A LEI GERAL DE PROTEÇÃO DE DADOS: NOÇÕES GERAIS

Luiz Carlos Buchain

RESUMO

A LGPD tem por objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A "sociedade de informações" extrai dos cidadãos uma gama crescente de dados pessoais que são oferecidos "gratuitamente" aos fornecedores de bens e serviços. Os dados pessoais são direitos de personalidade que decorrem do princípio geral da dignidade da pessoa humana.

Daí decorre que o controle e disponibilização dos dados pessoais na *web* tornou-se um grande desafio para a sociedade a medida em que, através da *internet*, é possível detectar as preferências do usuário. O que se leva em conta é a possibilidade de grupos empresariais e do próprio governo conquistarem poder econômico e politico sobre o indivíduo a partir da disponibilidade de suas informações. Aqui está em jogo a limitação e a legitimação do controle de dados pessoais e a tutela das liberdades individuais e a eficiência administrativa e empresarial.

Assim, são dois conceitos contraditórios em questão: o respeito aos direitos fundamentais dos indivíduos e o exercício da livre empresa. Ao mesmo tempo em que estimula o mercado de dados, a lei o regula de forma a garantir aos indivíduos o controle sobre seus dados.

O quadro jurídico para proteção de dados pessoais, através da legislação específica, tem sua eficácia, em larga medida, dependente da eficiência da Autoridade Nacional de Proteção de Dados (ANPO) e do Conselho Nacional de Proteção de Dados pessoais e privacidade.

PALAVRAS-CHAVE

Dados. Proteção de dados. Controlador. Operador. Titular. Informação.

Luiz Carlos Buchain

Possui graduação em Ciências Jurídicas e Sociais pela Pontifícia Universidade Católica do Rio Grande do Sul (1986), mestrado em DIREITO CIVIL pela Universidade Federal do Rio Grande do Sul (1996) e doutorado em DIREITO ECONÔMICO pela Universidade Federal do Rio Grande do Sul (2005). Atualmente é professor adjunto II da Universidade Federal do Rio Grande do Sul e advogado - Buchain Sociedade Individual de Advocacia.

INTRODUÇÃO

1. CAMPO DE APLICAÇÃO MATERIAL

1.1 OPERAÇÕES SUBMETIDAS AO REGIME LEGAL
1.1.1. A NOÇÃO DE "DADOS PESSOAIS"
1.1.2. A NOÇÃO DE "TRATAMENTO"
1.1.3. A NOÇÃO DE "ARQUIVO"

1.2. AS PESSOAS SUBMETIDAS AO REGIME LEGAL
1.2.1 O "TITULAR"
1.2.2 O "CONTROLADOR" e SUA DEFINIÇÃO
1.2.2.1 MÉTODO DE AUTENTICAÇÃO e RESPONSABILIDADE
1.2.3 O "OPERADOR"
1.2.4. O TERCEIRO

1.3. O CAMPO DE APLICAÇÃO TERRITORIAL

CONCLUSÃO

BIBLIOGRAFIA

INTRODUÇÃO

A LGPD tem por objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A proteção de dados pessoais[1] não se reduz somente a proteção da vida privada, com a qual está intimamente ligada mas, também, com a liberdade e o livre desenvolvimento da personalidade da pessoa natural. A Constituição de 1988, ao reconhecer o princípio da dignidade humana[2] (art. 1º, III) protegeu todos os direitos de personalidade, além de positivar garantias como o direito à liberdade de expressão (art. 5º, IX), o direito à informação (art. 5º, XV), a inviolabilidade da vida privada,[3] a intimidade (art. 5º, X), a garantia de Habeas Data (art. 5º, LXXII), a proibição de invasão de domicílio (art. 5º, XI) e a violação de correspondência (art. 5º, XII).

A atual "sociedade de informações" em que vivemos, intimamente ligada à utilização das Tecnologias de Informação e Comunicações – TIC – conhecidas como o acesso à *internet*, telefones móveis, televisão interativa, entre outros, extraem dos cidadãos/usuários uma gama crescente de dados pessoais que são

1 Danilo Doneda ensina que nem todo dado é considerado pessoal. Sua caracterização como pessoal exige a característica fundamental de ter um vínculo com a pessoa e revelar um aspectos objetivos de seu titular: "Este vínculo significa que a informação se refere às características ou ações desta pessoa, que podem ser atribuídas a ela em conformidade com a lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes ao seu consumo, informações referentes às suas manifestações, como sobre opiniões que manifesta e tantas outras". DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico. Joaçaba, v. 12.n.2, jul./dez. 2011, p.93.

2 É, portanto, em virtude da existência de uma cláusula geral e aberta de proteção e promoção da personalidade, que, no caso brasileiro, tem sido fundada especialmente no princípio da dignidade da pessoa humana, que se adota o entendimento de que o rol de direitos especiais de personalidade (sejam eles previstos na legislação infraconstitucional, sejam eles objeto de reconhecimento expresso na Constituição Federal, não é de cunho taxativo. SARLET, Ingo Wolfgang. Curso de Direito Constitucional, 3ª ed, p. 400. Ed. RT. SP-SP, 2013.

3 Inicialmente, nos EUA, o direito a privacidade se relacionava com a propriedade privada. Num segundo momento, a partir do artigo The Right to Privacy publicado por Samuel D. Warren e Louis D. Brandeis (1890), a privacidade passou a ser relacionada a proteção à inviolabilidade da personalidade. Assim, "o princípio que protege escritos pessoais e outras produções pessoais, não é contra o furto ou a apropriação física, mas contra toda forma de publicação, é na realidade não o princípio da propriedade privada, mas o da inviolabilidade da personalidade". Shapiro, 1996 apud DONEDA, Danilo. Da privacidade à Proteção dos dados Pessoais. Rio de Janeiro. Renovar. 2006.

oferecidos "gratuitamente" aos fornecedores de bens e serviços. Os dados pessoais são direitos de personalidade que decorrem do princípio geral da dignidade da pessoa humana[4]. Ademais, os dados podem ser utilizados para fins contrários ao Direito e a moral, como forma de perseguição política ou opressão econômica. Além disso, os dados coletados podem ser incorretos e representar erroneamente uma pessoa.

A TIC permite que uma infinidade de informações e dados dos cidadãos sejam extraídos da *web* justamente porque o funcionamento da rede é caracterizado por uma ampla liberdade de expressão e inclusão de dados pessoais, de forma que até mesmo os hábitos e preferências do usuário da *web* podem ser colecionados pelos fornecedores de bens e serviços. Trata-se do *superinformacionismo*[5], caracterizado pela imensa quantidade de informações que circulam na internet, permitindo facilmente a obtenção de rápidas informações sobre qualquer assunto ou pessoa.

