quando relacionados às crianças. Neste sentido, tudo o que se refere a dados pessoais de crianças e adolescentes deve submeter-se à norma. Para tanto, é fundamental que o responsável pelo tratamento dos dados pessoais de crianças e adolescentes esteja certo quanto à faixa etária do público que pretende alcançar e, então, adote os meios adequados à aferição da idade e dos riscos potenciais, inclusive utilizando uma linguagem acessível ao seu público. Nesse sentido, inclusive, o §6º do artigo 14 da LGPD afirma:

> *As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.*

[12] Cuidando do âmbito europeu, o Considerando se refere aos dados de crianças.

Isso significa que os Termos de Uso e Políticas de Privacidade de serviços e produtos voltados a crianças e adolescentes devem ser objetivos e em linguagem acessível. Portanto, termos prolixos, confusos, demasiadamente extensos e técnicos, ao menos no que depender da LGPD, estão com seus dias contados.

Essa disposição vai ao encontro do Princípio da Transparência, que garante aos titulares o direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento (cf. art. 6º, VI, da LGPD). Outrossim, deve acompanhar todos os demais princípios e direitos comuns aos titulares dos dados. Entre os princípios, destacamos os princípios da adequação (os dados coletados serão tratados exatamente como informado ao titular), da necessidade (os dados coletados são necessários para o serviço proposto?), da prevenção e da não discriminação (os dados não podem ser tratados com fins discriminatórios, ilícitos ou abusivos). Entre os direitos, dispostos no capítulo III da LGDP, destacamos que "toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade", bem como os direitos previstos no artigo 18, que garantem ao titular exigir do controlador: acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; informações sobre o compartilhamento dos dados e a possibilidade de não fornecer ou revogar o consentimento e as respectivas consequências.

Acerca das crianças, isto é, menores de 12 anos, nos termos do ECA, o legislador houve por bem dar atenção ainda mais especial (§2º do artigo 14 da LGPD), reforçando a necessidade de transparência, afirmando que o controlador deve esclarecer os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o mencionado artigo 18.

Nesse contexto, sem esgotar as infinitas possibilidades, um exemplo para cumprir o disposto na norma, no que se refere à sensibilização e à compreensão do público quanto aos riscos, seria tornar expresso o que representam algumas das permissões conferidas por meio de determinados termos de uso, a saber: quando se confere o direito de acesso ao calendário, abrem-se todos os eventos nele armazenados, assim como se torna possível um terceiro editar eventos antigos e criar novos. Isto significa que alguém, além do próprio usuário, terá acesso a sua rotina. O mesmo acontece com relação aos acessos permitidos à câmera de seu dispositivo, agenda de contatos, e-mails, SMS e telefone, dentre outros[13].

Ainda cuidando especificamente dos menores de 12 anos, a LGPD determina que o tratamento dos dados de crianças somente poderá ser feito mediante o "consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal". Desta maneira, há uma discussão doutrinária a respeito da validade do consentimento dado pelo adolescente impúbere não abrangido pela LGPD, isto é, o menor entre 12 e 16 anos. A respeito, questiona Renato Opice Blum[14] "se poderia a LGPD, ao silenciar sobre o consentimento dos pais no tocante à coleta de dados do adolescente, abrir exceção relevante à regra de nulidade da Lei Civil" (que considera, para os atos da vida civil,

[13] Tudo sobre permissões dos aplicativos no Android. *Kaspersky Daily*. Disponível em: https://bit.ly/30FHLFb. Acesso em: 21 jan. 2020.

[14] BLUM, Renato Opice. *Polêmica na proteção de dados de crianças e adolescentes*. Disponível em: https://bit.ly/37g86Mj. Acesso em: 21 jan. 2020.

os menores de 16 anos como absolutamente incapazes). Ainda, se, nesse caso, o menor teria "carta branca" para "decidir livremente sobre o futuro dos seus dados. E conclui: embora defensável, tal entendimento é certamente preocupante − com o que devemos concordar.

De todo modo, no que diz respeito às crianças, importante ressaltar que para atender à expectativa da norma e atingir o objetivo almejado, não basta fazer constar dos respectivos termos a classificação indicativa para uso do serviço, assim como implementar medidas inócuas para se obter o consentimento exigido. É preciso, contando com os avanços e a disponibilidade da própria tecnologia, oferecer os melhores esforços para certificar-se de que o consentimento foi dado ou autorizado pelo efetivo titular das responsabilidades parentais da criança, inclusive é o que preconiza o §5º do artigo 14 da LGPD.

Acerca das possibilidades e limites para tal consentimento, de rica valia é o Direito Comparado, na medida em que a lei não determina. A respeito, sob a égide do Regulamento Geral de Proteção de Dados Europeu (RGPD) ou General Data Protection Regulation (GDPR), em vigor desde 25/05/2018, o legislador italiano[15], por meio da Lei 163, publicada em 6 de novembro de 2017, no *Jornal Oficial da Itália*, fixou que quando necessário o consentimento dos pais ou responsáveis para o tratamento de dados de criança, só será considerado lícito se for dado ou autorizado pelo titular da responsabilidade parental da criança[16]. Neste sentido, entende o Poder Judiciário italiano, por exemplo, que a publicação de uma fotografia on-line se encaixa perfeitamente no escopo de proteção para o processamento de dados pessoais e sensíveis porque interfere na vida privada da criança. Assim, deve ser dada especial atenção à publicação de imagens de menores, mesmo que isso diga respeito aos próprios filhos. Inclusive, sob tal perspectiva, um acórdão do Tribunal de Mântua, Itália (novembro de 2017), estabeleceu que, para a publicação de fotos de crianças, é necessário o consentimento dos pais. Na ausência do acordo dos pais, a foto simplesmente não é publicável[17]. Essa questão nos conduz a refletir: considerando que os pais estejam de acordo com a publicação de fotos, vídeos, dados do pré-natal e outras peculiaridades da vida do menor, será que este também concordará com tal exposição, quando adolescente ou adulto? Como poderá exercer seu direito à autodeterminação informacional? A questão é, sem dúvidas, um convite ao debate…

Sob a mesma égide, em Portugal, o Projeto de Lei 120/XIII, publicado oficialmente em março de 2018, por meio de seu artigo 16, estabelece que para o tratamento de dados de crianças[18], o tratamento só será considerado lícito se houver o consentimento dos seus representantes legais, preferencialmente com recurso aos meios de autenticação segura, como o Cartão de Cidadão ou Chave Móvel Digital[19]. No Brasil, carecemos desse tipo documento; contudo, parece-nos uma das possibilidades a serem estudadas.

[15] Na Itália, a Lei estabelece tal necessidade para crianças menores de 16 anos.

[16] Garante per l'infanzia: consenso al trattamento dei dati personali a 16 anni. *Federprivacy*, 24 abr. 2018. Disponível em: https://bit.ly/2LK8U5n. Acesso em: 6 ago. 2018; GARANTE INFANZIA. *Parere Schema Secreto Regolamento 2016/679 EU*. Disponível em: https://bit.ly/2M2JAXX. Acesso em: 6 ago. 2018.

[17] SAETTA, Bruno. Minori e protezione dati personali. *Protezioni Dati Personali*, 7 set. 2018. Disponível em: https://bit.ly/36bEj69. Acesso em: 8 ago. 2018; SCHEMA di decreto legislativo recante […]. Disponível em: https://bit.ly/2G7LFNA . Acesso em: 7 ago. 2018.

[18] Em Portugal, a Lei estabelece tal necessidade para crianças menores de 13 anos.

[19] PORTUGAL. Presidência do Conselho de Ministros. *Proposta de Lei n.120/XIII*. Disponível em: https://bit.ly/2HlLLDk. Acesso em: 6 ago. 2018.

