Bernardo Menicucci Grossi
(Org.)

LEI GERAL DE PROTEÇÃO DE DADOS

Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial

Fi

Autores:
Alexandre Rodrigues Atheniense
Bernardo Menicucci Grossi
Bruna Cardoso Nunes
Camila de Oliveira
Daniel Evangelista Vasconcelos de Almeida
Douglas Dias Vieira de Figueiredo
Duarte Moura
Felipe Soares de Magalhães
Fernanda Araújo Couto e Melo Nogueira
Guilherme Henrique Gualtieri de Oliveira
Gustavo Batista Guimarães
Igor da Silveira Franco
João Lucas Vieira Saldanha
Lucas Sávio Oliveira
Marcos Souza
Maurício Leopoldino da Fonseca
Paulo Roberto Godoy Perilli
Pedro Henrique Rocha Silva Fialho
Ricardo Gomes Figueiroa
Sidney Cássio Alves Rocha
Tatiana Alves de Castro
Thiago Thomaz Siuves Pessoa
Vitor Eduardo Lacerda de Araújo
Wallace Almeida de Freitas
Zilda A. Gonçalves de Sousa

Em uma proposta que contempla diversidade e horizontalidade, contamos com membros com as mais diversas formações e não apenas da área jurídica, mas com conhecimentos na área financeira, tecnologia, consultoria, auditoria e até mesmo acadêmicos como colaboradores externos. Acreditamos firmemente que isso tem contribuído significativamente para a construção de uma visão mais aberta e democrática da Lei Geral de Proteção de Dados. Os impactos econômicos, jurídicos, políticos e sociais da Lei Geral de Proteção de Dados tem causado, muito rapidamente, uma grande reviravolta no cotidiano empresarial e na vida do cidadão brasileiro. Isso demonstra a importância de debatermos com mais frequência e profundidade o tema deste livro que certamente é o primeiro de muitos outros projetos a serem concretizados pela nossa Comissão. Trazemos ao público textos selecionados com objetivos e metodologias diversificados com a esperança de que isso contribua para o necessário depuramento da ciência e que constitua um convite para o leitor ingressar conosco nessa maravilhosa jornada.

9 786587 340210

editora fi.org

Lei Geral de Proteção de Dados

Lei Geral de Proteção de Dados

Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial

Organizador:
Bernardo Menicucci Grossi

Diagramação: Marcelo A. S. Alves
Capa: Lucas Margoni

O padrão ortográfico e o sistema de citações e referências bibliográficas são prerrogativas de cada autor. Da mesma forma, o conteúdo de cada capítulo é de inteira e exclusiva responsabilidade de seu respectivo autor.

Dados Internacionais de Catalogação na Publicação (CIP)

GROSSI, Bernardo Menicucci (Org.)

Lei Geral de Proteção de Dados: Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial [recurso eletrônico] / Bernardo Menicucci Grossi (Org.) -- Porto Alegre, RS: Editora Fi, 2020.

455 p.

ISBN - 978-65-87340-21-0

Disponível em: http://www.editorafi.org

1. Lei Geral de Proteção de Dados; 2. Direito empresarial; 3. Tecnologias; 4. Estado; 5. Brasil; I. Título.

CDD: 340

Índices para catálogo sistemático:
1. Direito 340

Sumário

Prefácio **11**
Bernardo Menicucci Grossi

Primeira seção
A Lei Geral de Proteção de Dados e suas particularidades

1 ..... **15**
O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado, específico e expresso
Fernanda Araújo Couto e Melo Nogueira
Maurício Leopoldino da Fonseca

2 ..... **45**
As bases legais para o tratamento de dados pessoais: muito além do consentimento
Guilherme Henrique Gualtieri de Oliveira

3 ..... **64**
O legítimo interesse como base legal para o tratamento de dados pessoais
Bernardo Menicucci Grossi

4 ..... **82**
Autonomia privada, renúncia contratual a direitos fundamentais e proteção de dados
Bruna Cardoso Nunes
Camila de Oliveira

5 ..... **102**
Autonomia privada e consentimento de crianças e adolescentes na Lei Geral de Proteção de Dados
Zilda A. Goncalves de Sousa
Igor da Silveira Franco

6 ..... **133**
O direito à privacidade e o direito à proteção de dados na Lei Geral de Proteção de Dados
Sidney Cassio Alves Rocha

7 151
Direito à explicação em decisões automatizadas
Daniel Evangelista Vasconcelos Almeida

8 177
Proteção de dados, privacidade e a Lei do Cadastro Positivo
Pedro Henrique Rocha Silva Fialho

9 192
Proteção de dados, privacidade e o Marco Civil da Internet
Paulo Roberto Godoy Perilli

10 214
A LGPD e o direito do trabalho: uma nova dinâmica na liquidação de pedidos nas ações trabalhistas
Wallace Almeida de Freitas

11 232
A concepção de privacidade através dos tempos: do rupestre à Lei Geral de Proteção de Dados Pessoais
João Lucas Vieira Saldanha

Segunda seção
O impacto da Lei Geral de Proteção de Dados em modelos de negócio

12 271
A importância da governança digital na advocacia
Alexandre Atheniense

13 285
LGPD e *Legal Design*
Felipe Soares de Magalhães
Thiago Thomaz Siuves Pessoa

14 313
LGPD e a privacidade desde a concepção
Lucas Sávio Oliveira

15 337
Análise jurídica dos incidentes de segurança e a responsabilidade civil no Brasil
Vitor Eduardo Lacerda de Araújo
Douglas Dias Vieira de Figueredo

16 ..... **359**
LGPD: a proteção de dados e o consentimento granular
Gustavo Batista Guimarães

17 ..... **366**
A escolha subjetiva de várias bases legais para o tratamento de dados pessoais
Marcos Souza

Terceira seção
Cases de implantação

18 ..... **375**
Cases de implantação LGPD: a evangelização dos colaboradores
Tatiana Alves de Castro

Quarta seção
A LGPD e o Poder Público

19 ..... **389**
Desafios da LGPD na adminstração pública e a (des)continuidade das políticas públicas
Ricardo Gomes Figueiroa

20 ..... **406**
Aplicação da Lei Geral de Proteção de Dados ao poder público
Zilda A. Goncalves de Sousa
Igor da Silveira Franco

21 ..... **443**
Proteção de dados dos trabalhadores e a competência da autoridade nacional de proteção de dados
Duarte Moura

Sobre os autores **451**

Prefácio

Bernardo Menicucci Grossi [1]

Em março de 2019, atendendo à reivindicação de um grupo de advogados e advogadas com atuação profissional na área de tecnologia, proteção de dados, propriedade intelectual e direito concorrencial, o Presidente da Ordem dos Advogados do Brasil, Seccional Minas Gerais, Raimundo Cândido Junior, autorizou a criação da Comissão Especial de Proteção de Dados da OAB/MG, o que nos permitiu reunir formalmente um grupo de profissionais e acadêmicos muito qualificados.

Esse grupo tem demonstrado um alto grau de comprometimento e disponibilidade ao dedicar parte do que há de mais precioso em suas vidas, o tempo, para atividades *pro bono* em benefício da classe da advocacia e do desenvolvimento desse mercado local.

Nossas reuniões mensais ocorrem sempre com a participação de convidados que generosamente compartilham suas experiências e desafios na construção de programas de governança de dados em empresas e escritórios de advocacia.

Em uma proposta que contempla diversidade e horizontalidade, contamos com membros com as mais diversas formações e não apenas da área jurídica, mas com conhecimentos na área financeira, tecnologia, consultoria, auditoria e até mesmo acadêmicos como colaboradores externos. Acreditamos firmemente que isso tem contribuído significativamente para a construção de uma visão mais aberta e democrática da Lei Geral de Proteção de Dados.

[1] Presidente da Comissão Especial de Proteção de Dados da OAB/MG.

Os impactos econômicos, jurídicos, políticos e sociais da Lei Geral de Proteção de Dados tem causado, muito rapidamente, uma grande reviravolta no cotidiano empresarial e na vida do cidadão brasileiro. Isso demonstra a importância de debatermos com mais frequência e profundidade o tema deste livro que certamente é o primeiro de muitos outros projetos a serem concretizados pela nossa Comissão.

Trazemos ao público textos selecionados com objetivos e metodologias diversificados com a esperança de que isso contribua para o necessário depuramento da ciência e que constitua um convite para o leitor ingressar conosco nessa maravilhosa jornada.

Belo Horizonte, Junho de 2020.

Primeira seção

A Lei Geral de Proteção de Dados e suas particularidades

1

O consentimento na Lei Geral de Proteção de Dados: autonomia privada e o consentimento livre, informado, específico e expresso

Fernanda Araújo Couto e Melo Nogueira [1]
Maurício Leopoldino da Fonseca [2]

I. Introdução

Após termos vivenciado os modelos de produção agrícola (centrado na terra), industrial (das máquinas a vapor e da eletricidade) e pós industrial (calcado nos serviços), temos, nos dias de hoje, um novo elemento em torno do qual se organiza a dinâmica social: a informação (BIONI, 2019, p. 18).

Alçada a protagonista das tomadas de decisão – seja nas grandes questões públicas de ordem política e econômica ou, mesmo, nas questões estratégicas privadas –, não é à toa que já se tem por hábito denominar a atual quadra histórica de "era da informação". Afinal, é por meio da captação e do tratamento de recursos informacionais que a sociedade do novo milênio se estrutura, impulsionada por uma evolução tecnológica recente que prima por desenvolver mecanismos cada vez mais sofisticados

[1] Sócia do escritório João Bosco Leopoldino Advocacia e Consultoria; graduada em Direito pela Universidade FUMEC, em 2008; Mestre em Ciências Jurídico-Empresariais pela Faculdade de Direito da Universidade de Lisboa, em 2013; Especialista em Contratos pela Fundação Getúlio Vargas, 2015; MBA em Gestão Estratégica de Negócios pela Universidade FUMEC, em 2017.

[2] Sócio Fundador do João Bosco Leopoldino Advocacia e Consultoria; graduado em Direito pela Universidade Federal de Minas Gerais, em 1990; Mestre pela Faculdade de Direito da Universidade Federal de Minas Gerais, em 2001; Especialista em Direito Administrativo pela UFMG, em 1992; Procurador do Estado de Minas Gerais, desde 1993.

para o processamento e a transmissão de dados. Estes, ao trafegarem em quantidade e em velocidade antes inimagináveis, passaram a transpor antigos limites físicos e geográficos, criando mesmo uma nova compreensão da relação tempo-espaço (BIONI, 2019, p. 20).

Nesta nova era, rompe-se com o modelo produtivo fordista para se instaurar um novo "padrão sócio-técnico-econômico", resultante do advento da internet e das novas ferramentas digitais e, cada vez mais, aperfeiçoado pelas chamadas tecnologias da informação e comunicação (TICs). Através delas, o conhecimento passa a ser o meio pelo qual se obtém ainda mais conhecimento, fazendo girar uma economia baseada no trato eficiente com a informação, num contexto em que consumo e circulação de bens se dá em escala global (BOFF; FORTES; e FREITAS, 2018, p. 16).

Some-se isso a diversidade de dispositivos que, a cada dia, vão permitindo um acesso cada vez maior à internet, em tempo integral. Isso faz com que a informática e a tecnologia estejam onipresentes na vida das pessoas, dando sentido integral e concreto à profetizada "relação homem máquina"[3].

Dentro desse contexto de ubiquidade computacional – e considerando toda a inteligência acumulada pela ciência mercadológica, em especial no que tange à promoção segmentada e personalizada dos bens de consumo –, os dados pessoais dos cidadãos se tornam fator estratégico para o sucesso dos negócios. Destarte, um novo modelo de negócios exsurge: nele, os consumidores não pagam em dinheiro pelos bens que desejam adquirir, mas dão, em troca do usufruto do produto ou serviço, diversas informações sensíveis sobre seus hábitos de compra. Estes, por sua vez, serão a força motriz da chamada publicidade comportamental, que se traduz em apelo de consumo direcionado, feito sob medida para cada cliente. Fazendo-se uso de diversas ferramentas online, dentre as quais se destacam os *cookies*, cria-se um super banco de

[3] Disponível em: https://www.internetinnovation.com.br/blog/ubiquidade-na-web-entenda-esse-conceito/. Acessado em 29/11/2019.

dados sobre as preferências do usuário, tornando quase infalível o impacto da mensagem publicitária expedida. Desta maneira, o consumidor deixa de ser agente passivo na relação de compra e passa a participar ativamente do processo, na medida em que, compartilhando opiniões e experiências quase em tempo real, torna-se também agente do processo de criação e desenvolvimento de produtos e serviços[4].

Mas, é como diz o ditado: "não há almoço grátis"[5]. Diante da grande relevância das informações pessoais para o mercado, é inevitável que os seus titulares sejam, eles mesmos, tratados como mero produto comercializável dentro dessa nova lógica mercantil. A prática do "*zero-price advertisement business model*" resume bem essa dinâmica[6].

Pertinente, portanto, lançarmos o seguinte questionamento: no contexto traçado, as pessoas detêm real controle sobre os dados que geram para o mercado? A missão deste artigo é, justamente, discorrer sobre e problematizar a questão do tratamento das informações pessoais no âmbito da sua utilização comercial e institucional – seja por corporações e, por que não, por órgãos estatais –, tendo como base o fundamento legal do consentimento dos indivíduos que são os seus titulares. Sem pretensão de esgotar o tema – ou mesmo de trazer uma solução definitiva aos dilemas que se apresentam –, ao longo do trabalho iremos discorrer sobre a acepção, as nuances e os limites do consentimento do titular para fins de tratamento de seus dados pessoais, no contexto específico trazido pela Lei

[4] "A economia customizada exige, para a obtenção de vantagens no mercado, que a comunicação da empresa se individualize, criando e fidelizando nichos de consumo. Nessa perspectiva, a interação direta com o consumidor e a segmentação do marketing passam a ser bastante valorizadas, ganhando relevo a concepção do marketing "one-to-one"". (MENDES, 2014, p. 89).

[5] Embora o ditado tenha se popularizado após a publicação do livro com o mesmo nome, de autoria do economista monetarista Milton Friedman, em 1975, a ideia de que não se pode conseguir alguma coisa sem dar nada em troca remonta o século XVIII, quando o filósofo e economista britânico Adam Smith publicou, em seu emblemático "A Riqueza das Nações", em 1776, no Capítulo II, que "não é da benevolência do açougueiro, do cervejeiro ou do padeiro que esperamos nosso jantar, mas da consideração que eles têm pelo seu próprio interesse. Dirigimo-nos não à sua humanidade, mas à sua auto-estima, e nunca lhe falamos das nossas próprias necessidades, mas das vantagens que advirão para eles".

[6] No modelo de "zero-*price advertisement business model*", "os usuários não pagam uma quantia monetária (zero-price) pelo produto ou serviço. A contraprestação deriva do fornecimento de seus dados pessoais, o que possibilita o direcionamento de conteúdo publicitário, e cuja receita pagará, indiretamente, pelo bem de consumo (advertisement business model)". (BIONI, 2019,p. 47).

Geral de Proteção de Dados, a Lei Federal 13.709/2018, doravante denominada LGPD. Ainda para fins de delimitação do tema, cabe esclarecer que não trataremos aqui da interessante discussão acerca da harmonização ou antinomia entre a LGPD e o Marco Civil da Internet (Lei nº12.965/2014) relativamente ao consentimento, eis que tal assunto demanda e merece protagonismo, a ser explorado em outra oportunidade[7].

II. Contexto normativo sobre privacidade e dados pessoais

Considera-se dado pessoal aquele que se encontra atrelado à projeção, à extensão ou à dimensão de uma determinada pessoa, tanto na sua esfera individual, quanto em sua esfera relacional.

Nos termos do artigo 5º da LGPD, dado pessoal é qualquer "*informação relacionada a pessoa natural, identificada ou identificável*", sendo considerado dado pessoal sensível – e passível de tratamento diferenciado – o "*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*".

Mas, para melhor compreensão acerca da atual base normativa para proteção dos dados pessoais, cumpre, primeiramente, apresentarmos uma breve evolução histórica do tratamento legal da privacidade e dos dados pessoais.

Embora a Constituição do Império, de 1824, já reconhecesse o direito à privacidade ao proteger o "*segredo da carta*" e a "*inviolabilidade da casa*", tal direito vinha apoiado sobre um lastro proprietário, haja vista ter como finalidade proteger os meios, e não o conteúdo privado em si.

[7] Trata-se, em linhas gerais, de discussão que aborda possível conflito e incompatibilidade entre o consentimento previsto no art. 7º, IX da Lei 12.965/14 ("MCI") e o disposto na Lei 13.709/18 ("LGPD"). Embora grande parte da doutrina especializada defenda posicionamento no sentido de que, neste ponto, houve a derrogação tácita do MCI pela LGPD – seja pelo critério temporal, seja pelo critério de especialidade – a nosso ver, não há, a princípio, incompatibilidade inequívoca e comprovada entre as duas regras, pelo que não se pode presumir a derrogação do inciso IX do art. 7º do MCI. No entanto, como dito, o assunto merece aprofundamento e protagonismo a ser explorado em estudo específico.

Os debates doutrinários a respeito do direito à privacidade tiveram início em 1890, quando Samuel Warren e Louis Brandeis publicaram o emblemático artigo nomeado "*The right to privacy*"[8], na Harvard Law Review. No texto, os autores discorreram sobre a necessidade de se ampliar a concepção do referido direito, dada a crescente divulgação, à época, de notícias sensacionalistas e de fofocas – o que decorria, diretamente, dos avanços tecnológicos que vinham facilitar a captação e divulgação desses tipos de conteúdos, em especial a invenção das máquinas fotográficas portáteis. Segundo Warren e Brandeis, seria preciso que a lei assegurasse às pessoas o direito de serem deixadas em paz ("*the right to be left alone*"), sendo que a sua infração configuraria uma violação ao direito da personalidade.

Já em 1948, foi publicada a Declaração Universal dos Direitos Humanos (DUDH), como uma norma comum a ser alcançada por todos os povos e nações – estabelecendo, em seu artigo 12, que "*ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques*".[9]

Logo adiante, na década de 1970, surgem várias leis e decisões judiciais – expedidas em diversos países –, bem como são aprovados diversos acordos internacionais que, em diferentes graus, compartilham o entendimento de que a privacidade constitui uma projeção da personalidade, merecendo, portanto, tutela jurídica (MACIEL, 2019, p. 8).

A consolidação da concepção de privacidade relacionada à proteção dos dados pessoais veio na década de 1980, quando cooperaram importantes instrumentos internacionais e transnacionais versando sobe o assunto. Cite-se, por exemplo, as Diretrizes da OCDE para para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais,

[8] Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf. Acessado em: 20/11/2019.

[9] Disponível em: https://nacoesunidas.org/direitoshumanos/declaracao/. Acessado em: 30/11/2019.

publicada em 1980; e, ainda, a Convenção 108 do Conselho da Europa, de 1981, que trata da "*proteção das pessoas relativamente ao tratamento automatizado de dados de caráter pessoal*".

Tendo evoluído sobremaneira a compreensão da necessidade de tutela jurídica eficiente da privacidade e dos dados pessoais, em 23 de novembro de 1995, o Parlamento Europeu e o Conselho da União Europeia publicaram a Directiva 95/46/CE, relativa à proteção das pessoas singulares (pessoas físicas) no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados[10].

Embora digna de admiração, é fato que tal Diretiva não conseguiu evitar a fragmentação da sua aplicação no âmbito da União Europeia. Tampouco o sentimento generalizado de que subsistiam riscos significativos à proteção efetiva dos dados pessoais dos cidadãos europeus – em especial no que tange às atividades realizadas pela via eletrônica[11]. Assim, a fim de assegurar um maior nível de segurança jurídica para a circulação de dados pessoais na União Europeia, optou-se por criar o Regulamento Geral de Proteção de Dados (GDPR), que, revogando a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados), estabeleceu regras de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Este novo Regulamento (GDPR) foi publicado em 27 de abril de 2016, mas somente passou a ser aplicável a partir de 25 de maio de 2018.

Paralelamente, no Brasil, a partir da década de 90, também começaram a surgir diplomas legais que alçaram a proteção da

[10] Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046&from=PT. Acessado em: 30/11/2019.

[11] "Considerando (9): Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE". Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acessado em: 20/11/2019

privacidade e dos dados pessoais a um novo patamar. Citam-se, como os principais:

i. O Código de Defesa do Consumidor (Lei 8.078/1990), que disciplina a criação de bancos de dados de consumidores e que prevê o direito de o consumidor ter livre acesso aos dados arquivados sobre a sua pessoa;
ii. A Lei do Habeas Data (Lei 9.507/1997), que é, em sua essência, a ferramenta jurídica para assegurar o conhecimento e a retificação de dados.
iii. O Código Civil (Lei 10.406/2002), que detalhou os direitos inerentes à personalidade, dentre os quais se encontram a privacidade e a intimidade; e que previu expressamente a adoção de medidas necessárias, pelo juiz, mediante pedido do interessado, para cessar eventual violação à sua vida privada;
iv. A Resolução do Conselho Federal de Medicina n.º 1.821/2007, que dispõe sobre o prontuário eletrônico e a proteção de dados médicos;
v. A Lei do Cadastro Positivo (Lei n.º 12.414/2011), que disciplina a formação e a consulta a bancos de dados com informações de adimplemento de pessoas, naturais e jurídicas – visando à formação de histórico de crédito –, bem como reconhece os direitos dos titulares dos dados, atrelando o tratamento à finalidade pretendida;
vi. A Lei de Acesso à Informação (Lei n.º 12.527/2011), que disciplina o tratamento dos dados pessoais no âmbito de sua aplicação; e
vii. O Marco Civil da Internet (Lei n.º12.965/2014 e o Decreto n.º 8.771/2016), que abordam consideravelmente o tratamento de dados pessoais em trânsito pelo ambiente da internet.

Finalmente, em 14 de agosto de 2018, diante da pressão decorrente da entrada em vigor do GDPR e após o escândalo do caso *Cambridge Analytica*, foi promulgada no Brasil a Lei Geral de Proteção de Dados Pessoais, Lei Federal n.º 13.709/2018 (LGPD), que trata sobre a proteção de dados pessoais e é claramente inspirada no GDPR, embora apresente pontos de divergência (MACIEL, 2019, p. 17). No atual contexto informacional, a LGPD busca harmonizar e atualizar conceitos de modo a mitigar riscos e a estabelecer regras claras sobre a proteção dos dados pessoais. (MALDONADO; BLUM, coord. 2019, p. 23).

É nesse cenário que se situa a análise abarcada por este artigo, relativa à acepção, às nuances e aos limites do consentimento do titular

para fins de tratamento de seus dados pessoais. Tudo isso dentro da moldura jurídica traçada pelos artigos 7º e 8º da referida LGPD.

III. A autodeterminação informativa:

Podemos conceituar a autodeterminação informativa como o "*direito que cabe a cada indivíduo de controlar e de proteger os próprios dados pessoais, tendo em vista a moderna tecnologia e processamento de informação*". Nesse sentido, o direito à autodeterminação informativa corresponde a uma espécie do direito à privacidade, na qual o indivíduo se mostra capacitado e informado o suficiente para exercer sua liberdade de decisão acerca do tratamento efetuado junto aos seus dados.

Nas palavras de VAINZOF, a autodeterminação informativa é:

> "*o controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo – conjuga as duas já mencionadas concepções de privacidade de dados: a primeira de caráter negativo e estático; e a moderna, em que a intervenção (proteção) é dinâmica, durante todo o ciclo de vida dos dados nos mais variados meios em que possa circular*." (MALDONADO; BLUM, coord. 2019, p. 27)

Inicialmente reconhecido pelo Tribunal Constitucional Alemão no julgamento do caso da Lei do Censo Alemã, de 1982, o direito à autodeterminação informativa pressupõe que, mesmo sob as condições da moderna tecnologia de processamento de informações (...), o indivíduo exerça sua liberdade de decisão junto às ações praticadas em relação aos seus dados[12].

Assim, é o exercício do chamado "direito à autodeterminação informativa" o que garante – ou pretende garantir – a cada cidadão ser

[12] MARTINS, Leonardo. *2ª Parte – DIREITO CONSTITUCIONAL MATERIAL I - (Direitos Fundamentais – Art. 1 – 19 GG) - Livre desenvolvimento da personalidade (Art. 2 I GG) - 20. BVERFGE 65, 1 (VOLKSZÄHLUNG) - Reclamação Constitucional contra ato normativo 15/12/1983.* Cinquenta Anos de Jurisprudência do Tribunal Constitucional Federal Alemão. Organização e introdução: Leonardo Martins. Prefácio: Jan Woischnik. Trad. Beatriz Henning et. al. Monevidéu: Fundação Konrad Adenauer, 2005. p. 233-234.

senhor das suas informações, ante as múltiplas possibilidades de coletas e tratamento de dados oferecidas pela tecnologia.

IV. O consentimento na LGPD:

Ao longo do tempo, tem-se compreendido a proteção dos dados pessoais como algo atrelado à autodeterminação informativa, recorrendo-se à técnica legislativa de eleger o consentimento do seu titular como um dos principais pilares normativos.

Entende-se, mediante a adoção da referida técnica, que, através do consentimento, o titular dos dados pessoais se vê capaz de emitir autorizações conscientes para os diversos tratamentos aplicáveis aos seus dados – podendo, portanto, exercer o pleno controle sobre o que deve ou não ser disponibilizado, bem como para quem e com que finalidade. Em última análise, pode ele, inclusive, revogar tal consentimento, quando não mais assinta com qualquer das formas de uso de seus dados.

Ao longo das gerações legislativas que abordaram a proteção da privacidade e dos dados pessoais, teve sempre o consentimento seu espaço de protagonismo, fazendo por merecer um crescente fluxo de adjetivações. Nas últimas legislaturas, segue ele gozando de grande relevância e recebendo complexa e extensa qualificação. Fala-se mesmo de uma verdadeira "hipertrofia do consentimento", fruto da compreensão de que a normativa existente não é capaz de dar a concretude prometida ao controle dos dados pessoais[13].

Em todo caso, o consentimento é um dos fundamentos legais do tratamento dos dados pessoais – tal como previsto no artigo 7º da LGPD[14] –, sendo definido, no referido regulamento, como a "*manifestação livre,*

[13] "Trata-se, assim, de uma espécie de hipertrofia do consentimento junto ao restante do corpo normativo de proteção de dados pessoais, o que é diagnosticado por um desenvolvimento incompleto dos seus outros "membros" que preencheriam a citada adjetivação e dariam concretude à prometida esfera de controle dos dados pessoais". BIONI, pág. 266.

[14] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular.

informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[15].

Em outras palavras, é através do consentimento – livre, informado e inequívoco – que os agentes de tratamento (controlador e operador) se põem autorizados a operar – realizar coleta, classificação, utilização, reprodução, transmissão e armazenamento – com os dados pessoais do titular.

Sendo um dos dez fundamentos legais para o tratamento dos dados pessoais, tem-se como premissa que o consentimento só pode constituir fundamento legal adequado quando, ao titular dos dados, for concedido o controle – uma verdadeira opção de aceitar ou de recusar os termos propostos pelo agente de tratamento, sem ser, por isso, prejudicado.

A rigor, ao requerer o consentimento do titular para realizar o tratamento de dados pessoais, o agente tem o dever de verificar se irá cumprir com todos os requisitos para obter um consentimento válido, pois cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto no art. 7º da LGPD (livre, informado, inequívoco e para finalidade determinada). Uma vez comprovado esse requisito, o consentimento apresenta-se como um instrumento que permite aos titulares terem o controle de que seus dados pessoais sejam ou não objeto de tratamento. Porém, do contrário, havendo vício na manifestação de vontade do titular, o dito consentimento será inválido e o tratamento de dados pessoais deverá ser considerado ilícito, haja vista a sua total vedação nessas circunstâncias, conforme previsto no parágrafo 3º do artigo 8º da LGPD[16]. Note-se que tal disposição não inovou, pois o Código Civil/2002, em seus artigos 138[17] e 139[18], já estabeleceu, de forma

[15] Art. 5º Para os fins desta Lei, considera-se: (...) XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

[16] "Art. 8º. (...). § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento".

[17] Art. 138. São anuláveis os negócios jurídicos, quando as declarações de vontade emanarem de erro substancial que poderia ser percebido por pessoa de diligência normal, em face das circunstâncias do negócio.

[18] Art. 139. O erro é substancial quando: I - interessa à natureza do negócio, ao objeto principal da declaração, ou a alguma das qualidades a ele essenciais; II - concerne à identidade ou à qualidade essencial da pessoa a quem se refira

bastante clara, a possibilidade de anulação do negócio jurídico quando a declaração de vontade emanar de erro substancial que possa ser aferido por pessoa de diligência normal, em face das circunstancias do ato.

Destarte, com o intuito de trazer efetividade ao princípio da autodeterminação informativa, fixou-se que a realização de uma operação de tratamento de dados pessoais – mediante a obtenção de prévio consentimento do titular – deve se pautar na observação de requisitos rigorosos, além de ser utilizada com parcimônia pelos agentes de tratamento, podendo ser considerado nulo o consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo, ou mesmo caso não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca[19].

Registre-se, por exemplo, a condenação do Google ao pagamento de multa de 50 milhões de Euros fixada pela Autoridade de Proteção de Dados francesa, a Commission Nationale de l'Informatique et des Libertés – CNIL, por violar os princípios de transparência e de informação contidos no GDPR ao não deixar claro para os usuários quais dados eram coletados e como eram utilizados[20]. Como as regras para um consentimento válido à luz do GDPR são muito semelhantes aos da LGPD, essa decisão da Autoridade francesa pode ser tida como paradigma apto a fornecer a compreensão do que seja um consentimento inválido/nulo segundo a legislação brasileira.

Deve o controlador ter em mente que a regulamentação do tratamento de dados pessoais visa a proteger os direitos fundamentais de liberdade e de privacidade, bem como o de livre desenvolvimento da personalidade da pessoa natural, cujos fundamentos são: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de

---

a declaração de vontade, desde que tenha influído nesta de modo relevante; III - sendo de direito e não implicando recusa à aplicação da lei, for o motivo único ou principal do negócio jurídico.

[19] Art. 9º. (...). § 1º Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca.

[20] Disponível em: https://www.cnil.fr/fr/la-formation-restreinte-de-la-cnil-prononce-une-sanction-de-50-millions-deuros-lencontre-de-la. Acessado em 03/12/2019.

informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem e o livre desenvolvimento da personalidade, dentre outros[21]. Além disso, deve ele se atentar para o fato de que, não obstante o tratamento se baseie na autorização do titular, isso não dispensa e, tampouco, diminui a obrigação de se observar os princípios da transparência, da necessidade, da finalidade e da adequação, previstos no artigo 6º da LGPD[22].

Nesse sentido, o consentimento para o tratamento dos dados pessoais não legitima a recolha de dados que não sejam necessários para a finalidade específica do tratamento e tampouco a utilização dos dados coletados para tratamento diverso daquele expressamente autorizado. De igual forma, autorizações genéricas e vagas são nulas para fins de tratamento de dados[23]. Ressalte-se, ainda, que, em se tratando de manipulação de dados pessoais sensíveis – aqueles que, via de regra, têm maior possibilidade de gerar discriminação –, a LGPD enfatiza e explicita que o consentimento deve ser destacado, para finalidades específicas.

---

[21] 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.

[22] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - segurança: utilização de medidas 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 difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

[23] Artigo 8º, §4º: O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.

Portanto, ao elegerem o consentimento como fundamento legal para tratar dados pessoais dos titulares, os controladores deverão encontrar soluções juridicamente viáveis para que as manifestações dos titulares sejam **legítimas**, preenchendo todos os requisitos legais para a sua validade.

IV. Elementos para a validade do consentimento na LGPD

Conforme vimos, o art. 5º da LGPD traz a definição de consentimento, qualificando esta manifestação de vontade do titular dos dados. Para que seja válido, o consentimento deverá ser:

- livre,
- informado,
- específico, e
- expresso.

O artigo 8º da LGPD, por sua vez, aborda as nuances do uso do consentimento enquanto base legal para tratamento de dados pessoais.

Segundo COTS (2019), o consentimento possui natureza jurídica contratual. O autor explica:

> *"O consentimento é uma base legal para tratamento de dados pessoais que possui nítida natureza contratual, pois, de um lado, há a manifestação da vontade de uma parte em tratar os dados pessoais para determinada finalidade e, de outro lado, há alguém que anui com tal tratamento. Obviamente que o tratamento de dados pessoais em si pode não ser a causa principal da relação jurídica entre as partes, mas o consentimento está longe de ser um contrato acessório, pois não é dependente de nenhum outro ajuste, mantendo-se vigente e eficaz por si mesmo"*[24].

O consentimento, contudo, para produzir efeitos válidos, nos termos da LGPD, deve possuir todas as características acima elencadas.

[24] COTS, Márcio (2019), pág. 86.

Livre

A qualidade de "livre" implica, primordialmente, a independência e a desvinculação da manifestação de vontade. A rigor, tal requisito pretende que o consentimento se dê em decorrência de uma escolha real e controlada do titular dos dados. Ao fazermos o raciocínio inverso, temos que, em havendo algum embaraço ou condição ao consentimento, deste já não mais se dirá que seja livre, estando a manifestação de vontade viciada.

Além disso, para que seja livre, a concordância com a utilização dos dados pessoais deve se ater ao mínimo necessário para se atingir a finalidade pretendida pelo titular. Para que se dê efetividade à proteção das informações, deve existir, portanto, a presunção de que o consentimento para o tratamento de dados que não sejam estritamente necessários para a consecução daquilo que foi autorizado, jamais poderá ser obrigatório.

Cumpre, por outro lado, explicitar que, caso o titular não deseje dar a autorização para o tratamento de dados atrelados, diretamente, à execução do contrato, correrá o risco de não poder ser atendido pelo prestador/controlador.

Em resumo, quando o titular não tiver escolha, sentindo-se coagido ou vindo a sofrer consequências negativas por sua recusa em consentir algo que vá além do objeto principal pretendido, então a sua vontade não poderá ser tida por livre. Qualquer elemento capaz de exercer influência ou constrangimento ao titular de dados pessoais acarretará a invalidez de seu consentimento ao tratamento dessas informações. A título de exemplo: um aplicativo de venda de passagens aéreas requer aos usuários autorização para ativar a localização por GPS e para acessar a galeria de fotos, como condição para a prestação dos serviços. Como justificativa, ela informa que utilizará os dados coletados para fins de envio de "publicidade comportamental". Ora, importante destacar que nem a geolocalização nem a galeria de fotos são relevantes para a execução do objeto contratual,

que é a venda de passagens aéreas. No entanto, considerando que o aplicativo não pode ser utilizado sem que o usuário dê o consentimento para acessar tais ferramentas, não poderá tal concordância ser tratada como livre.

De fato, toda vez que se verificar um desequilíbrio de poder entre o responsável pelo tratamento dos dados pessoais e o seu titular, o consentimento tenderá a ser, de alguma maneira, viciado. Cite-se, também à guisa de exemplo, um requerimento para tratamento de dados pessoais na vigência de uma determinada relação empregatícia: a vulnerabilidade do trabalhador em face de seu empregador claramente fará com que a recusa se dê por improvável, em razão de temor ao risco real de retaliação. Assim, havendo pretensão de tratamento de dados por parte de quem emprega, é pouco provável que a vontade do empregado se expresse livremente. E, mais do que isso: tendo em vista as demais bases legais que legitimam o tratamento de dados, parece-nos inadequada a fundamentação do tratamento de dados pessoais em sede de consentimento, quando atribuída a um vínculo trabalhista. Há, a nosso ver, bases legais mais adequadas a esse tipo de relação.

Nada obstante, em algumas situações específicas, mesmo na relação de emprego, pode ser que o consentimento seja uma forma apropriada de tratar os dados pessoais de empregados. Por exemplo, quando a empresa deseja ofertar aos seus empregados a facilidade de serem vacinados na própria empresa contra a gripe, mediante confirmação de interesse de cada empregado recolhendo destes o consentimento para esta finalidade específica. Todos os que quiserem poderão se beneficiar da vacinação realizada dentro das instalações da própria empresa. Por outro lado, aqueles que preferirem se vacinar na rede pública de saúde ou não aderir à campanha de vacinação, não serão penalizados pelo empregador de nenhuma maneira. Neste tipo de situação, o consentimento parece-nos adequado.

Informado

A LGPD prevê que o consentimento, além de livre, deve ser informado. Com base em seu artigo 6º, tal condição decorre, diretamente, do atendimento aos princípios da adequação e da transparência, estando o primeiro deles relacionado com a compatibilidade entre o tratamento executado pelo controlador e as finalidades informadas ao titular. O segundo (transparência), por sua vez, é garantia dada ao titular de que as informações prestadas pelo controlador – e que servirão para subsidiar a decisão sobre a conveniência ou não do ato de concordância – sejam claras, precisas e facilmente acessíveis. Isso significa que a mensagem do controlador deve ser de fácil compreensão para o titular, bem como expedida em linguagem informal e o mais simplificada possível. Além disso, ela deve ser completa, ou seja: por meio dela, o titular deverá ter uma noção realística acerca do procedimento ao qual seus dados pessoais serão submetidos. Nesse sentido, a mera utilização de farta documentação esparsa, ainda que abordando os diversos tratamentos efetuados pelo controlador – mas sem fornecer ao titular uma noção completa e clara daquilo que, efetivamente, será feito –, pode não se mostrar efetiva para a satisfação ao pleno direito à informação, o que caracteriza uma política de tratamento pouco transparente.

Nesse contexto, ganham destaque as Políticas de Privacidade, pois, em tese, passam a ser o documento formal a dispor, com detalhes, sobre quais os dados do titular serão coletados e tratados pelo controlador. Ainda que passíveis a diversas críticas, elas têm sido, em regra, uma boa maneira de minimizar a vulnerabilidade do titular, além de uma ferramenta eficaz para a obtenção de um consentimento válido. Este, por sua vez, tem por requisito inafastável a compreensão, por parte do titular dos dados, daquilo que ele está a aceitar. De tal maneira, podemos mesmo afirmar que os requisitos de adequação e transparência são – eis que estreitamente relacionados com os deveres de lealdade e licitude –, de fato, princípios fundamentais para o controlador, que deve fornecer informações prévias

ao consentimento aptas a permitir ao titular dos dados tomar decisões conscientes e, portanto, autônomas em relação ao tratamento. Importa ainda que tais informações se vejam adequadas a cada uma das diferentes classes de titulares que, eventualmente, possam vir a figurar como consentidores. Também sob essa perspectiva, a consequência do não cumprimento da transparência e/ou da adequação será a nulidade por vício do consentimento e, consequentemente, a ilegalidade do tratamento dos dados.

Segundo o GT29[25] – grupo de trabalho instituído ao abrigo do artigo 29.º da Diretiva 95/46/CE –, para que o consentimento se dê por informado, é necessária a comunicação, feita ao titular dos dados, sobre determinados aspectos do tratamento, tidos como cruciais para a autorização do tratamento. Para o referido órgão consultivo europeu, ao menos as informações abaixo identificadas são necessárias para a obtenção de um consentimento válido, considerando-se as disposições do GDPR:

(i) identidade do responsável pelo tratamento,
(ii) a finalidade de cada uma das operações de tratamento em relação às quais se procura obter o consentimento,
(iii) que (tipo de) dados serão recolhidos e utilizados,
(iv) existência do direito de retirar o consentimento,
(v) informações acerca da utilização dos dados para decisões automatizadas em conformidade com o artigo 22.º, n.º 2, alínea c), quando pertinente, e
(vi) sobre os possíveis riscos de transferências de dados devido à inexistência de uma decisão de adequação e de garantias adequadas, tal como previsto no artigo 46.

Relativamente aos Itens (i) e (iii), o GT29 esclarece que, se o consentimento ao tratamento pretendido puder ser invocado por múltiplos responsáveis (conjuntos), ou caso os dados possam ser transferidos ou tratados por outros responsáveis – que pretendam, assim,

[25] Trata-se de um órgão consultivo europeu independente em matéria de proteção de dados e privacidade. As suas atribuições encontram-se descritas no artigo 30.º da Diretiva 95/46/CE e no artigo 15.º da Diretiva 2002/58/CE.

invocar o consentimento original –, todas essas organizações deverão ser, previamente, identificadas.

Conclusivamente, o GT29 esclarece que , a depender das circunstâncias peculiares de um caso concreto, outras informações podem se fazer necessárias para que o titular dos dados obtenha, verdadeiramente, a compreensão acerca das operações de tratamento em causa.

A partir da mesma lógica de recomendação adotada pelo GT29, podemos dizer que, à luz da LGPD, para que o consentimento se dê por informado, deve o titular ter acesso a informações claras e suficientes para formar o seu convencimento – incluindo, mas não se limitando a:

1) quem é o agente controlador;
2) qual a finalidade do tratamento;
3) quais dados são necessários para alcançar o objeto pretendido;
4) quais os direitos do titular, conforme previsão do art. 18[26], em especial aqueles relativos à possibilidade de portabilidade dos dados a outro fornecedor, à eliminação dos dados tratados com o consentimento e à própria revogação do consentimento;
5) possibilidade de solicitar a revisão de decisões tomadas, unicamente, com base em tratamento automatizado de dados pessoais que afetem seus interesses;
6) possibilidade de revogar o consentimento a qualquer tempo, nos termos do art. 20[27];
7) realização de transferência internacional de dados, conforme previsto no art. 33[28].

[26] 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; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

[27] O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

[28] Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;

Específico

A característica da especificidade do consentimento decorre do preceituado no parágrafo 4º do artigo 8º, da LGPD, que prevê expressamente que a concordância deverá se referir a finalidades determinadas. Ademais, o artigo 11 aborda o tratamento de Dados Pessoais Sensíveis, dispondo, também, que a anuência deve ser dada para cada finalidade específica.

Corroborando esse entendimento, o artigo 9º da LGPD prevê que o titular tenha direito a acesso facilitado às informações sobre o tratamento de seus dados, determinando que tais informações sejam disponibilizadas de forma clara e adequada e indicando, dentre outras coisas, a finalidade específica do tratamento pretendido/realizado pelo controlador.

Resta, portanto, evidente que o consentimento do titular dos dados deve ser dado em relação a uma ou mais **finalidades específicas**; e que um titular de dados deve ter liberdade de escolha em relação a cada uma delas – sendo o requisito da especificidade destinado a assegurar certo grau de controle do utilizador, bem como transparência em relação ao titular. Tal exigência se encontra intimamente ligada à noção de consentimento informado, na medida em que, para anuir com o tratamento dos seus dados pessoais para uma ou mais finalidades específicas, o titular deve estar ciente tanto dos objetivos da operação como dos meios a ela aplicados.

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos; III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; V - quando a autoridade nacional autorizar a transferência; VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

A LGPD prevê, inclusive, a necessidade de novo requerimento de consentimento pelo controlador, caso este pretenda realizar tratamento para finalidade diversa daquela inicialmente autorizada pelo titular. Isso reforça a importância dos aspectos da determinação, da especificidade e da explicitude da finalidade do tratamento como critérios de validade para o consentimento, pois, como já foi dito, a autorização dada de forma genérica e abrangente é considerada nula, nos termos do já referenciado art. 8º, parágrafo 4º da LGPD.

Destarte, a combinação entre a necessidade de consentimento específico e a noção de limitação da finalidade trazidas na LGPD funciona, em verdade, como salvaguarda à inalterabilidade das finalidades dos processamentos de dados, vedando qualquer possibilidade de sua modificação, supressão ou alargamento após dada a anuência pelo titular. Tal garantia só se verá afastada caso venha a subsistir outro fundamento legal que melhor reflita a situação em concreto.

Expresso

Para que o consentimento seja válido, o artigo 8º da LGPD determina que ele se dê de forma inequívoca, ou seja, por meio de uma ação positiva ou mediante declaração por escrito – constando, neste último caso, de cláusula contratual destacada das demais, com fins de atestar uma manifestação de vontade expressa do titular.

Considerando ser do controlador o ônus da prova de que o consentimento foi dado nos termos da Lei, é ele quem deverá demonstrar, através de qualquer meio considerado idôneo, que a concordância foi dada inequivocamente para cada uma das finalidades pretendidas – comprovando, é claro, que ela se deu de forma específica e informada para cada um dos diferentes tratamentos. É somente assim que, da ação positiva e inequívoca do titular, restará a certeza de ter ele exercido, na plenitude, seu poder de deliberação, no sentido de permitir o tratamento de seus dados pessoais.

Vale lembrar que o consentimento deverá se referir a finalidades específicas, pois, ainda que expressa pelo titular, a anuência para o tratamento genérico não corresponde às exigências legais constantes da LGPD. De igual maneira, as autorizações pré-assinaladas constantes de sites e portais da internet – assim como a simples utilização dos serviços e/ou aquisição dos produtos fornecidos pelo controlador – não serão considerados manifestações de vontade do titular para fins de tratamento de dados.

Por fim, o controlador deve também atentar-se ao fato de que a concordância não poder ser obtido a partir do mesmo ato de adesão aos termos do contrato, ou mesmo de aceitação das condições gerais do serviço. Para gozar de validade, o consentimento ao tratamento de dados deve ser específico. Por conseguinte, a mera utilização normal de sites da internet, por exemplo, não pode ser considerada conduta apta a ensejar manifestação de vontade do titular no sentido de anuir com a operação de tratamento dos seus dados pessoais. Mesmo no ambiente virtual, é preciso que ele consinta com a pretensão do controlador em caráter inequivocadamente específico.

Usemos um exemplo prático para lançarmos luz ao que foi dito: imaginemos que uma *exchange* de *bitcoins* venha requerer que, para além do mero preenchimento de dados cadastrais, o usuário deva postar uma fotografia em posse do seu documento de identidade, assentindo, num gesto de cabeça, para uma câmera inteligente. Nesse caso, deve-se assinalar que, desde que tenham sido prestadas informações claras ao titular sobre a natureza da utilização das informações coletadas, é perfeitamente possível que as referidas ações solicitadas pelo controlador confirmem que o titular concordou expressamente com o tratamento de seus dados pessoais.

Em suma, é fato que, diante das exigências da LGPD, cada vez mais os titulares serão obrigados a manifestar a sua concordância expressamente para diversos tipos de tratamentos, por vários e distintos controladores. No contexto digital, em especial, é grande a demanda diária

por consentimento, o que acaba por acarretar num fenômeno conhecido por "fadiga do consentimento". É que, ao lidar com uma profusão de "cliques" – todos com o intuito de obter algum tipo de autorização – , o alerta dos mecanismos de consentimento termina por dispersar, já que informações relevantes sobre os termos da anuência passam a não ser lidas na sua totalidade.

Em todo o caso, a concordância deve ser obtida sempre antes de o controlador iniciar o tratamento dos dados pessoais. E, surgindo o interesse por novo tratamento para o qual a autorização ainda não foi dada – e cuja base legal seja o consentimento –, deverá o operador fazer novo requerimento ao titular, esclarecendo como pretende utilizar as informações coletadas.

VI. A revogação do consentimento:

A revogação do consentimento ocupa um lugar de destaque na LGPD, constando como um dos direitos do titular dos dados. Este possui, conforme o artigo 18, inciso IX, o direito de obter do controlador, a qualquer tempo e mediante requisição, "a revogação do consentimento, nos termos do §5º do art. 8º desta lei".

Por sua vez, o parágrafo 5º do artigo 8º da LGPD dispõe que:

> *"o consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação nos termos do inciso VI do caput do art. 18 desta lei".*

Por fim, o inciso VI do artigo 18 estabelece que é direito do titular de dados a: "*VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no artigo 16 desta Lei*". O art. 16[29]

[29]Art. 16: Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados

da LGPD, por sua vez, traz as hipóteses legais de manutenção dos dados pessoais após o término do tratamento pelo controlador.

Embora não haja previsão expressa sobre como o operador de tratamento deve atuar para que o direito à eliminação dos dados seja efetivado, fato é que o mecanismo a ser disponibilizado ao titular deve ser gratuito e facilitado. Ressalte-se que, preferencialmente, ele deverá, de certa maneira, corresponder ao procedimento utilizado para obtenção do consentimento. Nesse sentido, se a anuência tiver se dado por meio eletrônico – confirmação via *checkbox*, por exemplo –, a revogação também terá que ser feita por procedimento similar, sendo vedado ao controlador ativar processo online para obtenção da concordância e, simultaneamente, determinar que a revogação só ocorra a partir de requerimento via telefone, em horário comercial[30]. Destarte, pode-se

pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.

[30] Orientações do GT29 - "Se o responsável pelo tratamento for capaz de demonstrar que o serviço inclui a possibilidade de retirar o consentimento sem que daí advenham quaisquer consequências negativas, nomeadamente que a prestação do serviço perca qualidade prejudicando o utilizador, tal pode servir para comprovar que o consentimento foi dado livremente. O RGPD não exclui todos os incentivos, mas o ónus de demonstrar que o consentimento foi dado livremente em todas as circunstâncias recai sobre o responsável pelo tratamento.

[Exemplo 8] - Ao descarregar uma aplicação para telemóvel relativa a hábitos de vida, a aplicação solicita consentimento para aceder ao acelerómetro do telefone. Não se trata de algo necessário para a aplicação funcionar, mas é útil para os responsáveis pelo tratamento que pretendem saber mais acerca dos movimentos e dos níveis de atividade dos utilizadores. Posteriormente, se a utilizadora revogar esse consentimento, descobre que a aplicação só funciona parcialmente. Estamos perante um exemplo de prejuízo na aceção do considerando 42, o que significa que o consentimento nunca foi obtido validamente (e logo, o responsável pelo tratamento tem de apagar todos os dados pessoais acerca dos movimentos dos utilizadores recolhidos desta forma).

[Exemplo 9] - O titular de dados subscreve o boletim informativo de um retalhista de moda com descontos gerais. O retalhista solicita ao titular dos dados consentimento para recolher mais dados sobre preferências de compras para personalizar as ofertas em função das preferências do titular dos dados com base no histórico de compras ou num questionário cujo preenchimento é voluntário. Posteriormente, quando o titular dos dados revoga o consentimento, passa novamente a receber descontos de moda não personalizados. Esta situação não implica prejuízo, uma vez que apenas se perdeu o incentivo admissível.

[Exemplo: 10] - Uma revista de moda oferece aos leitores acesso para comprarem novos produtos de maquilhagem antes do lançamento oficial. Os produtos estarão disponíveis para venda brevemente, mas oferece-se aos leitores da revista uma antevisão exclusiva dos referidos produtos. Para beneficiarem da oferta, as pessoas devem dar a morada e concordar em subscrever a lista de endereços da revista. A morada é necessária para o envio dos produtos e a lista de endereços é utilizada para enviar ofertas comerciais de produtos, tais como cosméticos ou t-shirts, durante todo o ano. A empresa explica que os dados que constam da lista de endereços apenas serão utilizados para o envio de artigos e publicidade em papel pela própria revista e que não são partilhados com outras organizações. Caso o leitor não queira divulgar o seu endereço por esta razão, não existe prejuízo, uma vez que os produtos estarão disponíveis de qualquer forma."

concluir que o responsável pelo tratamento deve garantir que a revogação do consentimento ocorra de forma tão facilitada quanto aquela que deu causa à sua autorização.

A exemplo do que dispõem os considerandos do GDPR[31], o aspecto da facilidade para retirada do consentimento é requisito indispensável para que a concordância seja válida. Se o direito em questão não vier amparado pela forma prescrita no RGPD, então o mecanismo adotado pelo controlador não estará cumprindo a legislação. Além do que, ainda em observância ao princípio da transparência, deve o controlador deixar bem claro para os titulares como eles podem exercer o direito de revogação do consentimento – sendo que a revogação, por si só, é o bastante para interromper o tratamento, já a partir do processamento do pedido. No entanto, não é capaz de invalidar o tratamento efetuado anteriormente, desde que este tenha sido obtido com base no consentimento, o qual permanece lícito. Regra geral, a partir do requerimento de revogação, o tratamento deverá ser encerrado e, não havendo outro embasamento legal para manutenção dos dados pelo controlador, estes deverão ser apagados.

Lado outro, ainda que a manifestação de revogação venha acompanhada de pedido expresso do titular para deleção/destruição dos seus dados, o controlador poderá se recusar a fazê-lo caso tenha alguma necessidade legalmente justificada para mantê-los, cabendo apenas informar ao titular se o pedido dele será atendido, ainda que parcialmente, justificando eventual manutenção das informações pessoais em sua base.