Daí por que o controle e disponibilização dos dados pessoais na *web* tornou-se um grande desafio para a sociedade a medida em que, através da *internet*, é possível detectar as preferências do usuário, sejam artísticas, musicais, hábitos de vida, viagens, orientação sexual, crenças religiosas, etc. O que se leva em conta é a possibilidade de grupos empresariais e do próprio governo conquistarem poder econômico e politico sobre o indivíduo a partir da disponibilidade de suas informações. O grande desafio em questão é a limitação e a legitimação[6] do controle de dados pessoais[7] como forma de equilibrar as relações entre a tutela das liberdades individuais e a eficiência administrativa e empresarial.

Embora a proteção aos direitos e garantias fundamentais previstos na CF/88 tenham aplicação imediata (art. 5º, §1º da CF), e que tais direitos e garantias possam ter sua raiz identificada no princípio da dignidade da pessoa humana - verdadeira cláusula geral constitucional de tutela e promoção da pessoa humana - o fato é que a autoaplicabilidade das regras constitucionais não se mostram suficientes para garantir o efetivo direito dos cidadãos à proteção de seus dados. Essa estreita relação entre dignidade, privacidade e liberdade exige do poder público uma robusta tutela das informações relativas as pessoas tanto para afastar terceiros da esfera privada quanto para garantir os direitos fundamentais do cidadão.

4 "A tutela da personalidade – convém, então, insistir – não pode se conter em setores estanques, de um lado os direitos humanos e de outro as chamadas situações jurídicas de direito privado. A pessoa, à luz do sistema constitucional, requer proteção integrada, que supere a dicotomia direito público e direito privado e atenda à cláusula geral fixada pelo texto maior, de promoção da dignidade humana". A tutela da personalidade no ordenamento civil – constitucional brasileiro. TEPEDINO, Gustavo. https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil-constitucional_brasileiro Acesso em 06 de junho de 2019

5 Diz-se que a informação passou a ser insumo da produção, possuindo um papel tão importante quanto a força de trabalho e o capital.

6 A legitimação à obtenção da informação está intimamente ligada com o princípio do CONSENTIMENTO na utilização de dados pessoais. Art. 7º, I e art. 8º, § 5º da LGPD.

7 A necessidade de se proteger juridicamente os dados pessoais do cidadão se origina do fato de que dados possuem um grande valor econômico, possibilitando sua comercialização. As novas técnicas de informática conferem à intimidade um novo conteúdo. Os dados traduzem dados de personalidade e revelam comportamentos e preferências do cidadão, o que permite traçar um perfil psicológico e comportamental do indivíduo.

De outra forma, tanto o direito comum[8] quanto o direito civil, o CDC[9] ou mesmo o Marco Civil da Internet (lei 12.965/14), se revelaram insuficientes para abranger todas as hipóteses em que os dados merecem tratamento, especialmente porque a legislação citada não abarca toda a esfera de proteção necessária da vida privada: não conferem a pessoa natural a possibilidade de se opor a coleta de dados, de ter acesso aos dados e nem mesmo ser informado sobre a natureza e finalidade do tratamento de seus dados.

Empresas utilizam-se desses dados para produzir a chamada *publicidade comportamental* e desenvolver novas maneiras de rastrear os consumidores. Ao obter essas informações essenciais[10] para sua publicidade seletiva (realizada a partir dos dados coletados, em especial na *internet* e seu histórico de navegação) estas tornam-se a uma importante fonte de renda de diversas empresas.

Entretanto, é importante notar que o próprio legislador promoveu o diálogo entre a Lei Geral de Proteção de Dados Pessoais e o CDC, ao expressamente prever como fundamento da proteção de dados a defesa do consumidor (art. 2º, VI); ao estabelecer a possibilidade de que os direitos dos titulares de dados, quando também consumidores, possam ser igualmente exercidos perante organismos de defesa do consumidor (art. 18, § 8º); e ao determinar (art. 45) que as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. Por fim, a complementariedade das leis é consolidada (art. 64), o qual estabelece que os direitos e princípios expressos na LGPD não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que o Brasil seja parte[11].

Por essas razões, mostrou-se necessário criar um quadro legal específico para a proteção de dados pessoais visando conferir ao cidadão instrumentos legais que lhe permitam proteger-

8 Em legislação esparsa encontra-se diversos dispositivos regulando a proteção de dados. Entre outras, cita-se: CCB, CDC (art. 43), Lei de Interceptação Telefônica/ Telemática (L. 9.96/96), Lei Geral de Telecomunicações (L.9.472/97), lei de Habeas Data (L. 9.507/97), Lei do Sigilo das Operações de Instituições Financeiras (LC 105/01), Lei do Cadastro Positivo (L. 12.414/11), Lei de Acesso as Informações (L. 12.527/11), Lei de Invasão de Dispositivos Informáticos - lei Carolina Dieckman (L. 12.737/12), Marco Civil da Internet (L. 12.965/14) e na Política de Dados Abertos do Governo Federal (D. 8.777/16), Lei do cadastro positivo (Lei n. 12.414/2011, o sigilo dos agentes do fisco (art. 198 do CTN) e LC 105/01, que permite às autoridades administrativas a quebra do sigilo bancário até mesmo sem autorização judicial. Art. 6º da LC 105/2001.

9 Acerca da regulação da matéria pelo CDC, Claudia Lima Marques já afirmava a existência do direito a autoregulação de dados do consumidor: "Um direito de dispor de seus próprios dados pessoais foi positivado pelo CDC e transparece no art. 43, §§ 2º e 3º. O consumidor brasileiro tem direito de dispor de seus dados pessoais, de acessá-los e de saber que estes existem em algum banco de dados público ou privado...". Lima Marques, Claudia. Contratos no código de defesa do consumidor. 5ª ed. Ed. RT. SP-SP, 2006. p.829.

10 Há empresas dedicadas até mesmo a rastrear os passos dos consumidores em locais públicos, a partir de sinais de wi-fi de smartphones, fornecendo subsídios aos empresários para traçar o perfil dos consumidores visando oferecer-lhes produtos e serviços. Trata-se do FX Flow Intelligence. Conforme https://portalnovarejo.com.br/2015/09/7-tecnologias-para-monitorar-habitos-de-consumo/ acesso em 07/05/2019.