Por fim, cumpre lembrar que o tratamento de dados de crianças deve ser feito considerando o seu melhor interesse. É por essa razão que a Lei Geral de Proteção de Dados traz, no §3º do artigo 14, ressalvas quanto à possibilidade desse tratamento, sem o consentimento dos responsáveis, permitindo que, nessa condição, a coleta seja feita somente se necessária para: I) contatar os pais ou o responsável legal, desde que os dados sejam utilizados uma única vez e sem armazenamento; ou II) garantir a proteção da criança, vedando, em qualquer caso, o compartilhamento dos dados com terceiros.

Sem consentimento e fora das hipóteses de exceções previstas em lei, o tratamento de dados de crianças será considerado ilícito e, desta maneira, sujeito às sanções legais; da mesma maneira, o tratamento de dados de adolescentes que não observar o Princípio da Transparência ou quaisquer das demais normas e princípios da LGPD. O artigo 52 da Lei Geral de Proteção de Dados especifica que a violação às suas diretrizes sujeitará o infrator a advertência, publicização da infração, bloqueio ou eliminação dos dados pessoais, multa simples ou diária, de até 2% (dois por cento) do faturamento anual da pessoa jurídica ou grupo econômico no Brasil, limitada a 50 milhões de reais – deixando claro que tais penalidades poderão ser aplicadas de forma gradativa, isolada ou cumulativa, de acordo com a gravidade da infração, boa-fé do infrator, vantagens auferidas, cooperação do infrator, adoção de política de boas práticas e governança, entre outros critérios.

3. A responsabilidade além e em decorrência da LGPD

Segundo a LGPD, ela se destina a todas as pessoas naturais ou jurídicas, de direito público ou privado, independentemente do meio, do país de sua sede ou do país que estejam localizados os dados, desde que: I) o tratamento de dados seja realizado no Brasil; II) os dados tenham sido coletados no território nacional; III) o tratamento tenha por objetivo a oferta ou fornecimento de bens ou serviços a indivíduos localizados no Brasil. Não incidirá, todavia, quando os dados forem utilizados para fins: I) exclusivamente particulares e não econômicos (ex. agenda telefônica pessoal); II) exclusivamente jornalísticos, artísticos e acadêmicos; III) de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais; IV) ainda, não se aplicará quando os dados forem provenientes de países estrangeiros que ofereçam um nível de segurança jurídica adequado sobre este tema e sejam apenas processados em território nacional, sem que haja qualquer intenção do agente brasileiro em compartilhar ou comunicar estes dados pessoais com outros agentes, exceto o agente que primariamente transmitiu a informação[20].

A lente de aplicação da LGPD é tão ampla, que não é demais dizer que praticamente todas as empresas que lidam com dados de crianças e adolescentes lhe devem conformidade. Inclusive, diferente do que muitos imaginam, assim como os aplicativos, mídias sociais e sites, jogos também coletam informações pessoais e particulares de seus usuários. Assim como qualquer empresa de tecnologia, aquelas responsáveis por oferecer entretenimento através de jogos ou outras formas de interação ou diversão também precisam se adequar às exigências do regulamento europeu de proteção de dados, inclusive no que se refere à nomeação de um responsável pela segurança dos dados coletados. No mesmo

[20] BORELLI, Alessandra; ABRUSIO, Juliana (org.). *Os impactos da Lei Geral de Proteção de Dados em instituições de ensino*. Disponível em: https://bit.ly/2v3pq94. Acesso em: 21 jan. 2020.

sentido, empresas, escolas, universidades, hotéis, clubes e agremiações recreativas também precisam caminhar rumo à proteção dos dados pessoais de crianças e adolescentes.

Esse, inclusive, é um caminho que já vem sendo trilhado pelas grandes sociedades internacionais e multinacionais, tais como Twitter e Facebook, notadamente em razão do Regulamento Geral de Proteção de Dados (RGPD), europeu. Desde sua entrada em vigor, de acordo com o Twitter, a empresa está optando por proibir qualquer pessoa cuja data de nascimento – se ela foi fornecida no momento da inscrição ou posteriormente – indicar que eles tinham menos de 13[21] anos quando se inscreveram para usufruir do serviço[22]. Já o Facebook e o Instagram se comprometeram a não mais fazer "vistas grossas" em suas plataformas, bloqueando perfis de usuários menores de 13 anos de idade. Para ter suas contas reativadas e recuperar o acesso, segundo notícias, deverão provar que têm mais de 13 anos, por meio de um documento de identificação com foto emitido pelo governo[23].

As escolas também precisam se adequar à novel legislação. Diríamos, inclusive, que elas têm um papel de destaque, não só porque, por força da Lei de Diretrizes e Bases, a educação básica tem, entre suas finalidades, a promoção da cidadania e capacitação do aluno ao mercado de trabalho e convívio social – o que, na sociedade da informação, passa pela orientação então em tela, mas também em razão da influência positiva que podem promover na vida não só dos seus alunos, mas da família e de toda a comunidade escolar, notadamente os professores, inclusive a partir de medidas educacionais, de orientação quanto ao uso correto, lícito e seguro das novas tecnologias.

A respeito, ilustramos algumas medidas práticas apontadas pela mesa-redonda para discussão sobre os direitos das crianças, organizada em Bruxelas pela European Schoolnet, KU Leuven e Universidade de Gante[24]: tornar os temas "privacidade" e "proteção de dados" parte do conteúdo curricular de forma integrada a outras matérias; garantir maior atenção e critérios bem definidos na entrega de certas tecnologias a crianças, sobretudo para fins pedagógicos; incluir a prática de *gamificação* para conscientizar sobre "tratamento de dados", de modo a contribuir para melhor compreensão dos alunos acerca do processo de aquisição e comercialização de seus dados; utilizar recursos diversos para treinamento e compartilhamento de diretrizes, incluindo vídeos e ferramentas fáceis de serem utilizadas e projetos on-line, com foco em segurança digital, privacidade e proteção de dados, liderado por um coordenador de Tecnologia da Informação e Comunicação, dedicado a acompanhar os projetos e indicar outros cada vez mais significativos; envolver a indústria no processo de conscientização, firmando parcerias entre esta e escolas; entre outras iniciativas.

Mas, para orientar é preciso antes se orientar. É preciso, igualmente, estar *compliant*.

---

[21] Conforme artigo 8º do Regulamento europeu: "1. Quando for aplicável o artigo 6º, n. 1, alínea a), no que respeita à oferta direta de serviços da sociedade da informação às crianças, dos dados pessoais de crianças, é lícito se elas tiverem pelo menos 16 anos. Caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado pelos titulares das responsabilidades parentais da criança. Os Estados-Membros podem dispor no seu direito uma idade inferior para os efeitos referidos, desde que essa idade não seja inferior a 13 anos". Disponível em: https://bit.ly/2uoPCKW. Acesso em: 21 jan. 2020.

[22] PERSON, Jordan. Twitter is banning anyone whose date of birth says they joined before they were 13. *Motherboard*, 30 maio 2018. Disponível em: https://bit.ly/2J37fTa. Acesso em: 6 ago. 2018.

[23] Facebook vai suspender conta de usuários com menos de 13 anos de idade. *G1*, 25 jul. 2018. Disponível em: https://glo.bo/2MmNW9b. Acesso em: 6 ago. 2018.

[24] Report from the roundtable on the General Data Protection Regulation and children's rights. *Better Internet for Kids*. Disponível em: https://bit.ly/2u0bnyQ. Acesso em: 6 ago. 2018.

Como vimos, a realização do contrato de prestação de serviços escolares é uma das possíveis bases legais para o tratamento de dados de crianças e adolescentes. Mas, mesmo nesses casos, é mister especial atenção ao princípio da minimização da coleta (estritamente o necessário), bem como aos princípios da finalidade e necessidade. Assim, por exemplo, os dados dos alunos do último ano não podem ser compartilhados com a empresa de formatura ou com universidades nacionais ou estrangeiras, sem o devido consentimento. Por mais habitual e aparentemente inofensivas que determinadas práticas possam parecer no âmbito escolar, podem ser consideradas abusivas de acordo com o que dispõe a LGPD.