Diante do exposto, é essencial que o controlador saiba bem avaliar e definir as finalidades para as quais os dados serão efetivamente tratados,

---

Orientações do Grupo de Trabalho do Artigo 29º (GT29) - Orientações relativas ao consentimento na aceção do Regulamento (UE) 2016/679 - Adotadas em 28 de novembro de 2017 - Última redação revista e adotada em 10 de abril de 2018

[31] Considerando n.º 59 da GDPR estabelece: (59) Deverão ser previstas regras para facilitar o exercício pelo titular dos dados dos direitos que lhe são conferidos ao abrigo do presente regulamento, incluindo procedimentos para solicitar e, sendo caso disso, obter a título gratuito, em especial, o acesso a dados pessoais, a sua retificação ou o seu apagamento e o exercício do direito de oposição. O responsável pelo tratamento deverá fornecer os meios necessários para que os pedidos possam ser apresentados por via eletrónica, em especial quando os dados sejam também tratados por essa via. O responsável pelo tratamento deverá ser obrigado a responder aos pedidos do titular dos dados sem demora injustificada e o mais tardar no prazo de um mês e expor as suas razões quando tiver intenção de recusar o pedido.

bem como os fundamentos legais em que o tratamento se baseia antes de recolher as informações. Com certeza, em grande parte das vezes, o tratamento disporá de dois ou mais fundamentos possíveis. Como exemplo, citemos um caso no qual ele se dê mediante o consentimento, fazendo-se também necessário à execução de um contrato. Assim sendo, caso ocorra posteriormente a revogação da anuência, isso não significa que o responsável pelo tratamento tenha que apagar os dados processados, desde que eles sejam utilizados para alguma finalidade relacionada à execução do ajuste celebrado com o titular. Por conseguinte, o controlador deve, desde o início, ser muito claros quanto a tal finalidade, estabelecendo bem sua correspondência com cada um dos elementos presentes nos dados.

VII. O tratamento de dados de crianças e adolescentes:

> *Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.*
> *§ 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.*
> *§ 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.*
> *§ 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.*
> *§ 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.*

> *§ 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.*
> *§ 6º 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.*

Segundo o Estatuto da Criança e do Adolescente – ECA (Lei 8.069/90), criança é a pessoa com até doze anos de idade incompletos, e adolescente aquela que tem entre doze e dezoito anos de idade[32].

A LGPD, reconhecendo a maior vulnerabilidade e suscetibilidade dessa classe de titulares, criou para ela um nível de proteção maior, impondo ao controlador a obrigação de que o tratamento de dados referentes aos menores seja realizado "em seu melhor interesse"[33]. Logo, para que se dê efetividade a essa determinação legal, a operação com as informações pessoais de crianças e adolescentes deve ser pensada e realizada de maneira a não os prejudicar. Além disso, deve, ainda, trazer-lhes benefícios que, na ausência do tratamento, não seriam possíveis, ou seriam de mais difícil acesso (COTS, 2019, p. 115).

Note-se, portanto, que, quando o fundamento legal para o tratamento for o do consentimento, o controlador, além de ter que atuar em prol do melhor interesse do menor, deverá obter a anuência de forma específica e destacada de, pelo menos, um dos pais ou do responsável legal e, ainda, realizar todos os esforços razoáveis para verificar a autenticidade desse vínculo, considerando-se as tecnologias disponíveis para esse fim. Nesse

---

[32] Art. 2º Considera-se criança, para os efeitos desta Lei, a pessoa até doze anos de idade incompletos, e adolescente aquela entre doze e dezoito anos de idade. Parágrafo único. Nos casos expressos em lei, aplica-se excepcionalmente este Estatuto às pessoas entre dezoito e vinte e um anos de idade.

[33] Embora a expressão "em seu melhor interesse" seja bastante subjetiva e pouco assertiva, as diretrizes para o que seja o melhor interesse do menor estão dispostas no art. 227 da Constituição da República, *verbis*: "*Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, 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*".

sentido, resta evidente que o fornecimento da data de nascimento do titular é requisito para o cumprimento das disposições da LGPD[34].

No que se refere à observação dos princípios da finalidade, da transparência e da adequação previstos no artigo 6º da LGPD, a Lei, de forma redundante, reitera aquilo que se aplica a todas as demais classes de titulares, sem estabelecer obrigação adicional que decorra, especificamente, da qualidade de criança ou de adolescente. De tal maneira, determina que as informações coletadas pelo controlador não devem extrapolar aquelas estritamente necessárias à prática de atividades como: participação em jogos e aplicações de internet, dentre outras.

Por fim, cumpre destacar que o parágrafo 6º determina ao controlador a utilização de recursos necessários para que as informações de tratamento sejam simples, claras e acessíveis, não só considerando a compreensão do responsável legal pelo menor – que, conforme visto, deverá autorizar o tratamento, quando este for embasado no consentimento – mas, também, a dos próprios titulares dos dados. Parece-nos que, embora o intuito seja louvável, haverá hipóteses em que o entendimento sobre o alcance do tratamento poderá ser parcial ou mesmo inexistente, em especial quando se tratar de dados coletados mediante a disponibilização de serviços ou produtos voltados para crianças ainda muito pequenas.

Importante destacar que o consentimento é apenas um dos fundamentos jurídicos possíveis para o tratamento de dados de crianças e adolescentes. Contudo, algumas dessas bases legais não se coadunam com a disciplina do tratamento às informações pessoais de menores, como é o

[34] A verificação da idade não deve conduzir a um tratamento de dados excessivo. O mecanismo escolhido para verificar a idade de um titular de dados deve envolver a avaliação do risco do tratamento proposto. Nalgumas situações de baixo risco, pode ser adequado exigir que o novo subscritor do serviço revele o seu ano de nascimento ou preencha um formulário onde declara (não) ser menor. Caso tenha dúvidas, o responsável pelo tratamento deve reavaliar os seus mecanismos de verificação da idade num determinado caso e considerar se são necessárias verificações alternativas. O GT29 reconhece que pode haver casos em que a verificação seja difícil (por exemplo, quando as crianças que estão a dar consentimento ainda não estabeleceram uma «pegada» em termos de identidade ou quando a responsabilidade parental não pode ser verificada facilmente). Esta questão pode ser tida em conta quando for necessário decidir quais são os esforços razoáveis, mas é de esperar que os responsáveis pelo tratamento sujeitem os processos que utilizam e a tecnologia disponível a uma revisão constante.

caso do legítimo interesse do controlador e da proteção ao crédito (COTS, 2019, p. 116-117)[35].

VIII. Conclusão:

A disciplina do tratamento de dados pessoais se dá no contexto da sociedade informacional, tecnológica e digital, em meio à concretização da computação ubíqua, pervasiva e inteligente, que impõe ampla discussão sobre novas soluções jurídicas que venham com o intuito de regular a atuação dos players do mercado e de proteger a parte mais vulnerável da relação.

Assim sendo, é necessário que o Direito compreenda e absorva as dificuldades de se dar ao titular de dados pessoais a garantia de que suas escolhas sejam verdadeiramente fruto de uma manifestação de vontade livre e informada. Trata-se de uma questão substancial para que o debate acerca da legislação e do empoderamento do titular não se torne estéril.

Urge a implementação de medidas regulatórias e fiscalizatórias que promovam, com eficácia, a autodeterminação informativa daquele que está no epicentro das questões de privacidade: o cidadão. Somente assim, mediante uma harmonização do arranjo jurídico-normativo da privacidade com as ferramentas tecnológicas que lhe são subjacentes é que poderemos pensar numa real relação de paridade entre o titular dos dados e os operadores de tratamento, alcançando o fim pretendido – qual seja, a sua capacidade e autonomia para o controle de seus dados pessoais[36].

A proteção do titular como ponto central da regulamentação da proteção dos dados pessoais, contudo, não pode ser um obstáculo ao desenvolvimento econômico e aos avanços tecnológicos, o que impõe ao Jurista o grande desfio de criar soluções que, ao mesmo tempo, assegure

[35] COTS, Márcio, e OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais comentada. 2ª ed. Rev. Atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2019. págs. 116-117.*

[36] "Trata-se, portanto, de promover o encontro entre o arranjo jurídico-normativo da privacidade informacional com a realidade que lhe é subjacente, buscando-se novas formas para o venerado consentimento do titular dos dados pessoais, nutrindo-se, em última análise, a sua capacidade (autonomia) em controla-los". BIONI, 2019. p. 272.

ao titular dos dados a proteção de seus direitos e, também, permita o desenvolvimento econômico e tecnológico e a inovação através da livre iniciativa e da livre concorrência.

IX. Referências:

BIONI, Bruno Ricardo. **Proteção de dados pessoais – a função e os limites do consentimento**. 1ª Ed. Rio de Janeiro: Forense, 2019.

BRASIL. **Lei nº°13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Publicado no Diário Oficial da União de 15/08/2018.

BRASIL. **Lei nº°10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Publicado no Diário Oficial da União em 11/01/2002.

BRASIL. **Lei nº°8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Publicado no Diário Oficial da União em 16/7/1990 e retificado em 27/09/1990.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de Dados e privacidade: do direito às novas tecnologias na sociedade da informação**. Rio de Janeiro: Lumen Juris, 2018.

FRAZÃO, Ana. **Plataformas Digitais, Big Data e Riscos para os direitos da personalidade**. In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de. Coord. Autonomia privada, liberdade existencial e direitos fundamentais. Belo Horizonte: Forum, 2019. p. 333 – 348.

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18)**. 1ª ed. Goiânia: RM Digital Education, 2019.

MAIA, Roberta Mauro Medina. **Vivendo nas nuvens: dados pessoais são objeto de propriedade?** In: TEPEDINO, Gustavo; MENEZES, Joyceane Bezerra de. Coord. Autonomia privada, liberdade existencial e direitos fundamentais. Belo Horizonte: Forum, 2019. p. 669 – 695.

MALDONADO, Viviane Nóbrega e OPICE BLUM, Renato; coord. **LGPD: Lei Geral de Proteção de Dados comentada**. São Paulo: Thomson Reuters Brasil, 2019.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

PIRES, Eduardo; e ADOLFO, Luiz Gonzaga Silva. **Autonomia privada e suas limitações legais: reflexo da incidência indireta dos direitos fundamentais**. Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito (RECHTD). São Leopoldo/RS, v. 7, n. 2, maio-agosto 2015. Disponível em: http://www.revistas.unisinos.br/index.php/RECHTD/issue/view/540. Acessado em: 30/11/2019.

SARLET, Gabrielle Bezerra Sales; e CALDEIRA, Cristina. **O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana**. Revista Civilística.com. a. 8. n. 1. 2019. Disponível em: http://civilistica.com/o-consentimento-informado-e-a-protecao/ Acessado em: 01/12/2019.

SMITH, Adam. **A Riqueza das Nações**. Apres. Winston Fritsch. Trad. Luiz João Baraúna. São Paulo: Editora Nova Cultural. 1996.

VICENTE, Dario Moura. **A autonomia privada e os seus diferentes significados à luz do direito comparado.** Revista de Direito Civil Contemporâneo 2016, vol. 8, julho-setembro 2016. Acessado em: 01/12/2019.

UNIÃO EUROPEIA. GRUPO DE TRABALHO DO ARTIGO 29. **Orientações relativas ao consentimento na aceção do Regulamento (EU) 2016/679**. Disponível em: https://www.cnpd.pt/bin/rgpd/docs/wp259revo.1_PT.pdf. Acessado em: 29/11/2019.

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia (2016/C 202/02)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT. Acessado em: 30/11/2019.

UNIÃO EUROPEIA. **Regulamento 2016/679 de 27 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. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em: 28/11/2019.

2

As bases legais para o tratamento de dados pessoais: muito além do consentimento

Guilherme Henrique Gualtieri de Oliveira [1]

1. Introdução

Desde agosto de 2018 os debates acerca dos temas de privacidade, proteção de dados e segurança da informação tomaram conta de nosso país com o advento da Lei Geral de Proteção de Dados Pessoais (LGPD), uma lei cujo principal objetivo é estabelecer critérios e limites para o tratamento de dados pessoais, e que passará a ser exigida em todo território nacional a partir de agosto de 2020, quando entrará em vigor.

Até meados do ano de 2018 o tema da privacidade era pouquíssimo debatido em nosso país, mas com o advento da Regulação Geral de Proteção de Dados europeia (comumente conhecida como GDPR), e diante de escândalos reiterados de violação de dados, como o caso da Cambridge Analytica, que deixou evidente o quão poderoso pode ser o nível de controle que um agente de tratamento pode ter sobre os titulares dos dados tratados, a questão da privacidade e da proteção de dados pessoais passou a ser discutida como nunca, em âmbito mundial, tendo o Brasil iniciado sua caminhada nesse sentido.

Carolina da Silva Leme, em seu estudo sobre a proteção e o tratamento de dados do ponto de vista da legislação vigente, narra um

[1] Advogado, Especialista em Direito Tributário pela PUC-MG e certificado em *Privacy & Data Protection* e *Information Security* pela Exin Holanda.

pouco sobre o histórico do advento da Lei Geral de Proteção de Dados Pessoais em nosso país:

> Após aprovação da Regulamentação Geral de Proteção de Dados (GDPR) pela União Europeia e o escândalo da Cambridge Analytica, tornou-se ainda mais latente a necessidade de o Brasil editar legislação de proteção de dados mais aprofundada, visando a nortear a coleta, uso, armazenamento e processamento de dados entre entres públicos e privados, bem como se enquadrar no padrão internacionalmente exigido.
> A aprovação de uma legislação específica de proteção de dados traz também relação com o intuito de o Brasil pleitear seu ingresso na Organização para a Cooperação e desenvolvimento Econômico (OCDE) (KUJAWSKI; THOMAZ, 2018, p. 1). Isso porque, mencionado órgão traz diretrizes e orientações acerca do tema desde 1980 e, em 2013, as atualizou para adequá-las ao nível de sociedade de informação atual. Embora as orientações da OCDE não tenham força de lei, consistem em requisitos para seu ingresso, sendo essencial para o Brasil a edição de norma mais robusta acerca do tema (MONTEIRO, 2017, p. 6).
> Nesse contexto, aos 14 de agosto de 2018 foi sancionada a Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), a qual se aplica "a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados", salvo exceções estipuladas em seu artigo 4º.[2]

De acordo com o art. 1º, *caput*, da referida lei, esta é aplicável a todo o tipo de tratamento de dados pessoais, inclusive nos meios digitais (apesar de que, provavelmente, nos dias atuais, a maior parte dos tratamentos de dados pessoais se dê justamente pelos meios digitais), seja por pessoa natural ou jurídica de direito privado ou público e se presta a proteger a liberdade, a privacidade e o livre desenvolvimento da personalidade do ser humano:

[2] LEME, Carolina da Silva. Proteção e Tratamento de Dados sob o Prisma da Legislação Vigente. Disponível em: <http://www.veirano.com.br/upload/content_attachments/920/591112_FID_01_Protecao_tratamento_dados_original.pdf>. Acesso em 02 de dezembro de 2019.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural[3] (BRASIL, 2017).

Além disso, o art. 3º da LGPD dispõe que a lei aplica-se a qualquer operação de tratamento de dados pessoais, seja ela realizada por pessoa natural ou jurídica, independente do meio, do país da sede ou onde estejam localizados os dados, desde que a operação se dê no território brasileiro; o objetivo do tratamento for a oferta ou fornecimento de bens ou serviços no território brasileiro ou se os dados pessoais forem coletados em território brasileiro:

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional[4] (BRASIL, 2017).

Por se tratar de lei que mudará completamente a cultura de coleta de dados no Brasil, é razoável que as empresas brasileiras estejam um tanto quanto perdidas neste momento, com muitas dúvidas a respeito de quais dados pessoais podem ou não ser tratados, de que forma esse tratamento ocorrerá e até onde podem avançar, preservando o cumprimento da lei e a continuidade de seu negócio, em equilíbrio.

---

[3] BRASIL. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 02 de dezembro de 2019.

[4] BRASIL. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 02 de dezembro de 2019.

Contudo, um bom ponto de partida para estabelecer critérios objetivos dentro da corporação no sentido de definir a forma que os dados pessoais serão tratados é o art. 7º da LGPD, que estabelece as 10 bases legais para o tratamento de dados pessoais e que, juntamente com os princípios descritos no art. 6º, formam o alicerce para qualquer atividade que envolva tratamento de dados pessoais daqui para frente.

2. As bases legais da LGPD

Como dito anteriormente, a Lei Geral de Proteção de Dados Pessoais estabeleceu, em seu artigo 7º, que o tratamento de dados pessoais somente poderá ser realizado nas hipóteses taxativas previstas em cada um de seus 10 (dez) incisos, que são exatamente as 10 bases legais autorizadoras para o tratamento de dados pessoais, que passamos a analisar mais detidamente a seguir:

a) Mediante o fornecimento de consentimento pelo titular

Esta é, possivelmente, a base legal de tratamento de dados mais difundida pelos consultores e estudiosos do tema em geral, mas é importante ressaltar que se trata, ao mesmo tempo, daquela mais problemática no que tange à sua gestão.

Isso se deve ao fato de que a LGPD exige que o consentimento seja, além de livre e informado, fornecido por escrito ou por outro meio que demonstre a manifestação inequívoca de vontade do titular.

Quando o consentimento se der por escrito, ele deverá constar em uma cláusula destacada das demais contratuais, que não poderá ser genérica, justamente para que seja comprovado que aquele consentimento foi dado para uma finalidade específica de tratamento.

Tal exigência acaba por se traduzir no primeiro grande desafio no campo prático, uma vez que, atualmente, é extremamente costumeiro o uso do campo de acionamento contendo a declaração “Li e Aceito Todos os

Termos", o que, sabemos, quase nunca se comunica de fato com a realidade.

Caso não seja demonstrado que o consentimento foi livre, manifesto e inequívoco, o mesmo será considerado nulo, nos termos da Lei Geral de Proteção de Dados Pessoais, ao contrário do Código Civil, que estabelece que o vício de consentimento é ato anulável.

Pedro Silveira Campos Soares esclarece em seu artigo a diferença entre o vício do consentimento estabelecido pelo Código Civil (que o trata como vício anulável), para o vício do consentimento na LGPD (que é nulo, por determinação normativa):

> Mostra-se particularmente relevante notar que o consentimento previsto na LGPD deve ser livre e espontâneo, sob pena de configurar vício de vontade, a torná-lo nulo. Extrai-se daí diferença substancial entre o tratamento previsto no Código Civil e na LGPD para negócios jurídicos defeituosos, que deve ser objeto de atenção pelos agentes de tratamento de dados. De fato, enquanto para o Código Civil a manifestação atingida por vício de consentimento é, em regra, anulável, na LGPD esta mesma declaração configura hipótese de nulidade[5].

Diante disso percebe-se, antes de mais nada, que o vício de consentimento no contexto da LGPD é expressivamente mais gravoso do que aquele ocorrido no cenário das relações comerciais clássicas, já que quando regido pela Lei 13.709/2018, o vício de consentimento o torna nulo de pronto, sem sequer que haja a necessidade de qualquer comprovação complementar.

A de se convir, ainda, que problema maior no tratamento de dados pessoais com base no consentimento do titular, é o fato de que ele pode acabar se tornando um autorizador transitório, uma vez que pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado.

---

[5] SOARES. Pedro Silveira Campos. A Questão do Consentimento da Lei Geral de Proteção de Dados. Disponível em < https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados#_ftn1>. Acesso em 02 de dezembro de 2019.

Em outras palavras, caso uma empresa colete dados através do consentimento dos titulares desses dados, será necessário dispor de algum tipo de plataforma que permita a absoluta gestão dos consentimento concedidos, cronologicamente controlados, além da eventual exclusão dos dados diante de requisição do titular e que mantenha evidência dessa exclusão para fins de comprovação posterior, caso necessário, e tudo isso de forma gratuita.

Portanto, por mais que o consentimento se apresente como o mais famoso autorizador para o tratamento de dados pessoais, e, ainda, seja tentador adotar a facilitada solução de simplesmente coletar consentimento para qualquer operação, é altamente recomendável que se busque localizar dentro das demais bases legais a existência de uma que se encaixe adequadamente à natureza do tratamento, de forma mais robusta e confiável.

Além disso, é interesse levar em consideração que a coleta de dados se dê com base no consentimento somente de forma residual, caso não seja possível o tratamento de dados através de alguma outra das outras 9 bases legais expostas ao longo deste texto, com exceção, talvez, do legítimo interesse quando em casos muito particulares.

b) Para o cumprimento de obrigação legal ou regulatória pelo controlador

A 2ª base legal para tratamento de dados pessoais prevista pela LGPD é o cumprimento de obrigação legal ou regulatória pelo controlador. Este é um autorizador da LGPD que visa garantir que a lei não entre em conflito com outras legislações vigentes em nosso país.

Com efeito, trata-se de base que se presta a evitar antinomias, cenário que acabaria por gerar uma discussão sobre a possibilidade ou não do titular de dados registrar reclamação contra um tipo de tratamento de dados que estivesse em discordância com outra determinação legal.

Ana Frazão esclarece que, ao estabelecer esta base legal para tratamento de dados pessoais, o legislador pretendeu atender o interesse público, mas ressaltando que, mesmo nesses casos, o controlador deverá observar os princípios pertinentes previstos na LGPD:

> O inciso II do art. 7º da LGDP traz a hipótese de cumprimento de obrigação legal ou regulatória pelo controlador. Com efeito, em casos assim, o tratamento de dados é considerado necessário para atender o interesse público que justifica a obrigação legal ou regulatória. Todavia, mesmo nesse caso, os controladores deverão observar os princípios pertinentes, especialmente no que toca (i) à adstrição do tratamento à finalidade específica de cumprimento da determinação legal, (ii) à adoção dos meios adequados e necessários para tal, bem como (iii) à preocupação com todos os direitos do titular, dentre os quais se destaca o direito de ser informado do tratamento de dados (§ 1º, do art. 7º, da LGPD) e o direito de ter os dados disponibilizados nos exatos termos do que for especificado pela autoridade nacional (§ 2º, do art. 7º, da LGPD)[6] (FRAZÃO, 2018).

No caso de uma obrigação decorrente de lei acarretar em um tratamento de dados pessoais por parte de uma empresa, essa estará autorizada a trata-los de modo a cumprir a dita exigência legal ou regulatória.

Exemplificando, seria o caso de uma empresa transmitir os dados de seus empregados constantes de seus registros internos de RH à Secretaria Especial do Ministério da Economia (antigo Ministério do Trabalho), a fim de cumprir com a entrega da Relação Anual de Informações Sociais (RAIS). Nesse caso, os empregados não podem opor resistência ao compartilhamento de dados, uma vez que é necessária para o cumprimento de uma obrigação legal/regulatória por parte do controlador.

---

[6] FRAZÃO, Ana.Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Disponível em < www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018>. Acesso em 02 de dezembro de 2019.

É sempre importante deixar claro que o fato de o tratamento estar autorizado por qualquer uma das bases legais não afasta a necessidade de atendimento aos princípios trazidos pelo art. 6º da mesma lei.

c) Pela 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, observadas as disposições do Capítulo IV desta Lei;

Durante o trabalho de adequação à LGPD, uma das principais dúvidas que surgem é quanto à aplicabilidade da lei se aplica ao tratamento de dados pessoais realizado por parte da Administração Pública.

O inciso III do art. 7º da LGPD responde a esta pergunta de maneira categórica ao estabelecer que sim, órgãos da administração pública precisam se adequar e cumprir a lei ao tratarem e compartilharem dados pessoais para execução de políticas públicas ou respaldadas em contratos, convênios ou instrumentos congêneres, sem a necessidade de consentimento dos titulares.

Contudo, a Administração Pública é obrigada a fornecer ao titular dos dados informações claras e inequívocas sobre a base legal para o tratamento dos dados, a finalidade e quais os procedimentos utilizados ao longo do ciclo de vida do dado dentro dos sistemas da Administração Pública.

A Administração Pública somente não estará obrigada a cumprir com as exigências da LGPD no caso de tratamento de dados feito exclusivamente para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou de repressão de infrações penais.

Exemplificando uma hipótese de uso compartilhado de dados necessário à execução de políticas públicas, Ericson Scorsim nos apresenta

o exemplo clássico do o compartilhamento de dados pessoais dos cidadãos para fins de arrecadação de impostos e combate à sonegação fiscal:

> Também, é autorizado o tratamento de dado pessoal pela administração pública na hipótese de uso compartilhado de dados necessários à execução de políticas públicas. Exemplo: a política pública de tributação, com o compartilhamento de dados pessoais dos cidadãos, para fins de arrecadação de impostos[7].

De se ressaltar que os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado aos órgãos públicos, devendo fornecer acesso aos dados por meio eletrônico para a Administração Pública.

Uma grande diferença da aplicação da LGPD aos órgãos públicos para o âmbito privado diz respeito às penalidades aplicadas. Para a Administração Pública, não há a previsão de sanção pecuniária, mas apenas a advertência, a publicização da infração, bloqueio ou eliminação dos dados pessoais a que se refere a infração, sem prejuízo das sanções previstas no Estatuto do Servidor Público Federal, na lei de Improbidade Administrativa e na lei de acesso à informação.

d) Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

Também é permitido o tratamento de dados pessoais realizado com finalidade de estudo por órgãos de pesquisa, de modo que, sempre que possível, estes dados deverão ser anonimizados a fim de garantir a privacidade dos titulares no caso de possíveis vazamentos, uma vez que um dado anonimizado deixa de ser associável ao seu titular, considerando a utilização de técnicas razoáveis na ocasião do tratamento.

---

[7] SCORSIM. Ericson Meister. Lei brasileira de proteção de dados pessoais: análise de seu impacto para os titulares de dados pessoais, empresas responsáveis pelo tratamento de dados pessoais e setor público. Disponível em: < https://www.migalhas.com.br/dePeso/16,MI286453,21048-Lei+brasileira+de+protecao+de+dados+pessoais+analise+de+seu+impacto> Acesso em 02 de dezembro de 2019.

O artigo 5º, XVIII da Lei Geral de Proteção de Dados Pessoais define órgão de pesquisa da seguinte maneira:

> Art. 5º Para os fins desta Lei, considera-se:
> (...)
> XVIII - órgão de pesquisa: como um órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico[8] (BRASIL, 2017).

Uma prática já utilizada pelos órgãos de pesquisa com o intuito de anonimizar os dados pessoais é, por exemplo, quando em uma pesquisa para apuração de intenção de votos em uma eleição, haja a proporção de votação para cada candidato de acordo com sexo, escolaridade, região geográfica, classe social, etc.

O resultado da pesquisa é cumprido, ao ponto que é praticamente impossível saber quem foram as pessoas que demonstraram aquelas intenções utilizando-se de técnicas razoáveis para tentar atribuir um conjunto de dados a uma pessoa individualizada.

e) Quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

A 5ª base legal autorizadora do tratamento de dados pessoais é a necessidade para execução de um contrato ou de procedimentos preliminares relacionadas a um contrato que o titular dos dados figurará como integrante.

Nesse caso, o tratamento de dados se dará a pedido do próprio de titular dos dados para garantir a execução de um contrato ou de seus

[8] BRASIL. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 02 de dezembro de 2019.

procedimentos preliminares. Essa hipótese se assemelha um pouco com o tratamento de dados via consentimento, com a diferença de que o titular dos dados não poderá revogar o seu fornecimento a qualquer momento, uma vez que a outra parte estará resguardada pela LGPD para poder manter sob sua posse os dados fornecidos pelo titular enquanto durar a vigência do contrato e, se necessário, por um prazo posterior ao seu término.

Um exemplo seria a contratação por parte de um titular de dados de um serviço cujo objeto principal é o tratamento de dados pessoais, tal como acontece com a inserção de dados em um serviço de armazenamento em nuvem.

A ideia aqui é garantir que não seja possível a invocação do direito à privacidade como instrumento de fraude a contratos e obrigações entre particulares, já que, obviamente, tal direito encontra teto no ordenamento jurídico, como já havia sido sugerido por Warren e Brandeis em 1890, em sua obra científica "The Right to Privacy".

f) Para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307/96 (Lei de Arbitragem);

Outra base legal possível de ser utilizada pelo agente de tratamento é aquela referente a operações que visem o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Esse autorizador trazido pela LGPD é uma decisão acertada no intuito de garantir a efetiva postulação, incluindo o direito de produção de provas de uma parte contra a outra em um processo judicial (na maioria das vezes), administrativo ou arbitral, este último nos termos da Lei de Arbitragem.

Permitir que uma das partes se oponha a este tipo de tratamento de dados seria cercear o direito de defesa da outra em um processo e infringir os preceitos constitucionais da ampla defesa e do contraditório, e, como

dito anteriormente, a invocação do direito à privacidade com intuito de lesão alheia é torpe e inadmissível.

Esse posicionamento é reiterado por Ana Frazão que, em seu artigo, esclarece que essa ressalva, apesar de lógica, foi expressamente incluída no texto final da LGPD a fim de deixar claro que a proteção aos dados pessoais não compromete o direito que os integrantes de um processo possuem de produzi provas uns contra os outros:

> Outra importante hipótese de tratamento de dados é o exercício regular de direitos em processo judicial, administrativo ou arbitral (art. 7º, VI, da LGPD), ressalva fundamental para deixar claro que a proteção aos dados pessoais não compromete o necessário direito que as partes têm de produzir provas umas contra as outras, ainda que estas se refiram a dados pessoais do adversário[9] (FRAZÃO, 2018).

g) Para a proteção da vida ou da incolumidade física do titular ou de terceiro;

Ademais, a LGPD também admite o tratamento de dados feito com o intuito de proteger a vida ou a incolumidade física do titular dos dados ou de terceiros.

Trata-se de um autorizador legal cujo objetivo é garantir a proteção de bens de elevado interesse público, tais como a vida e a incolumidade física, desde que devidamente comprovada essa necessidade e exposta a finalidade do tratamento dos dados nesta situação.

Esta é uma base legal autorizadora para o tratamento de dados pessoais tão específica que até mesmo o art. 11, II, *e* da LGPD estabelece que dados pessoais sensíveis poderão ser tratados sem o fornecimento de consentimento do titular, caso sejam indispensáveis para a proteção da vida ou da incolumidade física do titular ou de terceiros, haja vista o enorme interesse público envolvido neste tipo de tratamento, bem como a

[9] FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Disponível em < www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018>. Acesso em 02 de dezembro de 2019.

garantia do direito fundamental à vida previsto no art. 5º da Constituição Federal de 1988.

Um bom exemplo deste tipo de tratamento de dados seria o caso de uma pessoa que, inconsciente, da entrada em um hospital que nunca esteve na vida, após sofrer um grave acidente. Nesse caso, o novo hospital pode precisar de todo o histórico médico do paciente constante de um outro hospital que ele costuma frequentar, estando, portanto, autorizado o médico que irá atende-lo a requisitar a documentação ao outro hospital, que poderá compartilhar toda a documentação que disponha daquele paciente, com objetivo restritivo de atender à situação.

h) Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

Seguindo a mesma ideia da base legal mencionada no item anterior, a LGPD também autoriza o tratamento de dados para a tutela da saúde, desde que realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

É também uma base legal que tem como plano de fundo o interesse público no tratamento dos dados pessoais, sendo objeto de regras específicas dentro da própria LGPD quando o controlador atuar na área da saúde. Provavelmente será um dos itens de maior debate ao longo da formação e consolidação da consciência de proteção de dados na sociedade brasileira.

Da mesma forma que o item anterior, esta também é uma base legal autorizadora para o tratamento de dados pessoais bastante específica, ja que o art. 11, II, f, da LGPD estabelece que dados pessoais sensíveis poderão ser tratados sem o fornecimento de consentimento do titular, caso sejam indispensáveis para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

Patrícia Peck, uma das maiores autoridades do tema no Brasil, esclarece em seu artigo que, em que pese o setor da saúde não estar obrigado a ter o consentimento em todas as situações de tratamento de dados pessoais, esta somente é válida para a tutela da saúde, que é um procedimento realizado exclusivamente por profissionais da saúde, serviços de saúde ou por autoridade sanitária.

> Um ponto importante da LGPD na saúde é que o setor não está obrigado a ter o consentimento em todas as situações de tratamento de dados (são as hipóteses de exceção tratadas principalmente nos artigos 7º, 10º e 11º). Isso mesmo! A dispensa ocorre nos casos de proteção à vida ou tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; obrigação legal ou regulatória; para execução de contratos com o titular dos dados; em processos judiciais ou administrativos; quando há legítimo interesse do controlador; ou, ainda, no caso de estudo por órgãos de pesquisa.
>
> Mas neste quesito, "os fins não justificam os meios", mesmo na causa da saúde, houve alteração na redação final do artigo 7º, inciso VIII, no qual ficou destacado que tutela da saúde é exclusivamente procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Além disso, a lei revela que é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados[10].

Uma especificidade do tratamento com base neste inciso é a autorização do art. 11 da referida lei para a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde nos casos de prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, com objetivo de obter vantagem econômica, desde que

[10] PECK, Patrícia. LGPD e saúde: os fins justificam os meios? Disponível em < https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude>. Acesso em 02 de dezembro de 2019.

em benefício dos interesses dos titulares de dados, sendo vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

Isso significa que qualquer outro tipo de comunicação ou uso compartilhado de dados referentes à saúde é categoricamente vedado pela LGPD quando amparado por esta base legal específica.

i) Quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais;

Ficando atrás, talvez, apenas do consentimento, a base legal mais difundida é, sem sombra de dúvidas, o legítimo interesse do controlador ou de terceiros. No entanto, assim como o consentimento, trata-se de base potencialmente problemática, sendo recomendada a sua utilização somente quando não houver outra base legal aplicável ao caso, pela nebulosidade e fragilidade que envolvem o tema.

Além de ser um tanto quanto difícil apontar, neste momento, o que seria o "legítimo interesse" do controlador ou de terceiros, uma vez que não há uma previsão legal no ordenamento jurídico brasileiro a respeito da definição deste termo, é sempre muito importante sopesar até que ponto o legítimo interesse do controlador ou de terceiro sobrepõe o do titular dos dados, ou fere alguma outra disposição expressa da LGPD.

O art. 10 do diploma sob análise determina que o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, no rol exemplificativo descrito abaixo:

> Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

> I - apoio e promoção de atividades do controlador; e
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei[11] (BRASIL, 2017).

Além disso, é importante esclarecer que os parágrafos 1º, 2º e 3º do referido artigo ensinam que, quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, além do que o controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.

Ademais é importante destacar que a Autoridade Nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Portanto, para que se possa utilizar esta base legal como autorizadora para o tratamento de dados é necessário identificar um interesse inequivocamente legítimo, demonstrar que o tratamento de dados é necessário para se atingir tal objetivo e tomar o devido cuidado para não violar nenhum dispositivo legal ou nenhum direito do titular daqueles dados, além de tratar somente os dados pessoais estritamente necessários para a finalidade pretendida.

Por fim, é recomendável que, seja qual for o interesse legítimo em questão, este esteja dentro de um escopo de expectativa que os titulares têm quanto à utilização de seus dados, de modo a evitar surpresas desagradáveis e eventuais oposições expressas por parte deles.

j) Para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

[11] BRASIL. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 02 de dezembro de 2019.

A 10ª e última base legal possível de utilização para se realizar o tratamento de dados pessoais é a proteção do crédito, em observância às regras especificas para este tema.

O objetivo do legislador foi evitar que titulares de dados pessoais se utilizem de uma brecha legislativa para criarem mecanismos de "calote", invocando o direito à privacidade em benefício da própria torpeza e possivelmente escaparem de cobranças por dívidas legítimas.

É de se estranhar que um titular de dados pudesse requerer exclusão dos seus cadastros dos bancos do SPC e do Serasa, por exemplo, sob a alegação de que não autorizou o referido tratamento ou que violaria a sua privacidade, safando-se, assim, de instrumentos que se prestam justamente a efetivar a cobrança do crédito.

Debates acalorados sobre um possível conflito entre a inclusão automática no Cadastro Positivo e a LGPD surgiram no meio acadêmico, discussão essa que possivelmente somente será resolvida com a efetiva atuação consultiva da Autoridade Nacional de Proteção de Dados.

Uma das missões da autoridade será, sem dúvidas, harmonizar as determinações de ambos os dispositivos legais, uma vez que é sim possível que o Cadastro Positivo siga as regras da LGPD, notadamente no que diz respeito à transparência e à informação sobre o tratamento dos dados pessoais.

Analisando esta questão, os advogados Thais de Gobbi, Elton Minasse e Yuri Camelo Ribeiro esclarecem que a LGPD é a única lei no mundo que prevê a proteção ao crédito como base legal específica para o tratamento de dados, o que possibilitou que a Lei do Cadastro Positivo não seja conflitante, uma vez que esta base legal é uma exceção à exigência do consentimento para realizar o tratamento:

> Curiosamente, entre as leis que versam sobre proteção de dados pessoais no mundo, a brasileira é a única a prever a proteção ao crédito como uma de suas bases legais para o tratamento de dados.
> Essa previsão possibilitou que a nova Lei do Cadastro Positivo esteja em consonância com a LGPD, já que não é mais necessário obter o consentimento

> do titular/cadastrado para usar os dados conforme as finalidades da lei. Sob esse aspecto, os dois textos convergem e conversam entre si.
> Contudo, essa conversa poderia ser mais clara. Ainda que a LGPD não estivesse em vigor quando da publicação da nova Lei do Cadastro Positivo, esta poderia ter utilizado os conceitos da LGPD sem prejuízo algum.
> Afinal de contas, o adjetivo "geral" contido na LGPD não deve ser desprezado: essa lei é a base normativa do microssistema brasileiro de proteção de dados pessoais, o que pode gerar discussões sobre o regime jurídico aplicável ao Cadastro Positivo naquilo que as duas leis conflitarem ou, de outra forma, não se harmonizarem perfeitamente[12] (2019, GOBBI; MINASSE e RIBEIRO).

3.Conclusão

O que se pretendeu ao longo deste artigo foi expor e esclarecer, de forma pormenorizada, todas as 10 bases legais admitidas e estabelecidas pelo art. 7º da LGPD, demonstrando que o tema vai bem além da mera questão do consentimento, tão propagado desde a publicação da Lei Geral de Proteção de Dados Pessoais.

Durante a exposição, utilizou-se de exemplos para facilitar a compreensão e difundir o conhecimento não apenas à comunidade jurídica, mas aos mais variados ramos de estudo sobre o tema, incluindo eventuais leigos no assunto.

A aplicação de algumas bases legais ainda pode gerar um certo receio em virtude da falta de orientação, mas é com a entrada em vigor da LGPD e a aplicação prática do tema no Brasil, principalmente com a atuação da Autoridade Nacional de Proteção de Dados, que terá papel não apenas de entidade punitiva, mas também como fonte de aconselhamento e segurança jurídica, em especial nos primeiros anos de vigência da lei, que poderemos atingir estabilidade normativa neste sentido.

---

[12] GOBBI, de Thais; MINASSE, Elton; RIBEIRO, Yuri Camelo. INTERFACE ENTRE A NOVA LEI DO CADASTRO POSITIVO E A LEI GERAL DE PROTEÇÃO DE DADOS. Disponível em < https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-ij/tecnologia/interface-entre-a-nova-lei-do-cadastro-positivo-e-a-lei-geral-de-protecao-de-dados>. Acesso em 02 de dezembro de 2019.

4. Referências

BRASIL. Lei Geral de Proteção de Dados Pessoais. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 02 de dezembro de 2019.

FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Disponível em < www.jota.info/opiniao-e-analise/artigos/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018>. Acesso em 02 de dezembro de 2019.

GOBBI, de Thais; MINASSE, Elton; RIBEIRO, Yuri Camelo. INTERFACE ENTRE A NOVA LEI DO CADASTRO POSITIVO E A LEI GERAL DE PROTEÇÃO DE DADOS. Disponível em <https://www.machadomeyer.com.br/pt/inteligencia-juridica/publicacoes-ij/tecnologia/interface-entre-a-nova-lei-do-cadastro-positivo-e-a-lei-geral-de-protecao-de-dados>. Acesso em 02 de dezembro de 2019.

LEME, Carolina da Silva. Proteção e Tratamento de Dados sob o Prisma da Legislação Vigente. Disponível em: <http://www.veirano.com.br/upload/content_attachments/920/591112_FID_01_Protecao_tratamento_dados_original.pdf>. Acesso em 02 de dezembro de 2019.

PECK, Patrícia. LGPD e saúde: os fins justificam os meios? Disponível em < https://www.serpro.gov.br/lgpd/noticias/2019/paciente-no-comando-lgpd-dados-sensiveis-saude>. Acesso em 02 de dezembro de 2019.

SCORSIM. Ericson Meister. Lei brasileira de proteção de dados pessoais: análise de seu impacto para os titulares de dados pessoais, empresas responsáveis pelo tratamento de dados pessoais e setor público. Disponível em: < https://www.migalhas.com.br/dePeso/16,MI286453,21048-Lei+brasileira+de+protecao+de+dados+pessoais+analise+de+seu+impacto> Acesso em 02 de dezembro de 2019.

SOARES. Pedro Silveira Campos. A Questão do Consentimento da Lei Geral de Proteção de Dados. Disponível em < https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados#_ftn1>. Acesso em 02 de dezembro de 2019.

3

O legítimo interesse como base legal para o tratamento de dados pessoais

Bernardo Menicucci Grossi [1]

1. A importância da proteção de dados na contemporaneidade

O direito à privacidade e o seu desdobramento na tutela da proteção de dados pessoais tem ganhado cada vez mais notoriedade no mundo contemporâneo em razão, acredita-se, da nitidez com que abusos recentes ganharam espaço na mídia internacional, como nos célebres casos envolvendo ataques terroristas como o de 11 de setembro, Edward Snowden e a política de monitoramento de chefes de Estado pelo governo estadunidense, o Wikileaks, a *Cambridge Analytica e o Facebook*, o *Brexit* e diversas campanhas eleitorais ao redor do mundo que cada vez mais se baseiam no perfilamento psicológico do eleitor e na construção de estratégias baseadas em *data analytics e big data*.

Não apenas por esses motivos, mas também por eles, houve uma aceleração dos projetos de lei envolvendo a proteção de dados pessoais no Congresso Nacional, o que culminou com a promulgação da Lei 13.709/18, a Lei Geral de Proteção de Dados - LGPD.

[1] Advogado, Doutorando em Direito Privado pela PUC Minas, Mestre em Direito Privado pela PUC Minas e Especialista em Direito Processual Civil pelo CAD. Presidente da Comissão de Proteção de Dados da OAB/MG e membro da Coordenação de Tecnologia e Inovação do Conselho Federal da OAB. É membro do Comitê Gestor do PJE do Tribunal de Justiça do Estado de Minas Gerais, Membro Efetivo do Instituto dos Advogados de Minas Gerais - IAMG e Membro Fundador do Instituto de Direito e Inteligência Artificial - IDEIA. Contato: bernardo@grossi.law

Essa breve recapitulação de eventos determinantes e prévios à aprovação da LGPD no Brasil é útil para ilustrar que o tema da proteção de dados não está limitado apenas ao âmbito do *compliance* empresarial ou às metas econômicas do Brasil em participar da OCDE ou de melhorar o grau de adequação de empresas que exportam para países da União Européia.

A regulação da proteção de dados, em verdade, tem relação direta com o exercício de direitos e garantias individuais, por vezes denominados de direitos fundamentais no âmbito interno ou como direitos humanos no âmbito internacional[2], e até mesmo com o conceito de democracia para o século 21. Como ilustra HARARI (2018, p.110-111):

> ... faríamos melhor em invocar juristas, políticos, filósofos e mesmo poetas para que voltem sua atenção para essa charada: como regular a propriedade de dados? Essa talvez seja a questão política mais importante da nossa era. Se não formos capazes de responder a essa pergunta logo, nosso sistema sociopolítico pode entrar em colapso. As pessoas já estão sentindo a chegada do cataclismo. Talvez seja por isso que cidadãos do mundo inteiro estão perdendo a fé na narrativa liberal, que apenas uma década atrás parecia irresistível.

O que Harari quer significar com isso é que passado o desafio da revolução agrícola e industrial, a tecnologia da informação já transformou em definitivo a nossa vida social, seja no aspecto íntimo ou coletivo, político ou econômico. E que a convergência da posse sobre dados pessoais dos cidadãos por grandes empresas ou países, que exercem análises cada vez mais impressionantes de seu *big data* para deles extrair inferências inimagináveis ao cálculo que o intelecto humano pode conceber diretamente, está a reclamar uma grande releitura através de uma regulação ostensiva e efetiva em âmbito global.

[2] Não se desconhece, aqui, a divergência conceitual entre cada um desses termos. Todavia, dado o recorte metodológico ora proposto o seu aprofundamento se mostrou desnecessário. Por todos, ver SÁ, Maria de Fátima Freire de. *Et. al.* (2017).

A assimetria de poder gerada em razão da grande concentração de dados pessoais em grandes conglomerados de tecnologia como, exemplificativamente, o *Google* ou *Facebook* acabam constituindo indutores naturais ao aproveitamento dessas oportunidades no campo empresarial, sendo cada vez mais relevante o envolvimento de toda a sociedade nesse debate para evitar abusos, manipulação e direcionamento de consumo e opinião e até mesmo reduzir a desigualdade econômica.

A mesma linha de pensamento é adotada por RODOTÁ (2008, p.19) já no prefácio de sua obra, segundo o qual a *proteção de dados é uma expressão de liberdade e dignidade pessoais e, como tal, não se deve tolerar que um dado seja usado de modo a transformar um indivíduo em objeto sob vigilância constante*.

Entretanto, o desafio da regulação dos dados pessoais, não bastasse a sua complexidade, é dotada de um complicador adicional. A diferença de visão sobre os direitos da personalidade entre os sistemas jurídicos Continental e do *Common Law*. Em uma economia de escala cada vez mais globalizada e integrada, evidencia-se o hercúleo desafio de normatizar homogeneamente os dados pessoais sem que isso prejudique o livre fluxo de pessoas e o comércio internacional.

E aqui posiciona-se o primeiro grande desafio que nos é lançado, uma vez que o viés utilitarista é muito mais visível nas análises econômicas realizadas pela doutrina e jurisprudência do *Common Law* enquanto, do outro lado, o sistema Continental continua a preservar o valor existencial humano como núcleo central de seu ordenamento, valorizando a dignidade da pessoa humana como princípio maior e fundamental de todo a ordem legal. Embora não se tratem de visões auto-excludentes, seus desdobramentos e particularidades acabam se tornando cada vez mais claros em conflitos individuais e em desafios a serem vencidos no dia-a-dia de indivíduos e empresas inseridos em ambas as dimensões.

Também em razão desta circunstância, a rápida consolidação da legislação brasileira e o estabelecimento de um marco regulatório para a proteção de dados pessoais tornou-se uma medida não apenas salutar,

mas essencial sob o aspecto jurídico, político, econômico e social. E, porque não, também democrático. Neste sentido, DONEDA (2019, p.41) observa:

> ... a proteção da privacidade identifica-se e acompanha a consolidação da própria teoria dos direitos da personalidade e, em seus mais recentes desenvolvimentos, afasta a leitura segundo a qual sua utilização em nome de um individualismo exacerbado alimentou o medo de que eles se tornassem o 'direito dos egoísmos privados'. Algo paradoxalmente, a proteção da privacidade na sociedade da informação, a partir da proteção de dados pessoais, avança sobre terrenos outrora improponíveis e nos induz a pensá-la como um elemento que, mais do que garantir o isolamento ou a tranquilidade, serve a proporcionar ao indivíduo os meios necessários à construção e consolidação de uma esfera privada própria, dentro de um paradigma de vida em relação e sob o signo da solidariedade - isto é, de forma que a tutela da privacidade cumpra um papel positivo para o potencial de comunicação e relacionamentos do indivíduo.

Inspirada no modelo de regulação de dados europeu, como não poderia deixar de ser em razão de nosso sistema jurídico de Direito Privado sofrer grande influência da tradição romano-germânica, a LGPD se apresenta como um sistema normativo amplo e integrado a diversos micro-sistemas regulatórios como o Marco Civil da Internet (Lei 12.965/14), o Código de Defesa do Consumidor (Lei 8.078/90), o Código Civil (Lei 10.406/02), além de um sem-número de atos normativos de órgãos setoriais como a ANS, BACEN, ANATEL, dentre outros.

2. A proteção de dados como liberdade positiva e as bases legais da LGPD

Sob a perspectiva de propor uma regulação mais efetiva dos dados pessoais e, principalmente, permitir ao indivíduo a completa expressão de sua individualidade e personalidade através da percepção que o mundo tem de si, a LGPD é consentânea com os conceitos de DONEDA (2018) e RODOTÁ (2008) de que há uma necessidade inevitável de se superar o conceito negativista do direito à privacidade, antes e historicamente

entendido como uma liberdade negativa capaz tão-somente de evitar a intromissão de terceiros ou do Estado na esfera íntima e na propriedade do indivíduo[3], o que foi muito bem ilustrado por este (*idem,* p.93) ao afirmar que:

> *... hoje a sequência quantitativamente mais relevante é 'pessoa-informação-circulação-controle' e não apenas 'pessoa-informação-sigilo', em torno da qual foi construída a noção clássica de privacidade. O titular do direito à privacidade pode exigir formas de 'circulação controlada', e não somente interromper o fluxo das informações que lhe digam respeito.*

Essa percepção é fundamental para que se compreenda, minimamente, a importância da regulação (efetiva) dos dados no mundo contemporâneo, com o que se alinham as assim chamadas *bases legais* contidas na LGPD que são, na verdade, as diretrizes maiores a autorizar a atividade de tratamento de dado por qualquer controlador.

A esse respeito, é preciso observar que o artigo 5˚, inciso X, da Lei 13.709/18 denomina a conceituação de *tratamento de dados* como qualquer atividade realizada com dados pessoais, citando-se, como exemplo, 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. Enfatiza-se que tais atividades, assim como quaisquer outras conhecidas ou que se inventem no futuro relacionadas à posse, manipulação ou interpretação de dados pessoais, são assim consideradas ainda que exercidas transitória ou temporariamente.

Igualmente, a figura do controlador também é definida em Lei, *ex vi* do artigo 5˚, inciso VI, da Lei 13.709/18, como sendo qualquer *pessoa natural ou jurídica, de direito público ou privado, a quem competem as*

[3] Tal qual o conceito de Louis Brandeis e Samuel Warren em seu célebre *The Right to Privacy* e do *right to be left alone,* mas também na tradicional conceituação da jurisprudência do *Common Law* de que a propriedade do indivíduo *is his castle*. O mesmo paralelo pode ser traçado em perspectiva histórica da legislação brasileira com sua prioridade ao *habeas data* como instrumento de assegurar ao indivíduo a ciência sobre suas informações pessoais utilizadas pelo Poder Público, dentre outros.

decisões referentes ao tratamento de dados pessoais. Isto é, não há nem mesmo a necessidade de que o controlador disponha, transitoriamente ou não, dos dados pessoais, bastando que lhe incumba, material, contratual ou legalmente, poder de decisão sobre os mesmos.

Ambos são conceitos extremamente abrangentes e que reclamam sempre interpretação extensiva, pois de outra forma se estaria a adotar uma prática restritiva do direito fundamental à dignidade da pessoa humana (art. 1°, inciso III, da Constituição Federal) que é o núcleo central do ordenamento jurídico brasileiro.

Essa é a visão, amplamente considerada, que garante uma carga de mínima eficácia ao direito à privacidade, à proteção de dados pessoais, à tutela da personalidade e, em último grau, à preservação da dignidade da pessoa humana, não havendo espaço para a superficialidade das interpretações apoiadas exclusivamente sob o pilar da autonomia da vontade, típicas e contemporâneas ao paradigma de Estado Liberal, e cuja superação há muito se encontra consolidada.

2.1 O desafio de conceituar o interesse legítimo do controlador em harmonia com o valor existencial humano

Admitido o recorte metodológico que este capítulo se propôs, deve-se observar que o art. 7° da LGPD, de forma razoavelmente harmônica com o regulamento europeu de proteção de dados, estabelece as hipóteses que legitimam a atividade de tratamento de dados pessoais como sendo: (a) o consentimento pelo titular; (b) o cumprimento de obrigação prevista em Lei ou obrigação regulatória do controlador; (c) para a execução de contrato ou de procedimentos preliminares a ele da qual o titular de dados seja parte e, sempre, a seu próprio pedido; (d) para o exercício do direito de defesa ou de ação em processo judicial, administrativo ou arbitral; (e) para a proteção da vida ou da incolumidade física do titular ou de terceiro; (f) para a tutela da saúde, apenas e exclusivamente quando em intervenção realizada por profissionais da saúde, serviços de saúde ou autoridade

sanitária; (g) para a realização de estudos por órgão de pesquisa, garantida sempre que possível a anonimização dos dados pessoais; (h) para a proteção do crédito, observada a integração com outras Leis em cada caso concreto; (i) pela 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; e, finalmente, (j) quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados.