11 Conforme ensina Cláudia Lima Marques, deve-se aplicar a teoria do diálogo das fontes para aplicação simultânea de toda a legislação sobre o assunto. O diálogo das fontes é definido como sendo "a aplicação simultânea, coerente e coordenada das plúrimas fontes legislativas, leis especiais (como o Código de Defesa do Consumidor, a lei de seguro-saúde) e gerais (como o CC/2002 (LG/2002/400)), com campos de aplicação convergentes, mas não mais iguais". MARQUES, Claudia Lima; et al., Manual de Direito do Consumidor. São Paulo: Ed. RT, 2008, p. 85-88.

se contra o abuso da exploração dos dados pessoais[12].

A generalização do uso da informática e da coleta de dados pessoais criou um novo e crescente mercado para sua troca entre agentes econômicos e, ao mesmo tempo, criou novos riscos tanto para a vida privada[13] quanto, de uma maneira mais genérica, aos direitos e liberdades individuais. Além disso, esse novo modelo econômico de economia digital, cujos exemplos globais são o *Goggle* (buscas na internet) e o *Facebook*[14] (redes sociais), está fortemente apoiado na exploração do comércio de dados, exigindo da sociedade a criação de um instrumento legislativo para regular esse verdadeiro mercado digital.

O direito de acesso e conhecimento dos dados pessoais abarca diversas posições jurídicas, conforme ensina Ingo Sarlet[15], expostas como sendo "a) o direito de acesso e conhecimento dos dados pessoais existentes em registros (bancos de dados); b) direito ao não conhecimento, tratamento, utilização e difusão de determinados dados pessoais pelos Estado ou por terceiros, aqui incluído o direito de sigilo quanto aos dados pessoais; c) direito ao conhecimento da identidade dos responsáveis pela coleta, armazenamento, tratamento e utilização dos dados; d) o direito ao conhecimento da finalidade da coleta e eventual utilização dos dados; e) direito a ratificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados".

Assim, são dois conceitos contraditórios[16] em questão – o respeito aos direitos fundamentais dos indivíduos em face da liberdade de circulação de dados e exercício da livre empresa[17] no mercado – que a nova legislação visa conciliar. Ao mesmo tempo em que estimula o mercado de dados (em especial o digital), o regula de forma a garantir aos indivíduo o controle sobre seus dados.[18] A

12 A LGPD, conforme disposto em seu artigo 18, garante aos indivíduos o direito de autodeterminação, ou seja, o direito a decidir por si próprio quando e dentro de quais limites seus dados pessoais poderão ser utilizados.

13 "Em causa, portanto, está o controle por parte do indivíduo sobre as informações que em princípio apenas lhe dizem respeito, por se tratar de informações a respeito de sua vida pessoal, de modo que se poderá mesmo dizer que se trata de um direito individual ao anonimato." SARLET, Ingo Wolfgang. Curso de Direito Constitucional, 3ª ed, p. 409. Ed. RT. SP-SP, 2013

14 O Facebook chegou a 127 milhões de usuários no Brasil. Conforme http://agenciabrasil.ebc.com.br/economia/noticia/2018-07/facebook-chega-127-milhoes-de-usuarios-no-brasil Acesso em 07/05/2019

15 SARLET, Ingo W; MARINONI, Luiz Guilherme: MITIDIERO, Daniel. Curso de Direito Constitucional. São Paulo, Revista dos Tribunais, 2014, p. 433/434.

16 Exemplifica o conflito entre os direitos fundamentais e a livre circulação de dados a decisão proferida em sede de apelação em ação coletiva proposta pelo Ministério Público, (AC 70069420503), Rel. Des. Ney Weidmann Neto, disponível em: www.tjrs.jus.br. Acesso em 07/05/2019, que não há abusividade na coleta de dados por empresas destinadas a formação de banco de dados dos consumidores, destinados a prospecção de cliente, ações de marketing e telemarketing. O fundamento empregado à decisão foi o de que os dados coletados e comercializados, apesar de serem privativos, "são comumente fornecidos por qualquer cidadão na prática dos atos da vida civil, não se tratando de informações de natureza totalmente sigilosa ou confidencial. Não há, no caso, qualquer ofensa à privacidade ou a qualquer outro direito fundamental dos consumidores." Aqui o TJRS não abordou a questão da autodeterminação informativa, sendo o julgamento anterior a vigência da LGPD.

17 "Por outro lado, como os direitos fundamentais irradiam efeitos imediatos, ou horizontais, para as relações interpessoais entre entes privado, pode haver conflito ou colisão com outros direitos fundamentais, como o direito à propriedade, à liberdade de contratar ou à liberdade de exercício de trabalho ou profissão." CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo. Vol. 13/2017, p. 59-67. Out-Dez 2017

18 Aqui vale lembrar que a LGPD adota o princípio da finalidade (também chamado de princípio da autodeterminação informativa), ou seja, os dados pessoais coletados são ou devem ser destinados a um fim específico onde haja correlação necessária entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. Trata-se, pois,

autodeterminação veda sua utilização para fins outros que não aquele para os quais o titular ofereceu seu expresso consentimento.

O quadro jurídico para proteção de dados pessoais[19], através da legislação específica, tem sua eficácia, em larga medida, dependente da eficiência da Autoridade Nacional de Proteção de Dados (ANPO) e do Conselho Nacional de Proteção de Dados pessoais e privacidade.

1. CAMPO DE APLICAÇÃO MATERIAL

O objeto de proteção conferida pela lei 13.709/18 está circunscrito num campo de aplicação material e territorial.

A proteção de dados se aplica a todo o universo de operações de tratamento de dados pessoais, com as exceções previstas no art. 4º da LGPD. Dentre as exceções previstas na lei temos: *(i)* o uso não econômico de dados por pessoa física, *(ii)* dados realizados para fins jornalísticos, artísticos ou acadêmicos e *(iii)* dados utilizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão a infrações penais. Há ainda a hipótese de exceção prevista no inciso IV do art. 4º da LGPD, segundo o qual não se aplica a lei aos dados "provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.".

1.1. OPERAÇÕES SUBMETIDAS AO REGIME LEGAL

A nova lei se aplica, de um lado, ao tratamento automatizado de dados pessoais e, de outro, a tratamentos não automatizados, ou seja, aqueles ainda realizados através de fichários ou meios similares. Inicialmente deve-se definir algumas noções:

1.1.1. A NOÇÃO DE "DADOS PESSOAIS"

A lei define "dado pessoal" como informação relacionada a pessoa natural identifica ou identificável"(art. 5º, I)[20] e, de outro lado, como "dado pessoal sensível" aquele sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dados genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II).

Sob outro aspecto, a lei considera não identificável, ou "anonimizado", os

de um desdobramento do direito à privacidade.