Ainda considerando as práticas habituais, não é difícil encontrar instituições de ensino que buscam obter junto aos seus contratantes informações sobre a origem étnica ou racial, sob a justificativa de ser importante para promover a integração de alunos; informações sobre crenças religiosas, sob a justificativa de sua importância para garantir a liberdade religiosa. Ocorre que, para efeitos da LGPD, alguns dados pessoais são considerados particularmente sensíveis, como aqueles capazes de revelar, por exemplo, a origem racial ou étnica de alguém, crenças religiosas ou filosóficas, dados genéticos, biométricos, dados relativos ao estado de saúde ou orientação sexual de uma pessoa, ou seja, informações que por sua própria natureza são passíveis de gerar condutas discriminatórias. Não significa que não podem ser tratados, porém, para tanto, é imprescindível que se avalie a real necessidade, os possíveis riscos e, em regra, é preciso obter consentimento de forma específica e destacada.

Se bem refletirmos, outras situações também podem resultar no tratamento de dados sensíveis, a exemplo: os serviços que oferecem refeições nas instituições de ensino, as conhecidas cantinas ou refeitórios, também guardam dados sensíveis. Considerando a limitação de determinados alunos à eventual ingestão de certos alimentos em razão de particulares ditames religiosos, temos que algumas escolhas específicas, por exemplo, são capazes de revelar as crenças (religiosas ou filosóficas) de pais e alunos.

Embora, a rigor, não sejam dados sensíveis, semelhante cautela é necessária com as informações que almejam relacionar o resultado de avaliações com o desempenho acadêmico do aluno. Quaisquer relatórios que possam rotular, identificar o aluno ou torná-lo identificável, devem ser únicos e exclusivamente direcionados ao aluno ou seu responsável legal. O mesmo deve ocorrer em relação à expedição de comunicados para, por exemplo, chamada de recuperação, mau comportamento, ranking de notas ou alunos em condição especial. Inclusive, na Europa, por receio de sanções, algumas escolas estão deixando de publicar os nomes dos alunos nas pautas, substituindo-os pela identificação da turma e número de aluno[25].

Por fim, cabe às escolas e a todos demais que tratam dados pessoais de crianças e adolescentes, a manutenção de políticas relativas à segurança da informação sempre atualizadas, a promoção da educação digital daqueles que lidam com os dados, assim como traçar meios para identificação e contenção de incidentes — lembrando que sua diligência será considerada diante de eventual aplicação de sanção, podendo ser uma âncora à sua reputação ou sobre ela.

[25] Escolas apagam nomes dos alunos nas pautas com medo de multas. *Diário de Notícias*, 14 jul. 2019. Disponível em: https://bit.ly/37dYTEg. Acesso em: 21 jan. 2020.

Com base nesse cenário, as instituições de ensino e demais pessoas que tratam os dados pessoais de crianças e adolescentes devem atualizar suas políticas, termos, processos e procedimentos, buscando a conformidade com a legislação, não só em razão das possíveis sanções, mas, sobretudo, tendo sempre em mente que não erra quem pensa, em primeiro lugar, na proteção dos direitos e bem-estar da criança e do adolescente.

4. Conclusão

Diante da constante exposição e datificação dos dados pessoas de crianças e adolescentes, indiscutível a necessidade de céleres providências para chamar à responsabilidade todos aqueles que intencionam utilizar estes dados. Isto porque, não somente a privacidade, mas a segurança deste público deve ser tratada com a máxima prioridade e quaisquer ações que os envolva deve ter sempre como premissa básica o seu melhor interesse.

Crianças e adolescentes, apesar da sua surpreendente habilidade diante dos diversos dispositivos e ferramentas digitais, dada sua condição peculiar de ser em desenvolvimento, não são capazes de compreender, em todas as dimensões, que os dados "oferecidos" como contrapartida no uso de serviços, constituem uma importante unidade de valor monetário e representa uma parte de sua privacidade. E, considerando essa fase de desenvolvimento e vulnerabilidade peculiar, a LGPD veio reforçar a Doutrina da Proteção Integral, trazendo luz e diretrizes específicas ao tratamento de seus dados pessoais, proporcionando expectativa de mudanças significativas e positivas.

5. Referências

A CADA segundo, 2 crianças entram na internet pela 1ª vez, diz Unicef. *Nações Unidas*, 8 fev. 2018. Disponível em: https://bit.ly/2ul4ES2. Acesso em: 21 jan. 2020.

BARON, Jessica. *Nossas crianças estão sendo "datificadas", e isso pode colocá-las em perigo*. Tradução de Daniel Salgado. Disponível em: https://bit.ly/2NMymGx. Acesso em: 21 jan. 2020.

BELLI, Luca. Seus dados são o novo petróleo: mas serão verdadeiramente seus? *O Globo*, 1º jun. 2017. Disponível em: https://glo.bo/2NK7Ddt. Acesso em: 21 jan. 2020.

BLUM, Renato Opice. *Polêmica na proteção de dados de crianças e adolescentes*. Disponível em: https://bit.ly/37g86Mj. Acesso em: 21 jan. 2020.

BORELLI, Alessandra; ABRUSIO, Juliana (org.). *Os impactos da Lei Geral de Proteção de Dados em instituições de ensino*. Disponível em: https://bit.ly/2v3pq94. Acesso em: 21 jan. 2020.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil*. Disponível em: https://bit.ly/30FEupc Acesso em: 21 jan. 2020.

BRASIL. *Decreto nº 99.710/1990*. Disponível em: https://bit.ly/2TNWdt9. Acesso em: 21 jan. 2020.

BRASIL. *Lei 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados. Disponível em: https://bit.ly/2NMYq4u. Acesso em: 21 jan. 2020.

BRASIL. *Lei 8.069, de 13 de julho de 1990*. Dispões sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: https://bit.ly/30RRGrn. Acesso em: 21 jan. 2020.

CACHAPUZ, Maria Cláudia Mércio; CARELLO, Clarissa Pereira. Tratamento à informação, dados nominativos e a interpretação possível à Lei de Acesso à Informação. *In*: ANDRADE, Francisco António Carneiro Pacheco de; CELLA, José Renato Gaziero; FREITAS, Pedro Miguel Fernandes (org.). *Direito, governança e novas tecnologias*. Florianópolis: Conpedi, 2017. p. 4-22. Disponível em: https://bit.ly/36a58aU. Acesso em: 21 jan. 2020.

CUNHA, Rogério Sanches; ROSSATO, Luciano Alves; LÉPORE, Paulo Eduardo. *Estatuto da criança e do adolescente*: comentado artigo por artigo. 7. ed. São Paulo: Saraiva, 2015.

ESCOLAS apagam nomes dos alunos nas pautas com medo de multas. *Diário de Notícias*, 14 jul. 2019. Disponível em: https://bit.ly/37dYTEg. Acesso em: 21 jan. 2020.

FACEBOOK vai suspender conta de usuários com menos de 13 anos de idade. *G1*, 25 jul. 2018. Disponível em: https://glo.bo/2MmNW9b. Acesso em: 6 ago. 2018.

FERREIRA, Luiz Antonio Miguel; DÓI, Cristina Teranise. *A proteção integral das crianças e dos adolescentes vítimas (Comentários ao art. 143 do ECA)*. Disponível em: https://bit.ly/2GdOtZn. Acesso em: 21 jan. 2020.

GARANTE INFANZIA. *Parere Schema Secreto Regolamento 2016/679 EU*. Disponível em: https://bit.ly/2M2JAXX. Acesso em: 6 ago. 2018.

GARANTE per l'infanzia: consenso al trattamento dei dati personali a 16 anni. *Federprivacy*, 24 abr. 2018. Disponível em: https://bit.ly/2LK8U5n. Acesso em: 6 ago. 2018.