Voltando-se para um aprofundamento inicial sobre o conceito de interesse legítimo do controlador, sempre que não conflitar com direitos e liberdades individuais, é preciso observar que cada uma das bases legais acima citadas são independentes e não necessitam, como regra, serem observadas simultaneamente. Daí porque é válido dizer-se que o interesse legítimo do controlador poderá fundamentar a atividade de tratamento de dados mesmo que o titular desses dados não tenha outorgado qualquer tipo de consentimento.

Por esse motivo, naturalmente surge um grande interesse em seu aproveitamento no desenvolvimento de atividades econômicas envolvendo a manipulação de dados pessoais conquanto a obtenção de consentimento individual pode se tornar uma tarefa excessivamente onerosa, dificultosa ou até mesmo inviável diante de uma manifestação positiva do titular de dados que provavelmente tenderá para a negativa. Se por um lado a base legal do interesse legítimo se apresenta como um facilitador no planejamento de um plano de governança de dados e na fundamentação do tratamento de dados pelo controlador, pelo outro a sua indiscriminada contextualização representa um risco para as liberdades individuais.

Assim, da mesma forma que se nota uma grande janela de oportunidades fundada no interesse legítimo do controlador, esse mesmo cenário se desdobra em um sem-número de hipóteses de violações de

direitos individuais ou do estabelecimento de práticas consideradas abusivas *a posteriori*, isto é, apenas quando questionadas administrativa ou judicialmente. Daí denotar-se o grande risco regulatório em sua escolha.

E para compreender a extensão desse conceito, nada melhor do que se começar pelas restrições a ele impostas, isto é, a subsunção aos direitos e liberdades fundamentais que reclamem a salvaguarda de dados pessoais.

Nada mais se está a afirmar que o valor existencial humano deve ser preservado como núcleo do sistema jurídico brasileiro se confrontado como interesse econômico existente na exploração de dados pessoais. SCHREIBER (2014, p.8) inicia sua obra sobre os direitos da personalidade com a seguinte contextualização:

> A tarefa não é nada simples. Poucas noções apresentam contornos tão fluídos. Sua longa trajetória filosófica não é unívoca, mas gravita sempre em torno da mesma ideia: a de que a espécie humana possui uma qualidade própria, que a torna merecedora de uma estima (dignus) única ou diferenciada. A dignidade humana não corresponde, portanto, a algum aspecto específico da condição humana, mas exprime, isto sim, 'uma qualidade tida como inerente a todo e qualquer ser humano', sendo frequentemente apresentada como 'o valor próprio que identifica o ser humano como tal'.

Ainda sob a perspectiva de delimitar conceitualmente os direitos de personalidade, tais quais diretamente referenciados pelo artigo 7°, inciso IX, da Lei 13.709/18, SÁ (*Et. Al.*, 2017, p.18) destaca que:

> Os direitos da personalidade voltam-se para os aspectos extrapatrimoniais da pessoa; aqueles que a definem e garantem a sua dignidade como forma de reduzir os abusos praticados em nome da autonomia da vontade do Estado Liberal. Protege-se, pois, a projeção do indivíduo no mundo; suas características fundamentais.

A contextualização dessa concepção apresentada por SÁ (*ibidem*), que de um modo geral uniformiza o ponto de convergência da doutrina e da jurisprudência, é ainda mais problemática ao se verificar que a projeção

da personalidade do indivíduo se dá cada vez mais a partir da prática de atos da vida civil através da *internet*. Isto é, o sujeito é e se percebe como tal também pela forma como se expressa e é visto em suas redes sociais e em sua bolha de convivência social. Daí porque se justifica a extremada preocupação em se estabelecer um direito à proteção de dados que contemple um controle sobre a circulação dos mesmos e não apenas como um mero instrumento para obstaculizar a intromissão alheia em sua vida privada. No momento histórico em que os traços divisórios de espaços públicos e privados são cada vez menos visíveis, principalmente em razão da exposição do indivíduo e de sua personalidade no mundo *online*, manter um controle efetivo e um instrumento capaz de salvaguardar abusos ao aspecto existencial humano é um imperativo fundamental para o ser do século 21.

DONEDA (2018, p.66-67) também externa o mesmo entendimento ao asseverar que:

> O surgimento da rede internet, por exemplo, decididamente alargou as possibilidades de comunicação e fez emergir um grande número de questões ligadas à privacidade. O impacto que a rede proporcionou, porém, já se encontrava de certa forma incubado em tecnologias anteriores, que provocaram fenômenos assemelhados e que, se hoje podem até parecer pálidos, devem ser considerados em relação ao que representaram à sua época (...). Assim, o telégrafo e o telefone, como instrumento de comunicação bidirecional, ou mesmo o rádio e a televisão contribuíram cada um deles para formar a consciência de que representavam um encurtamento de distâncias, do fim de limites antes intransponíveis, e, consequentemente, de uma interação mais frequente entre as pessoas, elementos que estão no âmago das questões relacionadas com a privacidade.

Por este motivo, torna-se claro que não há como conceituar objetivamente e de forma antecipada o conteúdo integral do interesse legítimo do controlador, conquanto cada caso concreto que se apresentar futuramente acabará por analisar necessariamente a violação de direito de personalidade do indivíduo envolvido, isto é, na esfera de sua dignidade como mandamento constitucionalmente protegido.

Todavia, isso não significa que alguns passos não possam ser dados em direção a um burilamento deste direito subjetivo do controlador como forma de otimizar a sua aplicação e favorecer a sua interpretação, ainda que dependente de elementos concretos de um dado caso futuro.

Não há dúvida de que o interesse legítimo do controlador estará sempre relacionado ao seu direito constitucionalmente assegurado de exercer a livre iniciativa, inclusive como um dos princípios fundantes da República, assim reconhecido no art. 1° e 170 da Constituição Federal.

Neste sentido, como expressão da atividade econômica desenvolvida pelo controlador, alia-se à sustentação de seu interesse legítimo os princípios constitucionais do desenvolvimento econômico, cultural, tecnológico, da busca por inovação, a livre iniciativa e a livre concorrência. Tais diretrizes constituem a pedra fundamental sobre a qual o controlador poderá se valer para a interpretação contextualizada de seu direito ao tratamento de dados independentemente de consentimento ou das demais previsões do art. 7° da Lei 13.709/18.

Em uma ponderação direta e isoladamente considerada, o sacrifício do valor existencial humano jamais poderá ocorrer se confrontado com os princípios constitucionais acima narrados. Daí porque um sopesamento de tais diretrizes consagradas pela Constituição tenderá a privilegiar, invariavelmente, a dignidade da pessoa humana.

Todavia, existem outros princípios e direitos muito relevantes que devem ser levados em consideração nessa difícil equação Constituem-se elementos informadores da interpretação a ser dada em um determinado caso concreto.

São eles a boa-fé objetiva (art. 113 da Lei 10.406/02) e os seus deveres laterais e a função social do contrato (art. 421 da Lei 10.406/02). Ainda que a Lei 13.874/19, conhecida como a Lei da Liberdade Econômica, tenha modificado a redação de diversos dispositivos do Código Civil para privilegiar a liberdade contratual e a autonomia privada, dele não eliminou o conceito de função social do contrato.

Além disso, ao se falar em liberdade contratual se está necessariamente adentrando o campo do consentimento, elemento este tornado desnecessário pela base legal do interesse legítimo do controlador.

A boa-fé, como elemento informador de conduta, não deve ser expressada apenas em relações contratuais (art. 422 da Lei 10.406/02), mas em todo e qualquer ato praticado na vida cotidiana, seja por pessoa natural ou jurídica (art.113 da Lei 10.406/02). Trata-se de um dever de agir ativamente de acordo com determinados padrões socialmente recomendados. MOTA[4] destaca as três características da boa-fé objetiva:

> A primeira pressupõe a existência de duas pessoas ligadas por uma determinada relação jurídica, que lhes imponha especiais deveres de conduta, de cada uma delas em relação à outra, ou, pelo menos de uma delas em relação à outra.

No tratamento de dados baseado em interesse legítimo do controlador, há nitidamente uma relação jurídica entre as partes conquanto este esteja a realizar a atividade de tratamento de dados pessoais do titular, ainda que este não tenha outorgado consentimento direto ou específico.

E continua (*ibidem*):

> Esses deveres, a segunda nota característica, são aqueles referentes ao comportamento exigível do bom cidadão, do profissional competente, enfim, de uma pessoa diligente, comportamento este expresso na noção de bonus pater familias.
>
> Deve-se observar também se a situação criada produziu na contraparte um estado de confiança no negócio celebrado, quando então deverá se tutelar essa expectativa. Desde que a contraparte tenha legitimamente confiado na estabilidade e segurança do negócio jurídico que celebrava impõe-se a tutela dessa confiança pelo princípio da boa-fé objetiva.

[4] A pós-eficácia das obrigações revisitada. Disponível em: https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/10194/7970 - Acesso 20 mar. 2020.

O dever impositivo de agir em acordo com o conceito de boa-fé objetiva, portanto, exigirá do controlador uma ênfase cada vez maior nos princípios da transparência, da prestação de contas e *accountability*. Mas não apenas isso. Finalidade, adequação, necessidade, prevenção e não-discriminação também devem ser potencializados e identificados na interpretação do conceito de interesse legítimo do controlador como reflexos indiretos do agir em boa-fé. Por óbvio, não há que se falar em qualquer intenção de lesar direitos individuais, haja vista a superação do antagonismo conceitual de boa-fé e má-fé. Em qualquer situação concreta analisada, sem a presença dos elementos dolo ou culpa, poder-se-á analisar um ato ilícito gerador de responsabilidade.

Posteriormente, conclui o referido autor (*ibidem*):

> O princípio da boa-fé regula não apenas a interpretação das cláusulas do contrato referida anteriormente, mas ainda o reconhecimento desses deveres secundários (não diretamente pactuados) derivados diretamente do princípio, independentemente da vontade manifestada pelas partes, a serem observados durante a fase de formação e de cumprimento da obrigação e mesmo, em alguns casos, após o adimplemento desta. São deveres que excedem o dever de prestação. Assim são os laterais de esclarecimento (informações sobre o uso do bem alienado, capacitações e limites), de proteção (evitar situações de perigo), de conservação (coisa recebida pela experiência), de lealdade (não exigir o cumprimento de contrato com insuportável perda de equivalência entre as prestações), de cooperação (prática dos atos necessários à realização dos fins plenos visados pela outra parte), etc.

Os então denominados deveres laterais à boa-fé objetiva, eis que não pactuados diretamente pelas partes mas a elas impositivos em decorrência do imperativo do dever de agir em acordo com a boa-fé, constituem elementos a serem levados em consideração na contextualização do interesse legítimo do controlador, devendo ser explicitados por este em suas relações com o titular, com os órgãos reguladores de seu setor e com a própria sociedade, em especial porque se estará a realizar o tratamento de dados sem o consentimento prévio e expresso pelo referido titular,

hipótese que indubitavelmente é capaz de ensejar inúmeras situações de risco de lesão a direitos de personalidade.

A partir dessa visão da LGPD como elemento necessariamente inserido nas relações com outros diplomas legais, princípios e deveres assim considerados como padrões de conduta a serem necessariamente observados, torna-se bastante relevante a referência ao *Opinion* 06/2014 do Grupo de Trabalho do Artigo 29 do Regulamento Europeu de Proteção de Dados[5], no qual se propõe um "teste" de interesse legítimo para ratificar a possibilidade de utilização dessa base legal.

A primeira etapa, considerada como a "avaliação dos interesses legítimos", envolve a identificação dos dados que serão tratados pelo controlador com base na conceituação de interesse legítimo. Ainda aqui, deve-se legitimar a atividade de tratamento de dados não apenas com base na inexistência de proibição legal, mas de forma consentânea com o princípio da boa-fé objetiva e com os princípios anteriormente destacados.

A segunda etapa, "impacto sobre o titular do dado pessoal", diz respeito à definição de quais dados serão coletados (e tratados, de um modo geral) sob a ótica do princípio da necessidade. Aqui, é fundamental a referência à previsão do artigo 10, §1°, da Lei 13.709/18 no sentido de que apenas os dados "estritamente necessário para a finalidade pretendida poderão ser tratados". A adoção do filtro da estrita necessidade tenderá a afastar situações de lesão a direitos individuais, de abuso de direito e de afronta à boa-fé objetiva.

A terceira etapa, por sua vez, o "equilíbrio entre os interesses legítimos do controlador e o impacto sobre o titular", novamente diz respeito à necessidade de balanceamento e equalização dos interesses do controlador e do titular, salvaguardando-se não apenas o padrão de conduta esperado das partes em acordância com a boa-fé e seus deveres laterais, mas com foco principal no agir com lealdade para não frustrar uma expectativa razoável do titular de que seus dados não seriam

[5] Disponível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf - Acesso 20 mar. 2020.

utilizados fora do contexto para o qual foram coletados ou cedidos. Este é um dos elementos casuísticos mais rigorosos no contexto analisado que denotam a total importância de se preencher o conteúdo conceitual de interesse legítimo de forma ampla apenas a partir de casos concretos.

A quarta e última etapa diz respeito às "salvaguardas desenvolvidas para proteger o titular de dados e evitar qualquer impacto indesejado". Nesse momento, incidem novamente com muita ênfase os princípios previstos no artigo 6˚ da Lei 13.709/18, devendo cada qual ser explicitado e evidenciado no agir do controlador em consonância com a boa-fé objetiva, não apenas como medidas de ordem técnica ou tecnológica, mas também com deveres de transparência, fluidez, prestação de contas, transparência e informação fácil e ostensivamente acessível.

Nessa perspectiva, o *Opinion* 06/2014 do Grupo de Trabalho do Artigo 29 do regulamento europeu enumerou algumas situações que, sob a sua particular ótica, poderiam representar eventual conflito entre o interesse legítimo do controlador e os direitos individuais do titular de dados, os quais são referenciados aqui a título ilustrativo: (a) exercício do direito à liberdade de expressão ou informação, inclusive na mídia e nas artes; (b) marketing direto convencional e outras formas de marketing e propaganda; (c) mensagens não comerciais não solicitadas, inclusive para campanhas políticas ou instituições de caridade; (d) execução de ações judiciais, incluindo cobrança de dívidas por meio de procedimentos extrajudiciais.; (e) prevenção de fraude no uso indevido de serviços ou lavagem de dinheiro; (f) monitoramento de funcionários para fins de segurança ou gerenciamento; (g) esquemas de denúncia; (h) segurança física, segurança da informação e de redes; (i) processamento de dados para fins históricos, científicos ou estatísticos; (j) processamento de dados para fins de pesquisas, incluindo pesquisas de marketing.

Todas essas hipóteses são exemplos claros da necessidade de um delicado equacionamento entre o interesse legítimo do controlador em desenvolver suas atividades de forma mais eficiente, lucrativa e ostensiva e o direito à privacidade do indivíduo. Ainda segundo a *Opinion* 06/2014,

seria importante levar em consideração a natureza e a origem do interesse legítimo desse controlador e também o impacto da ação a ser praticada na esfera individual do titular dos dados.

3. Conclusão

Alcançar uma conceituação definitiva sobre o interesse legítimo do controlador a ser utilizada para a solução de casos concretos ou para a definição de estratégias empresariais e na criação de políticas de governança de dados é uma tarefa demasiadamente árdua, especialmente em vista do conceito de pós-positivismo no qual essa análise se insere.

Todavia, não há que se falar aqui em qualquer carga de insegurança jurídica, mas da necessidade de uma compreensão ampla dos direitos e deveres, dos riscos e das oportunidades, na regulação de dados pessoais e, consequentemente, nas possibilidades de tratamento que se apresentam, notadamente aquelas baseadas em interesse legítimo.

A compreensão do conceito de boa-fé objetiva, que não é oposta ao conceito de má-fé, mas ao de boa-fé subjetiva, constitui o cerne da compreensão e da correta definição do conteúdo do legítimo interesse do controlador, dos limites de sua atuação e de seus deveres enquanto agente de tratamento de dados. Funciona, portanto, como verdadeira régua-mestra do conteúdo normativo do instituto do interesse legítimo do controlador

O teste do legítimo interesse, contemplado pela *Opinion* 06/2014 do Grupo de Trabalho do Artigo 29 do regulamento europeu, é um instrumento útil para a identificação de abusos em casos concretos, mas não se revela como medida única capaz de afastar a forçosa incidência do princípio da dignidade da pessoa humana.

Em qualquer situação, o interesse legítimo do controlador, para não conflitar com os direitos individuais do titular de dados, deverá ser exercido de acordo com os padrões de conduta impostos pela boa-fé objetiva, seus deveres laterais e com expressão da principiologia inserida

no artigo 6˚ da Lei 13.709/18, pois qualquer medida que importe em frustração de expectativa desse titular de dados certamente poderá ser interpretada como um abuso de direito, ainda que inexiste\a dolo ou alguma das modalidades de culpa na prática do ato que certamente será considerado ilícito.

4. Referências

ASHLEY, Kevin D. **Artificial intelligence and legal analytics: new tools for law practice in the digital age**. New York: Cambridge University Press, 2017.

BENKLER, Yochai. **The wealth of the networks: how social production transforms markets and freedom**. New Haven: Yale University Press, 2006.

BRANDEIS, Louis; WARREN, Samuel. **The right to privacy.** BRANDEIS, Louis; WARREN, Samuel. The right to privacy. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf - Acesso 20 mar. 2020.

CASEY, Michael J. Et. Al. **The truth machine: the blockchain and the future of everything**. New York: St. Martin's Press, 2018.

CASTELLS, Manuel. **The internet galaxy: reflections on the internet, business and society**. New York: Oxford University Press, 2001.

CRAWFORD, Susan. **Captive audience: the telecom industry and monopoly power in the new gilded age**. New Haven: Yale University Press, 2013.

CUPIS, Adriano de. **Os direitos da personalidade**, 2a ed. São Paulo: Quorum, 2008.

DEMPSEY, James X. Privacy and mass surveillance: balancing human rights and government security in the era of big data. In: PARENTONI, Leonardo (Coord.). D**ireito, Tecnologia e Inovação**. Vol. I. Belo Horizonte: D'Plácido, 2019, p.189-215.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**, 2a ed. rev. e atual. São Paulo: Revista dos Tribunais, 2019.

HAN, Byung-Chul. **Topologia da violência**. Petrópolis, RJ: Vozes, 2017.

HARARI, Yuval Noah. **21 lições para o século 21**. São Paulo: Companhia das Letras, 2018.

HARARI, Yuval Noah. **Homo Deus: uma breve história do amanhã**. São Paulo: Companhia das Letras, 2015.

LESSIG, Lawrence. **Code and other laws of cyberspace**. New York: The Penguin Press, 1999.

MALDONADO, Viviane Nóbrega (Coord.). **Lei Geral de Proteção de Dados Pessoais: manual de implementação**. São Paulo: Revista dos Tribunais, 2019.

MOTA, Maurício Jorge. **A pós-eficácia das obrigações revisitada.** Disponível em https://www.e-publicacoes.uerj.br/index.php/quaestioiuris/article/view/10194/7970 - Acesso 20 mar. 2020.

O'NEIL, Cathy. **Weapons of math destruction: how big data increases inequality and threatens democracy**. New York: Broadway Books, 2017.

PARISER, Eli. **The filter bubble: what the internet is hiding from you**. New York: the Penguin Press, 2011

PASQUALE. Frank. **The black box society: the secret algorithms that control money and information**. Cambridge: Harvard University Press, 2015.

RODOTÁ, Stefano. **A vida na sociedade da vigilância: a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada: uma visão jurídica da sexualidade, da família, da comunicação e informações pessoais, da vida e da morte**. Belo Horizonte: Del Rey, 1998.

SÁ, Maria de Fátima Freire de; NAVES, Bruno Torquato de Oliveira. **Direitos da personalidade**. Belo Horizonte: Arraes, 2017.

SANDEL, Michael J. **Justiça: o que é fazer a coisa certa**. Rio de Janeiro: Civilização Brasileira, 2019.

SCHREIBER, Anderson. **Direitos da personalidade**, 3a ed. rev. e atual. São Paulo: Atlas, 2014.

SUSSKIND, Richard. T**omorrow's lawyers: an introduction to your future**. Oxford: Oxford University Press, 2017.

TEPEDINO, Gustavo. Et. Al. (Coord.). **Lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro**, 2a tir. São Paulo: Revista dos Tribunais, 2019.

WHITMAN, James. **The two western cultures of privacy: dignity versus liberty**. In: Yale Law Journal, vol. 113, 2004, p.1551-1221.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the firht for a human future at the new frontier of power**.New York: Public Affairs, 2019.

4

Autonomia privada, renúncia contratual a direitos fundamentais e proteção de dados

Bruna Cardoso Nunes [1]
Camila de Oliveira [2]

1. Breves Aspectos da Autonomia da Vontade

O surgimento da expressão "Autonomia da vontade" na modernidade passa essencialmente pelo filósofo Immanuel Kant. Após muitos anos e análises jusfilosóficas, a autonomia da vontade passou a ser denominada como autonomia privada, porém para que se possa compreender a autonomia privada, é necessário precipuamente compreender o conceito de vontade e seguidamente a autonomia da vontade.

Para Kant a essência da liberdade é o que possibilita a explicação da autonomia da vontade. Trazendo luz ao conceito de vontade:

> A vontade é uma espécie de causalidade dos seres viventes, enquanto dotados de razão, e a liberdade seria a propriedade que esta causalidade possuiria de poder agir independentemente de causas estranhas que a determinam. (KANT, IMANNUEL, pg. 39)

Enquanto a autonomia da vontade para o referido filósofo pode ser entendida como:

[1] Acadêmica de Direito da Faculdade Dom Helder Câmara, Membro da Comissão de Proteção de Dados da OAB/MG.
[2] Acadêmica de Direito da Faculdade Dom Helder Câmara, Membro da Comissão de Proteção de Dados da OAB/MG.

> [...] a propriedade que a vontade possui de ser lei para si mesma (independentemente da natureza dos objetos do querer). O princípio da autonomia é pois: escolher sempre de modo tal que as máximas de nossa escolha estejam compreendidas, ao mesmo tempo, como leis universais, no ato de querer. Que esta regra prática seja um imperativo, isto é, que a vontade de todo ser racional lhe esteja necessariamente ligada como a uma condição, é coisa que não pode ser demonstrada pela pura análise dos conceitos implicados na vontade, porque isso é uma proposição sintética; seria mister ultrapassar o conhecimento dos objetos e entrar numa crítica do sujeito, isto é, da razão pura prática; de fato, esta proposição sintética que prescreve apodicticamente, deve poder ser conhecida inteiramente a priori. (KANT, Imannuel, pg. 36)

Entretanto, com o passar do tempo, como dito em supra, entendeu-se que a liberdade irrestrita, ou ilimitada advinda e pregada pela autonomia da vontade, necessitaria de uma atualização que, lhe conferisse determinados limites. Fato que culminou no surgimento da autonomia privada que para alguns autores é a atualização da autonomia da vontade e para outros princípios distintos.

2. Autonomia Privada

O princípio da autonomia privada, pode ser compreendido como a capacidade atribuída a determinado indivíduo de externar sua própria vontade, regulando as relações jurídicas das quais participe.

Para Francisco Amaral, a autonomia privada é "poder de autorregular relações jurídicas, dentro dos limites da lei" ou o "poder jurígeno outorgado aos particulares".

A autonomia privada como princípio jurídico, pode ser entendida, Segundo NAVES (2014, p. 96) como "norma jurídica que atribui aos particulares um poder", para o referido autor,

> A autonomia privada constitui-se da interação da autonomia crítica com a autonomia de ação, A autonomia crítica é o poder do homem de se compreender e compreender o mundo à sua volta, ou seja, é o poder de avaliar

> a si e ao mundo, estabelecendo relações a partir de seus pré-conceitos. A autonomia de ação é o poder de estabelecer dado comportamento, portanto, determinada pela compreensão de mundo, isto é, pela autonomia crítica. (NAVES, Bruno, 2014, p. 95)

Na lição de Perlingieri (2008, p. 338) a autonomia privada também pode ser compreendida como " [...] o poder reconhecido ou atribuído pelo ordenamento ao sujeito de direito público ou privado de regular com próprias manifestações de vontade, interesses privados ou públicos, ainda que não necessariamente próprios".

Ainda para o referido autor (apud LIMA, 1999, p. 33) a autonomia da vontade

> [...] abrange todas as liberdades pessoais garantidas constitucionalmente. Nesse sentido, a autonomia privada não se exprime apenas nos negócios jurídicos, mas também através da própria identidade do indivíduo dentro da órbita dos valores hierarquicamente dispostos na Constituição, destacando-se, no caso da Constituição de 1988, os arts. 5º, 6º e 7º.

Hans Kelsen (1995, p. 288, apud, JUNIOR, p. 121) sustenta que o princípio da autonomia privada exprime-se na seguinte fórmula: uma norma criada contratualmente poderá instituir direitos e obrigações só e exclusivamente para as partes que a formaram (ressalvados casos excepcionais, como os contratos a cargo ou em favor de terceiro, previamente admitidos por lei).

2.1 Autonomia Privada e Autonomia da Vontade

Estabelecer a distinção entre autonomia da vontade e autonomia privada não é uma tarefa simples. Vicente Raó (1997, p. 49, apud, NAVES 2014, p. 93) compreende a autonomia privada como o exercício e desenvolvimento da autonomia da vontade na ordem privada. Possuiriam sentido equivalente e representariam uma mesma realidade, isto é "um poder criador que atua de conformidade com o ordenamento jurídico."

Enquanto para outros autores, a autonomia da vontade e autonomia privada são compreendidas como dissemelhantes, vez que a autonomia da vontade seria uma liberdade individual enquanto a autonomia privada seria o poder de estabelecer normas jurídicas nos limites da lei.

> Autonomia da vontade, como manifestação de liberdade individual no campo do direito, e autonomia privada, como poder de criar, nos limites da lei, normas jurídicas, vale dizer, o poder de alguém de dar a si próprio um ordenamento jurídico e, objetivamente, o caráter próprio desse ordenamento, constituído pelo agente, diversa mas complementarmente ao ordenamento estatal. (AMARAL, Francisco, 2003, p. 347)

Seria a autonomia privada uma espécie de evolução da autonomia privada? Para Naves (2014, p. 94-95), a autonomia privada possui caráter substitutivo de uma pela outra, uma espécie de atualização da autonomia da vontade.

> A denominação autonomia privada veio substituir a carga individualista e liberal da autonomia da vontade. Ao direito, pois, resta analisar a manifestação concreta da vontade, segundo critérios objetivos de boa-fé, e não suas causas e características intrínsecas. Não é objeto do direito perquirir sobre o conteúdo da consciência interna de cada ser. Daí a justificativa pela expressão autonomia privada (...) com a nova hermenêutica, especialmente com os filósofos e psicólogos que trabalham a compreensão e veem a vontade como expressão culturalmente condicionada, (apud FIUZA, 2001, p. 101) "Se as pessoas celebram contratos, não é simplesmente porque desejam, mas porque são movidas por necessidades, ainda que falsas e fantasiosas".

2.2 Autonomia Privada e Direito de Personalidade

Como visto em supra, a autonomia privada é o poder concernente ao indivíduo de realizar suas próprias escolhas, estabelecer relações jurídicas, podendo regular interesses privados ou públicos, não se apresentando apenas nos negócios jurídicos, mas na individualidade de cada sujeito dentro dos valores dispostos na CR/88.

A individualidade de cada sujeito pode ser entendida como personalidade que, por sua vez, é constituída por diversas características referentes ao indivíduo atribuindo-lhes identidade e juridicamente passam a ser individualizados.

Para Schreiber (2012) os direitos da personalidade são a representação da projeção dos direitos fundamentais na esfera do direito civil, tornando mister a proteção destes

> Os direitos da personalidade representam, em larga medida, a projeção dos direitos fundamentais no campo do Direito Civil. A categoria dos direitos da personalidade nasce e se desenvolve justamente a partir da percepção de que não basta proteger os atributos essenciais da pessoa humana em face do Estado (tarefa historicamente atribuída ao direito público). É preciso protegê-la em face das outras pessoas, nas suas relações privadas.

Os direitos de personalidade possuem uma série de componentes concernentes ao sujeito de direitos, à exemplo, a intimidade, honra e privacidade, sendo esse último "ligado à exigência do indivíduo encontrar-se protegido na sua solidão, na sua paz e equilíbrio". (FERNANDES, 2017, p. 487).

Sabe-se que os referidos direitos merecem proteção, como afirmado em supra por Schreiber. Entretanto, quando o próprio sujeito, por sua própria iniciativa, dispõe contratualmente de um ou mais direitos, terá ainda a tutela constitucional dos mesmos?

3. Renúncia a Direitos Fundamentais e a Prática de *Ghostwriting*

Os direitos autorais têm proteção constitucional no título dos direitos e garantias fundamentais. A previsão consta do artigo 5º, inc. XXVII, "aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de suas obras, transmissível aos herdeiros pelo tempo que a lei fixar". Além da previsão constitucional, esses direitos estão regulamentados pela Lei 9.610/98 e ainda pela Lei 5.988/73, tendo sido essa parcialmente revogada por aquela.

> Em que pese ter sido omitida a terminologia "propriedade" no texto final da Lei 5.988/73, os conceitos relativos ao direito de propriedade permaneceram. [...] os direitos autorais foram considerados *bens móveis* para todos os efeitos legais. Toma por empréstimo e reproduz a regra segundo a qual *o autor temo direito de utilizar, fruir e dispor da obra literária, artística ou científica, bem como autorizar sua utilização ou fruição por terceiros, no todo ou em parte* (artigo 29). (PONTES, 2009, p.30)

Conforme o artigo 27 da Lei nº 9.610/98, os direitos morais do autor são inalienáveis e irrenunciáveis. Pontes (2009, p. 35) afirma que na relação contratual, a cessão total ou parcial dos direitos patrimoniais sobre a obra não obsta tais características inerentes. Com isso, na perspectiva do autor, as cláusulas que retirem do autor da obra os direitos sobre sua propriedade intelectual são nulas de pleno direito.

Na esfera do direito moral do autor, nos deparamos com o chamado direito de paternidade, que dá à autoria, em tese, a característica de direito personalíssimo.

> Integra o direito moral o direito de paternidade. Trata-se de uma das faculdades essenciais colocadas à disposição dos autores. Garante em favor do criador que, no ato de divulgação de sua obra, o seu nome permaneça, indissoluvelmente, vinculado à sua criação. Com essa característica, o direito de paternidade preserva o liame indelével entre o autor e a sua própria obra. (PONTES, 2009, p.36)

Todavia, no entendimento de Fernandes (2017, p.487), os direitos fundamentais não possuem caráter irrenunciável, podendo sim, sofrer "restrição ao direito de privacidade a partir do consentimento do próprio indivíduo, já que os direitos fundamentais, mesmo não sendo passíveis de renúncia plena, comportam formas de autolimitação".

O artigo 11 do código civil estabelece que "com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária". Contudo, o conteúdo do enunciado nº4 do Conselho de Justiça Federal

adotado na I Jornada de Direito Civil relativiza essa regra, "o exercício dos direitos da personalidade pode sofrer limitação voluntária, desde que não seja permanente nem geral".

Esse posicionamento pode ser muito bem ilustrado pelos exemplos de Anderson Schreiber:

> De fato, hoje não há dúvida de que o exercício dos direitos da personalidade pode ser limitado voluntariamente por seu titular. Quem decide participar de um *reality show*, como o *Big Brother Brasil* [...], concorda com uma limitação ao seu direito à privacidade e isso não deve ser vedado, *a priori*, pela ordem jurídica. O que a ordem jurídica deve fazer é controlar a legitimidade desta limitação, com base (i) no alcance, (ii) na duração, (iii) na intensidade e, sobretudo, (iv) na finalidade da autolimitação. Assim, um contrato que impõe a um químico industrial demissionário o dever de não trabalhar em seu setor pelo resto da vida não é legítimo, mas um contrato que impede o mesmo químico de trabalhar em empresa concorrente, durante dois anos, mediante ganho específico e significativo, em conformidade com o seu interesse e sem obstar sua futura reinserção no mercado, pode ser considerado legítimo. (SCHREIBER, 2012)

Em consonância com os apontamentos de Schreiber, a contratação sobre o direito de paternidade sempre terá caráter precário, gerando para o autor uma obrigação de não fazer por tempo determinado. Decorrido esse prazo, pode o autor reivindicar a paternidade, desobrigado de indenizar o contratante. Por segurança, o prazo deve constar expressamente do contrato. Na omissão contratual, aplica-se o prazo máximo de 5 anos previsto no artigo 51 da Lei nº9.610/98.

> Deste modo, as colisões que envolvam os direitos fundamentais nas relações traçadas entre agentes privados não podem ser solucionadas mediante regras apriorísticas, mas devem levar em consideração, especialmente, a tutela à dignidade humana em face da autonomia individual. A autonomia da vontade nas relações jurídicas não é mais importante que a tutela a uma vida digna do outro sujeito envolvido, porém, para realização deste sopesamento de interesses é indispensável a análise das situações in concreto (LIMA, 2009, p.9-10)

O amparo constitucional aos direitos do autor, deve a ele representar uma garantia, não uma limitação. Eventualmente podem se chocar os direitos e princípios tutelados pela Carta Magna, nesse caso faz-se necessária uma análise específica do caso concreto para que se encontre entendimento razoável de cuja aplicação o titular possa tirar o melhor proveito.

> Os direitos e garantias fundamentais consagrados pela Constituição Federal, portanto, não são ilimitados, uma vez que encontram seus limites nos demais direitos igualmente consagrados pela Carta Magna (Princípio da relatividade ou convivência das liberdades públicas). Dessa forma, quando houver conflito entre dois ou mais direitos ou garantias fundamentais, o intérprete deve utilizar-se do princípio da concordância prática ou da harmonização, de forma a coordenar e combinar os bens jurídicos em conflito, evitando o sacrifício total de uns em relação aos outros, realizando uma redução proporcional do âmbito de alcance de cada qual (contradição dos princípios), sempre em busca do verdadeiro significado da norma e da harmonia do texto constitucional com suas finalidades precípuas. (MORAES, 2011, p.27)

Para Ingo Wolfgang Sarlet, o regime jurídico dos direitos fundamentais se amolda à realidade, acompanhado a doutrina e jurisprudência.

> Importante, a essa altura, é a percepção de que o conceito e o correspondente regime jurídico dos direitos fundamentais depende das opções expressas e implícitas do constituinte histórico, mas também se encontra na dependência da construção e reconstrução permanente pela doutrina e jurisprudência, ademais de ajustes levados a efeito por meio dos mecanismos formais de reforma constitucional, como, aliás, ocorreu no caso brasileiro mediante a inserção do § 3º no artigo 5º, que dispõe sobre a incorporação e valor jurídico-normativo dos tratados internacionais de direitos humanos. (SARLET, 2015)

Ruas e Esteves (2016), sobre a renúncia em matéria constitucional, ensinam que “na renúncia o particular vincula-se a não invocar um direito fundamental do qual é titular, ou em outras palavras, a não exercer, temporária ou pontualmente, algumas das pretensões, faculdades ou

poderes que integram tal direito". Sobre as consequências jurídicas da renúncia, ainda afirmam que "o particular pode revogar a mesma, uma vez que, ao renunciar ao exercício de um direito, permanece na titularidade do mesmo".

> [...] a parte da doutrina que vê com olhos positivos a hipótese da renúncia procura fundamentar a sua opinião não numa negação absoluta dos direitos fundamentais, mas sim no exercício concreto de pelo menos um deles, o direito à liberdade, ou então o direito de livre desenvolvimento da personalidade. Assim, a renúncia não seria nada mais do que o resultado de uma análise compreensiva do sistema de direitos fundamentais, ao invés do exame do exercício de um direito isolado. (SANTOS, 2019 p.466)

É nesse sentido que afirmamos que existe sim uma relativização do caráter inalienável e irrenunciável de direitos fundamentais em favor da autonomia privada e do livre desenvolvimento da personalidade, desde que isso não resulte em relações contratuais abusivas, ilícitas e/ou maculadas pela má-fé. "Por isso, não se pode predicar dos direitos fundamentais uma característica de cogência autoritária. Fazê-lo seria contrário à própria dignidade que lhes dá fundamento [...] não se deve esquecer que a própria ação de dispor se trata de ato livre e, portanto, expressão do valor (e direito) fundamental da liberdade. " (SANTOS, 2019, p.467-468)

Sobre a possibilidade de renúncia a direitos fundamentais, Vicente Paulo e Marcelo Alexandrino fazem alguns apontamentos:

> a) a doutrina clássica, que considerava os direitos fundamentais absolutamente irrenunciáveis pelo seu titular, vem sendo substituída por uma nova orientação, que admite a referida renúncia em situações excepcionais; b) os direitos fundamentais, como totalidade, são irrenunciáveis; c) o núcleo substancial dos direitos fundamentais é irrenunciável; d) a renúncia voluntária ao exercício de um direito fundamental é admitida, desde que num caso concreto (a renúncia geral de exercício é inadmissível). (PAULO e ALEXANDRINO, 2003, p.29)

A cessão desses direitos nada mais é que uma das formas de os exercer, ainda que indiretamente. A vedação dessa possibilidade acabaria por limitar o exercício do direito. Tal proibição ofenderia a autonomia da vontade, bem como o princípio da dignidade humana no que concerne ao livre desenvolvimento da personalidade. Tomamos posicionamento favorável à escolha do autor sobre a forma de exercício dos seus direitos. Porém o que, a princípio, não deveria ocorrer, seria ficar o autor impossibilitado de voltar a exercê-los, diretamente, quando assim desejasse ou, no mínimo, quando findo o prazo legal ou contratado.

> A renúncia pode ser considerada também como uma forma de exercício do direito fundamental, uma vez que sua realização inclui a possibilidade de dispor do mesmo e inclusive de limitá-lo, desde que a renúncia seja uma expressão verdadeira do direito de autodeterminação e livre desenvolvimento da personalidade do titular. Acrescente-se a isso o fato de que, através da renúncia, o titular prossegue a realização de interesses e fins particulares que, de resto, certamente considera mais relevantes do que o exercício positivo do direito fundamental renunciado. (RUAS e ESTEVEZ, 2016)

Nessa lógica, faz-se adequada a análise da prática de *ghoswriting*, que, independentemente da (i)licitude, é uma realidade muito presente na atualidade, inclusive na produção científica. Nessas situações, o verdadeiro autor cria a obra encomendada e cede, contratualmente, todos os seus direitos sobre ela, comprometendo-se a permanecer no anonimato, enquanto a outra parte contratante é quem assume a falsa autoria. Nesse contrato o autor concorda em receber a contraprestação estipulada como pagamento pelo serviço prestado, logo, renuncia a quaisquer proveitos posteriores advindos da comercialização da obra. "Essa prática é denominada *ghostwriting* e quem a pratica é chamado de *ghostwriter* (escritor-fantasma), termos que indicam o anonimato do verdadeiro escritor nas publicações. " (GRIEGER, 2007, p. 247)

> Assim sendo, a validade das cessões do direito de paternidade por meio dos contratos conhecidos como *de nègre* ou *ghost writer,* nos quais um autor aceita a atribuição da paternidade de seu trabalho a outra pessoa, é matéria bastante

> discutível, trazendo principalmente à tona o problema da renúncia aos direitos da personalidade do autor. (ZANINI, 2015, p.293)

Para falar de *ghostwriting* é necessário, primeiramente, uma breve reflexão sobre as razões que levam um escritor a essa prática. Em maioria, os autores, ao negociar sobre suas obras, não se veem em pé de igualdade com a outra parte. Em geral, o autor é parte hipossuficiente e acaba tendo que aceitar os termos do contratante, porque do contrário, não terá condições de realizar de maneira autônoma, a devida comercialização da sua obra. Frequentemente, os termos desses contratos de cessão, se mostram abusivos, e mesmo assim são celebrados e produzem efeitos. Isso porque o autor se vê sem outra alternativa para perceber algum proveito econômico advindo de seu trabalho. Dessa forma, o autor não tem participação nos lucros, e acaba se contentando com o valor da contraprestação estipulada, em regra muito abaixo do que seria apropriado.

> [...] não têm conhecimento das questões autorais a envolver os seus direitos e experiência e segurança para entabular os negócios jurídicos representados por diferentes contratos, em especial os de cessão de direitos. Os autores mais experientes só conseguem, um melhor preço na negociação dos seus direitos autorais quando já galgaram renome artístico, advindos com reconhecimento de suas obras junto ao público consumidor. (PONTES, 2009, p.152)

Para que ocorra a renúncia ao exercício direto de um direito fundamental, em favor de interesse distinto que o titular julgue mais vantajoso, é essencial que ambas as partes tenham autonomia suficiente para contratar em igualdade. Dessa forma é possível uma negociação equilibrada, que não resulte em extrema vantagem para uma parte em extrema sucumbência da outra. É nesse sentido que discorre Jairo Néia Lima:

> Desde que as partes na relação *inter privatos* estejam numa situação de igualdade material, ou seja, partam de condições equânimes, caberá ao próprio renunciante a análise da necessidade última medida pode-se dizer que

> o renunciante definirá a extensão de sua própria dignidade. Dessa forma, nos conflitos onde estão envolvidos direitos fundamentais e autonomia da vontade, o exercício do primeiro poderá ser renunciado, de forma livre e consciente, sem que se altere sua característica de irrenunciabilidade. (LIMA, 2009, p.13)

O que ocorre, ocasionalmente, é o arrependimento do autor diante do grande sucesso da obra, o que o leva a judicializar a questão, em busca de indenização ou mesmo da publicidade da verdadeira autoria. Em situações como essa, o STJ já proferiu decisões desfavoráveis ao autor, entendendo pela plena renúncia contratual aos direitos.

Significativo exemplo disso é o acórdão proferido em recurso especial nº 1.387.242 - SP (2012/0162477-2). Trata-se do conhecido caso do livro *O Doce Veneno do Escorpião*, obra baseada na personagem Bruna Surfistinha, criada pela Recorrida Raquel Pacheco. A obra foi encomendada pela Recorrida e produzida pelo Recorrente Jorge Tarquini que "afirmou fazer jus à remuneração pela publicação, edição, e comercialização da obra em outras línguas e outros países, bem como a remuneração pela sua adaptação para o cinema, tudo em cumprimento ao contrato celebrado", nas palavras do ministro relator Paulo de Tarso Sanseverino.

Em 2011, o TJSP negou provimento à apelação de Jorge Tarquini em face de Raquel Pacheco e Editora Original LTDA EPP.

> Desta forma, percebe-se que o apelante sempre teve ampla ciência que não seria considerado autor da obra, não havendo nos autos nenhum elemento probatório que afaste este entendimento. No mais, deve ser aplicado ao contrato firmado entre as partes o princípio da boa-fé objetiva apoiado na autonomia da vontade ou no consensualismo, em que os contratantes de livre e espontânea vontade estabeleceram as regras da relação jurídica com a conseqüente observância das cláusulas firmadas, inclusive para fins de segurança jurídica. Acrescente-se, ainda, que participaram das tratativas pessoas maiores, capazes e esclarecidas quanto ao conteúdo e matéria avençadas, uma vez que é da praxe profissional do recorrente e da editora apelada. (TJSP, Des. Relator Coelho Mendes, Apelação nº0181194-46.2008)

O litígio foi apreciado pelo STJ em recurso especial, tendo sido o acórdão proferido no ano de 2015, confirmando o entendimento fixado em segunda instância. O ministro relator afirmou que o contrato de cessão de direitos autorais celebrado pelas partes:

> Estabeleceu que a posição assumida pelo autor da demanda na relação jurídica contratual que exsurgira entre editora, o autor e Raquel Araújo, era de um prestador de serviços, tendo o demandante plena ciência de que a autoria do livro não seria a ele concedida e que o trabalho por ele desempenhado na compilação das histórias contadas e escritas pela personagem "Bruna Surfistinha" seria remunerado na forma como previsto no referido acordo. (STJ, Min. Relator Sanseverino, RESP nº 1.387.242)

Além disso, no acórdão foi ressaltada a essencial contribuição da apelada para a elaboração da obra, uma vez que as ideias foram por ela narradas para que o g*host writer* as transcrevesse em formato literário. Na decisão a ré Raquel é designada "como autora, titular exclusiva dos direitos autorais, responsável pela originalidade e autenticidade da obra".

O autor Leonardo Zanini (2015, p.299) faz uma crítica à decisão apontando que "a lei autoral somente dá proteção às criações do espírito que foram expressas ou fixadas em um suporte, seja ele tangível ou não, sendo irrelevante se os fatos foram anteriormente narrados pela protagonista da obra". O autor ainda indica solução mais adequada aos ditames constitucionais do que a proferida pelo STJ, para os casos de *ghostwriting,* veja:

> Em suma, entendemos que quando o autor se obriga a não reivindicar a paternidade de determinada obra, autorizando sua publicação anônima ou em nome de outra pessoa, não há que se falar em renúncia ao direito de paternidade, mas sim em não exercício desse direito. A contratação é válida; entretanto, o não exercício do direito de paternidade ficará sempre vinculado a um prazo expressamente previsto no contrato, não superior a cinco anos. Findo o prazo estabelecido ou decorrido o prazo de cinco anos, ficará livre o autor para reivindicar a paternidade da obra, não havendo que se falar em pagamento de perdas e danos. Por outro lado, se o autor descumprir o acordado, reivindicando a paternidade antes do término do prazo, mesmo

> assim deverá ser reconhecido o seu direito de figurar como autor da obra, já que estamos diante de direito da personalidade irrenunciável, porém, o desrespeito à contratação poderá levar ao pagamento de perdas e danos. (ZANINI, 2015, p.301)

5. Lei Geral de Proteção de Dados e Renúncia Contratual a Direitos Fundamentais

A Lei Geral de Proteção de Dados, sob a ótica dos direitos fundamentais, confere proteção e garantia aos titulares dos dados pessoais. Conforme entendimento de Renato Leite (2018) mister é aos titulares a transparência, ou seja, obter "informações claras, precisas e facilmente acessíveis sobre a realização do tratamento".

Para Vainzof, (2019, p. 23) a lei nº13.709/18, tem como escopo a proteção dos direitos e garantias fundamentais do indivíduo, buscando equilíbrio no tratamento de dados pessoais:

> [...]busca a proteção de direitos e garantias fundamentais da pessoa natural, equilibradamente, mediante a harmonização e atualização de conceitos de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais. (VAINZOF, 2019, p. 23).

O artigo 1º da LGPD traz a seguinte redação "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. O que para Gallindo, Stilvemberg e Silva (2019)

> [...] evidencia que a natureza jurídica das normas protetivas de dados pessoais guarda encadeamento lógico com outras garantias constitucionais, a exemplo do direito à intimidade e à privacidade. Desta constatação, surgem reflexos importantes nas dimensões da amplitude normativa e da atividade legiferante no tocante a normas materiais em sede de proteção de dados pessoais.

Como demonstrado em capítulos anteriores, a proteção aos direitos fundamentais é prioridade, todavia, por força da autonomia privada, esses direitos são negociáveis. No tocante ao direito à privacidade, a LGPD introduz uma série de restrições à essa contratação. Essas medidas se fazem necessárias para amenizar as novas fragilidades dos indivíduos advindas do uso descomedido das mais recentes tecnologias informatizadas, "que torna a pessoa humana vulnerável a certas invasões em sua esfera pessoal." (EHRHARDT JÚNIOR e ACIOLI, 2019, p. 158)

> Paulatinamente os algoritmos estão adquirindo o poder de decodificar as pegadas digitais das pessoas das pessoas, inferindo e predizendo até mesmo aquilo que ninguém revela e que muitas vezes não tem nem mesmo consciência. Por meio do aprendizado de máquina, os algoritmos ainda podem "aprender" e modificar sua própria estrutura e suas regras, sem que haja propriamente controle ou mesmo previsibilidade sobre tais alterações e os resultados que daí decorrerão.[...] Sob a perspectiva dos usuários-consumidores, a inquietação é grande em relação à privacidade ou o direito aos dados pessoais. Além dos dados privados, muito do que é coletado sobre os indivíduos não diz respeito somente à sua intimidade, mas também a aspectos públicos da sua vida que, quando reunidos, ganham nova dimensão, possibilitando a categorização dos usuários em determinados perfis. (FRAZÃO, 2019, p.340)

O processo de automatização de decisões estratégicas baseadas nos dados pessoais coletados, vem transformando, segundo a autora (FRAZÂO, 2019, p.342), as máquinas e algoritmos "em verdadeiros oráculos do nosso tempo, possibilitando que eles possam julgar, classificar e pontuar os cidadãos em verdadeiros *rankings* dos quais pode depender o acesso a empregos, seguros, crédito [...]".

Acontece que em geral, as pessoas ainda não se preocupam com as consequências do comportamento *online*. Não há consciência de que os riscos são iminentes e que a ameaça recai sobre qualquer um que faça uso desses recursos. As pessoas têm sido iludidas por aplicativos atrativos que vão de redes sociais a serviços de entrega, passando pelos jogos, editores

de imagem, reprodutores de vídeo e uma infinidade de outras possibilidades.

O engano está em pensar que todos esses serviços estão sendo gratuitamente providos. A verdade é que tudo isso está sendo muito bem pago em forma de cessão de dados pessoais. Para utilizar esses aplicativos, é necessário que se faça um cadastro, ou mesmo que se autorize o registro de todos os atos praticados em rede. Ana Frazão (2019, p.246) ainda aponta ainda que "se a forma mais fundamental de poder em uma sociedade tecnológica e informacional é a capacidade de influenciar e manipular as pessoas".

Para a LGPD, não basta apenas que o titular dos dados dê consentimento para que os mesmos sejam tratados, mas que possua as informações de como e para que os seus dados estão sendo tratados. Nesse sentido, entendemos que antes do fornecimento de qualquer dado, é de suma importância que se tenha conhecimento do que o tratamento de dados significa e suas possíveis consequências na esfera da privacidade, para tanto, é necessário que se desenvolva a competência digital.

A competência digital é essencial para que se faça uso seguro e crítico das tecnologias digitais disponíveis, o que levará o titular dos dados a alcançar a autodeterminação informativa, colocando-o no cerne das operações que envolvam seus dados.

> [...]a autodeterminação informativa foi enunciado pelo Tribunal Constitucional alemão (Bundesverfassungsgericht) como consectário do direito fundamental ao livre desenvolvimento da personalidade e inviolabilidade da dignidade humana (Art. 1 I e 2 I GG). Essa conclusão levou a mudanças sensíveis no entendimento sobre proteção de dados pessoais. O direito à autodeterminação informativa, nessa nova senda, é visto como um requisito para a liberdade em um Estado Democrático de Direito. Ampliou, assim, a área de proteção jurídica desse direito. (ASSMANN, 2014)

6. Considerações finais

No contexto em que muitos têm acesso à internet, mas não possuem um mínimo conhecimento de seus direitos e garantias, tampouco a consciência sobre a relevância dos dados pessoais coletados, as regras inseridas pela LGPD visam proteger a parte mais frágil da relação contratual de tratamento.

Por outro lado, quando as partes demonstram condições equilibradas para a contratação, essa proteção perde o objeto, uma vez ausente tal discrepância que poderia resultar em contratos abusivos. Desse modo surge o questionamento: são cogentes ou dispositivas as normas da LGPD que estabelecem requisitos e garantias em favor do titular dos dados pessoais no contrato correspondente ao tratamento?

A resposta para essa indagação não é exata e, só será alcançada com a vigência da lei e a análise dos primeiros julgados a ela relacionados. Acreditamos que no que concerne ao direito à privacidade, a pessoa humana, no exercício de sua autonomia da vontade, poderá consentir a limitação ao direito que lhe é inerente. Isso desde que observadas as condições em que se deu a disposição dos referidos direitos, pois a todos os contratos é obrigatória a observância da boa-fé.

Diante dessa evolução digital que tende a ofender alguns dos direitos fundamentais da pessoa humana, é preciso levantar outras questões como a ausência de competência digital para que se tenha um efetivo controle sobre os dados pessoais.

Em um mundo que a cada dia apresenta mais avanços tecnológicos, que por si só limitam a privacidade, mostra-se mister a necessidade de trabalhar a competência digital na sociedade, para que não esteja vulnerável a contratos abusivos que não forneçam transparência e respeito ao tratamento de dados e à ordem emanada pela lei.

Sob outra perspectiva, em uma situação ideal, em que o titular dos dados tenha o devido conhecimento prévio, e esteja em condições de negociar com segurança, não seria exagero que as restrições contratuais

impostas pela LGPD, ainda assim se sobreponham à autonomia privada? Poderia o titular, nessas condições, renunciar a essa tutela?

Essas são questões que ainda não se pode responder com segurança, mas que certamente serão objeto de muitos estudos e debates doutrinários e jurisprudenciais.

7. Referências

AMARAL, Francisco dos Santos. **A autonomia privada como princípio fundamental da ordem jurídica.** p. 14-16

Assmann, Jhonata. **O direito à autodeterminação informativa no direito germânico e brasileiro.** Disponível em <https://repositorio.ufsc.br/handle/123456789/117169> Acesso em 18/11/2019.