19 Exemplo de normas de primeira geração são as leis do Estado Alemão Hesse (1970), a lei de dados da Suécia (1973), o Estatuto de Proteção de Dados do Estado alemão de Rheiland-Pfalz (1974) e a lei federal de Proteção de Dados da Alemanha (1977). Nos EUA foram aprovados, nesse mesmo período, o Fair Credit Reporting Act (1970), o Freedom for Information Act (1966) e o Privacy Act (1974). Em 1976, Portugal foi o primeiro país a estabelecer em sua constituição o direito fundamental à autodeterminação informativa (art. 35).

20 Segundo a teoria do mosaico, é irrelevante o fato de a informação do indivíduo pertencer à esfera da intimidade e vida privada, pois o que interessa é sua utilização. Assim, há dados que possuem aparência de inofensivos à violação, porém, quando colocados com outros dados, apresentam risco de violação da privacidade do cidadão. Nesse sentido BARROS, Bruno M. Correa de, OLIVEIRA, Clarissa T. Lovatto, SANTOS, Rafael de. O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais. Revista Videre, Dourados, MS, v.9, n.17.1. semestre de 2017. p. 21.

dados relativos a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5º, III). Assim, dados identificadores, tais como um endereço IP, é suscetível de identificar, ao menos indiretamente, uma pessoa física. O endereço IP é exemplo de dado pessoal porquanto existem meios técnicos e legais que permitem ao provedor de internet obter os dados cadastrais de um determinado usuário, através de seu endereço IP.

1.1.2. A NOÇÃO DE "TRATAMENTO"

A noção de "tratamento" é definida pela lei (art. 5º, X) como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, transferência, difusão ou extração."

Além da clara extensão da lista de operações qualificadas como "tratamento" , é preciso notar que a redação adotada pelo legislador (empregando a expressão "como as que se referem ...") confere a esta lista uma natureza ilustrativa e não limitativa, atribuindo a essa definição um caráter extremamente largo. Na realidade, nenhuma operação escapa do conceito de "tratamento" tendo ela por objeto dados pessoais. Apenas nas hipóteses em que a operação em tratamento se valha de outros dados, tais como dados anonimizados, por exemplo, será possível excluir a incidência da Lei Geral de Proteção de Dados.

Assim, está posto pela lei que toda e qualquer operação, não importando sua natureza, mas que colha dados pessoais, constitui um bem sob "tratamento"[21].

Além disso, estão excluídos do regime de proteção de dados pessoais: a) tratamento de dados realizado por pessoa natural para fins exclusivamente particulares e não econômicos ou, b) realizados para fins exclusivamente jornalísticos, artísticos e acadêmicos. Já as atividades de segurança pública, defesa nacional, segurança do Estado

ou investigação e repressão de infrações penais serão ser regidos por legislação específica que deverá observar o princípio da necessidade e proporcionalidade no trato dos dados, além do devido processo legal e a proteção e os direitos do titular previstos na lei 13.709/18.

1.1.3. A NOÇÃO DE "ARQUIVO"

A nova lei se aplica ao "tratamento de dados pessoais, inclusive nos meios digitais..."(art. 1º), o que abrange tanto o tratamento de dados automatizados (digitais) quanto aqueles consubstanciados em arquivos não automatizados. Nota-se que a preocupação do legislador foi a de estender a proteção de dados a todos os meios possíveis, independentemente da tecnologia utilizada para o tratamento.

A definição de "arquivo" pode ser dada como sendo todo o conjunto de dados

21 Quanto a tutela do sigilo de dados previsto na CF/88 e seu âmbito de aplicação, devemos lembrar a decisão do STF que, ao julgar o HC 83.168-1, rel. Min. Sepúlveda Pertence, reafirmou seu entendimento de que o inciso XII do art. 5º da Constituição protege a comunicação de dados, e não os dados em si mesmos. Esta interpretação tem sido criticada por dificultar o reconhecimento do direito fundamental à proteção de dados pessoais.

organizados, ainda que esta organização seja temporária ou desprovida de estabilidade no tempo e independentemente da tecnologia empregada no tratamento.

1.2. AS PESSOAS SUBMETIDAS AO REGIME LEGAL

O objetivo da lei é "proteger os direitos fundamentais de liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural"[22] cujos dados são objeto de tratamento, impondo obrigações a todas as pessoas intervenientes nesse tratamento: controlador e operador (agentes de tratamento) e encarregado.

1.2.1 O "TITULAR"

Segundo a LGPD, o "titular" é a pessoa natural[23] a quem se referem os dados pessoais que são objeto de tratamento", ou seja, a pessoa física identificada ou identificável. (art. 5º, V).

O titular dispõe do direito básico à proteção de dados pessoais em dupla dimensão: a) tutela da personalidade contra os riscos que ameacem sua personalidade em face da coleta, processamento, utilização e circulação dos dados pessoais, e, b) a atribuição ao titular do direito a garantia do poder de controlar o fluxo de seus dados na sociedade. Esse conceito envolve tanto um aspecto subjetivo (controle dos dados pelo titular) quando um aspecto objetivo (proteção contra os riscos causados pelo tratamento dos dados pessoais).

Somente as pessoas físicas são objeto da proteção legal. Além disso, para reconhecer-se a legitimidade de uma pessoa física a proteção da LGPD será necessário determinar se os dados tratados permitem sua identificação, direta ou indireta, sem o que o fato não estará submetido ao regime da lei.

Importante questão não tratada pela LGPD é aquela que diz respeito a cessação dos direitos do "titular" pela sua morte, nada especificando se poderiam ou não serem transferidos aos seus herdeiros. É regra aceita no direito nacional a de que os herdeiros do falecido, através de seu espólio, são parte legítima para defender diversos direitos. Assim, aos herdeiros da vítima dos danos decorrentes da "proteção de dados" deverá ser garantida a via legal para obter as reparações devidas.

Nesse sentido há o julgamento da T3 - TERCEIRA TURMA do STJ[24] que versa sobre

22 Inicialmente, o direito a privacidade era compreendido como um fenômeno coletivo, pois os danos causados pelo processamento impróprio dos dados são difusos. Posteriormente, a privacidade, até então compreendida como o "direito a ser deixado em paz" (*right to be alone*), passa a significar o direito de controle dos dados pessoais pelo indivíduo, o qual decide quando e onde seus dados podem circular. (Princípio da autodeterminação). Por fim, a privacidade e a proteção dos dados passa a se vincular a ideia de igualdade, em razão do crescente risco de seu uso com fins discriminatórios pelo Estado ou pelo mercado.

23 "Passou-se a compreender a proteção a autodeterminação informativa como fenômeno não apenas privado, mas, também, coletivo, já que em certas circunstâncias, os danos decorrentes da violação desse direito podem ser caracterizados como difusos, a exigir mecanismos jurídicos de tutela coletiva". CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo. Vol. 13/2017, p. 59-67. Out-Dez 2017.