PERSON, Jordan. Twitter is banning anyone whose date of birth says they joined before they were 13. *Motherboard*, 30 maio 2018. Disponível em: https://bit.ly/2J37fTa. Acesso em: 6 ago. 2018.

PORTUGAL. Presidência do Conselho de Ministros. *Proposta de Lei n. 120/XIII*. Disponível em: https://bit.ly/2HlLLDk. Acesso em: 6 ago. 2018.

REGULAMENTO Geral de Proteção de Dados. Disponível em: https://bit.ly/2sKSamh. Acesso em: 21 jan. 2020.

REPORT from the roundtable on the General Data Protection Regulation and children's rights. *Better Internet for Kids*. Disponível em: https://bit.ly/2u0bnyQ. Acesso em: 6 ago. 2018.

SAETTA, Bruno. Minori e protezione dati personali. *Protezioni Dati Personali*, 7 set. 2018. Disponível em: https://bit.ly/36bEj69. Acesso em: 8 ago. 2018.

TUDO sobre permissões dos aplicativos no Android. *Kaspersky Daily*. Disponível em: https://bit.ly/30FHLFb. Acesso em: 21 jan. 2020.

UNICEF. *Convenção sobre os Direitos da Criança*. Disponível em: https://uni.cf/38rvTJn. Acesso em: 21 jan. 2020.

Compreendendo o conceito de anonimização e dado anonimizado

Bruno Ricardo Bioni[1]
Professor

1. Dados anonimizados como a antítese de dados pessoais: o filtro da razoabilidade

A antítese do conceito de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto (HOUAISS; VILLAR, 2009, p. 140).

Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização (DONEDA, 2006, p. 44). Esse processo pode se valer de diferentes técnicas que buscam eliminar tais elementos identificadores de uma base de dados (COUNCIL OF EUROPE, 2018), variando entre: a) supressão; b) generalização; c) randomização e; d) pseudoanonimização[2].

Com maior ou menor grau de intensidade – *e.g.*, supressão ou generalização – nota-se um método cujo mote é gerenciar circunstancialmente a *identificabilidade* de uma base de dados. As características de cada dado e a percepção de eles estarem inseridos em uma gama de informações devem orientar tal análise.

Por isso, não há um único método ou uma combinação perfeita *ex ante* para parametrizar o processo de anonimização, devendo-se analisar contextualmente como este deve ser empreendido para que os titulares dos dados anonimizados não sejam reidentificados, nem mesmo por quem procedeu à sua anonimização.

Amarrar o conceito teórico de dados anônimos a uma *análise contextual*, com os olhos voltados para a irreversibilidade do processo de anonimização, joga luz diretamente sobre o fator problemático dessa proposição: o seu caráter elusivo ou mesmo a sua impossibilidade teórica (TEIXEIRA, 2015).

Torna-se cada vez mais recorrente a publicação de estudos que demonstram ser o processo de anonimização algo falível. A representação simbólica de que os vínculos de identificação de uma base de dados poderiam ser completamente eliminados, garantindo-se, com 100% (cem por cento) de eficiência, o anonimato das pessoas, é um mito (NARAYANAN; SHMATIKOV, 2010, p. 24).

Por essa lógica, qualquer dado pessoal anonimizado detém o *risco inerente* de se transmudar em um dado pessoal (TENE, 2013, p. 1.242). A agregação de diversos "pedaços" de informação (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, a qual era até então desfigurada (anônimo) – o chamado efeito mosaico.

---

[1] Doutorando em Direito Comercial e mestre em Direito Civil pela Universidade de São Paulo. Foi pesquisador visitante do Centro de Tecnologia, Sociedade, Direito e Internet da Universidade de Ottawa e do Departamento de Proteção de Dados Pessoais do Conselho da Europa. É Professor e Fundador do Data Privacy Brasil.

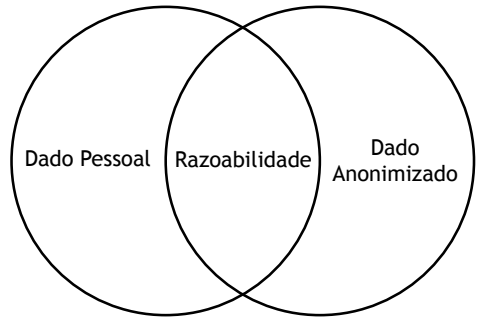
[2] Para muitos, a pseudoanonimização não é considerada uma técnica de anonimização. Isso porque se substituem, apenas, os identificadores diretos – *e.g.*, nome, CPF etc. – por pseudônimos – *e.g.*, números aleatórios, de modo que a pessoa permanece sendo identificável em razão de tais pseudônimos serem um retrato detalhado indireto delas (WP 29, 2014, p. 20).

Por isso, leis que adotam o conceito expansionista[3] de dados pessoais e, ao mesmo tempo, estabelecem uma dicotomia deste com dados anônimos correriam o risco de serem tautológicas. Isso porque haveria uma *redundância normativa*, já que dados anônimos seriam, em última análise, potencial e provavelmente, dados relacionados a uma pessoa identificável.

Para não gerar tal incoerência, a única saída foi a adoção de um "filtro" que delimitasse a *elasticidade* desse conceito expansionista – neste caso o termo identificável –, sob pena de a fronteira entre dados pessoais e dados anônimos ser sempre transponível.

E, nesse sentido, o direito comunitário europeu[4] e a LGPD[5] valeram-se do critério da razoabilidade para delimitar o espectro do conceito expansionista de dados pessoais. Não basta a mera possibilidade de que um dado seja atrelado a uma pessoa para atrair o termo identificável (WP, 2007, p. 1.749). Essa vinculação deve ser objeto de um "esforço razoável"[6], sendo esse o perímetro de elasticidade do conceito de dado pessoal como aquele relacionado a uma pessoa identificável.

A contrario sensu, se para a correlação entre um dado e uma pessoa demanda-se um esforço fora do razoável, não há que se falar em dados pessoais. Nessa situação, o dado é considerado como anônimo, uma vez que o "filtro da razoabilidade" barra o seu enquadramento como aquele relacionado a uma pessoa identificável[7].



Com isso, há coerência em se estabelecer conceitos diferentes para tais espécies de dados, sobretudo sob o ponto de vista de uma dicotomia mutualmente excludente entre eles, que é delimitada pelo fator da razoabilidade[8]. Do contrário, repita-se, haveria uma redundância normativa, na medida em que dados anônimos – sem o critério da razoabilidade – seriam sempre enquadrados dentro do conceito de dado pessoal, como aquele relacionado a uma pessoa identificável.

---

[3] A definição do conceito de dados pessoais pode seguir uma orientação expansionista (a partir da delimitação de "pessoa identificável") ou reducionista ("pessoa identificada"), respectivamente alargando ou restringindo o escopo de aplicação da lei (BIONI, 2019).

[4] A Diretiva 95/46 e a sua proposta de regulamentação adotam os conceitos de razoabilidade, respectivamente, nas considerandas 26 (vinte e seis) e 23 (vinte e três).

[5] Na definição de dados anônimos, de anonimização, bem como no dispositivo que prevê em quais hipóteses um dado anonimizado pode ser considerado como dado pessoal, a LGPD faz alusão ao termo razoável(is) – respectivamente, arts. 5º, II e III, e 18.

[6] Essa é exatamente a terminologia utilizada pelo art. 12, *caput*, da LGPD: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido".

[7] Ibidem, p. 21.

[8] Sobre as disputas interpretativas em torno do conceito jurídico indeterminado de razoabilidade, ver: BIONI, Bruno Ricardo. *Xeque-mate*: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI-USP, 2016, p. 34-35.