BRASIL. **Constituição** (1988). **Constituição** da República Federativa do Brasil. Brasília, DF: Senado **Federal**: Centro Gráfico, 1988.

BRASIL. **Código Civil** (2002). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em 17/11/2019.

BRASIL. **Lei Geral de Proteção de Dados** (2018). Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em 17/11/2019.

BRASIL. **Lei nº 5.988** (1973) Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5988.htm> Acesso em 17/11/2019

BRASIL. **Lei nº 9.619** (1998) Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9610.htm> Acesso em 17/11/2019

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional / Bernardo Gonçalves Fernandes**. 9. Ed. Ver., ampl. E atual. Salvador: Juspodivm, 2017.

EHRHARDT JÚNIOR, Marcos e ACIOLI, Bruno de Lima. **Privacidade e os desafios de sua compreensão contemporânea: Do direito de ser deixado em paz ao direito ao direito ao Esquecimento**. In: Autonomia Privada, Liberdade Existencial e Direitos Fundamentais. Belo Horizonte: Fórum, 2019. p.151-164.

FRAZÃO, Ana. **Plataformas Digitais, Big Data e Riscos para os Direitos da Personalidade.** In: Autonomia Privada, Liberdade Existencial e Direitos Fundamentais. Belo Horizonte: Fórum, 2019. p.333-348.

GALLINDO, Sergio Paulo Gomes. STIVELBERG, Daniel T. SILVA, Evellin D. **Proteção de dados pessoais como direito fundamental autônomo e competência legiferante privativa da união**. Disponível em < https://www.migalhas.com.br/dePeso/16,MI314538,61044-protecao+de+dados+pessoais+como+direito+fundamental+autonomo+e > Acesso em 05/11/2019

GRIEGER, Maria Christina Anna. **Escritores-fantasma e comércio de trabalhos científicos na internet: A ciência em risco.** Disponível em: < http://www.scielo.br/pdf/%0D/ramb/v53n3/a23v53n3.pdf > Acesso em: 03/10/2019

JORNADA DE DIREITO CIVIL, I, 2002, Brasília. **Jornada de Direito Civil**. Braília, 2003.

JUNIOR, Otavio Luiz Rodrigues. **Autonomia da vontade, autonomia privada e autodeterminação Notas sobre a evolução de um conceito na Modernidade e na Pós-modernidade.** Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/982/R163-08.pdf?sequence=4 > Acesso em: 02/10/2019

KANT, **Immanuel. Fundamentação da metafísica dos costumes**. Tradução de Paulo Quintela. Lisboa: Edições 70, 1997

LIMA, Cláudio Vianna de. **A arbitragem no tempo: o tempo na arbitragem. In: GARCEZ, José Maria Rossani. A arbitragem na era da globalização.** 2. ed. Rio de Janeiro: Forense, 1999. p. 33-59.

LIMA, Jairo Néia. **Colisão e renúncia a direitos fundamentais nas relações entre particulares.** 2009. 15p. Disponível em: < http://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/62 > Acesso em 01/12/2019

MAIA, Roberta Mauro Medina. **Vivendo nas nuvens: dados pessoais são objeto de propriedade?** In: Autonomia Privada, Liberdade Existencial e Direitos Fundamentais. Belo horizonte: Fórum, 2019. p.669-711.

MORAES, Alexandre de. **Direitos humanos fundamentais: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil, doutrina e jurisprudência. 9. ed. São Paulo: Atlas, 2011.**

NAVES, Bruno Torquato de Oliveira. **O Direito pela perspectiva da autonomia privada, relação jurídica, situações jurídicas e teoria do fato jurídico na segunda modernidade**. 2 ed. Belo Horizonte: Arraes, 2014.

PAULO, Vicente e ALEXANDRINO, Marcelo. **Direitos fundamentais. 2. ed. Rio de Janeiro: Impetus, 2003. 176p.**

PERLINGIERI, Pietro. **O Direito Civil na Legalidade Constitucional**. Trad. Maria Cristina de Cicco – Rio de Janeiro: Renovar, 2008.

PONTES, Hildebrando. **Os contratos de cessão de direitos autorais e as licenças virtuais *creative comoons***. 2 ed. Belo Horizonte: Del Rey, 2009. 172p.

RUAS, Celiana Diehl e ESTEVES, André Fernandes. **Renúncia contratual a direitos fundamentais.** Belo Horizonte: Revista Científica do Curso de Direito do UNIBH, volume IX, nº1, 2016. Disponível em: < http://revistas.unibh.br/index.php/dcjpg/index > 15/11/2019

SANTOS, Rodrigo Bley. **Renúncia a direitos fundamentais por meio de negócio processual.** Brasil: Revista Eletrônica de Direito Processual, 2019.Disponível em: < https://livros-e-revistas.vlex.com.br/vid/renuncia-direitos-fundamentais-meio-812851297 > Acesso em: 01/12/2019

SARLET, Ingo Wolfgang. **O conceito de direitos fundamentais na Constituição Federal de 1988.** 2015. Disponível em: < https://www.conjur.com.br/2015-fev-27/direitos-fundamentais-conceito-direitos-fundamentais-constituicao-federal-1988 > Acesso em 15/11/2019

SCHREIBER, Anderson. **Direitos da Personalidade.** In: Jornal Carta Forense. Disponível em: < http://www.cartaforense.com.br/conteudo/entrevistas/direitos-da-personalidade/8362 > Acesso em 18/11/2019

ZANINI, Leonardo Estevam de Assis. **Direito de autor**. São Paulo: Saraiva, 2015

5

Autonomia privada e consentimento de crianças e adolescentes na Lei Geral de Proteção de Dados

Zilda A. Goncalves de Sousa [1]
Igor da Silveira Franco [2]

The new consumer is the product itself. (John Perry Barlow)

1. Introdução

Sabe-se que o tratamento de dados pessoais de crianças e adolescentes é um tema de suma importância na atualidade ante sua posição de vulnerabilidade. Por este motivo o capítulo II da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018 – traz em seu escopo, na seção III, matéria acerca deste tipo de tratamento.

Citando Alessandra Vieira, "sabemos que encontrar um equilíbrio no uso das novas tecnologias e bem direcionar crianças e adolescentes para tirarem o melhor e mais seguro proveito de tudo que vem sendo oferecido no universo digital representa um importante desafio, não somente às famílias, mas à sociedade de maneira geral."

Importante se faz trazer a definição legal do que vêm a ser criança e adolescente. De acordo com a Lei 8.069/1990 (Estatuto da Criança e do

[1] Bacharel em Direito pela Universidade de Itaúna. Advogada de Direito Digital. Autora de artigos jurídicos. Membro da Comissão de Proteção de Dados da Ordem dos Advogados do Brasil - Seção de Minas Gerais

[2] Bacharel em Ciência da Computação na Universidade Federal de Minas Gerais (UFMG). Pós-graduado em TI Bancária pela Universidade de São Paulo (USP). Consultor Especialista em Integração, Qualidade de Dados, Governança e adequação da TI à LGPD, além de *Business Intelligence*, *Analytics* e Arquitetura de Sistemas. Membro da *Mensa International*.

Adolescente - ECA), "criança" é a pessoa com até 12 (doze) anos incompletos; e adolescente é aquela entre 12 (doze) e 18 (dezoito) anos incompletos.

Deste modo, vejamos o que a Lei Geral de Proteção de Dados (LGPD) traz sobre esse tema tão delicado e tão importante. Transcrevemos abaixo o art. 14, caput da referida Lei, qual seja:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

Têm-se por esse artigo que o tratamento de dados pessoais de crianças e de adolescentes deve estar sempre pautado no melhor interesse e na necessária proteção integral disposta no ECA. O melhor interesse deve ser interpretado como um fundamento básico de toda e qualquer ação que visa a proteção deste grupo. Assim, qualquer decisão envolvendo tais sujeitos de direito deve estar pautada no que é mais adequado para a satisfação dos seus anseios, podendo antepor, até mesmo, aos interesses dos pais.

O Regulamento Geral de Proteção de Dados da união europeia aprovado em 2016 e vigorando desde maio de 2018, traz impactos que ultrapassam e muito o continente europeu, representando uma baliza mundial quando o assunto é proteção dos direitos de crianças e adolescentes no tratamento de dados pessoais, servindo de espelho para a LGPD.

Importa-nos observar que a parte inicial da Considerada 38 da GDPR, reitera a necessidade de uma proteção especial aos dados de crianças e adolescentes, frente aos riscos e vulnerabilidades aos quais esse grupo pode estar submetido diante da sua vulnerabilidade. Assim, trazemos a importante Considerada 38 da GDPR:

> 38. As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos riscos, consequências e garantias em questão e dos seus direitos relacionados com o tratamento dos dados

> pessoais. Essa proteção específica deverá aplicar-se, nomeadamente, à utilização de dados pessoais de crianças para efeitos de comercialização ou de criação de perfis de personalidade ou de utilizador, bem como à recolha de dados pessoais em relação às crianças aquando da utilização de serviços disponibilizados diretamente às crianças. O consentimento do titular das responsabilidades parentais não deverá ser necessário no contexto de serviços preventivos ou de aconselhamento oferecidos diretamente a uma criança. (Tradução livre).

Corroborando com o relevante tema, temos outra importante referência internacional, o *Children´s Online Privacy Act* (COPPA), uma legislação americana em vigor desde 1998, que traz em seu escopo uma extensa regulamentação acerca do tema.

Não restam dúvidas que os dados pessoais são a nova moeda que tem impulsionado a economia, como prova disso, o Fórum Econômico Mundial já declarava em 2011 que, "os dados são uma nova classe de ativo econômico particularmente valioso. Meglena Kuneva, antiga comissária europeia pela proteção de dados, ressaltava que, "os dados pessoais são o novo petróleo da *Internet* e a moeda do mundo digital", já a revista londrina *The Economist* reforça a tese da importância dos dados pessoais ao afirmar que, "o recurso mais valioso do mundo já não é o petróleo, mas os dados."

> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

Segundo Alessandra Vieira, ''conforme se observa deste parágrafo, há limitação da aplicação de suas disposições às crianças, ficando fora destas restrições o consentimento manifestado por adolescentes. Apesar de alguns entendimentos, no sentido de que isso se trataria de lapso do legislador e não seria suficiente para excluir a obrigações dos agentes de coletarem dos adolescentes o consentimento específico e em destaque, entendemos que essas obrigações mais restritivas não se aplicam a

titulares a partir de 13 (treze) anos de idade, em relação aos quais será suficiente a obtenção do consentimento ordinário."

Alessandra Vieira, se baseia Relatório da Comissão Especial Destinada a Proferir Parecer ao Projeto de Lei 4.060/2012, onde há a intenção legislativa ao declarar a exigência mais elevada de consentimento ao tratamento de dados de crianças.

Pelo consentimento específico se extrai que, antes de iniciar a coleta dos dados de crianças, seja no contrato e nas políticas de privacidade ou em outro documento que se relacione a tal operação, seja feita a exposição detalhada sobre o ciclo de vida do tratamento, evidenciando os limites e as finalidades para as quais os dados serão tratados. Assegurando assim, ao usuário, o claro entendimento e o poder de escolha ao decidir se deseja realmente conceder sua autorização para tanto.

Assim, pelo consentimento em destaque, têm-se que o usuário deverá ter o claro entendimento sobre o tratamento que será realizado com seus dados pessoais. Finalmente, pode-se deduzir por este parágrafo que, a função do consentimento para o tratamento de dados pessoais de crianças visa sobretudo proteger os seus interesses individuais para que possam usufruir de maneira segura e consciente aos benefícios oferecidos pelas ferramentas disponíveis pela *Internet*.

> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

Os controladores de dados pessoais de crianças deverão manter públicos o contrato, a política de privacidade e os documentos correlacionados à coleta e tratamento destes dados. Tal imposição legal é uma medida para a garantia dos direitos do titular expresso no art. 18 deste mesmo diploma legal.

Têm-se pelo dispositivo acima citado que: serão assegurados aos titulares de dados mediante requisição ao controlador, a confirmação de

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 com o disposto na LGPD; portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa e revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

O parágrafo acima é claro ao enumerar as hipóteses em que a coleta de dados de crianças poderá acontecer sem o consentimento específico dos pais ou responsáveis legais. As coletas sem consentimento apenas se darão quando for necessária para contatar os pais ou o responsável legal; ou para sua proteção.

Frisa-que que essa dispensa de consentimento para a coleta de dados mencionada no artigo acima só poderá acontecer uma única vez e os dados não poderão ficar armazenados.

> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de *Internet* ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

Têm-se por esse diploma legal que as políticas e termos de privacidade de jogos, aplicações de *Internet* e afins não devem condicionar a participação de crianças ao fornecimento de dados pessoais que não sejam estritamente necessários. Tal exigência legal vai de encontro aos princípios da finalidade, necessidade e adequação.

> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

A determinação legal disposta neste parágrafo, obriga os controladores de dados pessoais a implementarem soluções técnicas suficientes e esforços razoáveis para que a verificação do consentimento específico e em destaque foi de fato de dado por pelo menos um dos pais ou pelo responsável legal da criança detentora dos dados. Essa verificação se dará de forma efetiva a fim de que a proteção dos titulares seja efetivamente assegurada.

> § 6º 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.

Resta clara neste parágrafo a preocupação do legislador com possíveis dificuldades que a criança possa enfrentar em não ter plena compreensão sobre os limites do tratamento dos seus dados pessoais, seja pela idade, e naturalmente pela falta de maturidade, ou desconhecimento, seja pelas limitações de ordem físicas, mentais, auditivas ou visuais do titular dos dados.

As informações prévias ao tratamento de dados devem se dar de maneira simples, clara e acessível, sendo indispensável a implementação de técnicas que permitam a acessibilidade dessas crianças e, mais uma vez, a obrigatoriedade de que as informações necessárias sejam prestadas aos

pais ou representante legal. Cabe-nos ressaltar que, a Lei n.13.146/2015 (Lei Brasileira de Inclusão da Pessoa com Deficiência - Estatuto da Pessoa com Deficiência), trata da obrigatoriedade de implementações de soluções de acessibilidade nos sítios da *Internet*.

Vejamos o art.63, da referida lei que dispõe sobre o tema:

> Art. 63. É obrigatória a acessibilidade nos sítios da Internet mantidos por empresas com sede ou representação comercial no País ou por órgãos de governo, para uso da pessoa com deficiência, garantindo-lhe acesso às informações disponíveis, conforme as melhores práticas e diretrizes de acessibilidade adotadas internacionalmente.
> § 1o Os sítios devem conter símbolo de acessibilidade em destaque.
> § 2o Telecentros comunitários que receberem recursos públicos federais para seu custeio ou sua instalação e lan houses devem possuir equipamentos e instalações acessíveis.
> § 3o Os telecentros e as lan houses de que trata o § 2o deste artigo devem garantir, no mínimo, 10% (dez por cento) de seus computadores com recursos de acessibilidade para pessoa com deficiência visual, sendo assegurado pelo menos 1 (um) equipamento, quando o resultado percentual for inferior a 1 (um).

Desta forma, a LGPD deve ser aplicada com estrita observação ao Estatuto da Pessoa com Deficiência, a fim de que a garantia do direito a acessibilidade de crianças com deficiência seja assegurada.

2. LGPD: consentimento de crianças e adolescentes

A LGPD nem iniciou sua vigência e os desafios começam com a interpretação na redação da Lei. Em uma análise da sessão III que dispõe do tratamento de dados pessoais de crianças e adolescentes, há margem para interpretações diversas.

Note que o título menciona: "Do tratamento de dados pessoais de crianças e adolescentes", e a partir do art.14, § 1º, as menções legais se referem apenas às crianças, vindo a mencionar adolescentes apenas no caput. Tem-se que o legislador deliberadamente não inclui os adolescentes

em qualquer parágrafo deste artigo, demonstrando a inação de criar balizas aos adolescentes, diferentemente das crianças. Cabe-nos ressaltar, que há alguns entendimentos no sentido de que se trataria de um lapso do legislador e que não seria suficiente para deixar os adolescentes de fora das obrigações impostas aos agentes, no que se refere a coleta de consentimento específico e em destaque.

Para Alessandra Vieira, "as obrigações mais restritivas não se aplicam a titulares a partir de 13 (treze) anos de idade, em relação aos quais seria suficiente a obtenção de consentimento ordinário."

No nosso entendimento o legislador direcionou o capítulo com uma exigência maior para o consentimento no tratamento de dados de crianças com até 12 (doze) anos incompletos (assim consideradas pelo ECA), não aplicando as mesmas restrições aos adolescentes considerados pelo ECA como, pessoa entre 12 (doze) e 18 (dezoito) anos incompletos.

Assim, o adolescente poderá consentir de forma ordinária para o tratamento de seus dados pessoais diante da oferta de serviços prestados pela sociedade da informação. Ainda, em reiteração a LGPD, entende-se que todas as informações e comunicações que digam respeito a este tratamento sejam prestadas de forma clara, simples e de fácil compreensão do menor.

3. Princípio da dignidade da pessoa humana e absoluta prioridade de crianças e adolescentes

O princípio da dignidade da pessoa humana deve ser aplicado concretamente nas questões inerentes à criança e ao adolescente, sendo um atributo constitucional previsto no artigo 227, da Constituição Federal, onde possui uma conotação de absoluta prioridade:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, 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.

O texto constitucional deixa claro a aplicação do princípio da dignidade da pessoa humana, considerando um dos fundamentos da República Federativa do Brasil, conforme previsto no artigo 1º, inciso III, da Constituição Federal:

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
> [...]
> III - a dignidade da pessoa humana.

Tem-se, portanto, que a dignidade humana da criança e do adolescente deve ser preservada em todos os seus aspectos, inclusive, para o efeito de proteção dos dados pessoais. Ademais, a criança e o adolescente possuem ampla proteção de âmbito infraconstitucional, conforme previsão contida nos artigos 17 e 18 do Estatuto da Criança e do Adolescente:

> Art. 17. O direito ao respeito consiste na inviolabilidade da integridade física, psíquica e moral da criança e do adolescente, abrangendo a preservação da imagem, da identidade, da autonomia, dos valores, ideias e crenças, dos espaços e objetos pessoais. (BRASIL, 1990, online)

> Art. 18. É dever de todos velar pela dignidade da criança e do adolescente, pondo-os a salvo de qualquer tratamento desumano, violento, aterrorizante, vexatório ou constrangedor.

Assim, tem-se que a dignidade da pessoa humana se fundamenta como um dos princípios basilares que devem ser observados no tratamento de dados pessoais de crianças e adolescentes. Neste sentido, Sarlet (2001, p. 60) afirma sobre a dignidade da pessoa humana que:

> Temos por dignidade da pessoa humana a qualidade intrínseca e distintiva de cada ser humano que o faz merecedor do mesmo respeito e consideração por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa corresponsável nos destinos da própria existência e da vida em comunhão dos demais seres humanos.

Verifica-se que, a dignidade da pessoa humana é intrínseca a todo ser humano, devendo ser aplicada juntamente com os preceitos fundamentais, onde se assegura os direitos e deveres inerentes à proteção. Nas palavras de Piovesan (2000, p. 54):

> A dignidade da pessoa humana, [...] está erigida como princípio matriz da Constituição, imprimindo-lhe unidade de sentido, condicionando a interpretação das suas normas e revelando-se, ao lado dos Direitos e Garantias Fundamentais, como cânone constitucional que incorpora as exigências de justiça e dos valores éticos, conferindo suporte axiológico a todo o sistema jurídico brasileiro.

Desta análise, pode-se dizer que o direito à privacidade se encontra ligado ao princípio da dignidade da pessoa humana, motivo pelo qual, o tratamento de dados pessoais de crianças e adolescentes somente poderão ser realizados atendendo ao melhor interesse do menor e diante do prévio consentimento dos pais ou responsável legal. Conforme já exposto acima, em apenas alguns casos, a lei ressalva a desnecessidade de consentimento dos pais ou do responsável legal, porém, trata-se de normas gerais que possuem como fundamento a autonomia privada, nunca podendo ser revestido de prejuízo ou que acarrete danos ao menor, respeitando assim o seu direito à privacidade.

Conforme assevera Silva (2009, p. 206), a respeito da garantia da privacidade, é:

> [...] o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando,

> onde e em que condições, sem a isso poder ser legalmente sujeito. A esfera de inviolabilidade, assim, é ampla, abrange o 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.

A rigor, a Lei Geral de Proteção de Dados deve ser aplicada essencialmente com a resguarda do princípio da dignidade da pessoa humana, conforme disposição contida em seu artigo 14, qual seja: "O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente".

Para tanto, a verificação do consentimento para o tratamento de dados da criança e do adolescente, deve estar amparado pelo conjunto de normas jurídicas, que em especial, estão previstas na Constituição Federal e no Estatuto da Criança e do Adolescente, desprendendo sempre uma atenção ao princípio da dignidade da pessoa humana e ao melhor interesse das crianças e dos adolescentes.

4. Autonomia privada

A autonomia privada se relaciona diretamente com o princípio da autonomia da vontade. Na lição de Diniz (2011, p. 40), a autonomia da vontade é: "[...] o poder de estipular livremente, como melhor lhes convier, mediante acordo de vontade, a disciplina de seus interesses, suscitando efeitos tutelados pela ordem jurídica".

Apesar da autonomia da vontade possuir uma definição semelhante com a da autonomia privada, este último possui elementos e conceito próprio, tanto que Cabral (2014, p. 111) assim explica:

> [...] numa visão simplista dos institutos, pode-se resumir a diferença afirmando que a autonomia da vontade se relaciona com a liberdade de autodeterminação (manifestação da vontade livre) e a autonomia privada ao poder de autor regulamentação (normas estabelecidas no interesse próprio).

Já na concepção de Amaral (2008, p. 345): "A expressão 'autonomia da vontade' tem uma conotação subjetiva, psicológica, enquanto a autonomia privada marca o poder da vontade no direito de um modo objetivo, concreto e real". Com efeito, o importante é destacar que a autonomia privada se trata de um princípio fundamental do Direito Civil, sendo a existência de vontades entre os particulares.

De acordo com os ensinamentos de Borges (2005, p. 70):

> No exercício de sua autonomia privada e, portanto, na realização de negócios jurídicos, as pessoas tem, do ordenamento jurídico, o poder criador, modificativo e extintivo de situações e relações jurídicas, no âmbito e na forma previstas pelo mesmo ordenamento que concede este poder. Ao regulamentar, de forma direta e individual, seus próprios interesses pessoais, o sujeito faz coincidir sua autonomia privada com os interesses que o ordenamento escolhe proteger. A competência pessoal e jurídica que o sujeito tem para autorregular certos interesses encontra sua fonte no ordenamento jurídico.

Na autonomia privada existe o elemento da liberdade, possuindo o alicerce jurídico no aspecto social, voluntário e da vontade de contratar. Por isso, a autonomia privada se configura pelo ato de fazer livremente e conforme o arbítrio. Possui também concepção de privacidade, pois todo o ser humano possui a liberdade e o arbítrio de contratar livremente com outrem, desde que presentes os requisitos legais para a validade do negócio jurídico.

Não obstante, no que tange à criança, esta liberdade de contratar fica mitigada em razão de caber aos pais ou responsável legal o fornecimento do consentimento para validação do negócio jurídico. Inclusive é um dos requisitos para a validade do negócio jurídico, conforme previsto no artigo 104, inciso I, do Código Civil: "A validade do negócio jurídico requer: I - agente capaz".

Deste modo, não é diferente com a Lei Geral de Proteção de Dados, ao fazer restrições ao tratamento de dados pessoais de crianças condicionado ao consentimento dos pais ou responsável legal. Respectiva previsão se encontra garantida pela Constituição Federal, que prevê em

seu artigo 229: “Os pais têm o dever de assistir, criar e educar os filhos menores [...]”. (BRASIL, 1988).

Assim, quando o constituinte aplicou limites quanto à autonomia privada da criança, o fez sob o pálio do melhor interesse da criança e também, afim de assegurar-lhes a devida proteção. O mesmo ocorreu quando o legislador infraconstitucional dispôs sobre a validade do negócio jurídico no Código Civil, considerando absolutamente incapaz de exercer os atos da vida civil os menores de dezesseis anos. Em relação aos maiores de dezesseis e menores de dezoito anos, o legislador os considerou incapazes relativamente para certos atos da vida civil.

Portanto, a Lei Geral de Proteção de Dados está em restrita consonância com a Constituição Federal e com o Direito Civil, que mormente zelam pela proteção integral, pelo melhor interesse e pela dignidade da pessoa humana da criança, motivo que, para certos atos, deve existir uma restrição, equilíbrio e mitigação da autonomia privada da criança e do adolescente como ocorre no tratamento de dados pessoais.

5. A questão do consentimento

Como dito, a aplicação da autonomia privada possui limites, cujo objetivo é não gerar danos ou conflitos aos demais princípios constitucionais, sobretudo ao melhor interesse da criança. Por isso, na visão de Diniz (2011, p. 42):

> É preciso não olvidar que a liberdade contratual não é ilimitada ou absoluta, pois está limitada pela supremacia da ordem pública, que veda convenções que lhe sejam contrárias e aos bons costumes, de forma que a vontade dos contraentes está subordinada ao interesse coletivo.

A autonomia privada será assegurada desde que exista um equilíbrio contratual de modo a respeitar a supremacia dos interesses coletivos e conferir um contrapeso nas relações jurídicas. Este efeito advém do

consentimento de crianças e adolescentes na Lei Geral de Proteção de Dados, que assim encontra-se previsto no artigo 14 e § 1º:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal. (BRASIL, 2018, online)

Conforme análise a seguir:

> Sabemos que o tratamento de dados pessoais já é, por si só, um tema importante. E o que dizer sobre o tratamento de dados pessoais de crianças e adolescentes? Frente sua posição de vulnerabilidade, é algo que requer ainda mais atenção e cuidado. Por isso o capítulo II da Lei Geral de Proteção de Dados Pessoais – lei nº 13.709/2018 – traz em seu bojo, na seção III, a matéria referente a esse tipo de tratamento, ação de especial importância na legislação atual e nas demais leis que abordam o assunto privacidade. (SERPRO, 2019)

Observe-se a importância do artigo 14 que garante o melhor interesse da criança e do adolescente, tanto que para o tratamento de dados pessoais da criança é necessário o consentimento específico, devendo ser realizado por um dos pais ou o responsável legal, e para o adolescente deve haver consentimento ordinário. Trata-se, segundo Diniz (2011, p. 45), de uma forma do Estado intervir:

> [...] não só mediante a aplicação de normas de ordem pública, mas também com a adoção da revisão judicial dos contratos, alterando-os, estabelecendo-lhes condições de execução, ou mesmo exonerando a parte lesada, conforme as circunstâncias, fundando-se em princípios de boa-fé e de supremacia do interesse coletivo, no amparo do fraco contra o forte, hipótese em que a vontade estatal substitui a dos contratantes, valendo a sentença como se fosse declaração volitiva do interessado.

O consentimento de um dos pais ou do responsável legal para o tratamento de dados de crianças previsto na Lei Geral de Proteção de

Dados, possui como fundamento a privacidade, conforme previsto no artigo 5º, inciso X, da Constituição Federal, que percorre também aos limites dos meios de comunicação, disposto no artigo 220, § 1º:

> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.
> § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.

Neste passo, sobre a coleta de dados digitais: "[...] a grande questão é que, na maioria das vezes, esse grupo de pessoas não são os proprietários dos aparelhos; os proprietários são os seus responsáveis". (SERPRO, 2019).

Sobre esta questão, verifica-se o seguinte:

> [...] imagine um aparelho que contenha informações salvas, como números de cartões de crédito e senhas (em razão da facilidade para compras online) e, igualmente, o fácil acesso proporcionado pelos apps de compras online, e o próprio aplicativo de compra de outros aplicativos (quando não gratuitos). Com toda essa tecnologia disponível e na mão delas, mais especificamente, se tornam muito fácil a obtenção e os downloads de programas pelas crianças (se a criança não souber escrever, basta apertar o botão de voz e fazer a pesquisa verbal sobre o tema de interesse). Chega-se, portanto, ao desafio do parágrafo quinto da Lei Geral de Proteção de Dados Pessoais: como identificar que o consentimento foi dado pela pessoa responsável, e não pela própria criança ou adolescente fazendo uso dos aparelhos? - aqui, talvez o uso de reconhecimento facial ou de identificação digital possa ser uma solução. (SERPRO, 2019)

Diante do exposto, as empresas devem investir nas formas de consentimento confiável, seja o consentimento específico ou o ordinário, de modo a aplicar concretamente o tratamento de dados. Nas palavras de Blum (2018): "a prova da concessão do consentimento dos pais com relação aos dados da criança há de ser feita pelo fornecedor, que deverá

empenhar esforços para confirmar a veracidade da manifestação dos pais (parágrafo 5º do art. 14, LGPD)".

Contudo, deve-se abranger a aplicação dos princípios da dignidade da pessoa humana, da boa-fé e de mecanismos de controle da autonomia privada, motivo que o legislador estabeleceu o consentimento dos pais ou do responsável legal para a realização da coleta de dados pessoais de crianças. Neste sentido, explica Schreiber (apud MORAES, 2006, p. 457):

> Nas relações existenciais de família, também se deve admitir a aplicação do princípio da boa-fé objetiva, como mecanismo de controle dos atos de autonomia privada, onde outros instrumentos, mais específicos, já não exercerem esta função. Imperativo faz-se, todavia, atentar, sobretudo em tais relações, para a incidência direta dos princípios constitucionais que, sendo hierarquicamente superiores à tutela da confiança e à boa-fé objetiva, quase sempre antecipam para os conflitos instaurados neste campo uma certa solução. Tal solução pode não apenas se mostrar contrária à solução recomendada pela boa-fé objetiva, onde sua base negocial tiver decisiva influência, mas se revela, mesmo em caso de convergência, fundamentada em norma mais elevada sob o ponto de vista da hierarquia do sistema jurídico vigente, característica importantíssima na sua conservação.

Assim, apesar de crianças e adolescentes terem o direito à privacidade para se autodeterminar no sentido de receberem informações pessoais e validar critérios a serem seguidos, cabem aos pais fixar e expressar os limites, atentando para o desenvolvimento integral do menor e dando prioridade aos seus interesses. Significa que cabem aos pais ou responsável legal o consentimento, porém não deixando de respeitar o direito à informação ao menor. Tanto que o controlador dos dados pessoais não poderá condicionar a participação de pais ou responsáveis legais em jogos, aplicações de *Internet* ou outras atividades inerentes à criança conforme estabelece o § 4º, do artigo 14, da Lei nº. 13.709/18:

> Art. 14.
> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de Internet ou outras

> atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

Nesse ponto, convém frisar o seguinte:

> [...] os controladores não deverão condicionar a participação dos titulares especiais deste artigo em jogos, aplicações de Internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade, a qual se encaixa perfeitamente no exemplo dado. É evidente que os termos de uso não são lidos pelas crianças e nem pelos adolescentes (tampouco os adultos o fazem), é uma questão cultural que precisa ser revista, mas, em contrapartida, a lei limita a atuação dos desenvolvedores impondo esse ditame, sendo bem-vinda a proteção proposta. (SERPRO, 2019)

Ademais, outras garantias encontram-se previstas na Lei em favor do melhor interesse da criança, conforme as disposições contidas nos §§ 2º e 3º, do artigo 14, da Lei nº. 13.709/18:

> Art. 14.
> [...]
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo. (BRASIL, 2018).

A justificativa do § 2º em manter pública a informação sobre os dados coletados é para melhor fiscalização. Cabem aos pais, responsáveis legais, sociedade e ao Estado analisar questões inerentes ao melhor interesse da criança para fins de proteção e ampla aplicação do princípio da dignidade da pessoa humana. Têm-se no § 3º, a ressalva do consentimento de pais ou responsáveis quando a coleta for necessária para a proteção do menor e pelo seu integral interesse.

Demais direitos estão previstos nos §§ 5º e 6º, do artigo 14, da Lei nº. 13.709/18, que estabelecem a forma razoável de consentimento e o uso de informações claras e simples para o tratamento dos dados pessoais:

> Art. 14.
> [...]
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
> § 6º 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. (BRASIL, 2018)3

Ressalta-se que o controlador é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais, ou seja, é quem fará a coleta dos dados. Quando, um a empresa detentora de site de jogos faz uma solicitação de cadastro de dados pessoais, deve proceder através de informações claras, acessíveis e simples, podendo o titular dos dados pessoais, a qualquer momento e mediante requisição, requerer a confirmação da existência de tratamento; o acesso aos dados; a correção de dados incompletos, inexatos ou desatualizados; a anonimização, bloqueio ou eliminação de dados; a portabilidade dos dados a outro fornecedor de serviço ou produto; e a revogação do consentimento.

Tem-se ainda, que a Lei nº. 13.709/18 possui amparo aos valores fundamentais do Direito quando se remete ao consentimento dos pais ou ao responsável legal quanto a utilização de tratamento de dados pessoais de crianças. Mormente a autonomia privada fica mitigada em razão da ampla proteção voltada para a criança. Nas palavras de Amaral (2008, p. 52):

---

3 <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

> Os valores fundamentais do Direito em geral e do civil em particular, como a justiça, a segurança, a liberdade, a igualdade, o direito à vida, a propriedade, o contrato, o direito de herança, etc., saem do seu habitat natural, que era o Código Civil, e passam ao domínio do Texto Constitucional que, além de reunir os princípios básicos da ordem jurídica, também estabelece os direitos e deveres do cidadão e organiza a estrutura político administrativa do Estado.

Assim, a autonomia privada e o melhor interesse da criança e do adolescente devem caminhar juntos, motivo que a Lei Geral de Proteção de Dados se preocupou em estabelecer limites e trazer um equilíbrio para não afastar o direito da privacidade, de modo a garantir a ampla proteção e a dignidade da pessoa humana, motivo que o consentimento de pais ou responsáveis legais são atributos a serem utilizados pelo controlador dos dados pessoais ao tratar dados de crianças e a observação no consentimento ordinário a ser fornecido pelo menor.

6. Coleta de dados

No Brasil, há a adoção do conceito expansionista de dado pessoal. Por este conceito têm-se que não apenas a informação relativa à pessoa diretamente identificada estará protegida pela Lei, como também aquela informação que possa tornar a pessoa identificável.

Para Rony Vainzof, "nome, prenome, RG, CPF, título de eleitor, número de passaporte, endereço, estado civil, gênero, profissão, origem social e étnica; informações relativas à saúde, à genética, à orientação sexual, convicções políticas, religiosos e filosóficas; números de telefone, registros de ligação, protocolos d *Internet*, registros de conexão, registros de acesso a aplicações de *Internet*, contas de *e-mail*, *cookies*, hábitos, gostos e interesses, são apenas alguns exemplos de dados pessoais que pautam a vida em sociedade."

Assim, dados pessoais são aqueles que têm capacidade ou potencial de identificar uma pessoa, demonstrando as características da sua personalidade. A Lei Geral de Proteção de Dados considera, de forma

ampla, em seu art. 5º, inciso I, dado pessoal como sendo "informação relacionada a pessoa natural identificada ou identificável".

Para a *General Data Protection Regulation* da União Europeia, em seu Regulamento nº 679/2016 do Parlamento Europeu e do Conselho, em seu artigo 4º, traz como definição de dado pessoal, qual seja:

(...) dados pessoais" referem-se a qualquer informação relacionada à identificação ou a possibilidade de identificação de uma pessoa natural („dados subjetivos"); uma pessoa natural identificável é aquela que pode ser identificada de forma direta ou indiretamente, em particular, fazendo referência a um identificador como nome, número de identificação, dados de localização, identificador online (IP) ou um ou mais fatores específicos como físicos, fisiológicos, genéticos, psicológicos, econômicos, culturais ou sociais que identificam uma pessoa natural.

O tratamento de dados tem um grande potencial de geração oportunidades e novos modelos de negócios. Contudo, se trata de uma atividade que oferece ameaças e riscos à proteção dos dados pessoais, com a possibilidade de exposição e utilização indevida ou abusiva de dados pessoais. Citando Moreli, "isto porque o mau uso destes dados pode originar afronta grotesca aos princípios inerentes à proteção da privacidade" (MORELI, 2016, p.96).

Para Moraes, proteção de dados é um direito fundamental que constitui uma das dimensões da dignidade da pessoa humana, entendida essa como: (...) um valor espiritual e moral inerente à pessoa, que se manifesta singularmente na autodeterminação consciente e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas, constituindo-se em um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que apenas excepcionalmente possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos (MORAES, 2017).

Para o tratamento de dados pessoais, existem regras a serem cumpridas de acordo com a LGPD. E como descrito nos tópicos alhures,

para a coleta de dados de crianças, mesmo que sejam portadores de direitos da autonomia privada e da privacidade, as regras são mais restritas, pois deve ser assegurado o melhor interesse do menor. Consoante a lição de Nunes:

> No caso de crianças, que segundo o Estatuto da Criança e do Adolescente são pessoas com até 12 (doze) anos de idade incompletos, o tratamento de dados e o repasse para terceiros só podem ocorrer com o consentimento específico e, em destaque, fornecido por pelo menos 01 (um) dos pais ou pelo responsável legal. Ou seja, as plataformas que possuem crianças como público alvo ou as aceitam não poderão ter acesso a informações pessoais, incluindo nome, data de nascimento e localização, sem que haja uma permissão clara de seus representantes legais. A única exceção a essa regra ocorre quando a coleta for necessária para contatar os pais ou o responsável em prol da criança. Nesse caso, as informações só podem ser utilizadas 01 (uma) única vez e sem armazenamento ou compartilhamento com terceiros. (NUNES, 2018)

Contudo, ressalta-se que: "As empresas não deverão condicionar a participação das crianças em jogos, aplicações de *Internet* ou outras atividades ao fornecimento de dados pessoais, além das que sejam estritamente necessárias à atividade". (NUNES, 2018)

Neste ponto, veja-se que o consentimento descrito no artigo 14, § 1º, da Lei nº. 13.709/18, deve ser cumprido por todas as empresas privadas e órgãos públicos para fins de coleta de dados pessoais, especialmente para que seja realizado de forma específica e em destaque por pelo menos um dos pais ou responsável legal.

Com efeito, há de se fazer uma diferenciação entre os absolutamente incapazes para os relativamente incapazes. Conforme descreve a legislação civil, os incapazes são os menores de dezesseis anos, não podendo exercer qualquer ato jurídico, por isso devem ser representados pelos pais ou responsáveis. Já o relativamente incapaz, que estão na faixa etária de dezesseis a dezoito anos, poderá exercer certos atos da vida civil, desde que apoiados por pais ou responsável legal.

Assim, quando a Lei Geral de Proteção de Dados dispõe acerca do consentimento de um dos pais ou responsável legal, deve-se atentar para

a questão dos absolutamente incapazes e relativamente incapazes, eis que podem alterar a maneira de exercer os atos jurídicos, devendo a empresa privada ou o órgão público atentar-se a tais peculiaridades.

Quanto às exceções sobre o consentimento para coleta de dados do menor, as seguintes hipóteses poderão ser consideradas: poder contactar os pais ou responsáveis ou para a proteção do menor ou adolescente. Porém, aos absolutamente incapazes ou relativamente incapazes, a empresa privada ou o órgão público deverão coletar e processar os dados pessoais de modo público, especificando a forma de utilização e os procedimentos quanto ao exercício dos direitos, conforme previsto no § 2º, do artigo 14, da Lei nº. 13.709/18. Conforme se observa a seguir:

> [...] um permissivo relevante, no parágrafo terceiro da LGPD, ao definir que poderão ser coletados dados pessoais de crianças sem o consentimento específico, e em destaque, dado por pelo menos um dos pais ou responsável legal, quando a coleta for necessária para contatar os pais ou o responsável legal, ou para a proteção dessa criança ou adolescente. Os dados deverão ser utilizados uma única vez e sem armazenamento e em nenhum caso poderão ser repassados a terceiros, sem o consentimento acima referido. Aqui, podemos citar as hipóteses de emergência, quando é necessário o contato com os pais ou responsáveis para pronto atendimento e notificação. (SERPRO, 2019)

Sobre a questão de jogos, aplicações de *Internet* ou outras atividades, os controladores não deverão condicionar a participação dos pais ou responsáveis ao fornecimento de informações pessoais da criança. Porém a questão é sobre a existência de vários sistemas tecnológicos em celulares e computadores, sendo que, em todos eles, é necessário o preenchimento de cadastro do usuário. Para se ter uma ideia, alguns destes aplicativos são: Facebook, Twitter, Instagram, Spotify, Deezer, Waze, Telegram e Pocket. Com efeito, a lei não especifica o que são informações pessoais além das estritamente necessárias à atividade, sendo que cada aplicativo em questão existe uma especificidade diferenciada.

Assim, como a norma jurídica encontra-se em aberto, o mais seguro para as empresas privadas e os órgãos públicos é confirmar a autenticação dos dados pessoais ao consentimento de pais ou responsáveis, uma vez que se trata do melhor interesse da criança, além de estabelecer a regra de proteção de acordo com o princípio da dignidade da pessoa humana.

A Lei Geral de Proteção de Dados Pessoais impõe às empresas privadas e aos órgãos públicos a obrigação de realizar todos os esforços razoáveis para verificar se o consentimento realmente foi dado pelos pais ou responsável legal, evitando qualquer fraude no sistema de coleta. Também trata de uma norma em aberto, devendo existir uma interpretação de que a empresa privada ou o órgão público tenha conferido de forma razoável e através da tecnologia disponível que o consentimento realmente foi dado por um dos pais ou responsável legal. Conforme alerta Nunes (2018):

> É responsabilidade do controlador da plataforma realizar todos os esforços razoáveis para trazer segurança aos envolvidos e para verificar se o consentimento de fato foi fornecido por 01 (um) dos pais ou responsável pela criança, considerando as tecnologias disponíveis. Além disso, todas as informações sobre o tratamento de dados deverão ser fornecidas de maneira simples, clara e acessível. A orientação é que os textos sejam elaborados considerando 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 também adequada ao entendimento da criança.

E nas palavras de Soares (2019)

> Esse rígido conjunto de requisitos, verdadeiros qualificadores do consentimento, deve ser corretamente apreendido e aplicado pelo agente de tratamento de dados, seja ele o controlador ou o operador. Deve, por igual, ser avaliado com cautela pelo respectivo encarregado de proteção de dados, incumbido da tarefa de desenvolver meios para a correta aplicação da lei e acompanhar, no âmbito interno da empresa, o seu cumprimento. [...] Neste particular, não parece suficiente meramente comunicar ao titular que seus dados poderão ser coletados. Cabe ao controlador ou operador informar a

> forma, duração e finalidade do tratamento dos dados, as suas responsabilidades, os riscos a ser suportados pelo titular, bem como a maneira de revogar autorizações anteriormente concedidas, de maneira transparente. Ao assim fazer, o titular terá condições de optar, ou não, por determinado produto ou serviço que colete dados, podendo, inclusive, manifestar consentimento específico para determinado tipo de tratamento e não para os outros visados pelo controlador ou operador, além de revogar tal consentimento a qualquer momento. Com esses ajustes, tomados com o apoio do encarregado de proteção de dados, e com suporte jurídico e técnico, é possível mitigar os riscos de descumprimento da LGPD e a aplicação de suas respectivas sanções pela Autoridade Nacional de Proteção de Dados.

Por fim, o tratamento dos dados pessoais de crianças e adolescentes devem ocorrer sempre de forma clara e simples para que seja de melhor entendimento do menor e com uso de recursos audiovisuais quando adequado. Mesmo que existam interpretações a serem feitas na legislação, a Lei Geral de Proteção de Dados deve ser aplicada de acordo com os princípios jurídicos e através das normas constitucionais, além de aplicação de outros ramos do Direito, como Direito Civil e Estatuto da Criança e do Adolescente, especialmente para a ampla proteção do menor.

A questão da coleta de dados de menores, conforme se analisou neste artigo, deve ser interpretado como fonte do Direito, especialmente quando se fala em autonomia privada. Embora a criança e o adolescente tenham o direito e a garantia de sua privacidade, deve existir um equilíbrio para que outras garantias sejam preservadas, como a da dignidade da pessoa humana e do melhor interesse do menor.

Trata-se, portanto, de garantias previstas na Constituição Federal, no Estatuto da Criança e do Adolescente e pelo Direito Civil, que determinam as regras específicas a serem cumpridas em favor do menor.

Desta análise, a Lei Geral de Proteção de Dados não pode se afastar das regras voltadas para as criança, motivo pelo qual o consentimento de pais e responsável legal para a coleta e tratamento dos dados pessoais se torna essencial e para o adolescente com o consentimento ordinário,

conferindo assim em um Estado Democrático de Direito e de ampla proteção.

De tal modo existem concepções na Lei que estão em aberto, como no caso de aplicativos de *Internet* e jogos, porém cabe ao Estado e ao Poder Judiciário equilibrar as regras de acordo com o caso concreto, eis que a tecnologia está em constante evolução. Assim, espera-se que em um futuro próximo, as regras previstas na Lei Geral de Proteção de Dados estejam sendo cumpridas fielmente, principalmente para preservar e garantir o melhor interesse da criança e do adolescente a seus dados pessoais.

7. Impacto da LGPD nas instituições de ensino

Sabe-se que a escola é o lugar onde as crianças e adolescentes passam grande parte de seus dias e essa caminhada escolar envolve uma memória histórica de dados pessoais que exigirá ajustes na forma de como essas instituições trabalham com as informações pessoais de pais e responsáveis, professores, alunos, colaboradores e visitantes.

Sobre o tema citamos Alessandra Vieira que dispõe o que se segue: "podemos dizer que uma instituição de ensino efetivamente preparada para os desafios da era digital é aquela que compreende o quão invasivo e violador pode ser o compartilhamento ou o vazamento de dados pessoais os quais dispõe por força da relação estabelecida com seu aluno."

Deste modo, a coleta e o armazenamento de dados pessoais de crianças e adolescentes pelas instituições de ensino requisita diligências de responsabilidade. É de suma importância que as instituições de ensino se adequem à LGPD e passem e ajam de acordo com as regras legais, tendo o cuidado de ao coletar dados pessoais de crianças e adolescentes o faça apenas quando for relevante, necessário e quando atender a uma finalidade específica, pois, a coleta que exceda o necessário poderá representar violação à Lei.

A coleta de dados pessoais realizada pelas instituições de ensino deve ter por base o consentimento e sobretudo, transparência. É de grande

importância que a finalidade para qual estes dados foram coletados seja clara, a fim, de garantir aos pais e responsáveis pelas crianças e adolescentes titulares destes dados a máxima transparência possível.

Resta mencionar que em caso de compartilhamento destes dados tão sensíveis, a família do titular deve consentir de forma prévia e expressa. As instituições de ensino devem garantir que a prioridade seja a proteção à privacidade dos titulares detentores dos dados que serão por ela tratados, assegurando ainda, medidas contínuas de prevenção e que os riscos aos quais envolvem esse tratamento sejam sempre levados em consideração.

Frente ao crescente desrespeito aos direitos de crianças e adolescentes no âmbito das coletas de seus dados pessoais para os mais diversos fins, necessário se faz que cuidados especiais sejam tomados para garantir que os modelos de governança das instituições de ensino sejam revistos e aprimorados para atender ao melhor interesse das crianças e adolescentes titulares dos dados pessoais objetos de tratamento.

Contudo, as instituições de ensino como segmento com a função de ensinar, deve conduzir movimentos que conscientizem crianças e adolescentes, bem como familiares, dos riscos que o universo digital os propicia, gerando efeitos positivos para toda a sociedade.

8. Considerações finais

Conclui-se que a evolução tecnológica ocorrida na última década permitiu uma verdadeira inclusão digital de grande parte da sociedade. Crianças, jovens, adultos e idosos, "entregam" suas informações pessoais para ter acesso a vídeos, criar perfis em redes sociais, participar de grupos *online,* ter acesso a *games* ou até mesmo apenas para ler uma notícia em um *site*.

Sabe-se que muitas são as atrações ofertadas pelas novas tecnologias, e pouco é o discernimento desta nova geração de crianças e adolescentes sobre os perigos do mundo cibernético. Acredita-se que os serviços oferecidos na *Internet* são gratuitos, quando é certo que há um valor muito

grande na captura dos dados pessoais como moeda de troca pela disponibilidade destes serviços.

Muitos usuários de aplicativos, principalmente crianças e adolescentes, não se atentam para os termos de uso e políticas de privacidade antes de inserirem seus dados de forma indiscriminada e concordarem com o que se fala naquelas letras tão pequenas. E justamente aí mora o perigo, pois quase ninguém lê o que dizem tais termos de uso e políticas de privacidade, apenas assinala o "li e concordo", sem se quer saber para qual finalidade seus dados poderão ser utilizados.

Com a inovação e a constante evolução da *Internet*, é indispensável que os órgãos públicos, entes privados e prestadores de serviços estejam atentos às regulamentações de proteção de dados pessoais trazidas pela LGPD, tendo por escopo a prevenção e a transparência como "carros chefe" de qualquer operação envolvendo dados pessoais de crianças e adolescentes.

Note-se que a LGPD traz em seu escopo disposições apenas sobre o consentimento parental para as crianças (até os 12 anos), deixando de fora os adolescentes. Esta não inserção, no entanto, não faz com que seus dados pessoais possam ser tratados sem nenhuma observância à Lei. Diante deste desafio, resta aos interessados em tratar esses dados que façam com que os termos de uso e da política de privacidade fiquem claros e de fácil entendimento, ainda que a autorização explícita dos pais ou responsável legal não conste no texto legislativo.

Diante das muitas empresas que produzem serviços voltados para o público de crianças, desde software de jogos até programas para ensinar línguas, devem estar aliadas às boas políticas de dados e termos de uso, que estejam em conformidade com a LGPD, garantindo que suas atuações se deem dentro das diretrizes de transparência e não acabem se sujeitando às duras multas legais que podem atingir valores astronômicos (até 2% do faturamento da companhia).

É essencial, portanto, que os entes privados e órgão públicos se adaptem à nova realidade atual e organizem seus programas de

compliance até a entrada em vigência da LGDP, atuando com enfoque na transparência e na implementação de deveres legais exigidos para tratamento de dados pessoais, garantindo que as medidas de prevenção a incidentes sejam sempre contínuas e adotadas de forma responsável.

9. Referências

AMARAL, Francisco. **Direito Civil**: introdução. 6 ed. Rio de Janeiro: Renovar, 2008.

BLUM, Renato Opice. **LGDP** – A Proteção de Dados Pessoais da Criança e a Polêmica do Consentimento do Adolescente. Medium, 2018. Disponível em: <https://medium.com/@opiceblum/lgdp-a-prote%C3%A7%C3%A3o-de-dados-pessoais-da-crian%C3%A7a-e-a-pol%C3%AAmica-do-consentimento-do-adolescente-d5f14d621edc>. Acesso em: 26 nov. 2019.

BORGES, Roxana Cardoso Brasileiro. Autonomia privada e negócio jurídico. **Revista do Curso de Direito da UNIFACS**, Porto Alegre, v. 5, p.69-87, set. 2005.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Palácio do Planalto, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 20 out. 2019.

BRASIL. **Lei nº. 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Palácio do Planalto, 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm>. Acesso em: 17 out. 2019.

BRASIL. **Lei nº. 12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Palácio do Planalto, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 20 out. 2019.

BRASIL. **Lei nº. 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Palácio do Planalto, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 out. 2019.

BRASIL. **Lei nº. 13.853**, de 08 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. Palácio do Planalto, 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1>. Acesso em: 20 out. 2019.

BRASIL. **Lei nº. 8.069**, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Palácio do Planalto, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acesso em: 20 out. 2019.

CABRAL, Érico de Pina. **A "autonomia" no direito privado**. São Paulo: Revista dos Tribunais, 2004.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro**: teoria das obrigações contratuais e extracontratuais. 27 ed. São Paulo: Saraiva, 2011.

NUNES, Natália Martins. **A proteção dos dados pessoais de crianças e adolescentes**. Jus Brasil, 2018. Disponível em: <https://ndmadvogados.jusbrasil.com.br/artigos/632195598/a-protecao-dos-dados-pessoais-de-criancas-e-adolescentes>. Acesso em: 26 nov. 2019.

MORAES, Maria Celina Bodin de. **Princípios do Direito Civil contemporâneo**. Rio de Janeiro: Renovar, 2006.

PIOVESAN, Flávia. **Direitos humanos e o direito constitucional internacional**. 4 ed. São Paulo: Max Limonad, 2000.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 2ª ed. Porto Alegre: Livraria do Advogado, 2001.

SERPRO. **O que crianças e adolescentes ganham com a nova lei?** Serpro, 2019. Disponível em: <https://www.serpro.gov.br/lgpd/noticias/criancas-adolescentes-lgpd-lei-geral-protecao-de-dados-pessoais>. Acesso em: 26 nov. 2019.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 32 ed. São Paulo: Malheiros, 2009.