24 REsp 1209474 / SP
Data do Julgamento 10/09/2013
DJe 23/09/2013
RJP vol. 54 p. 155
RSTJ vol. 232 p. 216
Ementa - RECURSO ESPECIAL. RESPONSABILIDADE CIVIL. DANO MORAL. CONTRATO DE CARTÃO DE CRÉDITO CELEBRADO APÓS A MORTE DO USUÁRIO. INSCRIÇÃO INDEVIDA NOS ÓRGÃOS DE PROTEÇÃO AO CRÉDITO. EFICÁCIA POST MORTEM DOS DIREITOS DA PERSONALIDADE. LEGITIMIDADE ATIVA DA VIÚVA PARA

o direito a indenização da viúva e do espólio por força da inserção de nome de falecido no cadastro de inadimplentes por suposta contratação de cartão de crédito após a morte do usuário. No caso, o aresto atribui legitimidade ativa à viúva para o pedido declaratório de "inexistência de contrato de cartão de crédito" e o respectivo "pedido de indenização" pelos prejuízos decorrentes da ofensa à imagem do falecido marido (aplicação do art. 12, parágrafo único, do Código Civil). Entretanto, o tribunal negou a legitimidade ativa do espólio para o pedido indenizatório, pois o contrato fora celebrado posteriormente a su morte, momento em que a personalidade do *de cujus* já não existia. *Mutatis mutandis*, os herdeiros de pessoa falecida podem ser considerados parte legítima para requerem, por exemplo, a retirada do consentimento dada pelo falecido[25] ao tratamento de seus dados pessoais.

Outra decisão paradigmática da Segunda Seção do STJ (RECURSO ESPECIAL nº 1.304.736 - RS (2012/0031839-3), rel. Min. Luiz Felipe Salomão – regime de recursos repetitivos) diz respeito a dados pessoais tratados por empresas que praticam o sistema de *scoring* (histórico de crédito) - o STJ definiu que não se faz necessária a autorização do consumidor para a tomada de seus dados por empresas que fornecem o serviço de *scoring*[26] de pontuação para fins creditícios. Ao mesmo tempo, a decisão confere aos titulares da informação interesse de agir, para a exibição de documentos, sempre que o titular pretender conhecer e fiscalizar documentos próprios ou comuns de seu interesse e em posse do controlador. O STJ considerou legítimo o sistema de *scoring* pela aplicação do art. 5º, IV, e pelo art. 7º, I, da Lei n. 12.414/2011 (lei do cadastro positivo). Note-se que o disposto no art. 7, X da LGPD expressamente autoriza o tratamento de dados pessoais para a "proteção do crédito", remetendo a matéria para o disposto na legislação pertinente.

Nesse sentido se manifesta Claudia Lima Marques[27] ao afirmar que "a elaboração, organização, consulta e manutenção de banco de dados sobre consumidores e sobre consumo não são proibidas pelo CDC – ao contrário, são reguladas por este, logo, permitidas".

POSTULAR A REPARAÇÃO DOS PREJUÍZOS CAUSADOS À IMAGEM DO FALECIDO. INTELIGÊNCIA DO ARTIGO 12, PARÁGRAFO ÚNICO, DO CÓDIGO CIVIL.
1. Contratação de cartão de crédito após a morte do usuário, ensejando a inscrição do seu nome nos cadastros de devedores inadimplentes.
2. Propositura de ação declaratória de inexistência de contrato de cartão de crédito, cumulada com pedido de indenização por danos morais, pelo espólio e pela viúva.
3. Legitimidade ativa da viúva tanto para o pedido declaratório como para o pedido de indenização pelos prejuízos decorrentes da ofensa à imagem do falecido marido, conforme previsto no art. 12, parágrafo único, do Código Civil.
4. Ausência de legitimidade ativa do espólio para o pedido indenizatório, pois a personalidade do "de cujus" se encerrara com seu óbito, tendo sido o contrato celebrado posteriormente.
5. Doutrina e jurisprudência acerca do tema.
6. Restabelecimento dos comandos da sentença acerca da indenização por dano moral.
7. RECURSO ESPECIAL PARCIALMENTE PROVIDO.

25 Segundo a RGPD em sua consideranda 27: "O presente regulamento não se aplica aos dados pessoais de pessoas falecidas. Os Estados-Membros poderão estabelecer regras para o tratamento dos dados pessoais de pessoas falecidas".

26 A matéria é objeto da súmula 550 editada pela Segunda Seção do STJ. Julgamento em 14/10/2015, DJe 19/10/2015, RSTJ vol. 243 p. 1093.
Enunciado - A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.

27 Lima Marques, Claudia. Contratos no código de defesa do consumidor. 5ª ed. Ed. RT. SP-SP, 2006. p.822.

1.2.2 O "CONTROLADOR" e SUA DEFINIÇÃO

A definição de "controlador" é fixada na LGPD como sendo a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados. Trata-se daquele que determina as finalidades e os meios de tratamento. O "controlador" corresponde a pessoa que toma a iniciativa e controla os meios técnicos ou humanos necessários a implementação do tratamento.

A noção de "controlador" é central no tema *proteção de dados*. É sobre ele que recai a maior parte das obrigações legais como, por exemplo, o de fornecer ao titular todos os seus dados por ele tratados[28] (art. 18), bem como a de reparar danos patrimoniais ou morais, pessoais ou coletivos, causados a outrem em razão do exercício da atividade de tratamento de dados. (art. 42).

1.2.2.1 MÉTODO DE AUTENTICAÇÃO e RESPONSABILIDADE

Há situações complexas nas quais será necessária aplicação de um método que permita identificar qual a entidade que age na qualidade de "controlador".

Como regra geral, o controlador deverá, primeiramente, ser considerado como a sociedade e não a pessoa que age em seu nome. A pessoa física será considerada controladora quando agir em nome próprio. A regra geral é a de que uma empresa ou um organismo público será responsável pelas operações de tratamento realizadas a seu encargo, no campo de sua atividade ou do risco empresarial assumido. Mesmo nas hipóteses em que uma pessoa física, através de uma empresa ou organismo público, utilizar dados para fins pessoais, a empresa ou o organismo deverá ser responsabilizada por atos de prepostos ou pela falta de "segurança" no tratamento dos dados pessoais (art. 44).