2. Calibrando o filtro da razoabilidade: critérios objetivos e subjetivos como fatores de uma análise de risco e os incentivos implícitos à pseudoanonimização

O legislador brasileiro procurou talhar uma norma neutra tecnológica[9]. Ao contrário de apontar para uma tecnologia em específico que poderia se tornar obsoleta ao longo do tempo, utilizou-se de um conceito indeterminado – razoabilidade – a ser significado e atualizado pelo próprio desenvolvimento científico. Simultaneamente, contudo, prescreveu balizas para reduzir a discricionariedade de tal exercício interpretativo e, com isso, alcançar um mínimo de previsibilidade quando tal norma viesse a ser colocada em movimento.

O primeiro eixo de análise é objetivo, sendo composto por uma matriz e dois elementos fatoriais respectivamente[10]: a) estado da arte da tecnologia; a.1) custo e; a.2) tempo[11]. Deve-se analisar o quão custoso e moroso seria reverter um processo de anonimização, de acordo com as tecnologias disponíveis para tanto. Trata-se, portanto, de uma análise dinâmica[12], a ser demarcada pelo próprio progresso tecnológico, que aponta qual deve ser o grau de investimento financeiro e temporal para se reidentificar uma base de dados anonimizada.

Por exemplo, há muito tempo se fala e se espera a chegada da computação quântica[13]. Quando isso acontecer, testemunhar-se-á um verdadeiro progresso acerca da capacidade, em termos quantitativos e qualitativos, de processamento de dados. Consequentemente, atualizar-se-á, por completo, o custo e o tempo quanto ao emprego das técnicas de anonimização, mas, também, por outro lado, das suas respectivas contratecnologias.

Em síntese, o primeiro eixo de análise propõe uma análise acerca do grau de *resiliência* de um processo de anonimização frente aos *padrões sociais*. Uma investigação de ordem objetiva cujo marcador é verificar como o estado da técnica calibra a escala de recursos (custo e tempo) para transmudar um dado anonimizado em dado pessoal.

---

[9] O conceito de "technology-neutral regulation" tem sido evocado para se discutir o desenho de modelos regulatórios capazes de estimular e acompanhar o desenvolvimento tecnológico, sem engessá-lo nem ser permissivo a riscos. Sobre isso: KOOPS, Bert-Jaap. Should ICT regulation be technology-neutral? *In*: KOOPS, Bert-Jaap; LIPS, Miriam; PRINS, Corien; SCHELLEKENS, Maurice (ed.). *Starting points for ICT Regulation*: Deconstructing prevalent policy one-liners. The Hague: TMC Asser Press, 2006. v. 9, p. 77-108. (IT & Law Series). ISBN 90-6704-216-1. REED, Chris. Taking sides on technology neutrality. *SCRIPT-ed*, Edimburgo, v. 4, n. 3, 2007; MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with 'technology' as a regulatory target. *Law, Innovation and Technology*, Abingdon-on-Thames, v. 5, n. 1, p. 1-20, 2013. Para a discussão no cenário nacional, ver: BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, v. 273, p. 123-163, 2016.

[10] A GDPR, em sua consideranda 26, também utilizada esses três fatores objetivos como delimitação à razoabilidade.

[11] Artigo 12 da LGPD. Art. 12, § 1º: "A determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios".

[12] A LGPD, em seu art. 5º, III e XI, define dado anonimizado a partir do emprego dos meios técnicos razoáveis disponíveis na ocasião (III) e no momento (XI) de seu tratamento. Esse tipo de avaliação torna-se, assim, contextual. Se, por um lado, essa análise contextual incentiva estudos sobre o tema, por outro, traz complicações à avaliação de seu cumprimento tendo em vista, por exemplo, diferenças quanto ao acesso à informação e recursos econômicos disponíveis entre os diferentes atores.

[13] Em 08.01.2019 foi lançado o primeiro computador quântico de uso comercial do mundo. Contudo, estima-se um período entre cinco e dez anos para que a computação quântica passe a ser adotada nos negócios. Assim, apesar de existente, essa tecnologia não compreenderia o estado da arte da tecnologia (ou meio técnico razoável disponível, nos termos da LGPD), tornando um encargo demasiado excessivo a expectativa de sua adoção. Disponível em: https://glo.bo/36eoGLd. Acesso em: 20 jan. 2020.

O segundo eixo de análise é subjetivo. Deve-se levar em consideração quem é o agente de tratamento de dados e se ele dispõe de "meios próprios"[14] para reverter o processo de anonimização. Ao invés de considerar quais são os padrões sociais acerca da reversibilidade de um dado anonimizado, foca-se em analisar qual é a capacidade individual de engenharia reversa de quem processa tais dados. Abre-se, com isso, dois vetores importantes de análise.

Em primeiro lugar, sob o ponto de vista do fluxo de dados dentro de uma organização. É cada vez mais comum que organizações segmentem as suas bases de dados de acordo com suas respectivas áreas de negócio e, até mesmo em alguns casos, empreguem práticas de anonimização para a geração de *business intelligence/BIA*.

Por exemplo, é o caso de uma grande rede de lojas varejistas que decide utilizar a sua base de dados de programa de fidelidade para melhorar o seu sistema de distribuição logística. Uma nova finalidade foi atribuída a um conjunto de dados, não sendo necessário saber quem são seus respectivos consumidores de forma individualizada, mas, tão somente, quais produtos têm mais ou menos entrada e saída de acordo com o perfil de vendas de cada um dos seus estabelecimentos geograficamente espalhados. Dessa forma, é factível a estruturação de uma nova base de dados sem que haja a associação direta ou indireta a indivíduos, podendo ser mantida, inclusive, em separado da outra base de dados (programa de fidelidade) que lhe deu origem.

Nesse cenário, o próprio agente tem informações adicionais, ainda que mantidas separadamente, para reverter o processo de anonimização. Ou seja, ele possui meios próprios para transmudar um dado aparentemente anonimizado em um dado pessoal, o que é revelado com base em uma análise subjetiva focada na sua própria capacidade de entropia de informação[15].

O cenário acima descrito é o que se convencionou chamar de pseudoanonimização, ou seja, uma falsa, superficial, técnica de anonimização que é quebrável em especial pela própria organização que a empregou.

A primeira reflexão que pode seguir a esse respeito é: por que a organização deveria empregar todo o esforço acima mencionado, se toda a carga regulatória da legislação de proteção de dados ainda assim recairá sobre ela (o dado não deixará de ser pessoal)?

Diferentemente da GDPR, a legislação de proteção de dados pessoais brasileira não sistematizou adequadamente a figura da pseudoanonimização, muito menos desenhou normativamente incentivos expressos para a sua adoção por parte dos agentes de tratamento de dados. Enquanto o regulamento europeu previu até mesmo o relaxamento de algumas obrigações legais[16], a lei geral brasileira de proteção de dados pessoais apenas citou pseudoanonimização de forma assistemática[17].

---

[14] Artigo 12 da LGPD. Art. 12: "Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente **meios próprios**, ou quando, com esforços razoáveis, puder ser revertido".

[15] Entropia da informação é o uso de uma informação auxiliar para a reversão do processo de anonimização. No caso em análise, as informações adicionais em posse do agente de tratamento.

[16] O artigo 11 da GDPR estabelece que, se o propósito do tratamento dos dados pessoais não exige (ou não exige mais) que o agente seja capaz de identificar o titular, o agente não será obrigado a manter informações adicionais para identificá-lo. E, por não sê-lo, estará escusado de garantir os direitos de acesso, retificação, exclusão e portabilidade do titular – a menos que o próprio titular, buscando exercer esses direitos, forneça as informações adicionais para sua identificação. Disponível em: http://bit.ly/3arPYRT. Acesso em: 20 jan. 2020.