SOARES, Pedro Silveira Campos. **A questão do consentimento na Lei Geral de Proteção de Dados**. Conjur, 2019. Disponível em: <https://www.conjur.com.br/2019-mai-11/pedro-soares-questao-consentimento-lei-protecao-dados>. Acesso em: 26 nov. 2019.

- **BRASIL. Lei nº 8.069, de 13 de julho de 1990.** <Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Acessado em 13.06.2019- Cots, Márcio. Lei Geral de Proteção de Dados Pessoais comentada [livro eletrônico]. - São Paulo: Thomson Reuters Brasil, 2018. **- LGPD:** Lei Geral de Proteção de Dados Pessoais comentada [livro físico] Viviane Nóbrega Maldonado e Renato Opice Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019. - **BRASIL**. **Lei nº 13.709**, **de 14 de agosto de 2018**. <Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acessado em 13.06.2019.

BORELLI, Alessandra Vieira. LGPD: Lei Geral de Proteção de Dados Pessoais comentada [livro físico] Viviane Nóbrega Maldonado e Renato Opice Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019.

CHILDREN´S ONLINE PRIVACY ACT (COPPA). Disponível em: https://privacylaw.proskauer.com/articles/childrens-online-privacy-prote/ Acesso em: 26 nov. 2019.

O GLOBO. Seus dados são o novo petróleo: mas serão verdadeiramente seus? Disponível em :https://oglobo.globo.com/opiniao/seus-dados-sao-novo-petroleo-mas-serao-verdadeiramente-seus-21419529. Acesso em: 26 nov.2019.

COMISSÃO ESPECIAL DESTINADA A PROFERIR PARECER AO PROJETO DE LEI NO 4060, DE 2012. Disponível em: https://www.jota.info/wp-content/uploads/2018/05/e7f7a9e30ca16d91b84c2caf5a80fb36.pdf. Acesso em 26 nov.2019.

GENERAL DATA PROTECTlON REGULATION 2016/679 (Tradução livre). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN. Acesso em: 26 nov.2019

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 26 nov.2019.

MORAES, Alexandre de. Direito Constitucional. 13. ed. Disponível em: < https://jornalistaslivres.org/wpcontent/uploads/2017/02/DIREITO_CONSTITUCIONAL-1.pdf>. Acesso em: 26 nov.2019.

MORELI, Luiz Fernando Villa. A proteção de dados pessoais e seus efeitos nas startups de tecnologia. In: JUDICE, Lucas Pimenta; NYBO, Erik Fontenele (Coords.). Direito das Startups. Curitiba: Juruá, 2016.

UNIÃO EUROPEIA. General Data Protection Regulation 2016/679. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 26 nov.2019.

RONY VAINZOF. - LGPD: Lei Geral de Proteção de Dados Pessoais comentada [livro físico] Viviane Nóbrega Maldonado e Renato Opice Blum, coordenadores. São Paulo: Thomson Reuters Brasil, 2019.

6

O direito à privacidade e o direito à proteção de dados na Lei Geral de Proteção de Dados

Sidney Cassio Alves Rocha [1]

1. Introdução: o direito à privacidade e o direito à proteção de dados

As origens da privacidade remontam a um passado bastante longínquo, com referências ao alemão Karl David August Röder na obra "*Grundzüge des Naturrechts oder der Rechtsfilosofie*" em 1846 (CORREIA e JESUS, 2013, p. 138) e, como conceito legal, a um artigo escrito por dois advogados de Boston/EUA chamados Samuel Warren e Louis Brandeis em 1890 (GLANCY, 1979, p. 1).

Fazendo um recorte mais moderno, o direito à privacidade é referido na lei Europeia como "direito ao respeito para a vida privada" e tratado como um direito internacional a partir da Declaração Universal dos Direitos Humanos (1948). A sua adoção na Europa se deu através da Convenção Europeia em Direitos Humanos (1950) e, nela, direitos como à vida privada, à correspondência, ao lar eram objetos de proteção, sendo proibida a interferência nesses direitos por autoridades públicas, a não ser em casos legítimos, de importância e de interesse público (FRA, 2018, p. 18).

[1] Advogado graduado pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas). Mestrando em Direito Penal pela PUC Minas. Especialista em Ciências Criminais pela PUC Minas. Engenheiro Eletricista pela PUC Minas. MBA em Gestão Empresarial pela FGV. E-mail: contato@sidneyrocha.com.br

É importante ressaltar que a adoção desses tratados foi realizada bem antes do desenvolvimento de computadores pessoais e da internet. Já a proteção de dados na Europa teve início com a adoção, por um Estado alemão, de legislação para controle de processamento de informações pessoais pelas autoridades públicas e grandes companhias, em 1970. Ao final de 1980, outros Estados europeus já haviam adotado legislação específica para proteção de dados (FRA, 2018, p. 18) e o principal instrumento legal europeu sobre proteção de dados, antes do Regulamento Geral de Proteção de Dados (GDPR), foi concebido em 1990 e adotado em 1995, através da diretiva 95/46/EC, quando "apenas 1% da população europeia estava usando a internet" (REDING, 2012).

Publicada em 1981 pelo Conselho da Europa, a Convenção de número 108 – Convenção para a Proteção de Indivíduos com Relação ao Processamento Automático de Dados Pessoais – tem como objetivo e propósito "assegurar, independente de nacionalidade, o respeito aos seus direitos e liberdades fundamentais, em particular seu direito à privacidade, com relação ao processamento automático de dados pessoais". A Convenção 108 era, e ainda permanece, o "único instrumento internacional legalmente vinculante no campo de proteção de dados", tendo sido ratificada por todos os Estados Membros da União Europeia (FRA, 2018, p. 24). O Uruguai foi o primeiro país não-Europeu a aderir, em agosto de 2013[2].

Também em 2013, as Nações Unidas publicaram a Resolução A/RES/68/167 (*Resolução sobre o direito à privacidade na era digital*)[3] e em 2016 a revisaram por meio da Resolução A/C.3/71/L.39/Rev.1 (*Projeto de resolução revisado sobre o direito à privacidade na era digital*)[4]. Tal resolução reconhecia a urgência no tratamento do tema ao notar que "violações e abusos do direito à privacidade na era digital podem afetar

[2] AGESIC. Tramitado: Uruguay se adhirió al Convenio 108. Disponível em: <https://www.agesic.gub.uy/innovaportal/v/2642/1/agesic/tramitado:-uruguay-se-adhirio-al-convenio-108.html>. Acesso em: 21 mar. 2018.

[3] Tradução livre: Resolution on the right to privacy in the digital age.

[4] Tradução livre: Revised draft resolution on the right to privacy in the digital age.

todos os indivíduos, incluindo, em particular, efeitos em mulheres, assim como em crianças e aqueles que são vulneráveis ou marginalizados (UN, 2016, p. 2).

A reforma da legislação da União Europeia sobre proteção de dados conduziu à adoção do Regulamento Geral de Proteção de Dados[5] (GDPR) em abril de 2016, após intensa discussão desde 2009. Seu período transicional (*vacatio legis*) foi de dois anos, tornando-se aplicável em 25 de maio de 2018 e revogando a diretiva 95/46/EC em toda a União Europeia.

2. Os diversos conceitos de privacidade

Solove (2008, p. 1) e Glancy (1979, p. 1) afirmam que a privacidade é um "conceito em desarranjo". Solove afirma que privacidade é um conceito que passa por vários outros, abrangendo (dentre outras coisas) "liberdade de pensamento, controle sobre seu corpo, isolamento em sua casa, controle sobre informações pessoais, liberdade de (estar sob) vigilância, proteção de sua reputação, e proteção de buscas e interrogatórios" (1967, p. 1). Fundamenta-se, conforme Correia e Jesus, na "dignidade da pessoa humana, tal como na autonomia privada e no livre desenvolvimento da personalidade, conferindo poderes de autodeterminação perante os outros indivíduos, a sociedade e o Estado" (CORREIA; JESUS, 2013, p. 144).

Segundo Westin, "privacidade é a afirmação de indivíduos, grupos, ou instituições para determinar para si mesmos quando, como, e em qual extensão, informações sobre eles são comunicadas a outros" (WESTIN, 1967, p. 7). Há uma íntima relação entre a (visão que se tem sobre a) privacidade e sistemas políticos. As forças que moldarão os aparatos legais e os aspectos culturais a serem cultivados e desenvolvidos podem ser mais

[5] Tradução livre: General Data Protection Regulation.

ou menos abertas a divulgação e compartilhamento, como a democracia, ou tendentes a vigilância e segredo, como o totalitarismo.

O regime totalitarista moderno "confia no segredo para o regime, [na] mais alta vigilância e [na] divulgação para todos os outros grupos" (WESTIN, 1967, p.23). De fato, as práticas são diametralmente opostas. Na democracia, exige-se uma postura social que favoreça a publicidade dos atos. Conforme Westin, "a sociedade democrática se baseia na publicidade como um controle sobre o governo, e na privacidade como um escudo para a vida individual e em grupo" (WESTIN, 1967, p.23).

Para Westin (1967, p. 31) há quatro estados básicos de privacidade individual: *solidão, intimidade, anonimato e reserva*. O primeiro estado da privacidade é a *solidão*, na qual o indivíduo é separado do grupo e se encontra livre da observação ou interação com outras pessoas. Este seria "o mais completo estado de privacidade que indivíduos podem atingir".

O segundo estado da privacidade é a *intimidade*. Nele a pessoa tem a opção de escolher com quem quer se relacionar de maneira reservada, íntima. O terceiro estado é o *anonimato*. Neste estado, o indivíduo se expressa publicamente (através de atos ou outra manifestação), porém sua identidade permanece oculta. O quarto, sendo o mais sutil e último estado da privacidade, é a *reserva*: "esta é uma barreira psicológica contra uma invasão indesejada" (WESTIN, 1967, 32).

Com a intenção de sistematizar o amplo conceito de privacidade, Solove (2008, p. 12) classifica as diferentes concepções em seis tipos gerais: (1) o direito de estar só (*right to be alone*), (2) limitado acesso a si (*limited access to self*), (3) segredo (*secrecy*), (4) controle sobre a informação pessoal (*control over personal information*), (5) personalidade (*personhood*) e (6) intimidade (*intimacy*).

O direito de estar só (*right to be let alone*) teve sua fundação a partir do direito de privacidade nos EUA. À época (final do século XIX), o advento das câmeras fotográficas portáteis e de baixo custo tornou qualquer pessoa em um potencial fotógrafo, enquanto anteriormente este ofício era destinado aos realmente profissionais, dadas as grandes dimensões dos

equipamentos existentes e seu proibitivo preço. O fato curioso é que a grave violação da privacidade era a proliferação de divulgação de fotos e fatos "alheios". Certamente causaria espanto e incompreensão a Warren e Brandeis, caso pudessem visualizar os dias de hoje, saber que a proliferação de dispositivos tecnológicos causaria a exibição descontrolada de fatos e fotos não alheios, mas, principalmente, pessoais por meio das atualmente chamadas redes sociais e aplicativos de comunicação instantânea.

Warren e Brandeis se preocupavam não somente com a nova tecnologia, mas principalmente como se daria sua interseção com a mídia. Na metade do séc. XIX havia menos de 1 milhão de leitores nos EUA, sendo que no final deste mesmo século, após o advento da nova tecnologia fotográfica portátil e de custo acessível desenvolvida pela Kodak, o número de leitores aumentou dez vezes chegando a 8 milhões, assim como quase aumentou em dez vezes o número de jornais (SOLOVE, 2008, p. 16). O que pensariam Warren e Brandeis ao tomar conhecimento do atual número de usuários publicando suas fotos na rede social mais famosa do mundo, o Facebook, com aproximadamente 2,32 bilhões de usuários ativos?[6]

Analisar a violação da privacidade nos dias atuais passa, necessariamente, por analisar o fenômeno da "autoviolação", ou "*self-invasion*". Este fenômeno está associado ao indivíduo não-reservado que ultrapassa seus próprios limites de privacidade. Simmel, 1950, apud Westin, 1967, afirma que essa falha em promover minimamente sua privacidade faz com que o "indivíduo revele tanto sobre si àqueles que estão a sua volta que seus relacionamentos deterioram e ele cessa de ter uma vida privada". Gerstein, (1978, p. 76), por sua vez, declara que "relacionamentos íntimos simplesmente podem não existir se não continuarmos a insistir na privacidade para eles".

[6] Statisa. **Number of monthly active Facebook users worldwide as of 4th quarter 2018 (in millions)**. Disponível em: <https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide>. Acesso em: 16 mar. 2019.

Warren e Brandeis acreditavam que o princípio da privacidade não se identificava em "obter lucro com a publicação [indevida], mas na segurança e tranquilidade obtidas com a possibilidade de prevenir qualquer publicação" (WARREN; BRANDEIS, 1890). Certamente, o aumento exponencial dessas possibilidades experimentado pelo atual sujeito de dados deveria, pela lógica, torná-lo bem mais rigoroso e seletivo quanto a divulgação e publicação de informações acerca de sua intimidade, o que, *contrario sensu*, não é o que parece acontecer de maneira geral.

Nas décadas vindouras, tal conceito (o direito de estar só) seria invocado outras vezes, inclusive na corte estadunidense, como em *Olmstead vs. United States* e *Katz vs. United States* (WARREN; BRANDEIS, 1890), como "o mais abrangente dos direitos e o direito mais valorizado pelos homens civilizados", de maneira que sua representação moldou "significantemente o direito constitucional" daquele país, tendo sido observado pelo juiz membro da Suprema Corte estadunidense Abe Fortas que "o direito de privacidade é, declarado simplesmente, o direito de estar só" (SOLOVE, 2008, p. 17).

Westin afirma que, apesar de ser possível levar uma vida a sós consigo mesmo ou com sua família, há trabalhos científicos mostrando que "não é a segurança em si que mantém animais da mesma espécie juntos, mas um desejo de estimulação de seus companheiros" (WESTIN, 1967, p. 10).

Solove (2008, p. 18), entretanto, apesar de creditar certo vanguardismo no artigo apresentado por Warren e Brandeis, afirma que o "direito de estar só vê a privacidade como um tipo de imunidade ou isolamento", considerando tal definição demasiada ampla e vaga.

De acordo com Solove (2008, p. 18), o segundo conceito analisado, o "acesso limitado a si" (*limited access to self*), é intimamente relacionado ao conceito anterior do "direito de estar só", talvez representando uma formulação mais sofisticada dele mesmo, que não equivale à "solidão", sendo esta uma forma de isolamento de outros indivíduos. Sua concepção é mais ampla abarcando a "liberdade da interferência governamental,

assim como a não-intrusão da imprensa e outros". Porém, tal conceito não apresenta uma noção de quais assuntos são privados, consequentemente, tornando incerto "que acesso implicaria [violação] de privacidade", uma vez que "certamente nem todos os acessos à própria pessoa infringem a privacidade, somente aqueles relacionados às dimensões específicas de si ou a assuntos ou informações particulares" (SOLOVE, 2008, p. 20).

O entendimento de privacidade como segredo (*secrecy*) é o terceiro conceito analisado por Solove, de acordo com o qual a "privacidade é violada pela divulgação de uma informação previamente oculta". A divulgação seletiva de informações sobre si representa, de fato, a ocultação do que poderia ser utilizado por outros em sua desvantagem ou em seu descrédito. Trata-se de uma decisão pessoal sobre o que evitar que seja divulgado sobre si e, por isso, o conceito de "privacidade como segredo pode ser entendido com um subconjunto da limitação do acesso a si", falhando, porém, em "reconhecer que indivíduos podem querer manter coisas privadas de algumas pessoas, mas não de outras" (SOLOVE, 2008, p. 23).

Ainda sobre esse conceito, Solove (2008, p.24) faz importante menção ao fato de que a privacidade "envolve mais que evitar divulgação, também envolve a possibilidade de o indivíduo garantir que aquela informação pessoal é utilizada para os propósitos desejados por ela". Tal conclusão está em plena consonância com os princípios informadores contidos no Regulamento Geral de Proteção de Dados (GDPR – *General Data Protection Regulation*) europeu, conforme artigo 5, 1, b, que estabelece que os dados pessoais devem ser "coletados para propósitos especificados, explícitos e legítimos e não sejam processados de uma maneira incompatível com tais propósitos" e com o artigo 13, 1, c, segundo o qual o sujeito de dados seja informado, dentre outros, sobre os "propósitos do processamento para os quais os dados pessoais são desejados (...)"[7]. A Lei 13.709/2018, também chamada Lei Geral de

[7] GDPR. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679

Proteção de Dados, em seu artigo 6º, informa que "as atividades de tratamento de dados pessoais deverão respeitar (...): I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular (...)"[8].

De acordo com Shils, 1956, apud Westin (1967, p. 26), há uma importante distinção entre privacidade e segredo ou reserva (*secrecy*): "No segredo, ele nota, a lei proíbe a divulgação da informação. Na privacidade, a divulgação 'é de acordo com a discrição do possuidor, e tais sanções como a lei provê são direcionadas apenas contra aquisição coercitiva' por pessoas para as quais o indivíduo não quer divulgar".

Entretanto, ressalva Solove, a privacidade é esperada mesmo em público, não sendo ela oposta necessariamente à publicidade, tratando-se de "questões que seriam inapropriadas para outros tentarem saber mais, muito menos reportarem sobre, sem o consentimento do sujeito" (BENN, 1971, apud SOLOVE, 2008, p. 24). Tal conclusão torna o conceito de segredo demasiado limitado para privacidade.

O controle sobre a informação pessoal (*control over personal information*) como teoria da privacidade, como autodeterminação sobre os vários aspectos da comunicação da informação pessoal a outros (quando, como, em que extensão, etc.), é uma das teorias predominantes. Mais uma vez, segundo Solove, também este conceito "pode ser visto como um subconjunto do conceito de limitação de acesso", tornando essa teoria demasiado limitada ao tratar, por exemplo, a informação como um *commodity* individualizado, um bem de propriedade particular, desprezando as situações nas quais a informação é "formada em relacionamento com outros", situação na qual estes outros possuem algum nível de direito e exigibilidade sobre a mesma. Ademais, a privacidade pode ser violada em situações que não envolvam uma informação pessoal, como a submissão de alguém a alguma propaganda ou manipulação de anúncios subliminares, fazendo com que a teoria da privacidade como

[8] Lei 13.709/2019: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

controle sobre a informação pessoal exclua muitos "aspectos da vida que comumente assumimos serem privados", desconsiderando a privacidade como parte de "uma estrutura social" (SOLOVE, 2008, p. 29).

A proteção da personalidade (*personhood*) é outra teoria da personalidade construída a partir de uma noção também de Warren e Brandeis sobre "personalidade inviolável" e, diferentemente das teorias anteriores, esta é "construída sobre um fim normativo de privacidade, a proteção da integridade da personalidade" (SOLOVE, 2008).

Stolze e Pamplona (2017, p. 67) conceituam direitos de personalidade como "aqueles que têm por objeto os atributos físicos, psíquicos e morais da pessoa em si e em suas projeções sociais". Tal conceituação situa a personalidade em uma esfera extrapatrimonial do indivíduo, tratando-se de "valores não redutíveis pecuniariamente". Segundo Solove (2008, p. 38), as teorias da privacidade como personalidade falham ao elucidar o conceito de privacidade porque "frequentemente não articulam uma definição adequada de personalidade", sendo tais teorias muito amplas e não restritas ao ambiente puramente privado, uma vez que expressamos publicamente muitas coisas que são únicas ao indivíduo, como, por exemplo, o artista que exibe publicamente sua pintura como expressão criativa do seu mais profundo e privado ser.

A intimidade (*intimacy*) possui conceituações diversas. Fried, 1970, apud Solove, 2008, afirma que "intimidade é o compartilhamento de informações sobre as ações, crenças ou emoções de alguém que este não compartilha com todos tendo o direito de não compartilhar com ninguém (...)". Solove afirma que nossos relacionamentos são compostos de diferentes graus de intimidade e autorrevelação, de maneira a valorizarmos a privacidade que nos permite "manter os desejados níveis de intimidade para cada de nossas variadas relações" (2018, p. 34).

No direito brasileiro, a intimidade possui conexão com alguns dos conceitos apresentados. Carlos Bittar afirma que:

> Diferentes denominações tem recebido esse direito, desde "*right of privacy*" ou "*right to be alone*" (no direito anglo-norte-americano); "*droit à la vie*

> *privée*" (francês); "*diritto alla riservatezza"* (italiano); "*derecho a la esfera secreta*" (espanhol); "direito de estar só"; "direito à privacidade" e "direito ao resguardo" (BITTAR, 2015, Locais do Kindle 2442-2446, tradução livre).

Percebemos que Bittar faz conexão do direito à intimidade com o direito de estar só (*right to be let alone*), direito de controle sobre a informação pessoal (*control over personal information*), direito ao segredo (*secrecy*) e ao direito de privacidade como diferentes denominações de um mesmo direito, o direito à intimidade. Porém, de maneira oposta, explica que se trata de "direito geral à intimidade, com particularizações à imagem, segredo e privacidade", ou seja, a privacidade seria um subconjunto da intimidade, sendo que esta última "tem-se reduzido com a internet e os novos meios eletrônicos" (BITTAR, 2015, Locais do Kindle 2456).

Sustenta Solove que as teorias de privacidade como intimidade são demasiadamente limitadas por "focarem exclusivamente nos relacionamentos interpessoais e nos sentimentos particulares engendrados por eles" (SOLOVE, 2008, p. 36).

Um ofensor natural à privacidade é a necessidade de vigilância. A vigilância é praticada desde a relação mais celular, como na família, na qual os pais vigiam seus filhos e cônjuges que vigiam uns aos outros, passando pela escola que imprime vigilância sobre seus alunos, pela relação empregatícia onde o empregador impõe a vigilância sobre os atos do empregado, até o Estado e a administração pública, que impõe seu poder de vigilância aos que se encontram nas extensões de seu domínio.

Westin descreve três tipos principais de vigilância moderna: observação, extração e reprodutibilidade de comunicação (WESTIN, 1967, p. 58). A "observação", segundo o autor, é realizada pelos próprios grupos sociais em que o indivíduo está inserido. Essa observação realizada pelos membros do grupo induzem o indivíduo a desempenhar (ou reproduzir) determinado comportamento, geralmente o aceito por aquele grupo. A necessidade de privacidade seria o "isolamento de ações e julgamentos

advindos da vigilância de outros" (MERTON, 1957, apud WESTIN, 1967, p.58).

Westin faz menção a uma suposta "desejável e vital" vigilância em locais públicos para garantir segurança física através do uso de "novos dispositivos de visualização e escuta". Tal pensamento ecoa na atualidade por meio de diversas políticas da administração pública. Uma iniciativa recente equipou o Carnaval de Salvador/BA com 430 câmeras com reconhecimento facial e 14 drones para identificar supostos criminosos com mandado de prisão em aberto[9].

A "extração" trata de "entrar na privacidade psicológica da pessoa requerendo que ele revele através da fala ou ações, por meio de partes de sua memória e personalidade que considera privadas" (WESTIN, 1967, 60).

O terceiro e último tipo de vigilância segundo Westin é um tipo "não-usual" chamado reprodutibilidade de comunicação. O autor o classifica assim porque à época não havia ainda sido bem estudado, devido ao seu "recente desenvolvimento" através dos novos dispositivos de gravação e câmeras. Ocorre que tais dispositivos já se encontram muito bem desenvolvidos na atualidade e em pleno uso pelas autoridades (e pela população em geral). O autor chama a atenção para o uso "secreto", não-autorizado pela pessoa objeto da gravação, exercendo pressão nos indivíduos que têm receio de serem expostos a situações embaraçosas se tais gravações forem reveladas publicamente.

3. Teorias sobre a privacidade e proteção de dados

O direito à proteção de dados emergiu como um direito autônomo com a publicação do Tratado de Lisboa. Lynskey afirma que "ainda permanece difícil identificar uma explanação coerente para a introdução

[9] Correio 24 horas. **Câmeras de reconhecimento facial vão ajudar a identificar criminosos no Carnaval**. Disponível em: <https://www.correio24horas.com.br/noticia/nid/cameras-de-reconhecimento-facial-vao-ajudar-a-identificar-criminosos-no-carnaval>. Acesso em: 19 mar. 2019.

de um direito à proteção de dados, em adição ao bem estabelecido direito à privacidade, no ordenamento legal da UE"[10] (2015, p. 93). Fato é que a Carta Europeia adquiriu status de lei primária e incluiu o direito à proteção de dados e o direito à privacidade. O artigo 16 do *Treaty on the Functioning of the European Union*[11] prescreve que "todos têm o direito à proteção de dados pessoais concernentes a eles" [12], provendo uma base legal independente para a legislação de proteção de dados (LYNSKEY, 2015, p. 87).

A regulação da proteção de dados na Europa abrange os aspectos de regulação social e econômica, controlando fluxos de dados pessoais (LYNSKEY, 2015, p. 81). Atualmente, três possibilidades são consideradas quanto à discussão envolvendo o direito à privacidade e o direito à proteção de dados.

O primeiro modelo delineia a privacidade e a proteção de dados como ferramentas complementares, com o objetivo de garantir respeito à dignidade humana. Tal asserção encontra guarida no direito à autodeterminação informativa baseada no direito de personalidade, este derivado, por sua vez, dos direitos à dignidade humana no direito básico alemão (LYNSKEY, 2015, p. 95).

As objeções a esse modelo baseiam-se no fato de que há pouco consenso quanto ao que efetivamente seja "dignidade humana" (ao menos na União Europeia); que o direito à proteção de dados não está incluso nos direitos baseados em dignidade; ao invés, está incluso no capítulo de "Liberdades" na Carta Europeia, e que os dados pessoais são bens disponíveis, ao contrário da dignidade humana.

O segundo modelo afirma que a proteção de dados pessoais é uma faceta do direito à privacidade, representando uma cisão interna dele, assim como o direito à privacidade representou uma separação do "direito

[10] "(...) it remains difficult to identify a coherent explanation for the introduction of a right to data protection, in addition to the well-established right to privacy, in the EU legal order".

[11] Official Journal. **Treaty on the Functioning of the European Union**. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:12012E/TXT&from=EN. Acesso em: 29 abr. 2019.

[12] Tradução livre: "Everyone has the right to the protection of personal data concerning them".

de estar só" (SOLOVE, 2004, p. 75). Tal assertiva também pode ser associada ao controle sobre as informações pessoais (*control over personal information*), no qual o direito à proteção de dados pessoais seria um subconjunto do direito à privacidade ou do *limited access to self*, tornando os dados pessoais uma *commodity*, bens disponíveis pelo seu titular e passíveis de valoração econômica.

Já o terceiro modelo sustenta que a proteção de dados se refere a um direito independente. Mesmo tendo grande interseção com o direito à privacidade, uma vez que ambos asseguram a proteção de dados, o direito à proteção de dados "serve a um número de propósitos a que a privacidade não serve e vice-versa" (LYSNKEY, 2015, p. 103).

Este último modelo parece ser o modelo adotado pela União Europeia em seu *General Data Protection Regulation* (GDPR), uma vez que claramente adotam a separação dos dois direitos em publicações oficiais sobre o direito de proteção de dados: "O direito ao respeito da vida privada e o direito à proteção de dados, embora proximamente relacionados, são direitos distintos"[13] (FRA, 2018, p. 18, tradução livre).

4. A Lei 13.709/2018 (LGPD): privacidade ou proteção de dados?

A lei 13.709/2018 (Lei Geral de Proteção de Dados) possui íntima relação com o direito de privacidade, tendo o respeito a ele como um de seus fundamentos, como consta em seus artigos 1º e 2º:

> *Art. 1º: Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.*
> *Art. 2º: A disciplina da proteção de dados pessoais tem como fundamentos:*
> *I - o respeito à privacidade;*

[13] "The right to respect for private life and the right to personal data protection, although closely related, are distinct rights".

O legislador considerou a intimidade como direito dissociado da privacidade ao conceder a ela proteção destacada como no inciso IV do artigo 2º:

> *IV - a inviolabilidade da intimidade, da honra e da imagem;*

Também é possível perceber tal dissociação na redação do artigo 17 que versa sobre os direitos do titular:

> 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.

A privacidade e a intimidade são tidas como direitos fundamentais na redação da Lei Geral de Proteção de Dados em seu artigo 17, porém seu artigo 1º cita somente a privacidade como objeto de proteção da lei (além da liberdade).

De fato, a intimidade encontra-se amparada em sua literalidade na Constituição Brasileira, conforme disposto em seu artigo 5º, X:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Porém, a privacidade não se encontra literalmente transcrita na Constituição Brasileira, sendo realizada sua associação indireta ao direito fundamental "vida privada", que mais se assemelha ao direito de isolamento, um aspecto da privacidade, assim como seria a própria intimidade um estado da privacidade, conforme Westin (WESTIN, 1967, 32). Já Bittar possui afirmações diferentes, ora apontando a privacidade como uma outra denominação da intimidade, ora apontando a privacidade como uma particularização da intimidade, ou seja, um subconjunto, assim como a imagem e o segredo (BITTAR, 2015, Locais do Kindle 2456).

A Lei Geral de Proteção de Dados apresenta indícios de que a privacidade consiste nesse leque de direitos conectados, uma vez que exige

a implementação de um programa de governança em privacidade (artigo 50, § 2º, I), cria um Conselho Nacional de Proteção de Dados Pessoais e da Privacidade na composição da Autoridade Nacional de Proteção de Dados (Artigo 55-C, II), estabelece a competência de elaboração de estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade (Artigo 55-J, XII), estabelece a elaboração da Política Nacional de Proteção de Dados e da Privacidade (Artigo 58-B, II) e pretende a disseminação de conteúdo sobre a proteção de dados pessoais e da privacidade à população em geral (Artigo 58-B, V). Não há menção direta à intimidade (a não ser nos dois dispositivos já descritos), ao isolamento, ao segredo ou a qualquer outro aspecto apresentado neste estudo.

A redação da lei alterna entre a utilização dos termos privacidade, proteção de dados, e privacidade, por um lado, e proteção de dados, por outro, de maneira indistinta. Não é possível distinguir um padrão que nos permita associar claramente a identificação da lei a algum dos três modelos apresentados de distinção entre privacidade e proteção de dados. Para que se perceba a indefinição na lei brasileira, no GDPR (*General Data Protection Regulation*), norma europeia que serviu de modelo para a legislação brasileira, não há, em 173 *recitals* e 99 artigos, uma única menção ao termo "privacidade", tratando exclusivamente e claramente do direito à proteção de dados, conforme disposto no *recital* 1:

> (1) A proteção de pessoas naturais com relação ao processamento de dados pessoais é um direito fundamental. O artigo 8(1) da Carta de Direitos Fundamentais da União Europeia (a "Carta") e o artigo 16(1) do Tratado de Funcionamento da União Europeia (TFEU) informam que todos têm o direito à proteção de dados pessoais concernentes a ele ou ela.[14]

No caso da lei brasileira compreendemos que apresenta um modelo *próprio* possuindo características do direito à proteção de dados e

[14] Tradução livre: (1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

acentuada interseção com outras características contidas no direito à privacidade, de base principiológica de garantia da dignidade humana, autodeterminação informativa e do livre desenvolvimento da personalidade.

5. Considerações finais

O conceito jurídico de privacidade remonta ao final do século XIX, tendo sido desenvolvido ao longo de vários anos, que se podem compartimentar didaticamente como fases. A privacidade é um conceito de difícil denominação e de pouca estabilização na seara jurídica, apesar de qualificado como direito fundamental, sendo desdobrada em diversos outros conceitos como intimidade, direito de estar só, segredo, dentre outros. Tais conceitos, ao menos nos autores estudados neste artigo, não são capazes de descrever precisamente o conceito de privacidade na vida humana.

O direito à proteção de dados caracterizou-se como direito autônomo na Europa, tendo valores e objetos de proteção próprios, fora do tradicional escopo da privacidade. Apesar disso, também há intensa discussão sobre seus aspectos característicos. De maneira geral, três modelos subsistem: o primeiro modelo considerando privacidade e proteção de dados como ferramentas complementares para a garantia da dignidade humana; o segundo modelo considerando o direito à proteção de dados como uma faceta do direito à privacidade e o terceiro modelo considerando o direito à proteção de dados como direito independente, com grandes áreas de interseção com o direito à privacidade.

A análise da Lei Geral de Proteção de Dados brasileira (lei 13.709/2018) nos remete a um modelo *próprio* em que um leque de direitos conectados apresenta ampla identificação com as características próprias do direito à proteção de dados, porém, calcados fundamentalmente no conceito de privacidade como garantia da dignidade

humana, autodeterminação informativa e do livre desenvolvimento da personalidade do sujeito de dados.

6. Referências

BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. 8. ed. rev. aum. e mod. por Eduardo C. B. Bittar – Edição do Kindle. São Paulo: Saraiva, 2015.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**. Brasília, 15 ago. 2018.

CORREIA, Pedro M. A. R.; JESUS, Inês O. A. **O lugar do conceito de privacidade numa sociedade cada vez mais orwelliana**, Direito, Estado e Sociedade, Lisboa, n. 43, p. 135-161, jul/dez 2013.

EUROPEAN Union Agency for Fundamentals Rights and Council of Europe (FRA). **Handbook on European Data Protection**. Luxemburgo: 2018.

GAGLIANO, Pablo Stolze; FILHO, Rodolfo Pamplona. **Manual de Direito Civil**. São Paulo: Saraiva, 2017.

GERSTEIN, Robert S. **Intimacy and Privacy**, Ethics, The University of Chicago Press, vol. 89, No. 1, pp. 76-91, 1978.

GLANCY, Dorothy J. **The Invention of the Right to Privacy**. Arizona Law Review, Arizona, vol. 21, n. 1, 1979.

LYNSKEY, Orla. **The Foundations of EU Data Protection Law**. Oxford: Oxford University Press, 2015.

REDING, Viviane. **Outdoing Huxley: Forging a high level of data protection for Europe in the brave new digital world**. Luxemburgo: Digital Enlightenment Forum, 2012;

SOLOVE, Daniel J. **The Digital Person: Technology and Privacy in the Information Age**. New York: New York University Press, 2004.

_____ **Understanding Privacy**. Cambridge: Harvard University Press, 2008.

WARREN, Samuel D.; BRANDEIS, Louis D. **The Right to Privacy**, Harvard Law Review, Boston, Vol. 4, N^0 5, pp. 193-220, 1890.

WESTIN, Alan F. **Privacy and Freedom**. New York: Atheneum, 1967.

UNITED NATIONS. **A/C.3/71/L.39/Rev.1 – The right to privacy in the digital age**. Nova York, U.N. General Assembly, 2016.

7

Direito à explicação em decisões automatizadas

Daniel Evangelista Vasconcelos Almeida [1]

1. Introdução

Com uma frequência cada vez maior, decisões diversas são automatizadas. Atualmente não é raro encontrar uma situação na qual alguém está sujeito a uma decisão automatizada. Dessa forma é necessário entender o que é uma decisão automatizada, quais os níveis possíveis de automação, os riscos aos quais se está exposto e, por fim, se há um direito a explicação quando uma decisão é automatizada.

O avenço tecnológico faz com que algoritmos, sequência lógica para se tomar uma decisão, fiquem cada vez mais complexos. Contudo, desde a década de 70 já há o uso de sistemas para a tomada de decisão, ainda de forma não autônoma, os quais foram chamados de "sistemas especialistas", servindo de apoio para a decisão de especialistas humanos. Atualmente, com o uso de redes neurais profundas (DNNs, do inglês *deep neural networks*), tem-se um problema no que se refere à explicação da decisão.

As DNN's são redes neurais que utilizam o aprendizado de máquina. Sistemas que utilizam essas redes são capazes de ajustar a decisão final com base em histórico de dados que são ou importados de uma base já existente ou até mesmo reimportados a partir de decisões do próprio sistema.

[1] Doutorando em Direito pela UFMG. Mestre em Direito Privado pela PUC Minas. Professor de Direito Civil da FAMIG. Professor da pós-graduação *lato sensu* da PUC Minas e CEDIN. Advogado especialista em Direito Digital. E-mail: danielevangelista@gmail.com

Esses sistemas podem ser utilizados em variadas situações, as quais podem impactar a vida de um indivíduo. Situações como obtenção de um plano de saúde, seguro de vida, empréstimo, emprego, benefício previdenciário, preço e elegibilidade para acesso à certos bens de consumo, tudo pode ser decidido com o uso de um sistema baseado em DNN[2].

O'Neil[3] afirma que sistemas de *profiling*, ou seja, sistemas que classificam usuários de forma automatizada com base em coleta e processamento de dados pessoais, podem ter consequências negativas. Por exemplo, um sistema utilizado para a concessão de crédito que utilize a perfilização pode discriminar uma pessoa que more em determinado bairro periférico e tenha certas características, colocando-a em um grupo de risco. Um outro uso desse mesmo sistema é o possível recrutamento dessa pessoa para um emprego. A seleção poderia ser feita com base em um sistema que levaria em consideração tais informações. Nesse contexto, é importante que se discuta se há um direito à explicação em sistemas de tomada de decisão de forma automatizada e em que consiste tal direito.

Para tanto, no tópico 2 será conceituada decisões automatizadas. Será feita a diferenciação entre declaração de vontade automatizada de decisão automatizada em sentido estrito. Adiante, no tópico 3, será estudada a forma de se tutelar juridicamente o algoritmo, perpassando pelo instituto da propriedade industrial. Serão demonstrados os vários elementos dos sistemas que permitem a tomada de decisão automatizada, como a marca, o software e o segredo industrial, demonstrando como é a proteção

No tópico 4, será analisado o caso da *Decolar* o qual demonstra quais são os riscos das decisões automatizadas. No tópico 5, serão estudadas a GDPR e da LGPD, sendo feita a análise se existe um direito à explicação e o que seria efetivamente concedido por ele. Será diferenciado direito à explicação do direito à revisão. Por fim, no tópico 7, será evidenciado como é possível a explicação de uma decisão que usa um algoritmo com *machine*

[2] MONTEIRO, Renato Leite. *Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais?*, Instituto Igarapé, Artigo Estratégico nº 39, Dezembro de 2018.

[3] O'NEIL, Cathy. *Weapons of math destruction: How big data increases inequality and threatens democracy*. Broadway Books, 2016.

learning utilizado para a tomada de decisões automatizadas. Por fim, demonstrar-se-á o entendimento do STJ sobre a auditoria de sistemas opacos para tomada de decisões.

1.1 Decisões automatizadas: conceito, funcionamento, espécies e demais aspectos preliminares

Inicialmente, é importante que se diferencie declaração de vontade automatizada de decisão automatizada. São conceitos distintos e merecem tratamento diverso. Por decisão automatizada entende-se que um sistema decide algo que tenha relevância em algum aspecto da vida da pessoa. Conforme Renato Leite Monteiro, "trata-se de sequências pré-definidas de comandos automatizados que, com base em dados pessoais e não pessoais, chegam a conclusões que podem sujeitar alguém a uma determinada ação"[4].

Por declaração de vontade automatizada entende-se a adoção de um sistema para averiguar o cumprimento de algum pré-requisito, que se cumprido irá ter alguma consequência prática. Assim, a declaração de vontade automatizada é binária, ou seja, o sistema não tem poder decisório, ele apenas averigua se os critérios foram cumpridos. Como um exemplo imagine uma *vending machine*, que entrega um produto se o indivíduo entregar uma quantia pré-determinada para a máquina.

A presente pesquisa investiga a explicação de decisões automatizadas, as quais serão tomadas a partir de um algoritmo, uma sequência de passos a serem seguidos para atingir um determinado objetivo. Assim, colocando-se um comando de entrada ter-se-á uma saída de acordo com os critérios estabelecidos no próprio algoritmo.

Na área da tecnologia, algoritmos são passos a serem seguidos por um módulo processador e seu respectivos usuários que, quando executados de forma correta conseguem realizar determinada tarefa. São verdadeiras linhas de código de programação.

---

[4] MONTEIRO, Renato Leite. *Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais?,* Instituto Igarapé, Artigo Estratégico nº 39, Dezembro de 2018.

Como visto na introdução, o avanço tecnológico faz com que algoritmos fiquem cada vez mais complexos. Enquanto na década de 70 o uso de sistema especialistas possibilitavam que o médico, por exemplo, fosse mais preciso em seu diagnóstico, atualmente é possível que está tomada de decisão seja feita a partir de uma rede neural profunda (DNN).

As DNN's são redes neurais que utilizam o aprendizado de máquina. Sistemas que utilizam essas redes são capazes de ajustar a decisão final com base em histórico de dados que são ou importados de uma base já existente ou até mesmo reimportados a partir de decisões do próprio sistema.

Um algoritmo feito com aprendizado profundo eventualmente poderá ser uma BlackBox, ou seja, o seu modo de funcionamento é desconhecido. Isso ocorre pois esse tipo de sistema é feito em similaridade com o pensamento humano. Assim, existe uma fase importante que é a de treinamento do sistema, a qual pode ser supervisionada ou não.

Exemplificando: imagine um sistema com base em aprendizado profundo para identificar pessoas. O cérebro humano sabe quais são as características principais de uma pessoa, quais sejam, pernas, braços, corpo, cabeça, olhos, boca, nariz, entre outras características. Agora pense: se você ver alguém que não tem uma perna, você interpreta que é uma pessoa? Claro. Por qual motivo? Pois ela ainda tem todos os outros requisitos. Mas como ensinar então um algoritmo a pensar como um humano, tendo em vista as mais variadas características possíveis?

É realmente algo complexo. Para isso, é necessária uma grande base de dados, a partir da qual o algoritmo irá aprender a identificar a partir de ajustes em pesos decisórios. Assim, para se treinar um sistema como esse, após a sua escrita deverão ser inseridas várias entradas que contenham humanos dizendo para o sistema que ali tem-se um humano. Ainda, imagens que não contenham humanos, dizendo para o mesmo que ali não contém humano. Ao final do processo, o sistema terá aprendido a identificar um humano, a partir de erros e acertos. Quanto maior for a fase de aprendizado, maior será a acurácia do sistema.

Carbonera et. al. [5] explica que para viabilizar o processo de treinamento da rede neural profunda é necessário um conjunto suficientemente grande de dados, no qual cada entrada deve ter um rótulo com a resposta esperada para a rede neural. Assim, o próprio sistema consegue se ajustar para cada ter uma acurácia cada vez maior. A decisão tomada não necessariamente é baseada em algo que um ser humano seria capaz de discernir, já que essa aprendizagem é autônoma. Ainda, o resultado pode ser diferente do antevisto por quem desenvolveu o algoritmo[6].

O problema é que a depender da forma como for escrito o sistema não será possível identificar os pesos que o mesmo adotou. Outro problema é que eventualmente a decisão não fará sentido para uma pessoa. Assim, esse sistema fictício pode identificar características que possibilitam a decisão se é ou não uma pessoa com base em critérios que não são inteligíveis pela mente humana. Por mais que eventualmente se tenha uma explicação, essa pode não fazer sentido.

Não é possível compreender a arquitetura do código sem que o mesmo seja analisado, já que em DNN's a fase de aprendizagem irá modificar os pesos decisórios. Portanto, não basta analisar o que o programador escreveu, já que a DNN possuíra características diferentes após a fase de aprendizado. Entender uma decisão automatizada de um algoritmo BlackBox importa no conhecimento de toda a sua forma de funcionamento, o que pode ser prejudicial para a companhia.

Fornecer a informação ao titular pode representar um problema para o controlador do sistema, pois muitas vezes são utilizadas DNN's, nas quais não se consegue identificar o processo de tomada de decisão, tão somente o comando de entrada e de saída. Informações sobre o processo de tomada de decisão pode ocasionar o conhecimento por completo do algoritmo utilizado, o que pode ser prejudicial para o controlador.

---

[5] CARBONERA, Joel; GONÇALVES, Bernardo; Clarisse de Souza. *O problema da explicação em Inteligência Artificial: considerações a partir da semiótica*. TECCOGS – Revista Digital de Tecnologias Cognitivas, nº 17, Jan-Jun 2018

[6] BURRELL, Jenna. *How the Machine "Thinks:" Understanding Opacity in Machine Learning Algorithms*. Rochester, NY: Social Science Research Network, 2015.

A decisão automatizada pode ser prejudicial para o titular do dado pessoal. Algumas situações ilustram tal afirmação:

1) Nos Estados Unidos foi desenvolvido um sistema para calcular a pena a ser cumprida por condenados. Contudo, o referido sistema pode dar uma pontuação consideravelmente maior para infratores de minorias étnicas.[7]
2) Na China, até o ano de 2020 existirá um sistema de avaliação de todos os cidadãos, sendo que a nota obtida irá determinar o acesso a bens de consumo.[8]
3) No Brasil é utilizado o sistema de *credit scoring* para se determinar a taxa de juros a ser ofertada para o consumidor.
4) O Grupo Pão de Açúcar desenvolveu um algoritmo para publicidade direcionada, com descontos exclusivos para determinados consumidores.[9]
5) Aplicativos como Uber excluem usuários com base em fórmulas próprias. (UBER, 2017)
6) A Polícia de Chicago desenvolveu um programa para criar uma lista com nomes de pessoas propensas a se envolver em crimes violentos totalmente baseada em informações coletadas sobre elas na Internet. (PINHEIRO, 2016, p. 96). A polícia Italiana também desenvolveu um sistema similar[10].
7) Há discussão sobre a possibilidade do algoritmo usado para determinar o *feed* de notícias do Facebook ter ajudado a eleger o presidente dos Estados Unidos, Donald Trump[11].
8) A Amazon utilizou um algoritmo para a contratação de funcionários, sendo que este deu preferência a candidatos do sexo masculino[12].
9) A Decolar.com responde atualmente à uma Ação Civil Pública por supostamente precificar o seu serviço de forma diferente com base na localização do IP do consumidor (ACP 0018051-27.2018.8.19.0001)
10) A ViaQuatro utilizou um sistema de reconhecimento facial no metrô de São Paulo, o qual possibilitava a identificação de emoções de usuários em situações distintas.

[7] Informação disponível em <https://www.bbc.com/portuguese/brasil-37677421>

[8] Informação disponível em <https://veja.abril.com.br/mundo/na-china-atos-dos-cidadaos-valerao-pontos-e-limitarao-seus-projetos/>

[9] Informação disponível em <https://braziljournal.com/pao-de-acucar-descobre-um-tesouro-nos-algoritmos>

[10] Informação disponível em <https://www.bbc.com/portuguese/internacional-46198655>

[11] Informação disponível em <https://exame.abril.com.br/tecnologia/por-que-o-algoritmo-do-facebook-pode-ter-ajudado-trump/>

[12] Informação disponível em <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>

Além dos casos acima citados que já acontecem de forma explícita atualmente, é possível se pensar em algumas outras consequências com a adoção de decisões automatizadas, dentre as quais destacam-se:

1) Um plano de saúde ou seguro de vida pode optar por não contratar em razão de algoritmos que preveem riscos para desenvolvimento de doenças. Nessa perspectiva, os motivos poderiam ser individuais ou coletivos.
2) Determinadas cláusulas contratuais podem ser feitas através de sistemas automatizados.
3) Um país poderia negar a entrada de um turista com base em uma decisão automatizada.

O problema em si não é a automação. Automatizar processos pode significar um ganho para a sociedade, já que serviços e produtos podem ser ofertados por preços melhores e em melhores condições. Contudo, os critérios utilizados para a automação podem ser prejudiciais aos titulares, sobretudo em se considerando a grande quantidade de informações pessoais disponíveis.

O problema se agrava ao passo que em um eventual processo judicial poderá ser determinada a auditoria de um algoritmo. Contudo, como já dito, poderá ser algo inútil, já que o sistema pode não ser inteligível por um humano.

1.2 A proteção jurídica das ferramentas de decisão automatizada

Lilian Edwards e Michael Veale[13] definem o sistema com DNN como se fosse uma caixa preta (black box). Os autores argumentam que nem sempre se saberá os motivos para se tomar determinada decisão, é como se o sistema inteligente fosse completamente imprevisível. Doran et al.[14] por sua vez, identifica três classes de sistema: opacos, interpretáveis e

[13] EDWARDS, Lilian; VEALE; Michael. *Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*. Duke Law & Technology Review, v. 16, n. 01, 2017, p. 18-84. Disponível em: <https://ssrn.com/abstract=2972855>. Acesso em: abr. 19

[14] DORAN, Derek; SCHULZ, Sarah; BESOLD, Tarek. *What does explainable ai really mean? a new conceptualization of perspectives.* Proceedings of the First International Workshop on Comprehensibility and Explanation in AI a*nd ML*, arXiv:1710.00794, 2017.

compreensíveis. Sistemas opacos são aqueles que não são passíveis de verificação dos motivos que levaram ao resultado pelo usuário. Sistemas interpretáveis permitem a compreensão desde que o usuário tenha um conhecimento técnico. Por fim, os sistemas compreensíveis oferecem tanto a decisão quanto uma compreensão para o usuário não técnico.

Importante ressaltar que com o aprendizado de máquina o motivo da decisão pode não fazer lógica para um humano. Isso ocorre pois, como já afirmado, o próprio sistema se adequa para alcançar o resultado, o que gera então incerteza sobre tais motivos. Isso se agrava em razão da possibilidade de solicitar explicação quando uma decisão automatizada é tomada.

A Lei nº 13.709, de 14 de agosto de 2018, conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD), em sua redação original, normatizava a possibilidade de revisão de uma decisão automatizada, sendo que esta revisão deveria acontecer necessariamente com a presença de um humano (*human in the loop*). Contudo, o caput artigo 20 foi modificado pela Medida Provisória 869 de 27 de dezembro de 2018, ratificada pela Lei nº 13.853, de 2019, sendo suprimida a possibilidade de revisão por pessoa natural. Com a redação atual, a partir de agosto de 2020, com a vigência da lei, quando alguma decisão for tomada "unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses", caberá ao titular o direito de solicitar revisão que não será necessariamente feita por um humano.

O § 1º deste artigo normatiza que o controlador deve fornecer informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados pelo sistema para a tomada da decisão, respeitado o segredo industrial. Por fim, o §2º disciplina que na ausência dessa transparência, a autoridade nacional de proteção de dados poderá auditar o sistema com o intuito único de verificação de aspectos discriminatórios.

O problema da explicação se agrava ante a imprecisão da norma. A partir da leitura do texto legal não fica claro o que vem a ser uma decisão

tomada unicamente com base em tratamento automatizado, quais decisões afetam os interesses dos titulares, nem qual é o grau de transparência e explicação que será exigível em situações assim. Por fim, a auditoria pela autoridade nacional pode não ser efetiva, na medida em que o sistema pode apresentar uma decisão com base em circunstâncias que não fazem sentido para um humano. É necessário questionar quais são as implicações jurídicas de uma decisão automatizada.

De um lado tem-se a companhia que desenvolveu o sistema e de outro o indivíduo que foi submetido a uma decisão automatizada. A explicação da decisão automatizada envolve a proteção dos dados pessoais e a proteção do sistema utilizado, o qual merece tutela jurídica. Além disso, envolve um problema técnico já que a explicabilidade de uma decisão automatizada pode não ser inteligível por um ser humano.

Lilian Edwards e Michael Veale[15] afirmam que é possível se pensar em um direito à explicação em dois momentos, um *ex ante* e um *ex post*. Em um primeiro momento, deve-se ter uma explicação dos elementos que compõe a decisão, como se fossem as regras de um jogo (*ex ante*). Assim, é possível se tutelar o titular, já que o mesmo saberá quais informações serão utilizadas e em qual contexto. O direito à informação *ex ante* se faz necessário em razão da possibilidade do titular conhecer quais são os fatores que determinam a tomada de decisão.

Contudo, eventualmente deve ser garantido um direito de explicação *ex post*. Os autores defendem que não basta a mera explicação dos motivos que compõe a decisão. Ademais, os autores reconhecem os impedimentos para que seja garantido o acesso ao algoritmo e os motivos que levaram àquela determinada decisão. Neste sentido, a proposta feita é a utilização da tutela coletiva para a garantia dos direitos individuais. Evidente que há a necessidade de tutela do titular frente às decisões automatizadas.

---

[15] EDWARDS, Lilian; VEALE; Michael. *Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*. Duke Law & Technology Review, v. 16, n. 01, 2017, p. 18-84. Disponível em: <https://ssrn.com/abstract=2972855>. Acesso em: abr. 19

Proteger o algoritmo é essencial para as companhias, posto que isto pode ser o bem mais precioso do negócio. A proteção do algoritmo, em uma análise preliminar, pode perpassar pelo segredo de negócios ou pela propriedade intelectual.