Uma segunda situação poderá ocorrer quando uma sociedade empresária fixa a finalidade do tratamento de dados (o resultado esperado), enquanto uma outra sociedade decida sobre os meios a serem empregados (o modo de chegar ao resultado pretendido). Trata-se da contratação, pelo controlador, de prestadores de serviços (denominados pela lei como *operadores*), os quais serão solidariamente responsáveis pelos danos causados (art. 42, I) quando descumprirem a LGPD ou quando não tiverem seguido as instruções lícitas do "controlador" (nesses casos o "operador" se equipara ao "controlador").

Uma terceira situação seria aquela em

28 Acerca da proteção de dados e seu "controlador" há interessante situação quanto aos "programas estaduais de nota fiscal". Com o fito de incentivar o cidadão a exigir a nota fiscal em suas compras, os Estados cadastram os consumidores em seus sistemas, usualmente através de seus CPFs, para concederem-lhes certos benefícios (como o desconto em tributos, p. ex.) a partir de seu consumo (e emissão da respectiva nota fiscal). Desse momento em diante, o Estado passa a receber todas as informações constantes nas notas fiscais de consumo dos cidadãos. Para além do valor da compra e sua data, o Estado colhe informações sobre todas as mercadorias adquiridas pelo cidadão, seu preço individual e até mesmo as marcas consumidas. Todos esses dados são armazenados no banco de dados das Secretarias da Fazenda. Tais informações vão muito além do necessário para o simples incentivo da emissão da nota fiscal. A rigor, o Estado precisaria apenas do valor gasto, o estabelecimento fornecedor e o CPF do cidadão. Estamos diante de situação em que o tratamento de dados pelo operador vai muito além da sua necessidade, indo de encontro ao próprio princípio da necessidade (art. 6º, III da LGPD). Nesse sentido Machado, Jorge e Bioni, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: Um estudo de caso no "Nota Fiscal paulista". LIINC em Revista, Rio de Janeiro, v. 12, n.2, p.350-364, novembro de 2016. http://www.ibict.br/liinc.

que se faz necessário identificar a entidade que exerceu a decisão de indicar o operador. Aqui vislumbram-se três hipóteses:

a) Situação em que a designação do controlador resulta de uma competência expressamente prevista em lei. Essa hipótese poderá ocorrer junto a órgãos da administração pública quando, por exemplo, um decreto autorize uma certa pessoa pública a implementar um tratamento, conferindo-lhe a determinação da finalidade e dos meios a serem empregados.

b) Uma segunda situação seria aquela em que inexiste disposição legal designando, expressamente, a identidade do controlador, o que nos remete às regras gerais do direito para determinar sua identidade. Assim, por exemplo, a regra geral de que o empregador responde pelos atos do empregado ou de que uma associação responde por seus membros ou aderentes.

c) Não sendo suficientes esses dois primeiros critérios, ainda nos cabe aplicar o método das "circunstâncias fáticas". Assim, analisam-se os termos dos contratos para enquadrar as relações entre seus partícipes na operação de tratamento. Além dos termos do contrato propriamente ditos, poderá ser levado em conta o efetivo grau de controle exercido por um partícipe na operação, a própria "imagem" da operação dada aos titulares e as expectativas que essa imagem poderia ter-lhes suscitado. Esses e outros elementos servirão de base para a indicação do controlador.

1.2.3 O "OPERADOR"

A LGPD define o "operador" como "a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (art. 5º, VII). Assim, a qualificação de "operador" exige da pessoa em causa o preenchimento de duas condições fundamentais: a) que seja uma entidade jurídica distinta do "controlador" e, portanto, dotada de personalidade jurídica própria e, b) que aja "em nome do controlador" . Esta segunda noção guarda alguma similitude com o contrato de mandato e significa que o *operador* deverá rigorosamente respeitar a LGPD e se limitar a obedecer as instruções lícitas do "controlador", sob pena de responsabilidade solidária (art. 42, I).

Resta daí que será encargo do operador provar, para elidir sua responsabilidade solidária, que seguiu rigorosamente a LGPD e as instruções lícitas do controlador. Nessa hipótese caberá ao operador o dever de esclarecer aos titulares que age em nome do controlador além do dever de avaliar a licitude de suas instruções.

Finalmente, todos os operadores devem zelar tanto pela obediência a LGPD quanto para que o contrato celebrado com o controlador aborde precisas e lícitas instruções à execução contratual, tudo como forma de elidir sua responsabilidade solidária prevista no art. 42, I da LGPD.

Interessa notar que no ARE 660.861 RG / MG o STF julgou, em regime de repercussão geral, que o provedor da internet[29] *Goggle* é responsável pelo pagamento de indenização por danos morais sofridos pela vítima (recorrente), em virtude da criação,

29 O art. 5º, VII, do Marco Civil da Internet, define aplicações de internet como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet", sendo, portanto, o provedor de aplicações de Internet qualquer entidade que proporcione ao usuário da grande rede mundial de computadores algo funcional, seja qual for a finalidade.

por terceiros, de conteúdo considerados ofensivos no sítio eletrônico de relacionamento *Orkut*. O prestador de serviço de um site de relacionamento (operador/*google*) que permite a publicação de mensagens na internet (pelo controlador/*orkut*), sem que haja um efetivo controle, ainda que mínimo, ou dispositivos de segurança[30] para evitar que conteúdos agressivos sejam veiculados, sem ao menos possibilitar a identificação do responsável pela publicação, deve responsabilizar-se pelos riscos inerentes a tal empreendimento. Observe-se que a responsabilidade neste caso foi apurada de forma objetiva, tendo em vista a incidência do Código de Defesa do Consumidor.

Entretanto, através do Marco Civil da Internet (lei 12.965/14, art. 19 e 21) o legislador dispôs que o provedor de aplicações de internet somente poderá ser responsabilizado civilmente se, após ordem judicial especifica, não tornar indisponível o conteúdo. Essa nova disposição tem o condão de alterar o conceito expresso pelo ARE 660.861 RG / MG do STF de que a mera publicação do conteúdo por terceiros acarretaria a responsabilidade objetiva do provedor

1.2.4. O TERCEIRO

Embora não haja a qualificação direta de terceiro na LGPD (art. 16, I), este pode ser definido como toda a pessoa física ou jurídica, além do titular, do controlador e do operador que, sob autoridade direta do controlador ou do operador, seja habilitada a tratar os dados. A noção de terceiro deve ser interpretada como designativa de sujeito desprovido de legitimidade ou autorização originais para tratar os dados pessoais, mas para quem é "autorizada a transferência" dos dados, desde que respeitados os requisitos e tratamento de dados dispostos na LGPG (art. 16, III).

A princípio, um terceiro recebedor de dados pessoais, de maneira lícita ou não, será equiparada a um novo controlador e, portanto, responsável pelos dados recebidos.