[17] Artigo 13 da LGPD. Art. 13. "Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de

No entanto, ainda assim, é possível chegar à conclusão de que há sim incentivos, mesmo que indiretos, a serem burilados na lei geral de proteção de dados pessoais. Na medida em que pseudoanonimização é o "meio do caminho"[18] entre um dado pessoal e um dado anonimizado, seria possível correlacioná-la às diversas menções que a LGPD faz para que os agentes de tratamento "sempre que possível" anonimizem os dados[19]. Isto porque a lógica normativa em questão é encarar o processo de retirada dos identificadores de uma base de dados como algo que *minimiza os riscos* de uma atividade de tratamento de dados. Esse é exatamente o mote de técnicas de pseudoanonimização, ainda que não retire por completo o caráter pessoal de um dado.

Soma-se, ainda, o fato de que técnicas de pseudoanonimização podem compor o espectro de medidas, políticas e processos de um programa de governança que é referenciado pela LGPD[20]. E, ainda, por ser uma medida tradicional de segurança da informação que pode reduzir significativamente os impactos de um incidente de segurança, a partir da simples constatação de que: a) uma base de dados pseudoanonimizada pode não ser reversível por terceiros-atacantes[21] e; b) certamente, gera menos riscos em relação a uma base de dados comprometida que não tenha havido o emprego de tais medidas.

Por fim, ainda quanto ao eixo de análise subjetiva, deve-se considerar o fluxo de dados para fora da organização. Nesse caso, como terceiros deteriam "meios próprios" para reverter o processo de anonimização dos dados. Trata-se de uma questão particularmente importante no que diz respeito a eventuais parcerias que envolvam o uso compartilhado de dados[22], mesmo que não sejam dados pessoais *a priori*.

---

estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoanonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas. […] § 4º Para os efeitos deste artigo, a pseudoanonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro". O tema foi uma das últimas inclusões na Lei, tendo sido inserido pela primeira vez em 24.05.2018, pelo relator, deputado Orlando Silva, no substitutivo 1 ao PL 4060/2012 apresentado à Câmara dos Deputados.

[18] Na pseudoanonimização, as informações adicionais que permitiriam a identificação do titular são mantidas em separado pelos agentes de tratamento, que podem, assim, reidentificar os dados se fizerem uso dessa informação. Contudo, caso excluam essas informações adicionais, os agentes não mais poderão efetuar a reidentificação "por meios próprios", caracterizando, assim, uma técnica de anonimização. É nesse sentido que a pseudoanonimização seria "o meio do caminho" para a anonimização.

[19] A LGPD estabelece a necessidade de que, sempre que possível, haja a anonimização dos dados utilizados em pesquisas (arts. 7º, IV, 11, II, "c", 13 e 16, II), assim como determina que, embora uma das exceções à eliminação dos dados após o término do tratamento seja o uso exclusivo do controlador, ela está condicionada à vedação do acesso aos dados por terceiro e à anonimização dos dados (art. 16, IV).

[20] Artigo 50 da LGPD. Art. 50: "Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. […] § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I — implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais".

[21] Como as informações adicionais que permitiriam a identificação do titular são mantidas separadamente e em posse dos agentes de tratamento, terceiros terão maior dificuldade em reverter a anonimização.

[22] Artigo 5º da LGPD. Art. 5º: "Para os fins desta Lei, considera-se: […] XVI — uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados".

Por exemplo, é muito comum que organizações se associem, mediante o compartilhamento e cruzamento de dados, para pesquisas científicas e outras atividades econômicas. Imagine o seguinte cenário:

a) uma pesquisa cujo objetivo é mensurar a eficácia de um determinado tratamento médico;
b) de antemão, reconhece-se ser necessário que a amostra de pessoas deve ser a mais ampla com objetivo de capturar pacientes com características distintas;
c) então, se faz necessária uma análise que envolva um conjunto de hospitais e clínicas médicas que trataram grupos de pacientes com diferentes perfis;
d) também se nota, desde logo, ser desnecessário o compartilhamento das bases de dados brutas (*raw data*), as quais identificariam diretamente cada um dos pacientes;
e) seria necessário apenas a indicação do perfil dos pacientes, os quais seriam agrupados de acordo com características semelhantes sem os tornar identificáveis *a priori*;
f) diversos testes de reidentificação foram executados, a fim de se assegurar e ser certificada a razoabilidade das técnicas de anonimização empregadas que correspondem ao estado atual da arte.

Apesar de a situação hipotética descrever um cenário no qual a pesquisa rodaria em cima de uma base de dados anonimizada (critério objetivo – item "e"), isso por si só não encerraria a discussão acerca dos riscos de reidentificação. Deve-se verificar, ainda, se algum hospital ou clínica participante poderia lançar mão de "meios próprios" capazes de reverter o processo de anonimização da base como um todo. Mais uma vez, entra em cena uma análise subjetiva que é focada na capacidade de um agente em específico. Pense, por exemplo, que um dos hospitais deteria uma alta capacidade de entropia de informação, em razão de: **a)** deter uma série de informações adicionais por conta da sua capilaridade no setor com atendimento a grande parte da população representada no estudo; **b)** possuir tecnologias de processamento de dados disruptivas, que superam os padrões praticados até então no setor.

Dessa forma, também é relevante observar a capacidade subjetiva de terceiros que ingressem no fluxo informacional de uma organização. Especialmente, quando se tem em vista atividades de enriquecimento de dados que envolvam agentes externos para viabilizar uma atividade de tratamento de dados.

Em síntese, o legislador brasileiro adotou uma estratégia normativa alinhada à premissa de que os dados anonimizados seriam sempre passíveis de reversão. Os dois eixos de análise acima descritos – objetivo e subjetivo – compõem uma matriz de risco[23] em torno de possíveis engenharias reversas de um processo de anonimização. A *resiliência* de tal processo é o que determinará se haverá algum tipo de intersecção entre dados anonimizados e dados pessoais, cujos elementos de análise são de ordem objetiva (razoabilidade) e subjetiva (meios próprios).

[23] Sobre a estratégia regulatória baseada no risco e, em particular, relacionada ao conceito de dado pessoal e dado anonimizado, veja-se: RUBINSTEIN, Ira; HARTZOG, Woodrow. Anonymization and risk. *91 Washington Law Review*, Washington, DF, v. 703, 2016; *NYU School of Law, Public Law Research Paper*, Nova York, n. 15-36. Disponível em: http://bit.ly/2TKMmo8. Acesso em: 20 jan. 2020.

3. Exemplificando alguns fatores de risco: os enigmáticos termos "no momento" e "ocasião" do tratamento

Ao invés de considerar anonimização como algo cujo resultado (*output*) é infalível, foca-se em uma abordagem que considera a aplicação sistemática de técnicas de anonimização com o objetivo de agregar consistência ao processo como um todo[24]. Por essa razão, a análise acerca de se um dado deve ser, de fato, considerado como anonimizado é eminentemente *circunstancial*. Os dois critérios de análise – objetivo e subjetivo – acima mencionados, ganharão vida somente a partir do contexto no qual está inserida uma atividade de tratamento de dados, sobre a qual se busca retirar, ao máximo, seus respectivos identificadores.

Aliás, não é por outra razão que a LGPD amarra o conceito de dado anonimizado e anonimização, respectivamente, à "ocasião" e ao "momento" no qual se dá uma atividade de tratamento de dados pessoais. Na medida em que a definição de atividade de tratamento de dados engloba nada mais do que 20 (vinte) ações,[25] tudo o que é feito com um dado, o processo de anonimização deve representar um conjunto de ações contínuo e logicamente ordenado que abrace toda a extensão do ciclo de vida de um dado – da coleta ao descarte.