Segredo de negócio pode ser definido como todo conhecimento aplicável à indústria, ao comércio ou à prestação de um serviço apto a conferir ao empresário uma vantagem competitiva em relação aos seus concorrentes[16]. Esta forma de proteção é eficaz desde que adotadas medidas de segurança pela companhia, como contratos de confidencialidade, por exemplo.

A Propriedade Intelectual tem o condão de proteger a criação e o criador, dando a este certos direitos para protegê-la. Tamanha a importância da proteção à propriedade intelectual que atualmente, no ordenamento jurídico brasileiro, trata-se de direito fundamental, inserto no Artigo 5º da Constituição da República Federativa do Brasil de 1988 (CR/88), incisos XXVII, XXVIII e XXIX.

O Direito Autoral, conforme artigo 1º da Lei de Direitos Autorais, trata, por óbvio, dos direitos do autor, bem como os que lhe são conexos. Assim, se diz que, conforme Bittar (2003), o Direito Autoral é a espécie de Propriedade Intelectual que tutela a proteção da criação e da utilização de obras intelectuais estéticas, seja na literatura, artes ou ciência.

Ao seu turno, a Propriedade Industrial é, conforme Bittar (2003), espécie de Propriedade Intelectual voltada para a utilidade das criações, no âmbito empresarial ou comercial, que se dá por meio da patente (invenções, modelos de utilidade, modelo industrial e desenho industrial) ou marca (de indústria, comércio ou de serviço e de expressão, ou sinal de propaganda) do produto.

Questiona-se a natureza dos algoritmos e a possibilidade de proteção enquanto propriedade intelectual. Tratando-se de ato criativo, é evidente que este poderá ser protegido pelo direito autoral, pois se trata de uma

[16] MARTINS, Fran. *Curso de Direito Comercial, volume 1: direito de empresa*. 37ª Ed. Rio de Janeiro: Editora Forense, 2014.

linha de programação inserida em um software, o qual possui proteção dada pela Lei 9.606/98. Ainda, outros elementos envolvidos poderão ser tutelados pela propriedade industrial, como por exemplo a marca utilizada pela companhia no sistema automatizado.

Por fim, vale ressaltar que há um direito de exclusividade na exploração de qualquer criação. Tal direito decorre da necessidade de se remunerar o criador, incentivando que o mesmo invente algo. Destacam-se três teorias.

A primeira teoria explicativa da propriedade intelectual é a teoria econômica, a qual possui uma perspectiva utilitarista[17]. Nesta vertente, justifica-se a proteção ao argumento de toda a coletividade seria beneficiada pela criação. Sob a análise econômica, justifica-se a proteção como um incentivo ao inventor, que poderá explorar os frutos de sua criação. Assim, é a exploração exclusiva é necessária para cobrir os custos de pesquisa e desenvolvimento da criação.

A segunda teoria explicativa é a Lockiana, segundo a qual o fruto do trabalho pertence ao criador[18]. A exploração exclusiva é baseada na constatação de que o inventor teve um trabalho para criar algo. Locke afirma que o homem é detentor do seu trabalho e que as forças empregadas podem gerar frutos, os quais pertencem ao indivíduo.

A terceira teoria é baseada na personalidade e tem como fundamento a doutrina de Hegel[19]. Segundo essa perspectiva, os direitos de propriedade são meios para o desenvolvimento e a realização da personalidade do indivíduo. Justifica-se a proteção da criação já que foi feita por uma pessoa, a qual inclusive deve ser o fundamento último de proteção estatal.

Todas as três teorias demonstram a necessidade da exploração econômica exclusiva para o criador. Em nenhuma se admite um uso sem autorização do autor. Desta feita, questiona-se a possibilidade de se

---

[17] YANISKY, Liu, Xiaoqiong (Jackie); RAVID, Shlomit. *When Artificial Intelligence Systems Produce Inventions: The 3A Era and an Alternative Model for Patent Law* (March 1, 2017). Cardozo Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2931828

[18] Idem

[19] Idem

relativizar a proteção de um algoritmo para que se garanta ao usuário acesso a informações pelas quais lhe é negado ou concedido determinados contratos.

Um algoritmo na forma BlackBox se justifica em razão da complexidade e custo para o desenvolvimento do mesmo, bem como em razão da competitividade de mercado. Assim, uma companhia não deseja que a concorrente forneça o mesmo serviço através do mesmo algoritmo[20].

1.3 Riscos associados à decisão automatizada

Para exemplificar o risco de se utilizar uma decisão automatizada será analisado o caso da Decolar.com, empresa de pesquisa de passagens e hotéis pela Internet. A pedido de sua concorrente, *Booking,* foi instaurado Processo Administrativo, no ano de 2016, sob o número 08012.002116/2016-21, no âmbito do Departamento de Proteção e Defesa do Consumidor, da Secretaria Nacional do Consumidor, do Ministério da Justiça. Conforme a denúncia, a *Decolar* estaria oferecendo reservas com preços diferentes, a depender da localização do consumidor, identificado por intermédio do Internet Protocol – IP, conduta denominada *geopricing*. Além disso, a *Decolar* ocultava a disponibilidade de alguns hotéis para algumas localizações, em favor de consumidores estrangeiros, conduta denominada *geoblocking*.

A *Booking*, para demonstrar o alegado, pesquisou simultaneamente a mesma hospedagem a partir de dois computadores diferentes, um São Paulo (Brasil) e outro em Buenos Aires (Argentina). Na busca constatou-se uma diferença de preço de 30% para algumas acomodações, além da indisponibilidade de algumas a depender da origem.

Atualmente, a *Decolar* é ré em uma Ação Civil Pública, autuada sob o número 0018051-27.2018.8.19.0001 em tramitação na 7ª Vara

[20] DONEDA, Danilo; ALMEIDA, Virgílio. *What is algorithm governance?* IEEE Internet Computing, v. 20, n. 4, p. 60-63, 2016. Disponível em: <http://ieeexplore.ieee.org/document/7529042/>. Acesso em; 20 jun. 2019.

Empresarial da comarca do Rio de Janeiro. Na petição inicial, o Ministério Público expõe os riscos e perigos da adoção do *geopricing* e do *geoblocking*.

Perceba que ambas as identificações são automáticas em razão da origem do acesso. Não há qualquer intervenção humana para a decisão do preço final ou disponibilidade do hotel. Ademais, o usuário não tem qualquer explicação sobre o preço ou disponibilidade do hotel.

Esse caso ilustra um problema ainda maior. A discriminação poderia ser em razão do CEP do usuário, ou seja, se o indivíduo morasse em um bairro de periferia poderia ter um preço maior até mesmo a indisponibilidade do serviço. Tudo isso de forma autônoma, sem a intervenção humana. Assim fundamentou o Ministério Público em sua petição inicial:

> *Assim é que, caso não haja a devida intervenção do Estado para regulamentar o mercado online, a experiência dos consumidores será diferente e as ofertas serão feitas dependendo do seu CEP, riqueza, gênero e idade. Um estudo recente identificou evidências de preços discriminatórios em cinco dentre dezesseis empresas de comércio eletrônico especializadas em reservas de hotéis e locação de automóveis. Para melhor discriminar seus clientes, as empresas podem se aproveitar da dificuldade do consumidor em processar escolhas complexas, especialmente aumentando parâmetros de qualidade e de preço para ampliar sua vantagem pelos erros e viés comportamental do consumidor. A assimetria de poder é ampliada pela ignorância do consumidor sobre o desenho do algoritmo e os dados coletados de seus clientes, o que facilita a discriminação. Uma outra maneira de estabelecer um comportamento discriminatório de uma maneira palatável é atribuir os desvios de preço às forcas dinâmicas do mercado. Consumidores aceitam que diferenças de preço são respostas a mudanças de oferta e demanda no mercado (precificação dinâmica) ao invés de considerar que se trate de uma manipulação de preço a partir de características pessoais do consumidor (precificação discriminatória). ACP decolar.*

Ezrachi [21] faz uma análise de como os preços de aplicativos são ofertados. O autor demonstra, por exemplo, que em 2000 foi descoberto

[21] Ezrachi, Ariel and Maurice Stucke, Virtual Competition: *The Promise and Perils of Algorithm-Driven Economy.* Cambridge: Harvard (2016)

que a *Amazon* praticava preços distintos para o mesmo produto com base na localização do consumidor. Após a descoberta, a *Amazon* se comprometeu a não mais utilizar dessa prática.

Cathy O'Neil [22] tece críticas a adoção de informações sobre a localização do indíviduo para a tomada de decisões, já que há discriminação através de um julgamento arbitrário a partir da origem geográfica do consumidor. Segundo a autora é necessário medir o impacto e conduzir auditorias dos algoritmos, examinando o código do software e todos os dados processados. Afirma ainda que falta transparência, acesso à informação em decisões automatizadas, cabendo a tutela coletiva para a regulação.

No processo judicial a *Decolar* recusou a mostrar seu algoritmo utilizado. O ministério público criticou a conduta, porém caso a *Decolar* apresentasse o algoritmo, sua maior concorrente, a *Booking*, teria acesso integral ao mesmo. Como visto no tópico 3, de fato é necessário que se proteja o algoritmo, já que este tem valor para o titular. Em que pese ser evidente o abuso na adoção do *geoblocking* e do *geopricing*, não é necessário a exibição do algoritmo nem para a caracterização do ilícito, nem para a correção do mesmo.

A ação judicial foi baseada no Código de Defesa do Consumidor. Isso aconteceu por dois motivos: i) a LGPD ainda não está em vigor; e ii) mesmo em vigor, há que se considerar o diálogo das fontes na aplicação de normas atinentes à proteção de dados, dentre as quais se insere a explicação de decisões automatizadas.

Outro caso que evidencia risco na adoção de decisão automatizada é o do reconhecimento facial feito pela ViaQuatro no metrô de São Paulo. Trata-se também de uma Ação Civil Pública ajuizada pelo Instituto Brasileiro de Defesa do Consumidor - IDEC – em face da Concessionária da linha 4 do metrô de São Paulo S.A. - ViaQuatro. A ré desenvolveu um sistema de câmeras que reconhece a presença humana e realiza a

[22] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. london: Penguin Books (2017),

identificação de emoção, gênero e faixa etária das pessoas posicionadas em frente ao equipamento.

Na petição inicial foi relatado que não houve informação clara e adequada aos consumidores quanto ao sistema, sendo que os mesmos eram obrigados a ceder informações naquele momento, sendo que o funcionamento não foi explicado. No processo discute-se a distinção entre reconhecimento facial e detecção facial. A autora argumenta que apenas utiliza detecção facial e que isso não é coleta de dados pessoais. Em síntese, reconhecimento facial permite a identificação de um sujeito específico dentre vários rostos analisados. Por sua vez, detecção facial permite a identificação genérica apenas, ou seja, não se identifica o indivíduo, apenas suas características para a formação de um perfil (*profiling*).

Ambos os casos demonstram a fragilidade de se identificar o motivo de eventual decisão automatizada. Perceba que no caso da Decolar foi possível identificar a distinção de preço, mas sem a análise do algoritmo em si. Talvez, analisando o algoritmo não seja possível identificar um viés ali inserido.

1.4 Revisão de decisões automatizadas na legislação europeia e brasileira (direito à explicação)

A GDPR - Regulamento Geral de Proteção de Dados da União Europeia - que entrou em vigor em 25 de maio de 2018, normatiza a proteção dos dados pessoais no âmbito da União Europeia, tendo uma aplicação transnacional. Como se trata de um regulamento, deve ser aplicado em todos os países europeus nos quais haja coleta de dados pessoais. Ainda, no Brasil tem-se a LGPD - Lei Geral de Proteção de Dados pessoais (Lei n. 13.709/2018), que normatiza a proteção no âmbito brasileiro. As duas legislações possuem abordagens distintas para a tomada de decisão automatizada.

A LGPD, em seu artigo 20, possibilita a decisão automatizada, desde que seja garantido ao titular o direito de revisão desta.

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade. (Redação dada pela Lei nº 13.853, de 2019)
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

Assim, entende-se que o controlador deverá fornecer informações sobre os procedimentos, porém será respeitado o segredo do algoritmo. Já na legislação europeia, a normatização é distinta. Na GDPR o direito à explicação deriva dos artigos 13, 14, 15 e 22(3).

Os artigos 13 e 14 na verdade referem-se à um direito de explicação *ex ante*. Já o artigo 15 da GDPR disciplina explicitamente sobre o direito de acesso às informações pessoais que o controlador possui. Tais dispositivos determinam que o controlador deve informar o titular quais são os usos e as finalidades da coleta e tratamento. Em verdade, estes artigos disciplinam a tutela da privacidade dos usuários, que pode ser lida como uma explicação em perspectiva *ex ante*. Dentre as normatizações, destaca-se o item h do artigo 15, que normatiza, dentre outros direitos dos titulares o de ter conhecimento sobre:

> *A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22, nº 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.*

Veja que é um direito do titular obter informações de quando serão tomadas decisões automatizadas. Mais ainda, conforme o artigo 22 normatiza, os titulares têm o direito de não se submeterem a decisões

exclusivamente automatizadas, salvo ser for necessária à execução do contrato, autorizada pelo ente estatal ou tiver o consentimento explícito do titular. Assim, é um direito do titular obter informações de quando serão tomadas decisões automatizadas.

Contudo, conforme interpretação feita por Floridi (et. al)[23], não há na GDPR um direito à explicação, mas sim um direito a ser informado (*right to be informed*). De acordo com os autores, não há base legal para se interpretar a GDPR como um marco para se garantir aos titulares informações precisas sobre os motivos das decisões automatizadas. O que existe, segundo os autores, é um direito de ser informado sobre como são tomadas as decisões, bem como de solicitar revisão.

Os autores ainda argumentam que na vigência do antigo regulamento de proteção de dados da Europa os tribunais interpretavam pela ausência de um direito à explicação, o que possivelmente será mantido. Por fim, os autores apresentam algumas sugestões, dentre as quais se destaca a adição do direito à explicação como uma obrigação legal na GDPR, bem como tornar claro o sentido de proteção existente na atual legislação, estipulando se há ou não o direito a acessar o sistema automatizado em si considerado.

No mesmo sentido Lilian Edwards e Michael Veale[24] afirmam que a GDPR dispõe um direito de não se submeter à uma decisão automatiza. Assim, não há um direito de explicação *ex post*. Ademais, os autores criticam a transparência falaciosa. Eles discutem uma forma efetiva de proteção que não seja só informar a decisão automatizada. No mesmo sentido, Sandra Wachter e Brent Mittelstadt [25] também defendem a inexistência a um direito à explicação na GDPR.

---

[23] FLORIDI, Luciano; MITTELSTADT, Brent; WACHTER, Sandra. *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation.* International Data Privacy Law, 2017, p. 1-47. Disponível em: <https://ssrn.com/abstract=2903469>. Acesso em abr. 2019

[24] EDWARDS, Lilian; VEALE; Michael. *Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*. Duke Law & Technology Review, v. 16, n. 01, 2017, p. 18-84. Disponível em: <https://ssrn.com/abstract=2972855>. Acesso em: abr. 19

[25] WACHTER, Sandra; MITTELSTADT, Brent. *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*. [s.l.]: LawArXiv, 2018. Disponível em: <https://osf.io/mu2kf>. Acesso em: 24 mai. 2019.

Como se depreende, é necessário que se investigue a distinção entre direito à explicação na perspectiva *ex ante* e *ex post*. Mais ainda, é importante que se diferencie o direito à explicação *ex ante* do direito a não se submeter a uma decisão automatizada. Conforme interpretação feita por Floridi (et. al), é possível interpretar o artigo 22 da GDPR de forma restritiva. Os autores argumentam que a regra geral é a impossibilidade da decisão automatizada, sendo que em exceções como a autorização expressa do titular e a necessidade do negócio permitem tal tipo de decisão[26]. Assim, é possível que seja feita uma leitura restritiva do artigo, impedindo que seja feita uma decisão automatizada[27].

De maneira similar é necessário que se diferencie o direito à explicação do direito de revisão. Dizer os motivos que levaram a determinado resultado, significa informar o titular sobre a decisão. Contudo, é melhor que se possibilite a revisão de tal conteúdo. Neste sentido, Lilian Edwards e Michael Veale[28] afirmam que o titular tem uma efetiva proteção quando pode rever a decisão automatizada e não quando tem direito a mera explicação.

1.5 Algumas técnicas para viabilizar o direito à explicação

Jenna Burrell[29], afirma que é inviável a compreensão de um sistema feito em forma de *black box*, já que com o aprendizado o sistema deixa de adotar uma lógica humana. Neste sentido, é impossível compreender os motivos determinantes da decisão. No mesmo sentido, Wachter,

[26] FLORIDI, Luciano; MITTELSTADT, Brent; WACHTER, Sandra. *Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation*. International Data Privacy Law, 2017, p. 1-47. Disponível em: <https://ssrn.com/abstract=2903469>. Acesso em abr. 2019

[27] MENDOZA, Isak; BYGRAVE, Lee A. *The Right Not to Be Subject to Automated Decisions Based on Profiling*. Rochester, NY: Social Science Research Network, 2017. Disponível em: <https://papers.ssrn.com/abstract=2964855>. Acesso em: set. 2019.

[28] EDWARDS, Lilian; VEALE; Michael. *Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for*. Duke Law & Technology Review, v. 16, n. 01, 2017, p. 18-84. Disponível em: <https://ssrn.com/abstract=2972855>. Acesso em: abr. 19

[29] BURRELL, Jenna. *How the Machine "Thinks:" Understanding Opacity in Machine Learning Algorithms*. Rochester, NY: Social Science Research Network, 2015.

Mittelstadt e Russell[30], afirmam que a compreensão de um sistema pode não ser inteligível para um humano. Os autores ainda defendem que há um interesse do controlador em não revelar o sistema, em vista da proteção inerente ao negócio, tal qual trabalhado no tópico 3 deste trabalho.

Wachter, Mittelstadt e Russell[31] afirmam que se deve buscar uma explicação sem que isso implique em acesso ao segredo de negócio, até mesmo porque isso pode ser ineficaz na prática. Os autores defendem a possibilidade de fornecer ao titular informações sobre os motivos da tomada de decisão e, a partir disso, possibilitar a revisão da mesma, já que se teria a compreensão do que pode ser alterado para obtenção de resultado distinto.

Lilian Edwards e Michael Veale[32] argumentam que há um caminho alternativo à explicação, mas que garante a proteção dos titulares. Os autores defendem que a busca por esse direito pode gerar uma falácia da transparência[33], na medida em que uma rede neural profunda decide de forma que um humano pode não compreender. Para os autores, tem-se uma tutela efetiva com a adoção de elementos protetivos do titular dos dados pessoais. Medidas como certificações e selos de privacidade garantem uma melhor tutela para decisões automatizadas.

Isso decorre do fato de que o titular não está interessado em uma explicação sobre a decisão, mas sim em revertê-la em caso de critérios equivocados. Portanto, ante a dificuldade técnica da explicação, garante-se a tutela do titular com a adoção de meios alternativos.

---

[30] WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual *Explanations Without Opening the Black Box: Automated Decisions and the GDPR*. SSRN Electronic Journal, 2017. Disponível em: <https://www.ssrn.com/abstract=3063289>. Acesso em: 24 mai. 2019.

[31] Idem

[32] EDWARDS, Lilian; VEALE, Michael. *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for*. Duke Law & Technology Review, v. 16, p. 18, 2017.

[33] No mesmo sentido é o entendimento de Ananny e Crawford (ANANNY, Mike; CRAWFORD, Kate. *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*. New Media & Society, v. 20, n. 3, p. 973–989, 2018).

Lilian Edwards e Michael Veale[34] afirmam ainda que os controladores de sistemas preferem utilizar sistemas em *black box* em razão da performance destes. Ao invés de pensar em explicabilidade, os controladores preferem adotar sistemas cada vez mais complexos e com níveis de aprendizagem cada vez mais profundos, fazendo com que seja praticamente impossível a explicação. Neste sentido, a explicação pode perpassar pelo campo da construção do sistema, garantindo uma explicação efetiva pode ser feita na origem do sistema.

Ananny e Crawford[35] defendem que a abertura da *black box* não garante uma explicação efetiva, já que há uma falácia da transparência. Garantir a explicação para o titular depende de uma compreensão efetiva sobre a forma que a decisão foi tomada. Não basta o controlador mostrar o sistema, ele deve informar os motivos que levaram àquela decisão discutida.

Do ponto de vista técnico é complexo a obtenção de uma explicação efetiva de um sistema que utilize uma rede neural profunda. Bohlender e Kohl[36] afirmam que não se tem um consenso sobre como tornar um sistema explicável. Portanto, a LGPD ao estabelecer uma auditoria do sistema em caso de automação pode não proteger o usuário.

A proteção do titular não necessariamente será em razão da explicação sobre uma decisão automatizada, mas sim de uma real possibilidade de modificação do resultado aliada à garantia protecionista contra agrupadores genérico e vieses inseridos na programação. Citron e Pasquale[37] exemplificam que em sistemas de score de crédito deve ser garantido aos titulares informação sobre quais dados o controlador possui

---

[34] EDWARDS, Lilian; VEALE, Michael. *Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for*. Duke Law & Technology Review, v. 16, p. 18, 2017.

[35] ANANNY, Mike; CRAWFORD, Kate. *Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability*. New Media & Society, v. 20, n. 3, p. 973–989, 2018.

[36] BOHLENDER, Dimitri; KÖHL, Maximilian A. *Towards a Characterization of Explainable Systems*. arXiv:1902.03096 [cs], 2019. Disponível em: http://arxiv.org/abs/1902.03096. Acesso em: set. 2019.

[37] CITRON, Danielle Keats; PASQUALE, Frank A. *The Scored Society: Due Process for Automated Predictions*. Rochester, NY: Social Science Research Network, 2014. Disponível em: <https://papers.ssrn.com/abstract=2376209>. Acesso em: ago. 2019.

e quais são as fontes obtidas. Dessa maneira, os indivíduos teriam uma proteção efetiva sobre uma decisão automatizada.

1.6 Entendimento do STJ sobre a explicação em decisão automatizada

Atualmente, tem-se o entendimento firmado no STJ de que a adoção de *credit scoring* não enseja ato ilícito para o consumidor. O *score* de crédito é uma fórmula matemática que pontua consumidores através de um banco de dados positivo de adimplentes, o que o difere dos bancos de dados negativos, ou seja, do cadastro de inadimplentes. O banco de dados positivo possui previsão no Código de Defesa do consumidor e na Lei 12.414/11 que foi regulamentada pelo decreto 9.936/19 e atualizada pela Lei Complementar nº 166, de 2019. Trata-se, então, da criação de banco de dados contendo informações sobre adimplemento de obrigações pecuniárias de pessoas naturais ou jurídicas. Conforme o artigo 2º inciso I da Lei 12.414/11 a finalidade desse banco de dados é subsidiar a concessão de crédito, venda a prazo ou outra transação que importar risco financeiro.

Para a formação do banco de dados não mais se faz necessária a autorização prévia do potencial cadastrado[38]. Atualmente, com a alteração legislativa, o padrão é que todos terão o cadastro até o momento que manifestarem expressamente a exclusão do sistema. Contudo, o envio do histórico de crédito ao consulente depende de autorização prévia do titular, conforme disposto no artigo 4º, inciso IV, alínea b da Lei do Cadastro Positivo.

O acesso ao banco de dados do *score* só será possível por aqueles que mantiverem ou pretenderem manter relação comercial ou creditícia com o cadastrado. Através da coleta desses dados o gestor deste fornecerá aos consulentes um *score* de pontuação do cadastrado, como forma de apoio na tomada de decisão na concessão do crédito, assim, quanto maior a

[38]O STJ através do Recurso Especial Nº 1.419.697 entendeu não ser necessária a autorização do consumidor para a realização do *score* de crédito, por não se tratar, esse serviço de banco de dados positivos, mas sim de uma classificação com a finalidade de se mensurar risco na concessão de crédito, ou seja, modelo estatístico.

pontuação do cadastrado menor o risco na concessão do crédito e, quanto menor a pontuação, maior o risco.

O STJ em novembro de 2014 decidiu pela legalidade do *score* de crédito, através do Recurso Especial Nº 1.419.697 - RS. Após audiência pública para o entendimento das variáveis do caso, o relator, Ministro Paulo de Tarso Sanseverino definiu *score* de crédito como um sistema de pontuação de consumidores para fins de concessão de crédito.

No Relatório o Ministro Sanseverino argumentou que a análise de dados pessoais entre contratantes sempre foi uma constante, mesmo antes do advento da internet. Contudo asseverou que com a internet houve uma crescente possibilidade de tratamento mais intenso de dados pessoais, isso com a finalidade de atestar a idoneidade das partes contratantes, da mesma forma como antes. Nesse sentido, desde que atendido os parâmetros legais, em especial o CDC e a Lei 12.414/11, não há ilegalidade na criação do *score* de crédito. Para tanto, os critérios para a pontuação devem ser claros, objetivos e transparentes.

Em seu voto, o relator afirmou que:

> *a metodologia em si de cálculo da nota de risco de crédito ("credit scoring") constitui segredo da atividade empresarial, cujas fórmulas matemáticas e modelos estatísticos naturalmente não precisam ser divulgadas (art. 5º, IV, da Lei 12.414/2011: ..."resguardado o segredo empresarial").*
> *[...]*
> *Isso não libera, porém, o cumprimento dos demais deveres estabelecidos pelo CDC e pela lei do cadastro positivo, inclusive a indicação das fontes dos dados considerados na avaliação estatística, como, aliás, está expresso no art. 5º, IV, da própria Lei nº 12.414/2011 ("São direitos do consumidor cadastrado ... conhecer os principais elementos e critérios considerados para a análise do risco de crédito, resguardado o segredo empresarial").*
> *Assim, essas informações, quando solicitadas, devem ser prestadas ao consumidor avaliado, com a indicação clara e precisa dos bancos de dados utilizados (histórico de crédito), para que ele possa exercer um controle acerca da veracidade dos dados existentes sobre a sua pessoa, inclusive para poder retificá-los ou melhorar a sua performance no mercado. Pg. 35*

O ministro argumentou que deve ser dado ao consumidor, desde que requisite, acesso aos seus dados utilizados para o cálculo de sua nota bem como aos critérios utilizados para a pontuação, ressalvado o segredo industrial. Ademais, deve ser dado ao consumidor a possibilidade de alterar esses dados, caso não sejam verdadeiros. Veja que o STJ já enfrentou a explicação em automação. Ora, o entendimento foi de que deverá ser explicado cálculo, mas sempre respeitando o segrego industrial.

Mesmo com a antiga redação da Lei 12.41.4/15 que exigia o consentimento prévio do cadastrado para a sua inserção em banco de dados positivos, o STJ entendeu que não se aplicaria ao *score* de crédito, já que esse, segundo entendimento, não tem natureza de banco de dados positivos, mas sim de metodologia de cálculo de risco para a concessão de crédito, ou seja, modelo estatístico. Assim, o STJ entendeu que é plenamente possível a adoção de sistemas automatizados para fornecimento de crédito.

Entendeu-se ainda que, caso haja abuso no tratamento dos dados, seja pela utilização de dados sensíveis, ou por excessos, tais como preferência esportiva, entre outras possibilidades, caberá o dever de indenizar por danos morais e materiais de forma objetiva e solidária pelo fornecedor do serviço de *score* de crédito, do responsável pelo banco de dados, da fonte e do consulente. Por fim, entendeu que o fato de ser dado ao consumidor uma nota insatisfatória, não gera, por si, indenização por dano moral, enseja somente a retificação.

Neste sentido, concluiu-se que é possível a adoção de sistema de *score* de crédito e que eventual explicação para o titular não passa pela análise do algoritmo, mas sim pelos dados analisados. O entendimento do STJ é de que deve ser protegido o algoritmo.

1.7 Conclusão

A pesquisa evidenciou que na atual sociedade existe uma grande gama de decisões automatizadas. Eventualmente a automação poderá

representar um risco para o titular de uma informação, haja vista a possibilidade de um viés decisório racista ou semelhante. Foi demonstrada a necessidade de se estudar algoritmos para tomada de decisões.

O sistema automatizado, por sua vez, possui um valor relevante para o controlador e por isso merece proteção jurídica com base na propriedade intelectual. Assim a explicação de uma decisão automatizada encontrará limite na proteção do sistema.

Deverá ser garantido ao titular o direito à explicação *ex ante*, o qual deriva do direito à informação do titular submetido à uma decisão automatizada. Ademais, deverá limitada a automação, impedindo que seja feita com base em dados sensíveis e agrupadores genéricos com propensão para segregação, tais como gênero, raça, classe social e origem geográfica. Contudo, acredita-se que não é possível que o titular decida não se submeter à uma decisão automatizada.

No que se refere à explicação *ex post*, deverá ser garantido este direito com ressalvas. Caso não viole o segredo assegurado ao controlador do sistema poderá ser aceita a explicação *ex post*. Com a explicação, deverá ser possibilitada a efetiva revisão, que deverá ser feita após com efetiva possibilidade de mudança na decisão, o que independe da presença de um humano

Demonstrou-se, por fim, que o STJ possui entendimento consolidado de que não é possível a auditoria de algoritmos para tomada de decisões. Contudo, com a vigência da LGPD haverá previsão expressa dessa auditoria. Assim, o entendimento do STJ é contrário à LGPD, razão pela qual será alterado. Questiona-se a viabilidade de se auditor um sistema, já que como visto a forma como se toma a decisão poderá não fazer sentido algum para o titular.

1.8 Referências

ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. **New Media & Society,** v. 20, n. 3, p. 973–989, 2018.

BOHLENDER, Dimitri; KÖHL, Maximilian A. **Towards a Characterization of Explainable Systems**. arXiv:1902.03096 [cs], 2019. Disponível em: http://arxiv.org/abs/1902.03096. Acesso em: 27 maio 2019.

BURRELL, Jenna. **How the Machine "Thinks:" Understanding Opacity in Machine Learning Algorithms.** Rochester, NY: Social Science Research Network, 2015.

CARBONERA, Joel; GONÇALVES, Bernardo; Clarisse de Souza. **O problema da explicação em Inteligência Artificial: considerações a partir da semiótica**. TECCOGS – Revista Digital de Tecnologias Cognitivas, nº 17, Jan-Jun 2018.

O'NEIL, Cathy, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. london: Penguin Books, 2017.

CITRON, Danielle Keats; PASQUALE, Frank A. **The Scored Society: Due Process for Automated Predictions.** Rochester, NY: Social Science Research Network, 2014. Disponível em: <https://papers.ssrn.com/abstract=2376209>. Acesso em: 24 mai. 2019.

DONEDA, Danilo; ALMEIDA, Virgílio. **What is algorithm governance?** IEEE Internet Computing, v. 20, n. 4, p. 60-63, 2016. Disponível em: <http://ieeexplore.ieee.org/document/7529042/>. Acesso em; 20 jun. 2019.

DORAN, Derek; SCHULZ, Sarah; BESOLD, Tarek. What does explainable ai really mean? a new conceptualization of perspectives. *Proceedings of the First International Workshop on Comprehensibility and Explanation in AI and ML*, arXiv:1710.00794, 2017.

EDWARDS, Lilian; VEALE, Michael. **Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for**. Duke Law & Technology Review, v. 16, p. 18, 2017.

EDWARDS, Lilian; VEALE; Michael. Slave to the Algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. **Duke Law & Technology Review**, v. 16, n. 01, 2017, p. 18-84. Disponível em: <https://ssrn.com/abstract=2972855>. Acesso em: abr. 19.

ERZACHI, Ariel and Maurice Stucke, Virtual Competition: The Promise and Perils of Algorithm-Driven Economy. Cambridge: Harvard (2016).

FLORIDI, Luciano; MITTELSTADT, Brent; WACHTER, Sandra. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. **International Data Privacy Law**, 2017, p. 1-47. Disponível em: <https://ssrn.com/abstract=2903469>. Acesso em abr. 2019.

MARTINS, Fran. **Curso de Direito Comercial, volume 1: direito de empresa**. 37ª Ed. Rio de Janeiro: Editora Forense, 2014.

MENDOZA, Isak; BYGRAVE, Lee A. **The Right Not to Be Subject to Automated Decisions Based on Profiling**. Rochester, NY: Social Science Research Network, 2017. Disponível em: <https://papers.ssrn.com/abstract=2964855>. Acesso em: set. 2019.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados Pessoais?**, Instituto Igarapé, Artigo Estratégico nº 39, Dezembro de 2018.

O'NEIL, Cathy. **Weapons of math destruction: How big data increases inequality and threatens democracy**. Broadway Books, 2016.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR. SSRN **Electronic Journal**, 2017. Disponível em: <https://www.ssrn.com/abstract=3063289>. Acesso em: 24 mai. 2019.

YANISKY, Liu, Xiaoqiong (Jackie); RAVID, Shlomit. **When Artificial Intelligence Systems Produce Inventions: The 3rd Era and an Alternative Model for Patent Law** (March 1, 2017). Cardozo Law Review, Forthcoming. Available at SSRN: https://ssrn.com/abstract=2931828.

8

Proteção de dados, privacidade e a Lei do Cadastro Positivo

Pedro Henrique Rocha Silva Fialho [1]

1. Contexto atual da LGPD

Nos dias atuais, é comum se ouvir uma frase que se tornou um verdadeiro clichê: "Os dados são o novo petróleo". Tal expressão, repetida à exaustão em conversas, apresentações e veículos de comunicação, se fundamenta na recente percepção por parte da população sobre o quão valiosos são os dados pessoais se devidamente utilizados por quem os detenha.

Aliado ao crescimento vertiginoso das empresas de tecnologia, que figuram hoje como as companhias mais valiosas do planeta e, em sua essência, vivem à base do tratamento de dados dos cidadãos, acontecimentos recentes, tais como vazamentos acerca da utilização desses dados, a influência que a sua manipulação exerce na vida das pessoas, alterando inclusive o curso de eleições, fez acender a luz vermelha sobre a forma como esses dados são tratados e utilizados.

Assim, um assunto que muitas vezes era ignorado pela maioria das pessoas ganhou destaque. Passou-se a questionar as razões pelas quais determinadas empresas faturam e valem tanto dinheiro sem, aparentemente, possuírem ativos ou produtos, ao menos do ponto de vista tradicional, tão valiosos.

---

[1] Pedro Henrique Fialho é Advogado, Pós-Graduado em Direito Empresarial pela PUC Minas. Professor substituto do Pré-Concursos. Membro da Comissão de Proteção de Dados e de Direito Empresarial da OAB/MG. Membro do grupo de estudos de Direito Empresarial da UFMG. Contato: pedro.fialho@mouraesiqueira.com

Em um mundo imerso na vida digital, foi criando-se uma percepção de certo monitoramento e se tornou algo comum buscar por algum serviço, produto ou simplesmente fazer uma busca por determinado assunto e ser bombardeado posteriormente por anúncios, propagandas, e-mails e outros canais de comunicação lhe oferecendo aquele serviço, produto ou tratando de algo similar àquilo que foi buscado anteriormente.

Quem nunca teve a impressão ou ouviu alguma pessoa dizer que após conversar sobre determinado assunto por telefone ou por aplicativo de mensagens, recebeu alguns dias depois algo relacionado àquele assunto? É praticamente certo que após fazer uma pesquisa na internet sobre um produto, suas redes sociais, seu e-mail e seu telefone receberão nas próximas horas ou até minutos, anúncios relacionados àquele produto. Seria o retorno de George Orwell?

Tornou-se de conhecimento público que dados foram utilizados para manipular eleições e votações de extrema relevância em democracias pujantes, e que muitos programas de fidelidade ou até mesmo aquele desconto concedido em troca do seu CPF em algumas lojas, na verdade tinham como objetivo final a coleta dos seus dados.

Noticiou-se que várias empresas que coletam dados dos seus usuários, sediadas nos Estados Unidos, violavam a privacidade dos seus usuários, franqueando o acesso a esses dados à NSA, agência de segurança americana.

Nesse cenário aparentemente assustador, a frase mencionada no início desse artigo parece fazer algum sentido, salvo por uma enorme diferença: enquanto que o petróleo é uma riqueza finita, os dados não são, e assim diversos países aceleraram seu processo de regulamentação dessa "nova riqueza".

O Brasil, ao contrário de países próximos que já possuem leis a respeito desse assunto há quase duas décadas (a Argentina possui uma lei desde o ano de 2.000) e da Europa que já possuía uma cultura de proteção de dados (apesar de o regulamento ter entrado em vigor recentemente), possuía escassa legislação e incipiente cultura a respeito do tema.

Buscando se adaptar aos tempos modernos e inspirada na GDPR (General Data Protection Regulation) europeia, a Lei Geral de Proteção de Dados brasileira foi sancionada em agosto de 2018, com previsão de entrada em vigor para agosto de 2020. Com a entrada em vigor da LGPD, o nosso ordenamento jurídico passará a prever as tutelas fiscalizatórias e sancionatórias aos agentes que realizam tratamento de dados, que deverão se ajustar às diretrizes consumeristas e à regulamentação da ANPD, que definirá os padrões éticos e operacionais de tal atividade.

Contudo, mais do que possuir uma legislação sobre a matéria, é consenso entre os especialistas que o principal problema brasileiro não é legal, mas sim cultural, uma vez que tal assunto de fato somente passou a ser discutido por aqui recentemente.

Com a entrada em vigor da lei batendo à nossa porta, as empresas iniciaram seus processos internos de adaptação e, a despeito da desconfiança de muitos agentes, de fato a lei veio para ficar, afinal, o tratamento e manipulação de dados se mostram cada dia mais presentes em nossas vidas, sendo que a regulação de uma matéria que envolve um direito tão sagrado como a nossa privacidade é de extrema relevância social.

Deve-se ressaltar ainda, que a adaptação aos termos da Lei e o efetivo tratamento de dados amparado em alguma das hipóteses previstas na lei deverá ocorrer por agentes privados e também pelo poder público, que lida diariamente com uma infinidade de dados pessoais.

2. Direito à privacidade

O direito à privacidade está diretamente relacionado com a necessidade de uma legislação que trate da proteção de dados pessoais.

A nossa Constituição Federal tutela expressamente a privacidade em seu artigo 5º, inciso X, assegurando que: 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.

O conceito de privacidade é muito amplo, protegendo além da intimidade, vida privada, honra e imagem das pessoas, o seu domicílio, a correspondência, as comunicações, o sigilo bancário e claro, os dados pessoais. De forma mais expressa, nossa Constituição prevê no inciso XII do artigo 5º que é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

No contexto atual, em uma sociedade denominada da informação e com excessiva exposição, na qual milhares de dados são trocados diariamente, como se promover a proteção de dados pessoais e, em sua essência, efetivar o direito constitucional à privacidade? Como conciliar o direito à liberdade com o direito à privacidade?

Liberdade e privacidade estão fortemente interligadas. Sem garantir a privacidade, não se possui liberdade, na medida em que pessoas livres tem o direito de evitar que terceiros manipulem ou acessem seus dados pessoais sem a sua permissão ou embasamento legal.

Portanto, a proteção de dados implementada pela LGPD, em sua essência é a efetivação do direito à privacidade, ao mesmo tempo tão amplo do ponto de vista conceitual, mas tão importante do ponto de vista social.

3. Lei do Cadastro Positivo

Há quem diga que um dos principais motores de qualquer economia é o crédito. É ele que proporciona o desenvolvimento da atividade produtiva. É ele que permite que um empresário adquira uma nova máquina, faça investimentos em seu negócio, se torne mais competitivo e dessa forma gere empregos no país.

Além do setor produtivo, o crédito permite o consumo das pessoas, a aquisição de bens e serviços, proporcionando a efetiva circulação do dinheiro e consequentemente o crescimento econômico.

A despeito de algumas ressalvas a tal premissa, é fato inquestionável que a oferta de crédito é, sem sombra de dúvidas, um fator importante para o desenvolvimento econômico de qualquer país.

O Brasil é amplamente conhecido por ser um país onde as taxas de juros bancários são absurdamente elevadas. As justificativas para tal realidade são diversas, passando pelas elevadas taxas de juros de título públicos, hoje sendo corrigidas para padrões internacionais, a grande concentração bancária que limita tal atividade nas mãos de poucos grupos, o enorme spread bancário e, do lado dos bancos, pela dificuldade de recuperação do dinheiro emprestado.

Em suma, o crédito no Brasil é muito caro, sendo esse um dos entraves a um maior desenvolvimento da nossa economia.

Com o objetivo de reduzir o custo do crédito no Brasil, a chamada Lei do Cadastro Positivo (Lei 12.414/2011) com suas últimas alterações realizadas em 2019, tem por objetivo beneficiar clientes com dificuldade de acesso ao crédito.

Em vigor desde 09 de julho de 2019, segundo estimativas do governo, as mudanças promovidas poderiam beneficiar cerca de 130 milhões de pessoas, incluindo-se 22 milhões de brasileiros que estariam fora do mercado de crédito apesar de apresentarem bons históricos de adimplência.

Integrantes do governo afirmam que, segundo o Banco Mundial, a lei poderá reduzir em até 45% a inadimplência do País, que em números atuais atingiria mais de 60 milhões de pessoas.

Fica evidente, portanto, o objetivo perseguido pela Lei do Cadastro Positivo, que ao disciplinar a formação e consulta a bancos de dados com informações de adimplemento de pessoas naturais e jurídicas, busca viabilizar uma maior precisão na análise do crédito e consequentemente o seu barateamento e expansão.

De acordo com a exposição de motivos, com a coleta e a disseminação de informações sobre adimplemento, as pessoas poderão se beneficiar do registro de pagamentos em dia de suas obrigações, de modo a permitir a construção de seu histórico de crédito. Dessa forma, o mercado de crédito e de varejo poderá diferenciar de forma mais eficiente os bons e os maus pagadores, com a consequente redução do risco de crédito por operação, que permitirá a redução dos custos vinculados à expansão do crédito de uma forma geral.

Importante destacar também, que a criação do histórico de crédito é particularmente benéfica para os bons pagadores de baixa renda, que em geral são percebidos pelo mercado como de alto risco, e, por isso, pagam as mais altas taxas de juros do mercado.

Ainda segundo a exposição de motivos e redação original da Lei, ao disciplinar a formação do histórico de crédito, a lei estabeleceu regras claras sobre as garantias e os direitos dos cidadãos em relação às suas informações pessoais, de modo a permitir a adequada proteção da privacidade do cidadão e possibilitar o tratamento de dados pessoais sob um patamar de licitude e boa-fé.

Os dados pessoais merecem uma tutela importante pelo ordenamento jurídico, pois eles representam a própria pessoa e o seu tratamento influencia diretamente a sua vida, modelando e vinculando a sua privacidade e também as suas oportunidades, escolhas e possibilidades. A sua utilização, portanto, deve ter como fundamento a autodeterminação de cada pessoa em relação à utilização de suas próprias informações, permitindo que o cidadão possa escolher livremente a sua entrada no cadastro, bem como o seu cancelamento.

Em suma, buscou-se dotar o País de um arcabouço legal que incentivasse a troca lícita de informações pertinentes ao crédito e as transações comerciais, reduzindo o problema da assimetria de informações e proporcionando novos meios para redução das taxas de juros e para ampliação das relações comerciais, sem, contudo, abrir mão da adequada proteção da privacidade das pessoas.

Conforme mencionado, originalmente a Lei condicionava a abertura do cadastro à prévia autorização do potencial cadastrado. Já pensando em LGPD, estaríamos aqui na primeira hipótese de tratamento de dados que é o consentimento expresso do titular.

Entretanto, com as alterações promovidas pela Lei Complementar nº 166 de 2019, a lógica da abertura do chamado cadastro positivo foi significativamente alterada, sendo que a inclusão de dados para a formação do histórico de crédito dos consumidores brasileiros passou a ser automatizada.

Em outras palavras, na proposta anterior, para que os dados de determinado consumidor brasileiro fossem inseridos no cadastro positivo, ele deveria expressamente consentir ou requerer. Com a alteração promovida, os seus dados foram ou serão inseridos automaticamente no cadastro, sem qualquer espécie de necessidade de prévia autorização.

A despeito de a Lei do Cadastro Positivo prever a possibilidade de exclusão das informações inseridas no cadastro mediante requerimento do cadastrado, a lógica do sistema deixou de ser opt-in, ao retirar a necessidade do consentimento, e se tornou opt-out, promovendo a inserção automática com a possibilidade de posterior exclusão a pedido do cadastrado.

Em razão da alteração promovida, entidades de defesa dos direitos dos consumidores criticaram o que chamaram de "invasão de privacidade" decorrente da inclusão automática. Além disso, iniciaram-se os questionamentos da medida, apontando um suposto conflito com a LGPD.

Surgiu-se assim o ponto de conflito: A LGPD, que protege a privacidade dos cidadãos foi violada pela Lei do Cadastro positivo e sua inclusão automatizada?

4. Lei do Cadastro Positivo x LGPD: Existe incompatibilidade entre as referidas normas?

Tenho percebido um entendimento equivocado em algumas conversas informais. Em razão do alarde decorrente da LGPD, muitas

pessoas acreditam, equivocadamente, que o tratamento de dados no Brasil, a partir da entrada em vigor da LGPD, somente poderá ser realizado mediante expresso consentimento do seu titular.

Tal premissa equivocada faz com que várias pessoas continuem relegando a discussão sobre dados pessoais para um plano secundário, na medida em que acreditam que, bastará que não permitam e assim o tratamento dos seus dados pessoais não ocorrerá.

Contudo, é importante deixar claro que a Lei Geral de Proteção de Dados em seu artigo 7º prevê dez hipóteses de tratamento de dados, sendo que o consentimento do titular é apenas uma delas.

Sem adentrar nas demais hipóteses, o inciso X do artigo 7º prevê que o tratamento de dados pessoais poderá ser realizado para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Verifica-se, portanto, que o tratamento de dados amparado na proteção do crédito, uma hipótese inovadora trazida na legislação brasileira, prescinde do consentimento do titular.

O conceito de proteção do crédito é muito amplo, sendo possível o enquadramento de várias atividades como sendo destinadas a promover a proteção do crédito.

O chamado cadastro positivo se enquadra justamente nessa hipótese, que é reduzir a inadimplência mediante uma maior precisão na análise do crédito. Os que o criticam alegam que, embora a base legal da LGPD ampare a forma de coleta de dados prevista na Lei do Cadastro Positivo, esta não foi cuidadosa em observar as diretrizes da LGPD.

Um exemplo apontado dessa suposta ausência de cuidado é em relação ao conceito de “dado pessoal sensível” na medida em que a LGPD traz um conceito mais amplo e melhor detalhado do que o conceito da Lei de Cadastro Positivo.

Outro exemplo apontado é quanto à base legal da responsabilidade solidária do banco de dados, da fonte e do consulente por danos causados ao cadastrado. Apesar de a LGPD estabelecer de forma expressa que controladores e operadores responderão solidariamente pelos danos

causados aos titulares, a nova redação da Lei do Cadastro Positivo faz referência apenas ao Código de Defesa do Consumidor.

Existem ainda críticas na linha de que a Lei do Cadastro Positivo deixou de regular devidamente aspectos práticos relativos ao cumprimento das obrigações nela previstas.

Um ponto de destaque seria relativo ao canal de comunicação para que o cadastrado possa requerer o cancelamento e exclusão do seu cadastro, na medida em que a Lei não apresenta detalhes sobre o seu funcionamento, apesar da obrigatoriedade de fornecimento pelo gestor de dados.

No tocante à previsão de que o cadastrado deverá ter acesso facilitado às informações sobre o tratamento de seus dados pessoais, as informações fornecidas pela Lei são insuficientes para que tal medida se efetive do ponto de vista prático. Vale lembrar que a LGPD prevê que esse tratamento inclui toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Nesse sentido, apesar de a Lei do Cadastro Positivo prever a obrigação de esclarecimentos sobre quais elementos e critérios serão utilizados para compor a classificação do crédito dos cadastrados, o que também é uma forma de tratamento de dados, não há obrigação de fornecer informações transparentes sobre o fluxo de vida dos dados pessoais do titular.

Além disso, ao contrário da LGPD, que prevê a autoridade específica para fiscalização do cumprimento da lei, a Agência Nacional de Proteção de Dados, a Lei de Cadastro Positivo não designa nenhuma autoridade específica, o que, em tese, poderia prejudicar a função fiscalizadora.

Por se tratar essencialmente de dados pessoais, entendo que a ANPD deverá exercer a função fiscalizadora e sancionatória também em relação à Lei do Cadastro Positivo, editando normas complementares sobre o

tema, e impondo medidas adicionais de cuidado e transparência para esclarecer a legalidade ou ilegalidade de determinadas condutas no âmbito do novo Cadastro Positivo. Ainda que a Lei do Cadastro Positivo com sua nova redação tenha entrado em vigor quase um ano antes da vigência da LGPD, a designação da ANPD, sem dúvida, demonstraria uma preocupação mais efetiva do legislador quanto à proteção de dados dos consumidores brasileiros no processo de formação de histórico de crédito.

Apesar de todas as críticas e/ou ressalvas apontadas acima, entendo que a Lei do Cadastro Positivo não se conflita ou promove uma mitigação dos direitos previstos na LGPD.

Em uma análise social sobre a Lei do Cadastro Positivo, existe um ditado popular que diz que "quem compra o que não pode, vende o que não quer". Tal frase expressa bem o problema que pode ser gerado em razão de distorções que o mercado de crédito pode propiciar.

Uma análise imprecisa de crédito pode permitir que uma pessoa que não tenha capacidade tome um empréstimo por exemplo. Essa pessoa não arcará mais com suas obrigações em determinado momento, aumentando assim o número de inadimplentes. Como o aumento do número de inadimplentes, as taxas e juros tendem a subir, o acesso ao crédito tende a ser dificultado e para determinado grupo, de fato, eliminada a possibilidade de acesso a crédito.

Nesse cenário tóxico, eventuais pessoas que possuem um bom histórico de adimplência e poderiam tomar crédito e honra-lo em condições mais favoráveis que as oferecidas pelo mercado são diretamente prejudicadas. Devido a analise equivocada que concedeu crédito a quem não podia pagar, os que podem, tem que tomar empréstimos em piores condições, se tornando assim potenciais novos inadimplentes, isso se não lhes for tolhida essa possibilidade.

Segundo a revista EXAME de Outubro de 2019, o Brasil possui 45 milhões de pessoas fora do sistema bancário, que movimentam mais de 800 bilhões de reais por ano. Esse cenário faz surgir uma disputa enorme entre bancos, fintechs, varejistas e bancos digitais, reforçando a premissa

de que as análises relativas ao histórico financeiro das pessoas são imprecisas.

Todo esse contexto reforça a necessidade da Lei do Cadastro Positivo, como uma das várias maneiras pelas quais se busca corrigir a distorção existente no mercado de crédito brasileiro. Ela vai resolver o problema? Provavelmente sozinha não, mas já é um primeiro passo nesse caminho.

Superada a questão da importância do cadastro positivo, voltemos à análise de sua interface com a LGPD.

Conforme já mencionado, a nova redação da Lei do Cadastro Positivo modificou o sistema de inclusão dos dados para a formação do histórico de crédito dos consumidores brasileiros, que passou a ser realizada de forma automática, sem que seja necessário o consentimento expresso do consumidor.

Os dados inseridos no cadastro positivo serão tratados para que seja possível determinar uma nota de crédito (score) do consumidor, tendo por base seu histórico. Essa nota de crédito servirá como uma espécie de selo de bom pagador, o que, pelo menos do ponto de vista teórico, permitiria uma facilitação das condições creditícias de tal consumidor.

De acordo com a proposta original da Lei do Cadastro Positivo, a inclusão dos dados demandaria prévio e expresso consentimento do consumidor, o que era considerado por muitos uma enorme garantia de proteção dos dados e preservação do direito à privacidade. Entretanto, a necessidade de se obter o consentimento prévio para inclusão dos dados no cadastro, do ponto de vista prático, poderia inviabilizar sua efetividade.

Por essa razão, e inspirando-se no Regulamento Geral sobre a Proteção de Dados da União Europeia, por opção legislativa, optou-se por atenuar o protagonismo do consentimento na LGPD ao listar, no art. 7º da lei, outras hipóteses legais para o tratamento de dados pessoais (bases legais), vinculando-as necessariamente à observância de fundamentos (art. 2º) e princípios (art. 6º). Nessas hipóteses, o tratamento de dados pessoais sem o consentimento de seus titulares não implica necessariamente descumprimento da LGPD.

E é justamente na hipótese legal da proteção do crédito que se ampara a Lei do Cadastro Positivo. Segundo o inciso X do artigo 7º da LGPD, o tratamento de dados sem o consentimento do titular é permitido tendo em vista as finalidades estabelecidas no art. 7º da Lei do Cadastro Positivo, quais sejam: i) realizar análise de risco de crédito do cadastrado; e ii) subsidiar a concessão ou extensão do crédito e a realização de venda a prazo ou outras transações comerciais e empresariais que impliquem risco ao consulente.