1.3. O CAMPO DE APLICAÇÃO TERRITORIAL

A transferência de dados pessoais tem um caráter internacional e estreitamente vinculado com o comércio eletrônico nacional e internacional. De acordo com *McKinsey Globral Institute* [31] "Ao longo dos últimos anos, o comércio eletrônico tem mudado a face do varejo: enquanto as vendas on-line crescem a taxas de dois dígitos em países desenvolvidos, o comércio tradicional permanece estável. Isso obriga os varejistas a repensar o papel de sua rede física de lojas". Verifica-se um constante crescimento do comércio de bens por meios eletrônicos.

Em decorrência da estrutura descentralizada da internet, as transações informacionais são realizadas por cruzamento de informações entre diversas jurisdições. Nesse sentido, a lei procura evitar a transferência

30 O aresto ainda observa que serviço prestado pelo provedor (Google) exige a elaboração de mecanismos aptos a impedir a publicação de conteúdos passíveis de ofender a imagem de pessoas, evitando-se que o site de relacionamento configure um meio sem limites para a manifestação de comentários ofensivos. Ainda que o fato ofensivo tenha sido elaborado por terceiros, não se exclui a responsabilidade do provedor em fiscalizar o conteúdo do que é publicado e se os usuários estão observando as políticas elaboradas pelo próprio site.

31 https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/o-papel-das-lojas-fisicas-em-um-mundo-digital Acesso em 22 de julho de 2019.

internacional de dados à países cujas jurisdições apresente um menor grau de tutela a sua proteção.

Sabidamente, muitas empresas internacionais adotam países conhecidos como *data haven* para realizar o processo de transferência, tratamento e armazenamento de dados, ou seja, em países que se caracterizam por não terem leis de proteção de dados ou disporem de leis mais brandas que não asseguram reais garantias a tutela dos dados pessoais.

A intenção do legislador nacional é de cobrir essa lacuna através da aplicação da lei nacional em caráter extraterritorial e, além disso, exigir que as empresas sejam obrigadas, ao se utilizarem de fornecedores no exterior, a garantir aos titulares dos dados forma idêntica de proteção oferecida pela lei nacional.

A aplicação extraterritorial[32] da LGPD resulta do disposto em seu art. 3º, o qual determina sua aplicação a qualquer operação de tratamento de dados feita por pessoa natural ou jurídica, pública ou privada, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que se verifique um dos três critérios distintos:

a) Tratamento de dados realizado no Brasil;

Nessa hipótese valerá o critério territorial, ou seja, todo tratamento de dados realizados no país estará sujeita a LGPD.

b) O tratamento de dados tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados para indivíduos localizados no território brasileiro.

Nesse caso, o tratamento dos dados pessoais poderá ser realizado em território alienígena, ou seja, estrangeiro. Imporá a aplicação da LGPD o fato do objetivo do tratamento ser destinada a oferecer bens ou serviços para qualquer pessoa situada no território nacional. É o caso, v.g., de sites chineses que oferecem produtos à brasileiros, em português, com entrega domiciliar no país.

c) Os dados pessoais objeto do tratamento tenham sido coletados no Brasil.

Aqui igualmente desimporta o local onde se deu o tratamento. Valerá a LGPD em todas as hipóteses em que os dados sejam coletados no país, o que implica numa tentativa de garantir efeitos extraterritoriais a lei brasileira.

Como se depreende do texto legal, o critério empregado pelo legislador pátrio para fixar a competência da LGPD despreza os "meios" de tratamento de dados, o país de sua sede (do "tratamento") ou o país onde estejam localizados os dados.

Tendo em vista os critérios empregados pela LGPD, seu campo de aplicação cobrirá praticamente todos os atos de tratamento realizados no Brasil ou que sejam destinados a pessoas situadas no seu território.

Importa analisar a extraterritorialidade das normas, questão ligada ao seu caráter instrumental e à implementação de políticas públicas. Através da extraterritorialidade

32 "Na atualidade, os típicos elementos referenciais de Estado não subsistem ..... Em contraposição ao território, ocorre a desterritorialização, onde as conexões informáticas se travam no espaço virtual, sem levar em consideração o local onde se situam os sujeitos que estão conectados à Internet. Assim, pode-se efetuar um contrato por meio de comércio eletrônico com alguém que se situa na outra esfera do mundo." Limberger, Têmis. Proteção dos Dados Pessoais e Comércio Eletrônico: Os Desafios do Século XXI. Revista de Direito do Consumidor. Vol. 67/2008, p.215

os países procuram estender seu poder regulamentar para todas as condutas que, de alguma forma, possam gerar efeitos em seu território[33].

A questão da jurisdição assume grande relevância, pois para garantir a extraterritorialidade os Estados precisam assegurar a aplicação de sua lei interna sobre condutas eventualmente praticadas fora de seu território, mas que nele produzem efeitos. Trata-se do princípio dos efeitos (*effects doctrine*) segundo o qual há incidência da lei nacional do local onde se verificam as consequências da prática ilegal. O que importa, neste caso, não é a nacionalidade ou domicílio dos partícipes da ilegalidade, mas o local (país) onde se produzirão seus efeitos; já o critério da *territorialidade* implica na aplicação da norma nacional para práticas ilegais ocorridas no próprio território nacional. A lei brasileira claramente se vale dos dois princípios quando diz que a lei aplica-se a qualquer operação de tratamento ..... independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados desde que operação de tratamento seja realizada no território nacional ou se os dados tratados tenham sido coletados no território nacional (territorialidade) ou se a atividade de tratamento tenha por objetivo a oferta de bens e serviços ou o tratamento de dados de indivíduos localizados no país (princípio dos efeitos).

O critério dos efeitos acaba por estender a jurisdição de um país sobre condutas que não se verificaram em seu território, mas cujos efeitos ali se dão[34]. A extraterritorialidade da lei brasileira não impede que a mesma conduta seja julgada pela lei estrangeira, ou seja, a lei vigente no local em que se deu o tratamento de dados. De outro modo, a lei brasileira poderá pretender julgar, no Brasil, os responsáveis pelos tratamento de dados realizados no exterior (mas cujos efeitos se dão no país), fato que poderá suscitar conflito positivo de jurisdição. A questão se revolverá no plano do direito internacional.

CONCLUSÃO

Após a fundamentação do direito a proteção de dados, que se caracteriza como uma espécie de direitos de personalidade, impõe-se descrever seus efeitos como sendo tanto de caráter negativo (direito de defesa), quanto de caráter positivo (direito à prestação). É um direito negativo ao delimitar uma esfera de proteção que não poderá sofrer a intervenção do poder estatal ou privado, exigindo a abstenção desses entes nesse sentido. Será positivo porque também enseja que o Estado tome condutas positivas tendentes a garantir ao cidadão a proteção desse direito.