A título de exemplo, listam-se ao menos 06 (seis) fatores de risco (RUBINSTEIN; HARTZOG, 2015) e algumas medidas de mitigação:

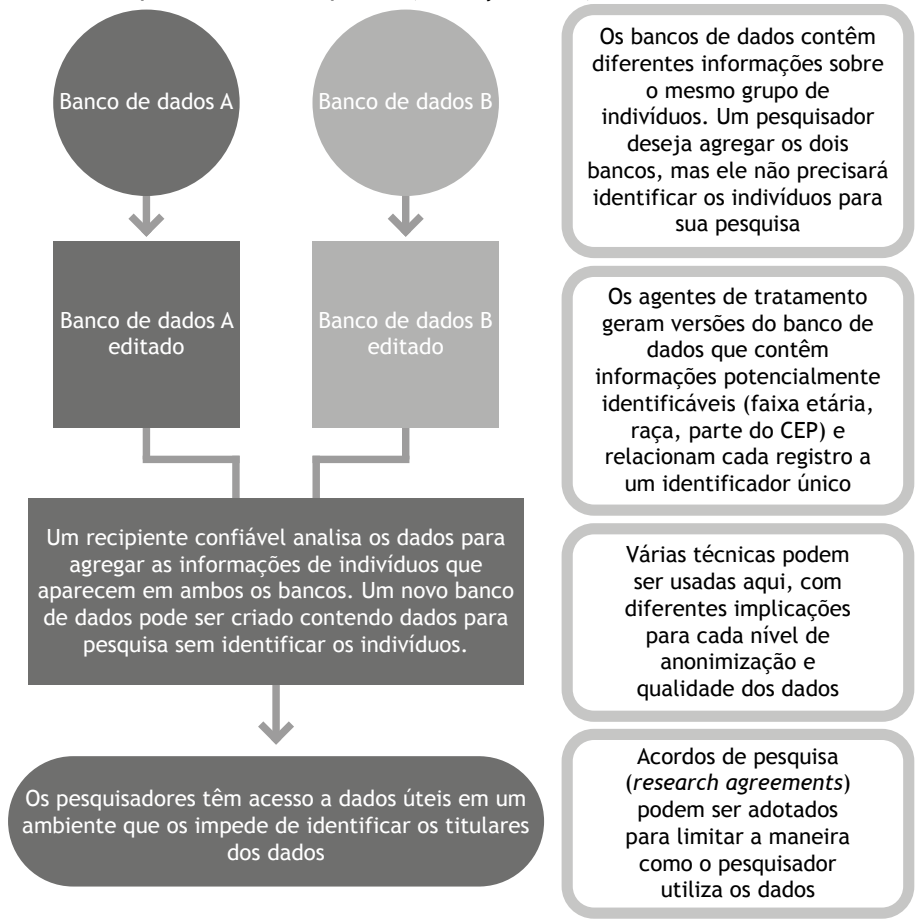
a) **Volume dos dados**: quanto maior for a quantidade de dados, maiores são as chances de alguém fazer o caminho inverso de um processo de anonimização. Desta forma, modelos de negócios, produtos ou serviços e, até mesmo, políticas públicas (incluindo de dados abertos) que envolvam grandes massas de dados devem proporcionalmente apresentar técnicas de anonimização correspondentes aos altos riscos de reidentificação em jogo;
b) **Natureza dos dados:** a natureza do dado (e.g., saúde, financeiro, geolocalização etc.) é determinante sobre o quão valiosas são eventuais informações que dele podem ser extraídas. Com isso, o apetite de terceiros e o quão recompensador seria reverter um processo de anonimização impulsiona os seus respectivos riscos de reidentificação;
c) **Cadeia da atividade de tratamento de dados (recipientes, compartilhamento e uso compartilhado)**: em muitas situações há uma complexa cadeia de atores para viabilizar um modelo de negócio ou mesmo uma política pública. Em regra, quanto maior for o ingresso de entidades para a geração ou mesmo o uso de uma base de dados anonimizada, mais elevado será o risco de sua reidentificação. Isto porque, não se aumenta apenas o volume do fluxo informacional (item "a"), como, também, a população que dele participa. Por exemplo, no caso acima mencionado relacionado à pesquisa científica, é comum se utilizar dos chamados "recipientes confiáveis". Esses são terceiros no qual organizações,

[24] Ao se considerar todo o ciclo de vida dos dados em sua divulgação, a análise (e preocupação) se desloca *do dado* – i.e. seus atributos, qualidades e riscos em determinado momento – para *o processo* – i.e. a realização de um conjunto de ações voltado à proteção da informação durante toda o seu processamento. RUBINSTEIN, Ira S. e HARTZOG, Woodrow. Anonymization and risk. *New York University Public Law and Legal Theory Working Papers 530*, 2015.

[25] Artigo 5º da LGPD: "Art. 5º Para os fins desta Lei, considera-se: […] X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração".

que desejam gerar uma nova base de dados (anonimizado) a partir dos seus bancos de informações, confiam a sua execução. Uma espécie de filtro com relação a quem deteria poder informacional para reverter o processo de anonimização. Nesse caso, o ingresso do terceiro no fluxo informacional se dá justamente para tornar mais resiliente o processo de anonimização.

Figura 1 — Information Commissioner's Office. Anonymisation: managing data protection risk code of practice. 2012. p. 42. (tradução livre)



d) **Gerenciamento de identidades e segmentação**: tão importante quanto colocar em prática processos de pseudoanonimização, é, também, controlar quem acessa as informações adicionais capazes de revertê-los. Por isso, é o caso de não só segregar fisicamente, mas, também, logicamente as bases de dados de uma organização (vide: exemplo supramencionado sobre uma rede varejista). Dessa forma, os riscos (internos) de reidentificação também passam a ser menores, na medida em que se reduz o número de atores que teria capacidade de juntar as peças do quebra-cabeça para formar a imagem dos titulares da informação. Nesse sentido, é importante destacar que o Decreto do Marco Civil da Internet (Decreto 8.771/2016) já determina a adoção de mecanismos

de gerenciamento de identidade a uma base de dados, inclusive com a previsão de sistemas de autenticação dupla e a individualização do respectivo usuário[26].

e) **Cláusulas contratuais**[27]: na medida em que fluxo informacional envolva cada vez mais agentes, em particular quando há o compartilhamento de dados para extração de informações, com ou sem os chamados "recipientes confiáveis", é cada vez mais comum cláusulas que: **a)** proíbam as partes de reverterem o processo de anonimização; **b)** delimitem o papel de cada um dos agentes de tratamento de dados de acordo com o objeto da atividade de tratamento de dados e, adicionalmente, vedando ou condicionando o repasse a terceiros que executariam tal atividade em nome de uma das partes; **c)** a destruição dos dados tão logo seja concluída a atividade de tratamento de dados ou caso haja a resolução de alguma condição pactuada;

f) **Atualização contínua**: anonimização é algo inacabado e fluido tal como é a própria definição da atividade de tratamento de dados, a qual procura capturar os dados em todos os seus movimentos. Ao expressamente correlacionar o conceito de dado anonimizado e anonimização ao "momento" e de acordo com a "ocasião" na qual um dado está sendo processado, a LGPD procurou deixar claro que as técnicas de anonimização devem considerar toda a jornada de um dado e, sobretudo, ser constantemente atualizadas. Por exemplo, não adiantará um contrato de processamento de dados, que especificou todas as técnicas de anonimização e inclusive a forma pela qual os "recipientes confiáveis" as colocariam em prática, se esse contrato foi firmado há bastante tempo e tais medidas já se encontram defasadas. O *continuum* de uma atividade de tratamento de dados, espelhado por nada mais do que 20 (vinte) ações diferentes, também deve nortear a *dinamicidade* com a qual se empregam técnicas de anonimização[28].

Com isso, o legislador convida os agentes de tratamento de dados a conceberem e aplicarem as melhores técnicas de anonimização de acordo com as particularidades das suas respectivas atividades. É uma empreitada multifacetada, de ordem técnica, organizacional e, inclusive, contratual com o objetivo de controlar os riscos associados à reidentificação de uma determinada atividade de tratamento de dados.

---

[26] Artigo 13 do Decreto 8.771/2016. Art. 13: "Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança: I – o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários; II – a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros; III – a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e IV – o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes".