Ao contrário do que alguns críticos alegam, de que a inserção automática estaria violando a privacidade dos consumidores, a Lei do Cadastro Positivo prevê expressamente a possibilidade de exclusão das informações inseridas no cadastro mediante simples requerimento do cadastrado, assegurando assim a autonomia da vontade, medida em estrita consonância com a LGPD.

Isso sem falar em outras disposições da Lei do Cadastro Positivo que demonstram uma efetiva preocupação do legislador com os princípios da finalidade, adequação, necessidade e transparência da LGPD, como: i) a garantia aos cadastrados de que poderão requerer a correção ou o cancelamento do cadastro (art. 5º, I e III); ii) a possibilidade de acesso do cadastrado às suas informações no banco de dados (art. 5º, II); iii) a informação aos cadastrados dos critérios considerados para a análise de risco de crédito (art. 5º, IV); e iv) a necessidade de informação prévia aos cadastrados sobre a identidade do gestor responsável pelos dados e sobre o armazenamento e o objetivo do tratamento dos dados pessoais (art. 5º V), que deve estar em consonância com o cumprimento da finalidade para a qual os dados pessoais foram coletados (art. 5º VII).

Dessa forma, ao prever que a proteção do crédito é uma base legal para a coleta e tratamento de dados, a LGPD possibilitou que a nova Lei do Cadastro Positivo esteja em perfeita consonância com ela, já que, conforme mencionado, não é necessário obter o consentimento do titular/cadastrado para usar os dados conforme as finalidades da lei.

Interessante mencionar que a legislação brasileira inovou na previsão de proteção ao crédito como uma das bases de tratamento de dados.

O que deve ser ressaltado mais uma vez é que os consumidores, na qualidade de titulares dos dados, possuem os direitos de informação, privacidade e livre acesso garantidos por ambos os dispositivos legais, afastando a ideia equivocada de que o cadastro estaria violando a sua privacidade.

Cumpre notar ainda que, muito embora à primeira vista a LGPD e a Lei do Cadastro Positivo possam aparentar algumas divergências, superada a questão da ausência da necessidade do consentimento prévio do consumidor, autorizada pela LGPD, a Lei do cadastro Positivo contém disposições que garantem os direitos de informação e privacidade dos consumidores em relação aos seus dados pessoais, assim como garantem a liberdade de manutenção ou não destes dados no cadastro positivo.

Além disso, uma queda na taxa de juros, efeito esperado pela Lei do Cadastro Positivo em razão da disponibilidade de um maior volume de informações para análise do risco de crédito, poderia configurar também "legítimo interesse" do controlador e da própria sociedade, o que estaria amparando o cadastro em outra base da LGPD para o tratamento de dados.

Outro ponto de suma importância é que as informações que serão inseridas automaticamente dizem respeito ao histórico positivo do consumidor, ao passo que as instituições que oferecem crédito já possuem acesso ao histórico negativo dos mesmos.

Conforme amplamente demonstrado, apesar de alguns pontos de suposta assimetria, a Lei do Cadastro Positivo está em sintonia com a LGPD, assegurando o direito à privacidade e proteção dos dados pessoais dos consumidores brasileiros.

A premissa de que o tratamento de dados pessoais somente poderá ocorrer mediante prévio e expresso consentimento do seu titular é equivocada, tendo em vista que a LGPD prevê dez bases para que o tratamento de dados seja realizado.

Tendo em vista a que finalidade buscada pela Lei do Cadastro Positivo se insere na hipótese de proteção do crédito previsto na LGPD, verifica-se a convergência entre as legislações, restando assegurada em ambas a autodeterminação dos dados pelos seus titulares, na medida em que o consumidor poderá requerer a exclusão dos seus dados do cadastro.

Analisando-se a Lei do Cadastro Positivo sob uma perspectiva global, ela é um passo positivo para o mercado de crédito brasileiro uma vez que poderá viabilizar uma redução das taxas de juros mediante uma análise mais precisa sobre o risco de adimplemento dos consumidores, auxiliando na correção de algumas distorções existentes.

Além disso, ela poderá ser um auxílio para que milhões de brasileiros ingressem no sistema financeiro formal, tendo em vista o volume assustador de consumidores com histórico positivo de adimplemento que ainda não conseguem ter acesso ao crédito regular.

Vale lembrar, contudo, que não necessariamente o cadastro positivo trará todos esses benefícios, ainda mais quando se enxerga um horizonte de curto prazo. Entretanto, ele sem dúvidas é um pontapé inicial na reformulação do sistema financeiro brasileiro e poderá contribuir para o desenvolvimento econômico brasileiro, amparado significativamente no consumo das famílias.

Por fim, tendo em vista as perspectivas positivas do cadastro positivo, aliado ao fato de que em sua essência ele se encontra em consonância com a LGPD, respeitando a privacidade e autodeterminação dos dados pelos seus titulares, resta-nos aguardar os seus resultados no mercado creditício brasileiro.

5. Referências

TEPEDINO, Gustavo; FRAZÃO, Ana; DONATO OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. Revista dos Tribunais, 1ª Edição, 2019.

PINHEIRO, Patrícia Peck. Proteção de dados pessoais: Comentários à lei n. 13.709/2018 (LGPD). Saraivajur, 1ª Edição, 2018.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. (coords.). Lei Geral de Proteção de Dados. 1ª Edição, 2019.

BRASIL. Código civil. 45. ed., São Paulo: Saraiva, 2009.

BRASIL. Constituição (1988). Comentários à Constituição do Brasil. São Paulo, Saraiva, 2013.

9

Proteção de dados, privacidade e o Marco Civil da Internet

Paulo Roberto Godoy Perilli [1]

1. Introdução

Embora as discussões, no Brasil, sobre temas como o direito à privacidade e a proteção de dados pessoais não tenham se desenvolvido no ritmo e na profundidade como em outros países, notadamente componentes do bloco europeu, por decerto podemos afirmar que, nos últimos anos, têm garantido especial espaço no ambiente jurídico nacional, não apenas por parte dos mais entusiastas e militantes da área, mas também pelo Poder Legislativo.

Isso porque, apesar da Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018, apenas ter sido promulgada em agosto de 2018, o cenário legal pátrio desde 2014 conta com uma importante moldura da tutela dos direitos humanos, do desenvolvimento da personalidade e do exercício da cidadania, especialmente voltada para os meios digitais. Estamos falando, senão, do chamado Marco Civil da Internet – Lei nº 12.965/2014.

Assim, a Lei Geral de Proteção de Dados foi uma notável consagração da proteção jurídica dos dados pessoais no Brasil, mas não cuidou de

[1] Professor de Direito Empresarial na Pontifícia Universidade Católica de Minas Gerais. Vice-Presidente da Comissão Especial da Lei de Proteção de Dados da OAB/MG. Eleito pelo *ranking* independente da *Acritas* como um dos 55 *StarLawyers* da América do Sul, pelos anos consecutivos de 2018 e 2019. Mestre em Direito Empresarial pela Faculdade de Direito Milton Campos. Pós-graduado em Direito Processual pela Pontifícia Universidade Católica de Minas Gerais. Graduado em Direito pela Pontifícia Universidade Católica de Minas Gerais. Palestrante pelo Centro Industrial e Empresarial de Minas Gerais – CIEMG. Autor e co-autor de livro jurídico e diversos artigos científicos publicados em revistas e livros jurídicos. Membro do grupo de pesquisa Constituição e Processo.

inaugurar a regulamentação do assunto (e tampouco a esgotará). Pelo contrário, a complexidade, a dinâmica e a mutabilidade são características naturalmente inerentes ao livre desenvolvimento da personalidade por parte dos indivíduos membros de uma sociedade democrática, sobretudo em fases históricas, como a presente, onde as tecnologias e a virtualização das relações reduzem distâncias e fomentam novas formas de engajamento (profissional, social, afetivo, dentre outros). Assim, as leis atuais seriam pretensiosas caso pretendessem exaurir a tutela jurídica de um aspecto tão primordial, e ao mesmo tempo volátil, como o desenvolvimento da personalidade e o subsequente direito à proteção dos dados pessoais.

Tal não impede, porém, analisarmos neste ensaio o crescente apelo das temáticas aqui enfrentadas, com destaque à privacidade e à proteção dos dados pessoais, no contexto jurídico dos direitos da personalidade. Portanto, perpassaremos pelo estudo dessas premissas na construção do direito atualmente e seu fundamental papel na consolidação das melhores dogmáticas legais de tutela dos interesses das pessoas naturais, em sede de autodeterminação informativa.

2. Construindo o paradigma atual do direito à personalidade no ordenamento brasileiro

Como muitas das digressões históricas sói sofrer, nem sempre há unanimidade ou confiabilidade científicas suficientes nas fontes de informações para se construir, seguramente, como surgiram e tiveram início determinadas preocupações e reflexões nas organizações sociais ao longo dos milhares de anos de existência. Assim, não é tarefa fácil reconstituir ou delimitar o momento em que, de fato, determinado aspecto da vida humana se tornou um foco de atenção, notadamente que devesse ser tutelado pelo direito.

Isso porque não se pode perder de vista que as leis não são feitas como fins em si mesmas, menos ainda como fruto de um esforço criativo-

filosófico por parte dos legisladores. Antes disso, a iniciativa legiferante (por vezes suplantada por um protagonismo Judiciário[2]), advém, senão, de uma necessidade do jurisdicionado, ainda que em maior ou menor grau discutida, reivindicada ou reclamada. Logo, é basilar entendermos que a lei não surge como fonte de direito pela vontade espontânea do legislador, mas sempre deve refletir um bem da vida ou uma regra de processo ou procedimento sobre os quais se sentiu necessidade de haver regulamentação.

Nesse contexto, como então entender a razão pela qual a Lei Geral de Proteção de Dados e, antes dela, o Marco Civil da Internet preconizaram a personalidade como um valor caro ao direito pátrio? É preciso, para se extrair adequadamente a norma dos textos legais supracitados, entender sua proposta, sua finalidade, ou, como Antonin Scalia bem pontua em sua obra *A Matter of Interpretation*[3], utilizar um método de interpretação pelo qual se busca o *original meaning* (ou *original intent*) do legislador[4].

Para tanto, é necessário pressupor que a sociedade que editou a regra, ou seja, a sociedade que lhe foi contemporânea, visava proteger certos direitos que as futuras gerações, inseridas em novo contexto, não poderiam imediatamente tirá-los da tutela jurídica. Com isso, podemos perceber que as leis, em regra, não só são editadas com um propósito específico (e não aleatoriamente), como geralmente o são para regulamentar situações após maturação do debate pela perspectiva social.

Por óbvio que, como toda regra, tal premissa comporta exceções, destacadamente quando houver patrocínio ou apadrinhamento político a uma ou outra causa, ou mesmo quando a lei, promulgada antes de uma discussão mais profunda, prestar-se a acompanhar vivamente a construção do pensamento pela sociedade. Fato é, porém, que a existência

[2] Exemplos disso são o ativismo judicial e as decisões estruturantes, cuja complexidade é digna de estudo em veículo próprio.

[3] SCALIA, Antonin. A Matter of Interpretation: Federal Courts and the Law. Princeton: Princeton University Press, 2018.

[4] SHAPIRO, Scott J. Legality. Cambridge, MA: Harvard University Press, 2011.

da uma lei presume prévia demanda social para abrigo de determinada situação pelo direito.

Vencidas essas considerações, pensar em ordenamentos jurídicos que possuem legislações específicas assegurando aos seus jurisdicionados o *respeito à liberdade de expressão* (artigo 2º, *caput*, Lei nº 12.965/2014), além dos *direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania* (artigo 2º, inciso II, Lei nº 12.965/2014), faz-nos remeter imediatamente ao que seria a acepção da personalidade juridicamente falando.

As primeiras preocupações humanas com a ideia da personalidade, como um valor a ser objeto de proteção, encontram substrato ainda no direito grego antigo (séculos antes de Cristo), quando a filosofia jusnaturalista da virtude começava a traçar a ideia de pessoa, e, ato contínuo, da proteção da personalidade. O que se entendia, à época, é que a personalidade deveria ser resguardada contra os chamados excessos, injustiças, desequilíbrios (no original, *hybris*), cometidos contra uma pessoa. Ao se cogitar excessos e injustiças, portanto, ter-se-ia uma noção, para as sociedades antigas, de que tais abusos eram interpretados como violações à imagem do indivíduo perante seu convívio (AMARAL, 2008).

A proteção rudimentar e embrionária da personalidade, então, surge como uma tutela do direito penal, focada no indivíduo como detentor de direitos no campo moral, e posteriormente é aprimorada para se desdobrar entre pretensões de ações públicas e privadas, não apenas de cunho penal. O próprio objeto da proteção da personalidade também se expande, para envolver a integridade física e a honra, por exemplo. Isso não significa que antes não houvesse disposições legais para coibir ofensas físicas entre pessoas, mas estas não tinham uma preocupação maior que não a manutenção da ordem. Logo, não viam a proteção da pessoa e da personalidade como um dos fundamentos para a preservação da integridade física (AMARAL, 2008).

Com isso, percebe-se que a tutela jurídica da personalidade se associa, em um dos seus precedentes mais remotos (Grécia), às

concepções filosóficas jusnaturalistas. Todavia, não é o mesmo jusnaturalismo que, séculos mais tarde, no período iluminista moderno, irá desencadear diversas revoluções políticas, sociais, científicas, artísticas e, inclusive, jurídicas.

Está-se falando do jusnaturalismo onde a ética se pauta no homem que quer frequentar a polis, quer exercer uma vida social e pública. O ser humano, na perspectiva jusnaturalista dos antigos pensadores, deveria procurar a virtude, apregoada como um senso comum de bons valores inerente a todas as pessoas. Com o passar do tempo, os pensadores iluministas resgatam o jusnaturalismo como fonte de direitos já no período moderno, mas a partir de uma racionalização do direito e do homem.

O homem deixa de ser visto como virtuoso e militante por uma vida na polis, passando a ser entendido como um ser individualista, frequentador de uma organização social por interesses egoístas. O divino e outros elementos de religiosidade deixam de ter um caráter justificativo tão forte para a compreensão da ética jusnaturalista, que agora deve ser entendida como o fiel cumprimento das regras. O direito, em tal processo de racionalização, adquire profundo traço contratualista (desde a organização da sociedade, a partir do contrato social, o processo como um contrato para Pothier, até a revisitação da doutrina contratual para chancelar a vontade como fonte de obrigações[5]).

Apesar da retomada do jusnaturalismo no período moderno, tem espaço uma dissidência jurídica, capitaneada por Savigny, que negava reconhecer a recepção dos direitos de personalidade por ausência de sua positivação (BIONI, 2019). Na perspectiva desse, o sujeito de uma relação

[5] Abandonam-se, aqui, as antigas ideias de fórmulas, rituais e sacramentos como elementos formados de contratos e obrigações, independentemente do real desígnio das partes. Tais concepções prevaleceram em grande parte do direito grego, romano e medieval, sendo que neste, anterior ao iluminismo, o contrato era visto como uma forma de justiça entre as partes, ou quando uma destas, deliberadamente, pretendia realizar graciosidades (doações) a outra. Assim, previamente à mudança de perspectivas jurídicas perante o direito contratual, este era lido a partir da ideia de justiça comutativa (LOPES, 2019).

jurídica não poderia ser, simultaneamente, também seu objeto, como melhor expõe o autor lusitano António Menezes de Cordeiro[6]:

> *Curiosamente, Savigny é apontado como negativista, em termos de direitos da personalidade, imputando-lhe mesmo o atraso no reconhecimento da figura. Todavia e em rigor, Savigny apenas questionou a possibilidade dogmática de construir um direito decalcado do direito de propriedade, mas dirigido ao próprio 'titular' e que poderia envolver diversos inconvenientes, entre os quais o reconhecimento de um direito ao suicídio. (...) Savigny não era contrário à tutela da pessoa: bem pelo contrário. Ele apenas duvidou da viabilidade dogmática dos direitos da personalidade, numa dimensão a que, de resto, ainda hoje teremos de atender.*

O período jusnaturalista do iluminismo não contribuiu para o desenvolvimento dos direitos da personalidade, preferindo encerrar sua atenção em questões patrimoniais. O subsequente positivismo pouco acresce ao aprimoramento da tutela da personalidade, dando continuidade ao caráter material da preocupação da tutela jurídica, sem maiores delongas sobre questões de personalidade não relacionadas a bens (BIONI, 2019).

Ocorre que a história, por meio dos regimes nazistas, demonstrou que o positivismo e suas abstrações permitiram ao terceiro *reich* acontecer nos limites da "legalidade". Otfried Hoffe, em sua obra Justiça Política[7], tem a oportunidade de tecer uma rica reflexão sobre as razões para a crise do direito pós Segunda Guerra Mundial, e encontra na chamada "dupla alienação" um importante fundamento. Para Hoffe, nos últimos dois séculos foi praticada, pelos filósofos e juristas, uma alienação no estudo da filosofia quanto a questões de moral e ética, e outra alienação no estudo do direito quanto a filosofia em si (distinta da filosofia jurídica) (HOFFE, 2005).

Muito se fala na notória distinção entre direito e justiça, da qual o primeiro não guarda qualquer relação de resultado com a segunda, mas

---

[6] CORDEIRO, António Menezes de. Tratado de direito civil: parte geral, pessoas. Coimbra: Almedina, 2011, v. 4.

[7] HOFFE, Otfried. Justiça política: fundamentação de uma filosofia crítica do direito e do Estado/Otfried Hoffe; tradução Ernildo Stein. 3ª ed. São Paulo: Martins Fontes, 2005.

não necessariamente deveria ser assim, sob pena de se perder a legitimação da dominação do direito sobre o homem. Seria necessário o desenvolvimento da ideia de justiça política, ao mesmo tempo reconciliando (i) a filosofia com a teoria do direito e do Estado e (ii) ambas teorias com a ética (HOFFE, 2005).

O ideário jurídico deveria, pois, retornar o estudo do direito e da filosofia do direito à preocupação com a justiça dos resultados, como por exemplo, das decisões judiciais (HOFFE, 2005). Isso abre espaço para uma mais antiga discussão, iniciada por Herbert Hart, no tocante à derrotabilidade das normas (*defeasibility*[8]), quando a solução proposta pela norma for deveras injusta no caso concreto, autorizando a sua "derrota" e não aplicação naquela situação jurídica. Por tais notáveis teorias serem merecedoras de abordagem em estudo próprio, faz-se aqui apenas uma especial menção às concepções desenvolvidas, que servem para ilustrar como a preocupação com a legitimação do direito jamais pode ser preterida.

Em meio a esse ambiente filosófico pós-positivista é que encontra fundamento a despatrimonialização (ou repersonalização) do direito civil, tendência normativa-cultural pela qual o centro da tutela jurídica passa a ser o ser humano, trazendo luz a todas as preocupações inerentes à humanização do direito privado, como a proteção da honra, da imagem e do nome. É necessária a concorrência tripartite da personalidade com os bens materiais e os negócios jurídicos, merecendo todos tutela específica do direito civil: nenhum pode ser descartado ou negligenciado pela norma (BIONI, 2019).

No Brasil, esse novo paradigma é liderado por Orlando Gomes, tanto em suas obras quanto na idealização do projeto de Código Civil, que serviu de inspiração e foi consideravelmente aproveitado no texto da Lei nº 10.405/2002 (BIONI, 2019). Veja-se que sequer é preciso se aprofundar no texto do Código Civil atual para se deparar com a tutela expressa dos

[8] Para melhor estudo da teoria da *defeasibility*, leia-se a obra original de Herbert Hart, *The Ascription of Responsibility and Rights* (1948).

direitos de personalidade, incluídos já a partir do artigo 11, inclusive aos quais é outorgada natureza intransmissível e irrenunciável, impassível de limitação voluntária.

Antes do Código Civil de 2002, porém, a Constituição de 1988 estabeleceu, como fundamento da república, a dignidade da pessoa humana, e como direitos e garantias fundamentais, a liberdade de manifestação de pensamento, de consciência e de crença. Ao mesmo tempo, assegurou o direito de resposta proporcional ao agravo, bem como indenização por dano moral ou à imagem (além do dano material). Tornou livre também a expressão da atividade intelectual, artística, científica e de comunicação, sem censuras, e, principalmente, invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas (inviolabilidade esta que acabou reprisada no artigo 21 do futuro Código Civil de 2002).

Todos esses valores refletem a nova centralização do direito na figura do ser humano, sendo sua tutela, ainda, inacabada. Isso significa dizer que a promoção do homem pelo direito deve ser elástica, não no sentido de ser flexibilizável, sopesável como algo passível de renúncia parcial, mas sim como uma proteção maior capaz de abarcar toda e qualquer situação, mesmo no silêncio de norma específica outorgando proteção legal (BIONI, 2019), como Gustavo Tepedino assevera:

> *Mais ainda, a tutela da personalidade, como bem se acentuou na doutrina alienígena, é dotada do atributo da elasticidade, não se confundindo, todavia, tal característica com a elasticidade do direito de propriedade. No caso da pessoa humana, elasticidade significa a abrangência de tutela, capaz de incidir a proteção do legislador e, em particular, o ditame constitucional de salvaguarda da dignidade humana a todas as situações, previstas ou não, em que a personalidade, entendida como valor máximo do ordenamento, seja o ponto de referência objetivo (TEPEDINO, 2008).*

Por isso é que se mostram tão caros os atributos capazes de tornar a tutela jurídica dinâmica e mutável, para acompanhar a realidade do jurisdicionado e seu livre desenvolvimento da personalidade. Antes de

destinatário da norma, esse é também a sua fonte, e deve ser preconizado a todo momento.

Como consequência, o novo ambiente tecnológico, por exemplo, não pode escapar de tal filtro, sobretudo porque atua como agente, em duas frentes, quanto à sobredita elasticidade do direito de personalidade. Na primeira, as tecnologias e seus impactos na virtualização das relações inauguram, a cada inovação, um novo cenário de desenvolvimento da personalidade, fazendo surgir experiências por vezes ainda não vividas pelo ser humano. Na segunda, ao mesmo tempo em que permitem novas formas de exercício da personalidade, trazem consigo a necessidade de proteção e tutela dessa em situações não imaginadas (e, potencialmente, não consolidadas em veículo legislativo anterior).

Ao imaginar a personalidade como o conjunto de características que distingue uma pessoa da outra (aí incluídos nome, honra, integridade física e psíquica, enfim, tudo que, corpórea ou incorporeamente, dê forma ao prolongamento da pessoa humana), sequer poderia ser diferente.

Tamanha amplitude de questões nos traz a necessidade, então, de realizar um corte temático, para delimitar o escopo do presente ensaio. Um essencial aspecto da personalidade, que é sempre foco na leitura das inovações, é a privacidade. Esta é, senão, uma das formas de garantir o livre desenvolvimento daquela, que se revigora como um desafio jurídico a cada nova situação. Aprofundaremos, então, nessa vertente específica.

3. A privacidade e os dados pessoais

Como visto anteriormente, a personalidade foi uma preocupação inconstante ao longo da histórica, até assumir os contornos do paradigma da proteção jurídica atual. Seja por força de correntes jurídicas diversas, do ideário social, do modelo filosófico ou do sistema legal, não foram poucos os fatores que influenciaram na construção da tutela presente sobre a personalidade.

A premissa que serve de ponto de partida, porém, é que a personalidade humana não somente é tutelada, mas verdadeiramente compõe o cerne do ordenamento, consagrando-se como um valor, fundamento e princípio do desenvolvimento do direito e da filosofia do direito. Assim, para que possamos avançar neste estudo com maior adesão e praticidade (reduzindo o caráter filosófico), é necessário definir o que é a privacidade como viés do direito de personalidade.

A privacidade pode ser conceituada 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, sem a isso poder ser legalmente sujeito* (SILVA, 2013). Assim, *a privacidade é regida pelo princípio da exclusividade, cujos atributos principais são a solidão (o estar-só), o segredo, a autonomia* (FERRAZ JÚNIOR, 1993).

Doutrinadores estrangeiros (Samuel Warren e Louis Brandeis), analisados por Têmis Limberger, na mesma linha, conceituam *the right to privacy, as a part of the more general right to the imunity of the person – the right to one's personality* (LIMBERGER, 2007). E discorrendo sobre a regulamentação norte-americana sobre o tema, continuam:

> *The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into na undesirable and undesired publicity and to protect all persons, whatsoever;* (...) *It is the unwarranted invasion of individual privacy which is reprehended, and to be, so for as possible, prevented* (LIMBERGER, 2007).

Em outras palavras, o direito à privacidade envolve diretamente a concepção de um espaço que o indivíduo possa se portar e desenvolver sua personalidade sem expectativas sociais. Só que, exatamente ao se cogitar um ambiente livre para exercício genuíno da individualidade pelo indivíduo, tem-se o primeiro desafio para a tentativa de se tutelar a privacidade: tal direito de personalidade precisa ser material, substancial, efetivo, e não meramente formal (NETHER, 2018).

Vale resgatar, aqui, que a Constituição de 1988 reconheceu, como direitos fundamentais, a inviolabilidade da intimidade, a vida privada, a

honra e a imagem das pessoas. Ora, vemos, por um lado, tamanha importância alçada à proteção da vida privada (aí incluída a privacidade), mas como exercer tal tutela em sua plenitude e assegurar sua eficácia? Não são raros os exemplos de intangibilidade de previsões legais das mais variadas, por falta de adesão e impossibilidade material de cumprimento. Assim, como evitar que esse destino fatídico ocorra também com o direito à privacidade?

As dificuldades para a implantação do direito à privacidade, por óbvio, não são poucas, pequenas ou isoladas. Muito pelo contrário, está-se diante de um direito que muitas vezes contraria a própria característica do ser humano em adentrar na vida privada do outro. E relembrando que a privacidade, objetivamente, é conjunto de informações de titularidade de um indivíduo a quem cabe exclusivamente o controle, certo é que a sua proteção por parte do direito envolve, desde logo, evitar o acesso indevido pelo próprio homem sobre a privacidade de terceiros.

Veja-se que a doutrina estrangeira também reconheceu que a invasão indevida à privacidade deve ser repreendida e, tanto quanto possível, prevenida. Nesse contexto, paulatinamente se construiu a ideia do chamado dado pessoal, a ser entendido como signo indentificador do indivíduo, um elemento que, derivado de uma pessoa, empresta conteúdo à personalidade e irá destacar seu respectivo titular do restante da sociedade, como uma projeção ou extensão desse (BIONI, 2019).

Pensar que tais signos contribuirão para a projeção da personalidade do titular traz mais complicações à gestão jurídica do dado pessoal, pois além de ter, supostamente, acesso somente quando autorizado pelo titular, deverá comportar também retificações para corrigir desvios de informação (e, via de consequência, de imagem, personalidade, do titular). Portanto, não é menos objeto de tutela, que a privacidade combatente da invasão indesejada ao dado pessoal, o zelo pela integridade e fidelidade do conteúdo a ser divulgado a respeito do titular.

O dado pessoal, embora tenha sido fartamente alardeado pela LGPD, já que está presente desde o seu nome e durante todo o texto, não foi

gestado no ordenamento por essa. Legislações especiais já reconheciam sua existência como objeto de tutela jurídica, mas foi apenas com a LGPD que o dado pessoal foi sistematizado como a *informação relacionada a pessoa natural identificada ou identificável* (artigo 5º, inciso I).

Percebe-se que o legislador adotou a concepção expansionista para designação do dado pessoal, ao incluir na previsão legal não apenas a informação relativa à pessoa natural identificada, onde há vínculo imediato entre dado e titular, mas também a informação de pessoa natural identificável, onde o titular é indeterminado por não haver vínculo direto entre aquele e o dado (BIONI, 2019). Opção em sentido contrário seria o legislador unicamente eleger, como dado pessoal, a informação de pessoa natural específica, afunilando o escopo de abrangência da proteção normativa.

Não sendo esse o caso, porém, a distinção se apresenta somente para enriquecimento do debate. Fato é que, pelo arcabouço legal brasileiro, há proteção das informações relacionadas a pessoas naturais, identificadas ou identificáveis.

Voltando algumas décadas no tempo, é curioso perceber que, ainda em 1984, foi instituída a Política Nacional de Informática, por meio da Lei nº 7.232, com preocupação à proteção dos dados pessoais e da privacidade das pessoas usuárias da informática. Isso porque tal Política deveria atender ao princípio *do estabelecimento de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas* (artigo 2º, inciso VIII), tendo delegado à lei específica a estruturação e exploração de bancos de dados (artigo 3º, parágrafo 2º) e as *Matérias referentes a programas de computador e documentação técnica associada (software) e aos direitos relativos à privacidade, com direitos da personalidade* (artigo 43).

Portanto, mesmo implantado em menor escala à época, até porque as tecnologias não eram tão intrínsecas ao estilo de vida humano, já se vislumbrava fonte de tutela jurídica do dado pessoal e da privacidade dos

indivíduos. Com o passar dos anos e o desenvolvimento de novos aparelhos e tecnologias, e com a farta propagação desses no meio social, a partir da quase universal prestação de serviços de acessibilidade à informática, tomou corpo a formatação social atual, fortemente marcada (e, verdadeiramente, dependente) das tecnologias.

Diz-se dependente porque, ainda que no âmbito pessoal um indivíduo consiga deixar de se valer das tecnologias e institutos da informática para se relacionar com a sociedade (na remota hipótese de assim o querer), fato é que, no aspecto profissional, é praticamente impossível se cogitar o exercício de atividade laborativa sem ao menos um tipo de contato com tecnologias (aplicativos de comunicação, endereço de correspondência eletrônico, provedor de serviços, plataformas de serviços, *softwares* de gestão financeira, administrativa e contábil, sistemas virtuais de prestadores e tomadores de serviços, sistemas virtuais de vendedores e consumidores de produtos, serviços de assistência técnica e ao consumidor, enfim, uma verdadeira infinidade de frentes).

Assim, mesmo o trabalhador exercente da mais analógica ou braçal função, em algum momento precisará interagir com uma forma de tecnologia, pois estas compõem hoje o próprio DNA da organização profissional, em maior ou menor escala. Isso se diga também quanto à administração pública, direta ou indireta, que precisou se automatizar para conseguir atender a demanda de serviços públicos por parte dos cidadãos. Logo, literalmente não há como "escapar" da tecnologia nos tempos atuais.

Ocorre que essa mesma tecnologia, desde um primeiro contato (simples cadastro, por exemplo), exige da pessoa física por detrás daquele cadastro a inclusão de diversas informações sobre sua personalidade para franquear o acesso e uso da plataforma, *software*, enfim, serviço de qualquer natureza. Então a tutela jurídica do dado pessoal e da privacidade incide já nesse primeiro momento, e mesmo antes, por exemplo, quando o usuário não cadastrado tem seus dados colhidos a partir da singela

navegação e interação não "logada" (isto é, sem ter feito *login*) em um ambiente tecnológico.

Ainda que não possa a pessoa natural negar o fornecimento de dados pessoais, isso não significa que o recebedor de tais dados poderá realizar o tratamento que lhe aprouver, indiscriminadamente. A partir da vigência da LGPD em agosto de 2020, de início atrairá o recebedor, para si, a fundamental responsabilidade de zelar contra invasões externas ou vazamentos indevidos das informações coletadas, preventiva ou repressivamente. Ao mesmo tempo, precisará militar pelo aculturamento da privacidade *interna corporis*, para se preservar a divulgação mínima dos dados aos seus colaboradores.

Como dito acima, é da natureza do ser humano se imiscuir na vida privada do outro, motivo pelo qual é essencial a consciência, por parte dos gestores de dados pessoais, acerca da sua utilização e manejo apenas pelos colaboradores que o precisarem para exercício de suas respectivas funções. Mesmo a esses, deve ser franqueado acesso sóbrio, evitando o repasse informal de dados por curiosidade ou desatenção dos colaboradores. Um fácil exemplo é o de vazamento de dados a partir de registros fotográficos lançados em redes sociais pelos colaboradores ou pela "fofoca" de informações. Se há um setor financeiro em uma empresa (independentemente do porte), não há necessidade de divulgar os dados da folha de pagamento a ninguém que não componha tal departamento.

Quando se tem em mente um ambiente virtual, a situação se apresenta mais gravosa, porque o banco de dados (geralmente volumoso) é obtido a partir do rastreio de diversas informações, inclusive por meio de *cookies*[9], e se mostra especialmente suscetível à invasões e ataques, além de acessos indevidos por pessoas com contas de uso de outras.

Por outro lado, esse mesmo cenário eletrônico de relações constitui um risco ao titular dos dados porque esse, infinitas vezes, sequer tem conhecimento sobre a coleta de informações a seu respeito por parte das

[9] Arquivos pelos quais sítios eletrônicos conseguem captar e armazenar, ainda que em caráter temporário, informações diversas sobre o acesso do usuário à plataforma.

plataformas, *softwares* e prestadores de serviços *online*. Também quando tem conhecimento da coleta, não sabe ao certo todos os dados que foram coletados e, sobretudo, qual a destinação, a finalidade e o tratamento que lhes serão dados.

O direito constitucional à inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, então, muito necessita de uma regulação mais rica em padrões de condutas (de segurança e transparência) e procedimentos de contato com os titulares. Dentre os exemplos de regulação enfrentados neste ensaio, veremos com mais riqueza de detalhes as providências introduzidas pelo Marco Civil da Internet.

4. O Marco Civil da Internet na tutela da privacidade

Como enfrentado acima, seja em legislações mais recentes ou de décadas atrás, fato é que o direito hodierno simplesmente não pôde fechar os olhos à tutela da personalidade como um direito do ser humano. Assim, dentre os diplomas legais que buscam regulamentar matérias afetas à privacidade, merece especial destaque o Marco Civil da Internet – Lei nº 12.965/2014.

Como uma reação à pretensão de regulamentação da internet, no país, pelo direito penal (aspecto que seria fatal à inovação tão primordial a esse segmento), surgiu o Marco Civil da Internet. Seu caráter é eminentemente principiológico, já que não se propõe à pretensa função exaurir a regulamentação da internet e dos dados pessoais (BIONI, 2019).

Logo no início do texto, é preconizada a proteção da privacidade como um dos princípios da disciplina do uso da internet no Brasil (artigo 3º, inciso II). Para tanto, garantiu o Marco Civil da Internet que o acesso a esta, internet, deveria ser essencial ao exercício da cidadania (artigo 7º), mas, ao mesmo tempo, observar o "miniestatuto-microssistema" (BIONI, 2019) criado pelo legislador para tratar do manejo das informações pessoais eletronicamente.

Isso significa, nos termos da lei, ser assegurado ao usuário o direito de *inviolabilidade da intimidade e da vida privada* (artigo 7º, inciso I), *inviolabilidade e sigilo do fluxo de suas comunicações pela internet* (artigo 7º, inciso II), *inviolabilidade e sigilo de suas comunicações privadas armazenadas* (artigo 7º, inciso III), *não suspensão da conexão à internet* (artigo 7º, inciso IV), *não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento* (artigo 7º, inciso VII), *informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais* (artigo 7º, inciso VIII), *consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais* (artigo 7º, inciso IX) e *exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento* (artigo 7º, inciso X).

Por óbvio que tais previsões merecem análise sistêmica, isto é, no âmbito do Marco Civil da Internet e de outras leis correlatas, mas sua pincelada específica aqui tem o efeito de evidenciar o forte caráter de transparência imposto aos provedores de conexão à internet e de aplicações de internet, enquanto entidades responsáveis pelo tratamento de dados pessoais. Veja-se que é enfatizada a necessidade de consentimento prévio dos usuários para grande parte das hipóteses de coleta e tratamento de dados, bem como a possibilidade de exclusão dos dados após o fim da relação entre as partes.

No que pertine especificamente ao tema privacidade, salta aos olhos a preocupação do legislador em não autorizar o fornecimento a terceiros dos dados coletados pelos provedores, sem consentimento ou permissão legal, e em resguardar a inviolabilidade da vida privada e da intimidade dos usuários.

Assim, aqueles prestadores de serviços de conectar o usuário à internet ou de aplicação de internet se tornaram expressa e legalmente responsáveis pela guarda, dentre outros, dos dados pessoais, devendo atender, no exercício dessa, *à preservação da intimidade, da vida privada,*

da honra e da imagem das partes direta ou indiretamente envolvidas (artigo 10) e *ao sigilo das comunicações privadas e dos registros* (artigo 11).

Nas palavras de Bruno Ricardo Bioni:

> *Tal garantia é vital para que os cidadãos possam se relacionar uns com os outros, trocando confidências e expressando as suas opiniões sobre os mais variados assuntos, quer sejam fúteis ou não, sem que seus posicionamentos se voltem contra eles. Por essa razão, o sigilo das comunicações é tido como um direito fundamental, tamanha sua importância para tal tipo de interação social.*
>
> *Isso porque, ao assegurar que todo e qualquer tipo de interferência à confidencialidade das comunicações será excepcional – somente mediante ordem judicial -, encoraja-se o engajamento social, em vez de sufocar e inibir o processo comunicacional. Note-se, pois, novamente, o valor social que está por três da privacidade, sendo, nesse caso específico, a confidencialidade e o sigilo das comunicações.*

Nessa linha de raciocínio, é interessante pensarmos em como a privacidade é comercialmente interessante para o crescimento e consolidação das empresas. Há um verdadeiro ciclo vicioso de fomento recíproco: quanto maior a privacidade assegurada aos usuários, mais é catalisada a interação social, e mais se torna rentável e atrativa a plataforma utilizada. Logo, há como se defender até mesmo o próprio interesse do provedor em intensificar o sigilo e a privacidade das informações colhidas e que estabelecem fluxo por seu intermédio.

Independentemente da percepção dos provedores à rentabilidade da privacidade, tem-se que as previsões do Marco Civil da Internet traduzem o início do movimento de alçar a privacidade aos negócios dos provedores *by design* e *by default*, e não apenas como uma etapa de adesão do serviço prestado. Quer-se a preocupação legítima dos provedores com a privacidade e não apenas sua leitura como uma "fase" da atividade prestada. Ora, considerando o grau de importância do tratamento de dados pessoais à subsistência dos provedores, a prestação de contas por parte desses aos titulares é consequência matemática.

Isso significa que, para além dos protocolos, posturas, políticas, procedimentos, planos e estratégias empresariais dos provedores para segurança dos dados, o próprio negócio em si deve ser arquitetado e desenhado tomando a privacidade como um elemento essencial e indissociável, verdadeiramente parte do *business*. O que se pretende é o desenvolvimento e estabelecimento de uma cultura onde a privacidade componha o núcleo do exercício da atividade dos provedores tal como as demais questões inerentes ao seu objetivo social, e não apenas uma imposição regulatória a ser respeitada durante a persecução daquele.

O paradigma deve ser alterado para que a privacidade esteja, desde o nascedouro, presente no ambiente eletrônico. E lembrando que, como visto anteriormente, a privacidade faz parte da personalidade humana, não há como se conceber seu livre desenvolvimento sem a cautela, o sigilo e a responsabilização por parte daqueles que, atualmente, tão visceralmente lidam com dados pessoais.

Não é por outro motivo que Marco Civil da Internet resguarda os titulares ao ponto de estabelecer que a inviolabilidade e o sigilo das comunicações privadas, pela internet, são irrenunciáveis, tornando nulas de pleno direito quaisquer cláusulas contratuais que diversamente queiram registrar. Com isso, a lei cria um chamado núcleo duro de direitos, com o intuito de preservar a integridade do fluxo informacional através da indisponibilidade de direitos pelos titulares (BIONI, 2019).

Inclusive, durante o processo de tramitação legislativa do Marco no Brasil, foi até mesmo citado enrijecimento (endurecimento) da proteção à privacidade especialmente graças ao episódio de vazamento de documentos da Agência de Segurança dos Estados Unidos, por Edward Snowden, a partir de 2013, tornando público um programa de espionagem global. Após tal acontecimento, o artigo 7º da lei, que versa sobre os direitos e garantias dos usuários, foi contemplado com mais três prerrogativas de natureza protetiva aos dados pessoais (BIONI, 2019).

Seguindo a linha das diretrizes constitucionais, portanto, o "miniestatuto" do Marco Civil da Internet, mesmo que em linhas mais

gerais, pretendeu tornar responsabilizáveis os provedores, ou seja, introduzir a ideia da *accountability* aos agentes que viabilizam a interface dos usuários à internet, pela tutela dos dados pessoais, tudo em busca da preservação da privacidade dos respectivos titulares.

5. Considerações finais

A partir da breve digressão feita sobre a personalidade humana e suas diversas formas de proteção pelo direito, vê-se que, em tempos de profunda presença de tecnologias na rotina diária das pessoas, torna-se impositivo um olhar especial das leis a esse ambiente. Ao considerarmos que, na avassaladora maioria dos casos, todas essas tecnologias convergem a um espaço comum denominado internet, é essencial uma regulamentação jurídica a fim de criar, ainda que de forma coercitiva em um primeiro momento, os pilares para uma cultura de privacidade.

O papel do Marco Civil da Internet, juntamente com outras leis setoriais, é exatamente esse. Inaugurando uma série de princípios e fundamentos para o exercício da atividade de conexão e aplicações na internet pelos provedores no país, o Marco se encarrega de trazer o consentimento do titular dos dados na relação de pressupostos para a atividade dos provedores. Embora quatro anos depois a quase obrigatoriedade de consentimento tenha sido desmistificada pela LGPD, ao trazer um rol contendo dez hipóteses autorizativas do tratamento de dados pessoais não sensíveis, o Marco foi emblemático na tutela da proteção à privacidade no ambiente virtual.

Percebe-se que a autodeterminação informativa foi o critério eleito pelo legislador para a salvaguarda dos dados pessoais, pois como pontua Bruno Ricardo Bioni:

> *Todas as normas desembocam na figura do cidadão-usuário para que ele, uma vez cientificado a respeito do fluxo de seus dados pessoais, possa controla-lo por meio do consentimento. Essa perspectiva de controle perpassa desde a fase de coleta e compartilhamento dos dados com terceiros até o direito de deletá-*

> *los junto ao prestador de serviços e produtos de Internet ao término da relação. (BIONI, 2019).*

Assim, para se cumprir a objetivo maior do ordenamento jurídico, de ser capaz de tutelar dinamicamente situações ainda não vividas ou experimentadas com as mesmas leis, sem a constante necessidade de interferência legiferantes, percebe-se que o Marco Civil da Internet inaugurou, com propriedade, a proteção da privacidade dos usuários desse tipo de serviço no Brasil.

Ao estabelecer a privacidade como um dos princípios do uso da internet no país, ao lado de medidas voltadas à transparência do provedor frente ao usuário, e à proteção dos registros, dados pessoais e comunicações privadas, o Marco Civil da Internet se posicionou como um precedente para o movimento de reformulação da cultura empresarial, notadamente dos ambientes eletrônicos.

Como enfrentado anteriormente, o constante avanço tecnológico implica diretamente na descoberta de novas experiências não vividas pelas pessoas e novas vertentes, via de consequência do direito de personalidade, o que exige elasticidade (com segurança jurídica) ao arcabouço legal. Exatamente por meio de uma norma principiológica é que se conseguirá conjugar elementos recém descobertos na realidade dos jurisdicionados a uma legislação que não seja diretamente contemporânea. E, principalmente, somado a tudo isso, está o papel dos princípios constitucionais regulamentados pelo Marco, e demais veículos normativos, na construção e consolidação de um novo paradigma de gestão dos dados pessoais na atividade profissionais dos provedores e também de outras empresas que dele se valem na persecução de seus objetivos sociais, jamais perdendo de vista a privacidade devida aos titulares.

6. Referências

AMARAL, Francisco. Direito civil: introdução. Rio de Janeiro: Renovar, 2008.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento.** 3ª Reimp. Rio de Janeiro: Forense, 2019.

BRASIL. Constituição da República Federativa do Brasil de 1988, de 05 de outubro de 1988. Brasília, **DOU de 05.10.1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 04 de dezembro de 2019.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Brasília, **DOU de 11.01.2002.** Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 04 de dezembro de 2019.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Brasília, **DOU de 15.08.2018.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 04 de dezembro de 2019.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, **DOU de 11.01.2002.** Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 04 de dezembro de 2019.

CORDEIRO, António Menezes de. **Tratado de direito civil: parte geral, pessoas.** Coimbra: Almedina, 2011, v. 4.

COULANGES, Fustel de, DANIES, Numa. **A cidade antiga: estudo sobre o culto, o direito e as instituições da Grécia e de Roma.** Tradução de Roberto Leal Ferreira. São Paulo: Martin Claret, 2009.

CABRAL, Marcelo Malizia. **A colisão entre os direitos de personalidade e o direito de informação.** In: MIRANDA, Jorge, RODRIGUES JUNIOR, Otavio Luiz, FRUET, Gustavo Bonato (org.). Direitos da personalidade. São Paulo: Atlas, 2012.

MALDONADO, Viviane Nóbrega, BLUM, Renato Opice, coord. **LGPD: Lei Geral de Proteção de Dados comentada.** São Paulo: Thomson Reuters Brasil, 2019.

FERRAZ JÚNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.** Revista da Faculdade de Direito da Universidade de São Paulo, v. 88, p. 439-459. 1993. Recuperado de <http://www.revistas.usp.br/rfdusp/article/view/67231>.

GENERAL DATA PROTECTION REGULATION EU. Disponível em: <https://gdpr-info.eu/>. Acesso em: 04 de dezembro de 2019.

HOFFE, Otfried. **Justiça política: fundamentação de uma filosofia crítica do direito e do Estado/Otfried Hoffe; tradução Ernildo Stein**. 3ª ed. São Paulo: Martins Fontes, 2005.

LIMBERGER, Têmis. **O direito à intimidade na era da informática: a necessidade de proteção dos dados pessoais.** Porto Alegre: Livraria do Advogado, 2007.

LOPES, José Reinaldo de Lima. **O direito na história: lições introdutórias.** 6ª ed. São Paulo: Atlas, 2019.

NETHER, Nicholas Augustus de Barcellos. **Proteção de dados dos usuários de aplicativos.** Juruá, 2018.

PALMA, Rodrigo Freita. **História do Direito.** 5ª ed. São Paulo: Saraiva, 2015.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018 (LGPD).** São Paulo: Saraiva, 2018.

SCALIA, Antonin. **A Matter of Interpretation: Federal Courts and the Law**. Princeton: Princeton University Press, 2018.

SHAPIRO, Scott J. ***Legality***. Cambridge, MA: Harvard University Press, 2011.

SILVA, José Afonso da. **Curso de direito constitucional positivo.** 36ª ed. rev. e atual. São Paulo: Malheiros, 2013.

TEPEDINO, Gustao. **Temas de direito civil.** 4ª ed. Rio de Janeiro: Renovar, 2008

10

A LGPD e o direito do trabalho: uma nova dinâmica na liquidação de pedidos nas ações trabalhistas

Wallace Almeida de Freitas [1]

1. Introdução

A Lei 13.467/2017 alterou o parágrafo primeiro do art. 840 da CLT, acrescentando que o pedido "deverá ser certo, determinado e com a indicação de seu valor"[2]. Tal regra era imposta somente nas ações judiciais processadas pelo rito sumaríssimo, com valor da causa inferior à quarenta salários mínimos. Antes da reforma, em regra, o autor da ação trabalhista atribuía à causa valor superior a quarenta salários mínimos, ainda que sua pretensão econômica com o feito não se equivalesse à quantia apontada. Formada a relação processual e apresentada a defesa e documentos (dados) do contrato de trabalho é que se constataria efetivamente as irregularidades da relação de emprego e suas respectivas mensurações.

A partir da vigência da reforma trabalhista, implementada pela Lei 13.467/2017, impôs-se ao autor da ação trabalhista a obrigação de liquidez

---

[1] *Advogado. Especialista em Direito Imobiliário pela Escola Paulista de Direito – EPD. Presidente da Comissão DTI da OAB Subseção Contagem – MG. Membro da Comissão de Proteção de Dados da OAB/MG.*

[2] BRASIL. DECRETO-LEI N. 5.452, DE 1º DE MAIO DE 1943. DA FORMA DA RECLAMAÇÃO E DA NOTIFICAÇÃO. Art. 840 - A reclamação poderá ser escrita ou verbal. § 1º Sendo escrita, a reclamação deverá conter a designação do juízo, a qualificação das partes, a breve exposição dos fatos de que resulte o dissídio, o pedido, que deverá ser certo, determinado e com indicação de seu valor, a data e a assinatura do reclamante ou de seu representante. (Redação dada pela Lei nº 13.467, de 2017). Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em 24 de junho de 2019.

dos pedidos, sob pena de indeferimento da petição inicial e arquivamento da ação. Em que pese a técnica adotada pelo legislador, a legislação é omissa em relação aos meios para que se afira o valor das irregularidades na relação de emprego. Os documentos (dados) do contrato de trabalho são de posse exclusiva das empresas e o seu não fornecimento na rescisão contratual impede o ex-empregado de adotar tal técnica. Se ao pedido for atribuído valor superior (cheio) ao reconhecido em sentença, poderá o autor ser condenado em honorários advocatícios de sucumbência. Se o pedido for indeferido, corre-se o risco de uma condenação em litigância de má-fé, sem a possibilidade de deferimento da gratuidade de justiça e consequente obrigação de recolhimento de custas processuais e honorários periciais, se houver a prova técnica.

A alternativa encontrada pelos ex-empregados aumentou a litigiosidade[3] entre as partes em razão da necessidade de duas ações judiciais: (**i**) uma para obtenção dos documentos (dados) do contrato de trabalho através da Ação de Produção Antecipada de Provas; (**ii**) outra para indenização das irregularidades cometidas no contrato de trabalho através da Ação Principal – Reclamação Trabalhista, constatadas e quantificadas a partir da cognição dada pelos documentos (dados) da primeira ação.

Diante das irregularidades cometidas por empresas durante o contrato de trabalho a ação trabalhista terá pedidos os quais, para liquidação individualizada, necessitam de documentos (dados) do contrato de trabalho, tais como ficha de registro, fichas financeiras, controles de jornada, contratos de gestão e avaliações de desempenho, estes dois últimos relacionados ao pagamento de participação nos lucros e resultados pelo(a) empregador(a). Estes documentos (dados) são de posse exclusiva das empresas, as quais negam suas disponibilizações aos ex-empregados

[3] Conforme relatório analítico da Justiça do Trabalho, em que pese a distribuição de ações nas varas do trabalho ter reduzido, "no TST, foram recebidos 240.840 casos novos, 16,4% a mais que em 2017. Nos TRTs, foram recebidos 929.030 casos novos, 10,9% a mais que em 2017". Disponível em http://www.tst.jus.br/documents/18640430/24641384/Relatório+Anal%C3%ADtico+2018/80a3fb9b-ca42-dd32-2a7d-89f3092627b7. Acesso em: 3 dez. 2019.

na rescisão contratual. A disponibilização extrajudicial de tais documentos (dados) tem como objetivo o cumprimento integral do quanto exposto no art. 840, parágrafo primeiro da CLT para a distribuição da ação principal.

Indisponíveis os documentos (dados) do contrato de trabalho, impossível se torna a liquidação dos pedidos, como já reconhecido pelo Tribunal Regional do Trabalho da 3ª Região em diversas demandas. Por mais que os pedidos de horas extras sejam certos, a liquidação destes está condicionada à verificação dos controles de jornada para constatação dos dias em que o ex-empregado se ativou em sobrejornada, teve os intervalos inter e intrajornada suprimidos, feriados e repousos semanais remunerados laborados e não compensados. Ou seja, possibilitar o cálculo do pedido estritamente nos dias em que faz jus, ainda que sob análise parcial e subjetiva[4].

Pretendemos apresentar com o presente artigo uma alternativa (solução) para a cognição das irregularidades do contrato de trabalho, identificáveis e indenizáveis à luz da legislação trabalhista, viabilizada pela Lei Geral de Proteção de Dados Pessoais. Partiremos da problematização de se os dados dos empregados nas relações empregatícias se inserem na qualificação de dados pessoais da LGPD.

Nesta esteira buscaremos compreender (**i**) em que consistem os dados dos empregados na relação de emprego, sobretudo aqueles que controlam a jornada (absenteísmo) e desempenho das atividades e funções; (**ii**) se constatada a classificação de determinados dados do contrato de trabalho como dados pessoais, a forma de controle, tratamento e disponibilização destes pelo empregador, tanto na relação contratual, quanto após a extinção do contrato de trabalho e; (**iii**) quais sanções

[4] **PODER JUDICIÁRIO JUSTIÇA DO TRABALHO** – TRIBUNAL REGIONAL DO TRABALHO DA 03ª REGIÃO – 45ª VARA DO TRABALHO DE BELO HORIZONTE – **PAP 0010367-83.2018.5.03.0183** – REQUERENTE: ANA FLAVIA DOS SANTOS REQUERIDO: LOCALIZA RENT A CAR SA Vistos, etc. I. Defiro a petição de produção antecipada da prova. II. Notifique-se o requerido para ciência do presente procedimento e para - no prazo de 5 (cinco) dias - juntar aos autos as provas que entender pertinentes, nos termos do art. 381 e seguintes do CPC, sob pena de serem admitidos como verdadeiros os fatos que, por meio do documento ou coisa, o requerente pretende provar (arts. 382, 398 e 400 do CPC). Ressalte-se que não cabe a este juízo se pronunciar acerca da ocorrência ou não dos fatos, tampouco das consequências jurídicas em caso de não apresentação da documentação requerida, nos termos do que dispõe o art. 382 do CPC. III. Intime-se o requerente para ciência. IV. Após a apresentação, venham os autos conclusos. BELO HORIZONTE, 11 de maio de 2018. HENRIQUE DE SOUZA MOTA Juiz(a) do Trabalho Substituto(a)

impostas aos empregadores diante das irregularidades no controle, tratamento e disponibilização dos dados do contrato de trabalho e o foro competente para a aplicação das sanções.