33 Embora os países pretendam aplicar sanções ou expedir ordens a empresas ou pessoas físicas sediadas ou domiciliadas no exterior, os efeitos extraterratoriais da lei nacional sofrem limitações impostas pela soberania dos outros países, especialmente através das chamadas blocking laws destinadas a impedir que em território nacional se produzam efeitos de ordens proferidas por autoridades

34 Nesse sentido Daniela Copetti Cravo sobre a extraterritorialidade do Regulamento Geral da Proteção de Dados Europeu: "O primeiro ponto de destaque do Regulamento é a extensão dada à proteção, que pode alcançar agentes que não tem presença na União Europeia, desde que os dados de um residente da União Europeia sejam processados em decorrência da oferta de um produto ou serviço. A outra hipótese é quando o comportamento de um indivíduo na União Europeia seja monitorado, o que demonstra a possibilidade, nas duas hipóteses, de aplicação extraterritorial do Regulamento. CRAVO, Daniela Copetti. Direito a Portabilidade de Dados. Rio de Janeiro, Lumen Juris, 2018. p. 28/29.

Desta forma, sob o ponto de vista negativo, nenhuma lei poderá eliminar esse direito da ordem jurídica, pois se trata de um direito constitucional fundamental. Desde a o ponto de vista de seu caráter positivo, caberá ao Estado o dever de garantir ao cidadão a proteção de dados pessoais, múnus que o Estado se desincumbe através da promulgação da LGPD.

Ainda deve-se concluir com a alusão a eficácia vertical e horizontal[35] do direito a proteção de dados, aplicando-se tanto a ordem pública quanto a privada. Sua aplicação vertical deriva da própria ordem constitucional através da previsão do *habeas data*, que assegura o conhecimento de informações relativas à pessoa do impetrante, constantes de registros públicos ou bancos de dados de entidades governamentais ou de caráter público (art. 5º, LXXII da CF/88). A eficácia horizontal se dá nas próprias relações jurídicas entre particulares. Registre-se, aqui, que todos os bancos de dados privados possuem caráter público, ainda que seja gerido por organismo privado, pois trata-se da uma espécie de direito fundamental à proteção da personalidade, uma vez que os dados armazenados dizem respeito a privacidade do titular.

Desta forma, somente deixa de ser cadastro *público* aqueles utilizados por pessoas físicas destinadas o uso não econômico, dados realizados para fins jornalísticos, artísticos ou acadêmicos e dados utilizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão a infrações penais.

O reconhecimento da eficácia horizontal da LGPD é essencial para a proteção da personalidade num sistema econômico onde a informação pessoal se constitui num insumo de excepcional relevância para que grandes empresas tomem suas decisões de investimento, estratégia, produção, distribuição e locação de pontos de venda a partir de acurada análise das informações obtidas sobre a renda, preferências e comportamento dos cidadãos.

A LGPD vem regular a proteção de dados e reconhecer que a informação – dados pessoais – transformou-se em verdadeiro insumo da produção, adquirindo tanta relevância quanto o capital e o trabalho. Esse quadro evolutivo proporcionou a solidificação da sociedade de informação, onde as conexões realizadas através das Tecnologias da Informação e Comunicação (TIC), tendo como suporte a *internet*, promover a informação e da difusão de dados.

Desta forma, deve-se reconhecer que, para além da defesa da privacidade, o que se protege e se regula através da LGPD é o poder de acesso e o controle das informações pelo cidadão.

BIBLIOGRAFIA

BARROS, Bruno M. Correa de., BARROS, Clarissa T. Lovatto, OLIVEIRA, Rafael Santos de. O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais. Revista Videre, Dourados, MS, v.9, n.17.1. semestre de 2017. p. 21.

CRAVO, Daniela Copetti. Direito a Portabilidade

35 Quando se fala nas eficácias vertical e horizontal, pretende-se aludir à distinção entre a eficácia dos direitos fundamentais sobre o Poder Público e a eficácia dos direitos fundamentais nas relações entre os particulares.

de Dados. Rio de Janeiro, Lumen Juris, 2018.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. Revista de Direito Civil Contemporâneo. Vol. 13/2017, p. 59-67. Out-Dez 2017.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro. Renovar. 2006.

LIMA MARQUES, Claudia. Contratos no código de defesa do consumidor. 5ª ed. Ed. RT. SP-SP, 2006.

MASSO, Fabiano Del; ABRUSIO, Juliana e FLORÊNCIO FILHO, Marco Aurélio. Marco civil da internet. Lei 12.965/14. Ed. Revista dos Tribunais. São Paulo. 2014.

MACHADO, Jorge e Bioni, Bruno Ricardo. A proteção de dados pessoais nos programas de Nota Fiscal: Um estudo de caso no "Nota Fiscal paulista". LIINC em Revista, Rio de Janeiro, v. 12, n.2, p.350-364, novembro de 2016. http://www.oboct.br/liinc

MARQUES, Claudia Lima; et al., Manual de Direito do Consumidor. São Paulo: Ed. RT, 2008, p. 85-88.

MENDES, Gilmar. Curso de direito constitucional. 2ª ed. São Paulo. Saraiva, 2008.

OPICE BLUM, Renato; NOBREGA MALDONADO, Viviane. Comentário ao GDPR. Ed. RT, SP-SP, 2018.

OPICE BLUM, Renato; NOBREGA MALDONADO, Viviane. LGPD Lei Geral de Proteção de Dados. Comentário. Ed. RT, SP-SP, 2019.

RODOTÁ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro, Renovar. 2008.

SARLET, Ingo Wolfgang. Curso de Direito Constitucional, 3ª ed, p. 400. Ed. RT. SP-SP, 2013.

TEPEDINO, Gustavo. A tutela da personalidade no ordenamento civil – constitucional brasileiro.

https://www.academia.edu/31740015/A_tutela_da_personalidade_no_ordenamento_civil-constitucional_brasileiro

https://www.mckinsey.com/br/our-insights/blog-made-in-brazil/o-papel-das-lojas-fisicas-em-um-mundo-digital

https://portalnovarejo.com.br/2015/09/7-tecnologias-para-monitorar-habitos-de-consumo/

http://agenciabrasil.ebc.com.br/economia/noticia/2018-07/facebook-chega-127-milhoes-de-usuarios-no-brasil

http://www.ibict.br/liinc.

Publicado originalmente na Revista dos Tribunais, São Paulo, ano 108, n.1010, p. 209-229, dez.2019