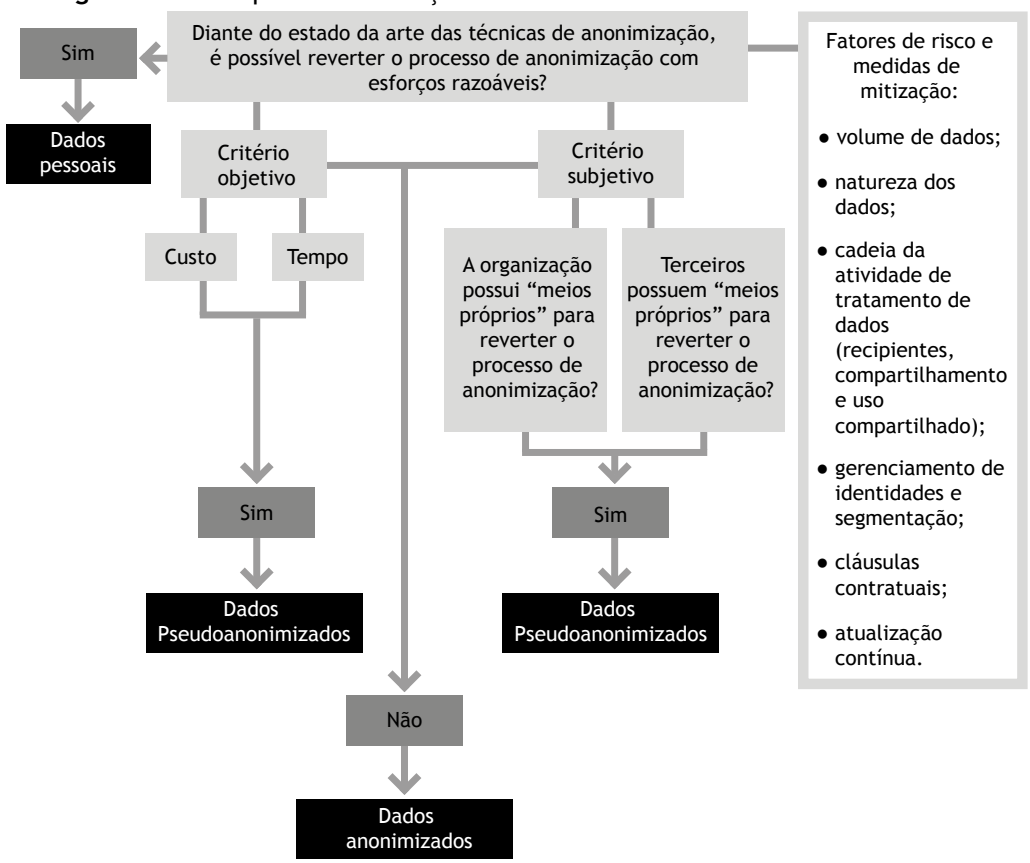
[27] FTC. *Protecting consumer privacy in an era of rapid change*: recommendations for businesses and policymakers, 2012; ROSENFELD, Dana B.; HUTNIK, Alysa Zeltzer. Data security contract clauses for service provider arrangements (pro-customer). *Practical Law Company*, 2011.

[28] Nesse sentido, uma das práticas previstas para se avaliar condutas pelo Modelo de Maturidade de Privacidade (*Privacy Maturity Model*), criado pelo Instituto Americano dos Contadores Públicos Certificados e pelo Instituto Canadense de Contadores (AICPA/CICA), é a otimização, i.e. "a revisão e a avaliação periódicas são utilizadas para garantir a melhoria contínua de determinado processo". Disponível em: http://bit.ly/2RA0FZP. Acesso em: 20 jan. 2020. A aplicação desse modelo de análise (e a conformidade especificamente a essa prática) foi observada no tratamento de dados pessoais efetuado pela municipalidade de Seattle. Ver: Future of Privacy. City of Seattle: Open data risk assessment, 2018. Disponível em: http://bit.ly/37cEuPP. Acesso em: 20 jan. 2020.

4. Conclusão: modelo analítico acerca do processo de anonimização de um dado

A análise acerca de se a natureza de um dado pessoal, submetido a um processo de anonimização, pode ser transmudada envolve uma série de elementos. O teste da Figura 2 agrupa logicamente os 07 (sete) critérios normativos prescritos pela própria LGPD e, ainda, lista, paralelamente, uma série de fatores, com base na literatura revisada, que ajudam na identificação do quão tolerável (razoável) são os riscos de reversão das técnicas de anonimização aplicadas.

Figura 2 — Entropia de Informação



5. Bibliografia

ARTICLE 29 WORKING PARTY. *Opinion 04/2007 on the concept of personal data*. Disponível em: http://bit.ly/2G99aFY. Acesso em: 20 jan. 2020.

BAPTISTA, Patrícia; KELLER, Clara. Por que, quando e como regular as novas tecnologias? Os desafios trazidos pelas inovações disruptivas. *Revista de Direito Administrativo*, Rio de Janeiro, v. 273, p. 123-163, 2016.

BIONI, Bruno Ricardo. *Xeque-mate*: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil. São Paulo: GPoPAI-USP, 2016.

BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

COUNCIL OF EUROPE. *Handbook on European data protection law*. Luxemburgo: Publications Office of the Europe Union, 2018. Disponível em: http://bit.ly/30OT26d. Acesso em: 20 jan. 2020.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

HOUAISS, Antônio; VILLAR, Mauro de Salles. *Dicionário Houaiss da língua portuguesa*. Rio de Janeiro: Objetiva, 2009.

KOOPS, Bert-Jaap. Should ICT regulation be technology-neutral? *In*: KOOPS, Bert-Jaap; LIPS, Miriam; PRINS, Corien; SCHELLEKENS, Maurice (ed.). *Starting points for ICT regulation*: deconstructing prevalent policy one-liners. The Hague: TMC Asser Press 2006. v. 9, p. 77-108. (IT & Law Series). ISBN 90-6704-216-1.

MOSES, Lyria Bennett. How to think about law, regulation and technology: problems with 'technology' as a regulatory target. *Law, Innovation and Technology*, Abingdon-on-Thames, v. 5, n. 1, p. 1-20, 2013.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and fallacies of "personally identifiable information". *Communications of the ACM*, Nova York, v. 53, n. 6, p. 24-26, 2010. Disponível em: http://bit.ly/30G9CVq. Acesso em: 20 jan. 2020.

REED, Chris. Taking sides on technology neutrality. *SCRIPT-ed*, Edimburgo, v. 4, n. 3, p. 263-284, 2007.

RUBINSTEIN, Ira S.; HARTZOG, Woodrow. Anonymization and risk. *New York University Public Law and Legal Theory Working Papers 530*, Nova York, 2015.

TEIXEIRA, Lucas. Teoricamente impossível: problemas com a anonimização de dados pessoais. Disponível em: http://bit.ly/367kuwQ. Acesso em: 20 jan. 2020.

TENE, Omer. Privacy law's midlife crisis: a critical assessment of the second wave of global privacy laws. *Ohio State Journal*, Columbus, v. 74, n. 6, p. 127-1262, 2013.

Coordenação editorial
Marcelo Alexandre Barbosa

Capa
Esmeralda Luana Wonke Scopesi

Editoração, revisão, impressão e acabamento
Tikinet

Revisão
Camila Corrêa | Tikinet
Maísa Kawata | Tikinet

Diagramação
Marcus Gisolfi | Tikinet

Formato
175 x 245 mm

Mancha
140 x 210 mm

Tipologia
Trebuchet MS

Papel
Capa: Cartão Revestido 250g/m^2
Miolo: Offset Branco 75g/m^2

Acabamento
Cadernos de 16pp.
costurados e colados – brochura

Tiragem
700 exemplares

Março de 2020