Na primeira parte deste artigo traçaremos breves considerações sobre a reforma trabalhista com enfoque na liquidação de pedidos das ações judiciais, as omissões do legislador para o cumprimento desta regra e o meio adotado pelos operadores do direito para evitar sanções judiciais pelo excesso no pedido ou até mesmo sua inadequação à realidade do contrato de trabalho sem, no entanto, deixar que se exerça o direito de ação sem a perquirição da realidade do contrato de trabalho, por mero receio de perda do pedido.

Em seguida, analisaremos os aspectos gerais e classificação dos dados pessoais do empregado obtidos pelo empregado, sua forma de controle e tratamento a partir das regras estabelecidas na Lei 13.709/2017 e o dever de disponibilização destes dados.

A terceira parte do artigo é destinada à análise da competência para aplicação da responsabilidade do empregador e o papel da Autoridade Nacional de Proteção de Dados em relação aos dados pessoais obtidos na relação de emprego.

2. Reforma trabalhista: breves considerações

A adequação da legislação trabalhista ao novo contexto socioeconômico esteve longe de ser consensual e ainda hoje é objeto de questionamentos de diversos setores da sociedade, sobretudo daqueles que tiveram suas atividades suprimidas nas relações de emprego, como no caso dos órgãos de representação de classes. A prometida retomada do emprego com a modernização das regras dos contratos de trabalho se revelou como mera expectativa, ante a mantença dos altos níveis de desemprego que assolam a sociedade brasileira.

Ainda assim, houve evolução nas regras das relações de emprego e aumento da técnica nas ações judiciais trabalhistas, como é o caso da regra

de liquidação dos pedidos destas ações. Se antes o empregado tinha a liberdade de acionar o ex-empregador judicialmente e não sofrer ônus econômico, ainda que se tratasse de mera aventura processual, hoje sua responsabilidade foi aumentada, seja pelo rigor a ser adotado no conhecimento do pedido a ser feito e sua consequente mensuração, seja pelas sanções que lhe são impostas pelo acionamento judicial do ex-empregador por mera expectativa de direito. Custas judiciais, honorários periciais e advocatícios de sucumbência e até mesmo condenação por litigância de má-fé são consequências que precisam ser observadas antes do ajuizamento da ação.

Não obstante o critério escolhido pelo legislador na determinação de atribuição de valores aos pedidos das ações judiciais trabalhistas, o ex-empregado se vê num limbo jurídico com sua expectativa de reparação das irregularidades do contrato de trabalho, antes constatadas após a fase de contestação, onde tinha oportunidade de perquirir a documentação do contrato de trabalho através da impugnação fundamentada dos documentos que geriram suas atividades. A regularidade de banco de horas previsto em norma coletiva só pode ser constatada com o detalhamento da jornada diária de trabalho, comumente registrada pelas empresas em controles eletrônicos. A evolução salarial, proventos e descontos só podem ser aferidos através das fichas financeiras e fichas de registros de empregados. O desempenho das funções e atividades mensurados pelo empregador para pagamento de participação nos resultados não pode ser refutado sem o acesso e conhecimento de contratos de gestão e avaliações de desempenho.

Estes dados, por sua vez, não são compartilhados pelo empregador durante o contrato de trabalho, tão menos disponibilizados aos ex-empregados na rescisão contratual, impossibilitando a liquidação dos pedidos na competente ação judicial trabalhista.

A medida processual encontrada pelos operadores de direito fora a Ação de Produção Antecipada de Provas (CPC, arts. 381 e seguintes). A referida medida cautelar, tecnicamente, proporciona acesso aos

documentos (dados) do contrato de trabalho e, verificadas irregularidades, o apontamento específico e a apuração dos respectivos valores das irregularidades e sua consequente ação judicial. Não verificadas irregularidades ou verificada a inviabilidade econômica da ação principal tem o operador do direito elementos técnicos para o convencimento da parte da improcedência da demanda.

3. Liquidação dos pedidos na ação trabalhista

Os documentos (dados) do contrato de trabalho são de posse exclusiva das empresas, os quais não se tem conhecimento de disponibilização durante o contrato de trabalho, jamais conferindo aos empregados a possibilidade de obtenção de cópia, ainda que em formato eletrônico[5]. Nas dispensas do contrato de trabalho, com ou sem justa causa, são entregues somente documentos que põem fim a relação de emprego e conferem ao ex-empregado *status* para recebimento do FGTS e Seguro Desemprego.

O pedido de antecipação de provas basea-se no fato de que, por mais que os pedidos de horas extras sejam certos, a liquidação destes pedidos está condicionada à verificação dos controles de jornada para constatação dos dias em que o ex-empregado se ativou em sobrejornada, teve os intervalos inter e intrajornada suprimidos, feriados e repousos semanais remunerados laborados e não compensados. Os contratos de gestão e avaliações de desempenho, por sua vez, são indispensáveis à análise dos pagamentos da Participação nos Lucros e Resultados. A liquidação individualizada dos pedidos necessita da ficha de registro, fichas

[5] **PODER JUDICIÁRIO JUSTIÇA DO TRABALHO** – TRIBUNAL REGIONAL DO TRABALHO DA 03ª REGIÃO – 7ª VARA DO TRABALHO DE BELO HORIZONTE – **PAP 0010071-07.2018.5.03.0007** – REQUERENTE: DORALICE DA COSTA AMORIM REQUERIDO: LOCALIZA RENT A CAR SA DESPACHO. Vistos. Considerando-se que a ré **não nega possuir os documentos**, **não lhe compete decidir se a reclamante necessita ou não da documentação para interposição da ação principal**. Determina-se, pois, que a reclamada apresente os documentos requeridos pela autora, em 48 horas, sob pena de multa diária de R$ 500,00 (quinhentos reais) até o limite de R$ 50.000,00 (cinquenta mil reais). Intime-se. Cumprida a determinação supra, intime-se a autora para vista dos documentos apresentados pela ré, em 05 dias úteis. Após, façam-se os autos conclusos. BELO HORIZONTE, 27 de fevereiro de 2018. JURACI GONCALVES JUNIOR (sem destaques no original).

financeiras, controles de jornada, contratos de gestão e avaliações de desempenho.

Os documentos (dados) do contrato de trabalho preenchem o quanto estabelecido no art. 381 do Código de processo Civil, considerando que, para sua produção antecipada: (**i**) são "próprios" ou "comuns"; consistem em documentos criados e utilizados pela empresa para controle e registro dos atos praticados no contrato de trabalho – registro do empregado, reajustes, férias, afastamentos médicos, controle da frequência e jornada desempenhada e controle do desempenho, atribuindo notas para consequente pagamento de participação nos resultados; (**ii**) encontram-se em poder exclusivo das empresas (cointeressada), tanto em formato físico, quanto eletrônico; (**iii**) o "risco de perecimento", haja vista não se conhecer a forma de armazenamento.

A produção antecipada de provas tem sido o meio adequado à cognição da parte das supressões ocorridas no contrato de trabalho[6]. De sua análise, restando evidenciadas as irregularidades, serão os pedidos coerentes com o direito pretendido[7]. As horas extras realizadas antes e depois da jornada prevista somente terão seus pedidos concretizados nos

[6] **PODER JUDICIÁRIO JUSTIÇA DO TRABALHO** – TRIBUNAL REGIONAL DO TRABALHO DA 03ª REGIÃO – 7ª VARA DO TRABALHO DE BELO HORIZONTE – **PAP 0010071-07.2018.5.03.0007** – REQUERENTE: DORALICE DA COSTA AMORIM REQUERIDO: LOCALIZA RENT A CAR SA DESPACHO. Vistos. Considerando-se que a ré **não nega possuir os documentos**, **não lhe compete decidir se a reclamante necessita ou não da documentação para interposição da ação principal**. Determina-se, pois, que a reclamada apresente os documentos requeridos pela autora, em 48 horas, sob pena de multa diária de R$ 500,00 (quinhentos reais) até o limite de R$ 50.000,00 (cinquenta mil reais). Intime-se. Cumprida a determinação supra, intime-se a autora para vista dos documentos apresentados pela ré, em 05 dias úteis. Após, façam-se os autos conclusos. BELO HORIZONTE, 27 de fevereiro de 2018. JURACI GONCALVES JUNIOR (sem destaques no original).

[7] **PODER JUDICIÁRIO JUSTIÇA DO TRABALHO** – TRIBUNAL REGIONAL DO TRABALHO DA 03ª REGIÃO – 36ª VARA DO TRABALHO DE BELO HORIZONTE – **PAP 0010081-52.2018.5.03.0136** – REQUERENTE: ANA PAULA DE OLIVEIRA SOUZA CASTANHEIRA REQUERIDO: LOCALIZA RENT A CAR SA PROCESSO:0010081-52.2018.5.03.0136 C O N C L U S Ã O - Pje-JT Nesta data, faço os autos conclusos ao MM Juiz do Trabalho. BELO HORIZONTE, 19 de fevereiro de 2018. IANDRA SALVIANO ARAUJO D E S P A C H O - Pje-JT Tratando-se de ação de produção antecipada de provas fundamentada no inciso III do artigo 381 do CPC, de aplicação subsidiária ao Processo do Trabalho, não se exige a comprovação de urgência para se aferir o interesse jurídico da Parte Autora na medida. Assim, determino a citação da Parte Reclamada para que exiba, no prazo de 30 dias, os documentos requeridos pela Parte Autora na inicial. Caso a Parte Ré alegue que os documentos requeridos pela Parte Reclamante não existem, siga-se o procedimento determinado no art. 398, § único, aplicável analogicamente ao caso vertente, designando audiência de instrução, se for o caso. Por outro lado, cumprida a determinação, proceda-se à extinção do processo, tendo em vista que, nos termos do art. 381, §3º, do CPC, "A produção antecipada da prova não previne a competência do juízo para a ação que venha a ser proposta".Cumpra-se. BELO HORIZONTE, 19 de fevereiro de 2018. GERALDO MAGELA MELO Juiz(a) do Trabalho Substituto(a)

períodos que não foram compensadas ou pagas. Como consequência, o valor dado ao pedido, na forma do art. 840, parágrafo primeiro da CLT será condizente (proporcional) com a ilegalidade cometida. Também o será o valor apurado em reflexos.

Não há possibilidade de preenchimento do requisito processual de atribuição dos valores aos pedidos sem análise prévia da documentação. As decisões recentes consideram, primeiramente, que o valor dado à causa será a soma dos pedidos indicados pelo autor na petição inicial, sendo que tal valor será o teto máximo de eventuais condenações e indenizações na demanda e, por conseguinte, se o valor atribuído à causa não se apresentar adequado à natureza e extensão dos pedidos deduzidos na petição inicial, a irregularidade resultará na extinção do processo sem resolução de mérito e no arquivamento do feito[8]. Este entendimento já era adotado antes mesmo da vigência da Lei 13.467/2017 (Reforma Trabalhista)[9]. Os

[8] **PODER JUDICIÁRIO JUSTIÇA DO TRABALHO TRIBUNAL REGIONAL DO TRABALHO DA 03ª REGIÃO** 1ª Vara do Trabalho de Pedro Leopoldo RTOrd 0010041-08.2018.5.03.0092 AUTOR: ELSON DE SOUZA AMENO RÉU: GABRIEL SALES - FAZENDA DOS BORGES, MINERACAO FAZENDA DOS BORGES LTDA Vistos os autos**, Conforme o disposto no artigo 840, §1º, da CLT**, com a redação dada pela Lei nº 13.467/2017, **a reclamação** escrita **deverá conter**, dentre outras, a breve exposição dos fatos de que resulte o dissídio, **o pedido**, que deverá ser certo, determinado e **com indicação de seu valor**, sob pena de extinção sem resolução do mérito (§3º). Assim, **as ações propostas a partir da vigência da Lei nº 13.467/2017 devem** conter também o valor do pedido, isto é, devem **ser líquidas**, além da necessidade dele ser certo e determinado. Desse modo, como já ocorre no procedimento sumaríssimo (art. 852-B, §1º, CLT), também no ordinário **caberá ao reclamante atribuir valor a cada um dos pedidos que fizer, sob pena de extinção do processo, sem resolução do mérito (art. 840, §3º, CLT)**. Analisando a petição inicial, constata-se que o reclamante não liquidou o pedido referente ao pagamento de horas extras decorrentes da supressão do intervalo intrajornada, violando o disposto no artigo 840, §1º, CLT. Diante do exposto, verificando que a petição inicial não atende a um dos requisitos legais, **julgo extinto o processo sem resolução de mérito, nos termos do artigo 485, IV, CPC**. Vale ressaltar, ainda, que o reclamante não juntou o instrumento de procuração outorgado a seu advogado, em descumprimento ao disposto no artigo 103 e seguintes do CPC/2015. Defiro o benefício da justiça gratuita à parte autora, uma vez que a remuneração descrita na cópia do TRCT (Id 6fe1ccf) demonstra o recebimento de salário inferior a 40% do limite máximo dos benefícios do Regime Geral de Previdência Social (art. 790, §3º, CLT). Custas pela parte autora, no importe de R$ 790,00, calculadas sobre o valor dado à causa (R$ 39.499,98), ISENTA. Retire-se o processo de pauta e intime-se o reclamante. PEDRO LEOPOLDO, **19 de Janeiro de 2018**. DANIEL FERREIRA BRITO Juiz(a) do Trabalho Substituto(a). (sem destaques no original).

[9] **PODER JUDICIÁRIO JUSTIÇA DO TRABALHO TRIBUNAL REGIONAL DO TRABALHO DA 03ª REGIÃO 35ª VARA DO TRABALHO DE BELO HORIZONTE RTOrd 0011558-16.2017.5.03.0114 AUTOR: LILIAN ALVES SACRAMENTO GUEDES RÉU: LOCALIZA RENT A CAR SA**

CONCLUSÃO Cumprimento a determinação verbal de V. Exa., faço os presentes autos conclusos. Belo Horizonte, 13 de novembro de 2017. Carmélia Andalécio - Analista Judiciário. Vistos etc. Convalido os termos da conclusão supra, embora não assinada digitalmente. Conforme se depreende do art. 292 do CPC, **o valor da causa constará sempre da petição inicial e será, havendo cumulação de pedidos, a quantia correspondente à soma dos valores de todos eles**. Diante disso, vê-se que **há uma regra para se apontar o valor da causa**. Não há que se falar em escolha de rito pela parte autora. A legislação trabalhista é clara: os dissídios individuais cujo valor não exceda a 40 vezes o salário mínimo vigente na data do ajuizamento da reclamação ficam submetidos ao procedimento sumaríssimo (art. 852-A da CLT). Observados os dois dispositivos legais supra apontados, **vê-se que a petição inicial da forma como**

pedidos liquidados de forma cheia, ou seja, além do que é devido, sem apuração real e, por conseguinte, somados e indicados ao valor da causa, se excessivos, poderão ensejar em condenação por litigância de má-fé[10]:

Aplicada a Lei 13.467 de 2017, ainda serão utilizados na base de cálculos para incidência de honorários periciais, honorários de sucumbência e custas processuais. Por outro lado, se liquidados aquém do que realmente é devido, poderá ensejar em prejuízo à parte por limitação do valor do teto da condenação, comprometendo assim o seu acesso à justiça.

Analisados os pedidos através dos documentos do contrato de trabalho, mormente os controles eletrônicos de jornada e fichas financeiras, a dialética processual na ação principal, acaso proposta, será produzida a partir de documentos pertinentes às duas partes, produzidos

---

apresentada, sem valores de pedidos, leva o pleito ao rito sumaríssimo. Observado o art. 852-B, caput, da CLT, e seu inciso I, o pedido deverá ser certo ou determinado e indicará o valor correspondente, o que, se não for atendido pela parte autora, levará o processo ao arquivamento (Art. 852-B, parágrafo primeiro). Por conseguinte, **uma vez que não foram apresentados os valores de cada pedido**, ou ao menos o valor de um pleito que demonstre que o processo deve correr pelo rito ordinário, o seu somatório não excede os 40 salários mínimos. Tem-se, pois, que o processo corre pelo rito sumaríssimo e, assim, **por não ter o autor da ação cumprido o disposto no inciso I do art. 852-B da CLT, cumpro o disposto no parágrafo primeiro de tal artigo, arquivando a reclamatória**. Retire-se o feito de pauta. Custas, pelo(as) reclamante(s), no suporte de R$10,64, calculadas sobre R$532,00, valor mínimo das custas processuais, nos termos do art. 789 da CLT. Isento(as). Dê-se ciência a(os) reclamante(s) e reclamado(as). Após, arquivem-se os autos. BELO HORIZONTE, 22 de Novembro de 2017. MARCO TULIO MACHADO SANTOS Juiz(a) Titular de Vara do Trabalho (sem destaques no original).

[10] **NJ - Produção antecipada de provas é cabível para viabilizar liquidação de pedidos da ação trabalhista principal** publicado 02/08/2018 00:17, modificado 02/08/2018 00:17. O TRT mineiro, em voto da relatoria da juíza convocada Gisele de Cássia Vieira Dias Macedo, julgou favoravelmente o recurso apresentado por uma trabalhadora contra uma locadora de veículos, buscando o reconhecimento de seu direito à produção antecipada de provas. Ela alegou que, para ajuizamento da ação trabalhista principal, deveria efetuar a liquidação separada dos pedidos, necessitando da ficha de registro, fichas financeiras, controles de jornada, contratos de gestão e avaliações de desempenho. Justificou seu pedido diante da indisponibilidade desses documentos e da consequente impossibilidade de liquidação dos pedidos. Entendendo desnecessária a medida proposta, o juízo de 1º grau extinguiu o processo sem resolução do mérito, nos termos do artigo 485, VI, do CPC, por falta de interesse processual. Mas esse não foi o entendimento da relatora do recurso, que considerou justificada a ação no tocante à liquidação dos pedidos, já que a lei exige que o pedido deve ser certo, determinado e com indicação de seu valor, dentre outras exigências (artigo 840, §1º, da CLT). **Nesse contexto, e citando julgados no mesmo sentido, a julgadora entendeu que, para se verificar a efetiva jornada cumprida, inclusive o trabalho em dias de repousos e feriados, bem como o pagamento das horas extras realizadas e da PLR de 2017, será imprescindível a juntada aos autos dos controles de jornada, da ficha de registro de empregado, fichas financeiras e contratos de gestão e avaliações de desempenho, justificando a produção antecipada de provas requerida pela ex-empregada**. Por fim, a relatora frisou que a medida poderá, inclusive, viabilizar a autocomposição, justificar ou evitar o ajuizamento de ação. Portanto, determinou o retorno do processo à Vara de origem para seu regular prosseguimento. O entendimento foi acompanhado pelos demais julgadores da 6ª Turma. **Processo PJe: 0010275-14.2018.5.03.0181** (ROPS) — Acórdão em 05/06/2018 (sem destaques no original). Disponível em https://portal.trt3.jus.br/internet/conheca-o-trt/comunicacao/noticias-juridicas/nj-producao-antecipada-de-provas-e-cabivel-para-viabilizar-liquidacao-de-pedidos-da-acao-trabalhista-principal. Acesso em 19/10/2018.

pela empresa e infirmada sua validade pelo ex-empregado. Como consequência, a celeridade processual prevalecerá, além de uma perfeita cognição levada ao Juízo, o qual pronunciará uma decisão equânime.

O que se pretende com os documentos (dados), como exposto, é obter um lastro probatório mínimo, já que a posterior liquidação dos pedidos na ação principal, com a prova documental obtida antecipadamente, possibilitará a apuração dos direitos suprimidos e o preenchimento do requisito contido no artigo 840, parágrafo primeiro da CLT, a autocomposição entre as partes ou ainda a verificação da inviabilidade da ação principal, vez que haverá a possibilidade daqueles pedidos alegados pelo autor não serem confirmados na prática, quando compulsados os documentos (dados) do contrato de trabalho.

A liquidação dos pedidos é ato complexo, consubstanciado em documentos (dados) fidedignos, envolvendo ainda resoluções, portarias, dentre outras regras, para sua elaboração. Correção monetária, reflexos em FGTS, recolhimentos previdenciários devem ainda compor os pedidos. Ou seja, a liquidação dos pedidos seguirá as mesmas regras de liquidação de sentença. Se para a segunda os documentos (dados) do contrato de trabalho são imprescindíveis, na primeira não será diferente.

Novamente, em termos práticos, o conhecimento antecipado das provas possibilitará técnica, dialética processual consubstanciada em documentos, uma tutela jurisdicional mais precisa, sem subjetividades ou atos protelatórios. Este foi o sentido da reforma trabalhista que, em que pese posições a favor ou contra, primou por um processo mais justo, com foco exclusivo no jurisdicionado.

4. Consequências do indeferimento do pedido: litigância de má-fé, custas processuais e honorários advocatícios de sucumbência

Apesar da nova dinâmica processual na liquidação de pedidos implicar em um processo mais técnico, o rigor imposto pela regra de atribuição de valor a cada um dos pedidos e seus respectivos reflexos gera

um desequilíbrio jurídico. É que no pacote de alterações do direito material e processual trabalhista foi incluída a condenação das partes sucumbentes em honorários advocatícios e o deferimento da gratuidade de justiça está condicionado à real situação econômica do autor da ação. Indeferida a gratuidade de justiça estará o autor da ação sujeito ao pagamento das custas processuais e honorários advocatícios de sucumbência. Mas a consequência prática não para por aí. Indeferido o pedido, poderá o autor ainda ser condenado por litigar de má-fé. O pedido de horas extras além da jornada normal de trabalho, por exemplo, caso indeferido, poderá implicar em litigância de má-fé, com consequente condenação da parte sucumbente em honorários advocatícios de até 15% do valor do pedido, além das custas processuais, ainda que outros pedidos tenham sido deferidos.

Adentrar no mérito do grau de exigência da legislação trabalhista e da flexibilização das condenações das partes pela inobservância dos critérios objetivos da ação é tarefa difícil, construída pela dialética da operação do direito, que requer tempo. Contudo, nos parece sem resposta a operacionalização de tais regras e de difícil acatamento por vias céleres.

A CLT impôs um conjunto de regras objetivas para o processamento da reclamação trabalhista, como a aqui problematizada – liquidação dos pedidos na ação trabalhista – sem oferecer, na mesma medida, institutos para sua consecução. Para tanto, a Produção Antecipada de Provas prevista no CPC tem sido a via (processual) adotada pelas partes na relação de emprego que pretendem demandar em juízo. Uma ação judicial para cognição das condições do contrato de trabalho para ajuizamento de outra ação judicial para reparação de possíveis irregularidades.

Com a vigência da nova legislação trabalhista uma nova regra fora imposta ao autor da reclamação trabalhista sem que lhe fosse, também, proposto o caminho para cumprimento desta nova regra. Apesar de o Código de Processo Civil possuir medida alternativa para o cumprimento da regra da liquidação do pedido, ainda assim não resolve o problema da situação, em que após a apresentação dos documentos (dados) do contrato

de trabalho se verifica a impossibilidade ou inviabilidade econômica de uma reclamação fadada ao insucesso e com grandes chances de condenações por litigância de má-fé, custas processuais e de honorários de sucumbência.

Entendemos que a Lei Geral de Proteção de Dados fornecerá a solução adequada a esta lacuna que a nova legislação trabalhista submeteu o reclamante. Isso, por óbvio, considerando que os dados obtidos do(a) empregado(a) durante o contrato de trabalho sejam relacionados como dados pessoais pela Lei 13.709/2018.

É ao que nos dedicaremos na segunda parte deste trabalho.

5. Dados pessoais e a relação de emprego: controle, tratamento e sujeito de dados

A Lei Geral de Proteção de Dados é a primeira lei brasileira voltada especificamente à regulação da obtenção e tratamento de dados pessoais. Antes de sua edição a regulação era através de "microsistemas de proteção de dados pessoais", tais como o CDC e o Marco Civil da Internet[11].

O conceito de dado pessoal pode ser extraído da própria LGPD, que o define como "informação relacionada a pessoal natural identificada ou identificável" (art. 5º, I). Os sistemas de tecnologia proporcionam o agrupamento de dados pessoais para que, a partir de um conjunto de informações, se faça inferências e se delibere sobre o resultado obtido com este tratamento[12]. O mesmo ocorre com o "tratamento" de dados pessoais, onde o inciso X do artigo 5º descreve todas as características desta etapa, tais como coleta, armazenamento, utilização e eliminação[13].

---

[11] PARENTONI, Leonardo; LIMA, Henrique. *Protection of Personal Data in Brazil: Internal Antinomies and International Aspects*. DO-10.2139/ssrn.3362897JO-SSRN Electronic Journal. Disponível em https://www.researchgate.net/publication/332890732_Protection_of_Personal_Data_in_Brazil_Internal_Antinomies_and_International_Aspects. Acesso em 30 de junho de 2019.

[12] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019. p. 38. Portanto, que um banco de dados deve ser necessariamente atrelado à ideia de um sistema de informação, cuja dinâmica explicita, sequencialmente, um processo que se inicia pela coleta e estruturação dos dados, perpassa a extração da informação que, por fim, agrega conhecimento.

[13] BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. 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,

As informações geradas pelo empregado nas relações de emprego, no desempenho das atividades e funções do contrato de trabalho se revestem integralmente, em nosso sentir, das definições de dado pessoal, coleta e tratamento dadas pela Lei 13.709/2018. Os dados pessoais do empregado obtidos no momento da contratação são estruturados em arquivo próprio do empregador, comumente em documento denominado ficha de registro. Em tal documento são inseridos dados ao longo do contrato de trabalho, tais como férias e seus respectivos períodos aquisitivos e concessivos, evoluções salariais, promoção de cargos, afastamentos médicos e exames clínicos periódicos.

A jornada de trabalho é a atividade do contrato com maior controle do empregador, sendo o fator preponderante para o pagamento de salário, por exemplo. Em regra, o controle de jornada é realizado por meio eletrônico[14], gerando um histórico completo e em tese irrefutável das atividades do empregado dentro ou fora da empresa. São registradas as entradas, intervalos e pausas, saída, frequência semanal, ou seja, todo o histórico cronológico em dado período. Os dados gerados no controle de jornada permitem ao empregador análise tanto de questões legais, quanto de gestão de mão de obra e recursos humanos. A aferição da jornada diária de trabalho para fins de compensação ou pagamento de horas extras, a fruição de intervalos e pausas legais, tais como as dos artigos 71 (alimentação e descanso) e 384 (intervalo da mulher), ambos da CLT são exemplos de dados e inferências geradas pelo referido controle.

Outras informações específicas são geradas pelo empregado no desempenho de suas funções e atividades, a depender do objeto social

utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[14] PORTARIA Nº 1.510, DE 21 DE AGOSTO DE 2009. Publicada no DOU de 25/08/2009. O MINISTRO DE ESTADO DO TRABALHO E EMPREGO, no uso das atribuições que lhe conferem o inciso II do parágrafo único do art. 87 da Constituição Federal e os arts. 74, § 2º, e 913 da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, RESOLVE: Art. 1º Disciplinar o registro eletrônico de ponto e a utilização do Sistema de Registro Eletrônico de Ponto - SREP. Parágrafo único. Sistema de Registro Eletrônico de Ponto - SREP - é o conjunto de equipamentos e programas informatizados destinado à anotação por meio eletrônico da entrada e saída dos trabalhadores das empresas, previsto no art. 74 da Consolidação das Leis do Trabalho - CLT, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943.

desenvolvido pelo empregador. O programa de participação nos resultados da empresa, por exemplo, gera dados específicos de avaliação de desempenho que aferem o cumprimento de metas para o recebimento do montante estipulado para tal verba. Ainda assim, a dinâmica nos parece ser a mesma. Obtenção de dados pessoais do empregado desde o processo seletivo para o cargo, inserção de dados deste em sistema próprio, controle da jornada e frequência de trabalho, das metas, controle financeiro, controle via GPS quando desempenhada atividade fora da sede social do empregador. Em síntese, o empregado tem monitorada toda sua atividade no desempenho de suas funções.

Dado o limite deste artigo não nos é permitido fazer um juízo da legalidade da obtenção destes dados e a responsabilização do empregador nos excessos da sua coleta, tratamento e disponibilização. Partimos do pressuposto que a obtenção, controle e tratamento destes dados se dê nos limites da Lei e se faça para um melhor desempenho e competividade no mundo dos negócios. O judiciário, mormente a justiça do trabalho, tem tratado as exceções com rigor e preenchido com prudência as lacunas deixadas pelo legislador. Consideramos que a obtenção dos dados atende às duas partes da relação de emprego, pois se assim não o fosse não teria o empregado meios de acompanhar o desempenho de suas funções e fazer frente às irregularidades que porventura surjam. É o caso da compensação de jornada, em que a ausência de uma base de dados centralizada e única impossibilitaria às partes a compensação das horas trabalhadas além ou aquém da jornada prevista.

6. LGPD e jurisdição trabalhista: o papel da autoridade nacional de proteção de dados nas relações de emprego

Os dados gerados pelo empregado no contrato de trabalho, em que pese obtidos, controlados e tratados pelo empregador para gestão dos recursos humanos do negócio desenvolvido, se inserem no contexto da proteção dos dados pessoais regulada pela Lei 13.709/2018. Portanto, o

empregador deve adequar sua atividade empresarial não só no que se refere a dados pessoais de clientes e fornecedores, mas também de todos os empregados, especificando desde o início da relação contratual quais dados serão obtidos, controlados, tratados, armazenados e, sobretudo, disponibilizados.

Se hoje é uma faculdade do empregador disponibilizar os dados do ex-empregado, porquanto não imposta nenhuma sanção pela legislação trabalhista ou processual pela negativa de acesso extrajudicial aos dados, tal não mais o assistirá a partir da vigência da LGPD, cujas sanções variam desde advertência até multa pecuniária que pode alcançar o montante de R$ 50.000.000,00 (Art. 52). A aplicação das sanções, no entanto, está condicionada a procedimento administrativo.

Em termos práticos, para eficácia da Lei Geral de Proteção de Dados Pessoais nas relações de emprego, o papel da Autoridade Nacional de Proteção de Dados é mais que relevante na edição de normas e procedimentos neste aspecto (art. 55-J, II). A ausência normativa sobre os dados pessoais em contratos de trabalho favorece uma das partes do contrato e não viabiliza a solução de demandas por outra via que não a judicial. A edição de tais normas necessita de análise empírica das relações de emprego para conhecimento, sistematização, categorização deste tipo de relação jurídica e incidência da norma.

O poder judiciário trabalhista também tem papel preponderante nesta fase, sobretudo pelas inferências que seu histórico de dados das demandas pode fornecer. São extensas as possibilidades de inferências a partir dos dados da justiça do trabalho através de jurimetria, por exemplo. O processo judicial trabalhista tramita há alguns anos em plataforma eletrônica, onde os dados das ações são estruturados.

7. Conclusão

As ações trabalhistas sofreram significativas alterações com o advento da reforma trabalhista a partir de novembro de 2017, impondo às

partes maior técnica no ajuizamento das reclamações, em especial ao autor da ação que tem o dever de certeza e quantificação dos pedidos. Evitamos juízos de valor favoráveis ou contra as regras de liquidação dos pedidos, focando nos termos práticos do seu cumprimento, buscando alternativas de cognição do contrato de trabalho, o que atualmente é feito pela via judicial da Ação de Produção Antecipada de Provas do Código de Processo Civil.

A regra de liquidação dos pedidos do parágrafo primeiro do art. 840 da CLT não pode ser cumprida pelo autor da ação quando o acesso aos documentos do contrato de trabalho lhe é negado pelo ex-empregador. A referida Ação de Produção Antecipada de Provas foi a alternativa encontrada pelos operadores de direito para cognição dos documentos do contrato de trabalho e constatação específica das irregularidades cometidas, quantificando-as por meio de liquidação, nos mesmos moldes daquela realizada para a sentença transitada em julgado para, por fim, distribuir a Reclamação Trabalhista.

Apresentado este cenário, demonstramos que a Reforma Trabalhista fora omissa quanto a forma de cumprimento do requisito objetivo de liquidação dos pedidos e, tão menos, há na legislação qualquer sanção imposta ao empregador que nega acesso extrajudicial ao ex-empregado aos documentos do contrato de trabalho. Neste contexto, o trabalhador, parte hipossuficiente nesta relação jurídica, se vê num limbo jurídico. Sua hipossuficiência fora mitigada, junto com a inversão do ônus probatório. Custas processuais, honorários advocatícios de sucumbência e até mesmo condenação em litigância de má-fé são possíveis consequências da falta de técnica no ajuizamento da ação.

A CLT reformada não resolveu o problema da regra de liquidação. O Código de Processo Civil proporciona a solução parcial, mas pela via judicial, o que se mostra contraproducente. A medida cautelar tem se tornado a regra para Reclamações Trabalhistas. Uma ação judicial para outra ação judicial.

Considerados os dados do contrato de trabalho como dados pessoais, a solução a ser adotada é a de notificação do ex-empregador para disponibilização dos documentos do contrato de trabalho, amparado pela Lei Geral de Proteção de Dados, posto que os dados gerados pelo empregado se inserem no contexto da Lei 13.709/2018. Tal questão por si só não encerra a negativa da empresa de acesso aos dados do contrato de trabalho: a vigência da Lei somente no segundo semestre de 2020 e a falta de normas específicas para a relação de emprego são questões a serem enfrentadas.

Neste contexto, é necessário que a Autoridade Nacional de Proteção de Dados – ANPD edite normas voltadas especificamente para os dados pessoais obtidos no contrato de trabalho, sua forma de controle, tratamento e disponibilização. Uma ação conjunta com o Ministério do Trabalho e Emprego e o Poder Judiciário proporcionarão um novo direcionamento nestas relações jurídicas, com consequente pacificação social.

Ousamos afirmar que o acesso aos dados do contrato de trabalho terá o mesmo efeito que a reforma trabalhista de redução das ações judiciais. A liquidação dos pedidos trouxe maior técnica para a ações e o acesso aos documentos do contrato de trabalho a sedimentará. Muitas destas se mostram inviáveis economicamente para o ex-empregado que imaginava há época de sua distribuição fazer jus a diversos pedidos. Somente após o acesso aos documentos, depois de apresentada a defesa, é que se constatava efetivamente a irregularidade e que esta fora a exceção.

A Lei Geral de Proteção de Dados Pessoais, portanto, é o remédio extrajudicial para solução de um requisito processual, sem custo, célere e que em grande parte dos contratos de trabalho excluirá a possibilidade de uma Reclamação Trabalhista, posto permitir uma cognição completa do cumprimento da legislação nas relações de emprego. As ações judiciais tratarão especificamente das irregularidades cometidas, com provas objetivas, reduzindo o grau de litigiosidade nas demandas ajuizadas,

sobretudo pelo litígio se fundar em documentos, restringindo provas de outras naturezas às exceções.

8. Referências

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2019

BRASIL. DECRETO-LEI N. 5.452, DE 1º DE MAIO DE 1943. DA FORMA DA RECLAMAÇÃO E DA NOTIFICAÇÃO. Art. 840 - A reclamação poderá ser escrita ou verbal. § 1º Sendo escrita, a reclamação deverá conter a designação do juízo, a qualificação das partes, a breve exposição dos fatos de que resulte o dissídio, o pedido, que deverá ser certo, determinado e com indicação de seu valor, a data e a assinatura do reclamante ou de seu representante. (Redação dada pela Lei nº 13.467, de 2017). Disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em 24 de junho de 2019.

PARENTONI, Leonardo; LIMA, Henrique. *Protection of Personal Data in Brazil: Internal Antinomies and International Aspects*. DO-10.2139/ssrn.3362897JO-SSRN Electronic Journal. Disponível em https://www.researchgate.net/publication/332890732_Protection_of_Personal_Data_in_Brazil_Internal_Antinomies_and_International_Aspects. Acesso em 30 de junho de 2019.

11

A concepção de privacidade através dos tempos: do rupestre à Lei Geral de Proteção de Dados Pessoais

João Lucas Vieira Saldanha [1]

1 Introdução

O direito à privacidade sempre foi algo difícil de se definir com clareza e objetividade, até, porque, à medida que os instrumentos de difusão de dados e informações se tornaram mais poderosos e acessíveis, a própria concepção do que é privacidade sofreu mutações dentro daquilo que o paradigma ao qual se inseria permitia.

Apenas a título de exemplificação, se numa era anterior às revoluções industriais bastava se ocultar fisicamente para garantir a "privacidade", a cada inovação científica na comunicação e no monitoramento, mesmo no que tange a tecnologias "pré-digitais", a ideia de isolamento ou anonimato se tornou mais frágil diante da facilitação da rastreabilidade e do registro dos indivíduos, suas ações, propriedades e características.

A verdade é que desde que o primeiro desenho rupestre ilustrou um indivíduo determinado realizando uma tarefa que o distinguia dos demais, nasceu o conceito de registro de dado pessoal.

Pode parecer exagero a princípio, mas um olhar mais sensível revelará que o primeiro banco de dados da história da humanidade –

[1] João Lucas Vieira Saldanha é advogado especialista em Proteção de Dados, Direito Digital e Compliance; Sócio Fundador do escritório "Saldanha & Gualtieri – Advogados Associados", Sócio e Data Protection Officer na empresa "Tripla", membro da Comissão de Proteção de Dados da OAB/MG, do "ISACA - Information Systems Audit and Control Association", ISFS, PDPF, PDPP e DPO pela EXIN Holanda; consultor de privacidade e proteção de dados, pesquisador e autor de diversos artigos sobre o tema.

externo às nossas próprias mentes, é claro – foram as paredes das cavernas. Quando histórias eram contadas e marcadas na rocha para que pudessem ser consultadas e replicadas posteriormente, o que tínhamos era um verdadeiro precursor dos livros, cadernos, e, por que não dizer, dos discos rígidos.

Evidentemente que na idade da pedra a possibilidade de se traçar um paralelo entre indivíduo e sua representação rupestre era muito baixa, mas à medida em que os métodos de registro de dados foram se refinando, passando pelos papiros, pergaminhos, livros, e, por fim, computadores, temos que se tornou mais simples relacionar pessoa a dado pessoal, ao ponto em que hoje em dia um sistema é capaz de identificar o seu usuário até mesmo por padrões de digitação.

Neste cenário, a pergunta que surge, inevitavelmente, é: como proteger a privacidade individual em uma sociedade informacional em que nossas relações se pautam justamente na constante e acelerada troca de dados? Ou, mais do que isso: como garantir que seus dados pessoais sejam preservados, ressalvada a sua intimidade, sendo que a todo momento os mesmos são coletados, processados, tratados e difundidos?

Diante deste contexto restaram duas opções para a humanidade: refrear o desenvolvimento das tecnologias de tratamento e compartilhamento de dados pessoais, o que, honestamente, nunca foi uma opção de fato, ou adaptar a própria concepção de privacidade.

Durante séculos a concepção de privacidade esteve entrelaçada com o conceito de intimidade, ou daquilo que é privado, como, de fato, a morfologia da palavra aponta. Tínhamos, portanto, que a privacidade gerava e decorria da escolha de "não integrar", do segredo ou até do anonimato em si. Inclusive, essa ideia por muito tempo resultou na defesa de que o anonimato era algo de direito, sendo que referida ideia deu origem, inclusive, a direitos como aquele do esquecimento.

Ocorre que, como dito, não seria viável defender que a privacidade estivesse ligada ao anonimato em um contexto socio-tecnológico no qual quase todas as relações interpessoais, comerciais, profissionais,

acadêmicas e de bens e serviços se baseiam, justamente, na difusão e transparência de dados e informações pessoais, já que na sociedade informacional a velocidade de transmissão de dados constitui um dos mais valiosos e fundamentais elementos do desenvolvimento.

Mas então como promover a privacidade dentro de um paradigma de tamanha exposição? A ideia aqui é que a própria concepção de privacidade deve se adaptar, migrando de um abrigo no anonimato, para a morada do controle e da plena ciência. Se o indivíduo não pode mais contar com o anonimato, deve, pelo menos, ter ciência sobre quais dados pessoais estão sendo tratados, a forma como esse tratamento ocorre e qual é a finalidade do tratamento em questão.

Diante da adoção de tecnologias de rastreamento, identificação, big-data, internet das coisas, biometria, compartilhamento de dados entre instituições, dentre outros, torna-se necessário o estabelecimento de parâmetros e critérios que visem a proteção dos dados pessoais como bens pertencentes ao "titular de dados", ou seja, à pessoa natural a que fazem referência, e não como ativos, impassíveis de direitos, das instituições que os tratam.

O próprio reconhecimento do indivíduo como verdadeiro "proprietário" dos dados já é, por si só, uma conquista no sentido da privacidade, já que por muitos anos temos assistido às instituições tratarem dados como verdadeiros insumos, alimentando sua atividade sem qualquer preocupação com finalidades, adequação, minimização, transparência e responsabilização, certas de que a falta de cautela com o saneamento do processo de tratamento poderia representar, no máximo, prejuízo financeiro, quase sempre às custas da privacidade do titular de dados pessoais.

Impossível não fazer referência aos incontáveis vazamentos que figuraram os noticiários nos últimos anos, quase todos resultantes de processos de tratamentos de dados pessoais que não se preocupavam com a segurança dos dados tratados. Isso quando não falamos do próprio mercado que nasceu da comercialização ativa e deliberada de bancos de

dados pessoais, o que, por sua vez, é a concretização da ideia de que os dados pessoais têm sido vistos como mercadoria, e não como bens-da-vida passíveis de tutela estatal.

Com isso, evidencia-se que a concepção de privacidade, ao deslocar sua definição para o campo da transparência, dá a luz ao princípio da autodeterminação informativa, que é justamente a ideia de que é o titular dos dados quem deve ter plena ciência acerca do tratamento dos seus dados pessoais, incluindo destinação e eliminação, resguardados, obviamente, os direitos de terceiros.

É dentro deste novo paradigma que se estabelece a recém-nascida reconcepção de privacidade, como estado decorrente da transparência acerca dos tratamentos existentes sobre seus dados pessoais e consequente voz ativa na objeção a esses tratamentos quando não obedecerem a princípios básicos de segurança, legitimidade e razoabilidade, e não como fruto do anonimato, como ocorria na concepção clássica.

É evidente que ideias como o direito ao esquecimento não desapareceram, mas o protagonismo da definição de privacidade e proteção de dados agora passa para a utilização sustentável e responsável (responsável, aqui, também, como algo que é digno de responsabilização civil e administrativa) das informações coletadas, pelas instituições, e no emprego leal dos referidos dados, sem que se dê destinação diversa daquela informada ao titular e, certamente, que não se empreguem fins discriminatórios ou danosos às informações coletadas.

Assim, temos que o nascimento das legislações de proteção de dados, como a General Data Protection Regulation (GDPR) europeia e a Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira, é consequência inevitável da nova roupagem dada à concepção de privacidade, já que, se o anonimato não é mais o alicerce da privacidade, mas sim a autodeterminação informativa, é necessário que se estabeleça um critério normativo objetivo para o que é tido como “tratamento legítimo”.

É importante destacar que a criação das mencionadas leis não vem apenas para benefício dos titulares de dados, mas também das instituições

que realizam tratamento de dados, já que com o advento de um código regulatório que determina com clareza e objetividade o que é e o que não é tratamento legítimo de dados pessoais, fica mais fácil para que as mencionadas instituições desempenhem suas atividades sem serem surpreendidas com acusações de mal uso de informações pessoais, construindo, assim, um cenário de segurança jurídica.

A verdade é que, uma vez estabelecidos os critérios normativos por meio das legislações e portarias emitidas por autoridades responsáveis, as instituições que tratam dados somente precisarão adaptar seus processos ao que está determinado no ordenamento, sem nem mesmo ter que conceber as soluções por conta própria, se atentando apenas ao que as normas determinam, no âmbito da legalidade, e ao que os mais conceituados *frameworks* de segurança do mundo estimam como padrões razoáveis de segurança.

2. A segurança da informação e seus pilares

Antes de se adentrar no conceito de privacidade em si, é fundamental que viajemos no tempo para um período muito anterior a qualquer definição perceptível de proteção de dados pessoais. Isto porque, para que possamos falar em privacidade, é preciso compreender que muito antes de tal conceito surgir de maneira independente, outro, mais abrangente e ancestral, já se prestava a regulamentar o tratamento de informações registradas e transmitidas: a segurança da informação.

Com o emprego da alegoria, se as pinturas rupestres são o mais antigo exemplo que se tem sobre a o registro de informações, a primeira vez que um homem de Cro-Magnon decidiu destruir uma imagem após a sua criação para que não fosse mais vista, nasceu o conceito de segurança da informação.

Isto se deve ao fato de que, se ele, como dono da informação, optou por não permitir que esta fosse vista por mais ninguém, e, subsequentemente a destruiu, ele manipulou justamente o que hoje temos

como sendo os três pilares clássicos da segurança da informação: Confidencialidade, Integridade e Disponibilidade.

A confidencialidade decorre da ideia de que a informação só deve ser acessada por aqueles aos quais se destina ou que cujo uso se pretende, a princípio, mantendo-se inacessível por aqueles que não podem ou não precisam saber o seu conteúdo.

No caso da integralidade, surge a noção de que uma informação se presta ao seu objeto quando é incólume, e não foi alterada ou eliminada de forma que comprometa a sua compreensão e utilidade.

Por fim, temos a disponibilidade, que ilustra a necessidade de que uma informação, quando presumidamente existente dentro de um sistema que justifique tal presunção, deve estar disponível para aqueles que a ela têm acesso, quando necessária, ou, ao menos, que se tenha o registro de sua indisponibilidade quando resultante de eliminação formal.

Durante muito tempo estes três pilares foram vistos como o alicerce da ciência de segurança da informação, já que basicamente qualquer desdobramento possível dentro do tema poderia ser tratado em seu arcabouço.

Com o passar dos anos percebeu-se a necessidade de que três novos pilares fossem adicionados ao rol de princípios da segurança de informação, diante do alvorecer de novos obstáculos e particularidades concernentes ao tratamento de informação no mundo, são eles: a autenticidade, a irretratabilidade e a conformidade.

Assim, temos por autenticidade a necessidade de que uma determinada informação, mesmo que confidencial, íntegra e disponível, seja também confiável. A autenticidade nos traz a preocupação com a legitimidade da fonte que criou ou inseriu no sistema a informação em questão, de modo que fontes ilegítimas ou pouco confiáveis devem ser refutadas ou afastadas. Aqui surge a necessidade de que haja registro do autor ou criador da informação tratada, não apenas objetivando o seu lastro, mas também apurações futuras quanto à sua veracidade ou correição.

Já no que tange à irretratabilidade, ou, como também é chamado, princípio do não-repúdio, o intuito é impedir que ocorra negativa de autoria ou de ciência quanto a determinada informação por parte de seus autores e manipuladores. Manter registro de autoria e manipulação da informação assegura não apenas a sua autenticidade, ao cumprir com as necessidades práticas deste próprio pilar, como já ilustrado alhures, mas também garante que não seja possível a declaração de ignorância por parte daqueles que tinham, sim, ciência do conteúdo da informação.

Por fim, temos o novo pilar da conformidade, que diz respeito ao tratamento "lícito" das informações dentro de seu próprio contexto normativo. Além de se garantir a confidencialidade, a integridade, a disponibilidade, a autenticidade e irretratabilidade da informação, é também necessário que tudo isso se faça dentro do escopo regulamentar inerente à natureza daquela informação ou do negócio que a manipula.

De todos os pilares da segurança da informação, clássicos ou modernos, o da conformidade talvez seja o que mais se comunica com o nosso contexto atual, e muito disso se deve ao surgimento de legislações como a General Data Protection Regulation europeia ou a própria Lei Geral de Proteção de Dados Pessoais brasileira.

O motivo pelo qual é importante compreender tais conceitos de segurança de informação antes de adentrar na concepção de privacidade, em si, é que por muitos séculos a implementação dos institutos que hoje vislumbramos como sendo pilares da segurança da informação foram a coisa mais próxima do que se chama atualmente de privacidade, mesmo que, quando de seu nascimento, sequer houvesse sido cunhado o termo "segurança da informação".

Como mencionado anteriormente, até mesmo os hominídeos mais primitivos, quando optavam por destruir uma pintura rupestre – novamente com emprego do lúdico – estavam controlando o seu grau de acesso e disponibilidade, ao garantir que ninguém mais tivesse conhecimento acerca daquela informação específica.

Esta mesma lógica se aplica a qualquer informação tida como sigilosa pela igreja católica através dos séculos, ou mesmo confidencial aos olhos da uma realeza. A verdade é que os pilares de segurança da informação somente fazem interseção com o tema em voga quando, eras depois, veio a ser levantado o questionamento: quando as informações dizem respeito a pessoais naturais, o que deve ser levado em consideração?

3. Warren, Brandeis e o direito de ser deixado a sós

A primeira vez, de que se tem notícia, em que se formulou uma declaração oficial, no contexto jurisdicional ou legal, que possa ser diretamente associada ao conceito de privacidade, se deu em 1604 pelo então advogado geral da Inglaterra, Sir Edward Coke, que, em meio a uma gravíssima crise de aprisionamentos em massa, declarou que o domicílio é inviolável, pois "a casa do homem inglês é, para ele, como seu castelo".

Entretanto, por mais que tal conceituação seja relevante do ponto de vista histórico, e, que a segurança da informação seja ciência antiga, existindo desde antes mesmo de ser batizada, foi apenas em 1890 que veio a ser elaborado o que hoje é considerado como o primeiro trabalho científico que estabeleceu uma definição formal de privacidade sob a ótica de direito individual.

Trata-se do famoso artigo científico "The Right to Privacy", publicado em dezembro de 1890 pelos advogados Samuel Warren e Louis Brandeis, na revista Harvard Law Review.

O artigo, tido como a primeira publicação que se preocupa em conceituar a privacidade como direito, e defini-la, o faz ao determinar que a privacidade seria o direito de ficar a sós, de ser deixado em paz, ou "*the right to be let alone*" no idioma original.

No famoso documento científico os autores argumentam que:

> "nos tempos primórdios, o Direito deu cura apenas para a interferência física na vida e na propriedade, no caso de violações vi et armis. Logo, o "direito à vida" servia apenas para proteger o sujeito de agressões em suas diversas

> formas; liberdade significava liberação da contenção física em si; e o direito à propriedade segurava o direito real às terras e gados de seu dono. Posteriormente, veio o reconhecimento da natureza espiritual do homem, de seus sentimentos e intelecto. Gradualmente o escopo daqueles direitos legais se expandiu; e agora o direito à vida passou a significar o direito de desfrutar da vida, - **o direito de ser deixado em paz**; o direito à liberdade garante o exercício dos privilégios civis; e o termo "propriedade" cresceu para acomodar cada modalidade de sua forma – intangível ou não." (WARREN e BRANDEIS, 1890, p.1) – sem grifos no original

Ao pontuar que Direito evoluiu para além da tutela física da vida e dos bens, os autores apontam que o amadurecimento da sociedade civil refletia no reconhecimento de valores intangíveis da vida humana, como honra e propriedade intelectual, e, por consequência, no nascimento de novos objetos de tutela legal.

Já naquela época pairava no ar profunda preocupação de que os avanços tecnológicos poderiam colocar em xeque o direito do indivíduo de desfrutar a vida em paz e sossego, respeitada a sua privacidade. No mesmo artigo Warren e Brandeis denunciam que o aprimoramento técnico do empreendimento midiático estava em vias de invadir o domicílio e a intimidade doméstica, usando como exemplo a fotografia instantânea e chegando a defender que "*a fofoca não mais é recurso dos ociosos, mas verdadeiro mercado*" (WARREN e BRANDEIS, 1890, p.4).

Na verdade, ao que indicam as fontes, a recomendação de escrita do artigo partiu de Warren diante de um desagradável episódio envolvendo a invasão de um casamento privado por jornalistas, o que por sua vez deu causa a um questionamento abrangente sobre a limitação da violabilidade da vida íntima de pessoas naturais em colunas sociais de periódicos, apesar de esta informação não ser totalmente confirmada.

Fato é que, independentemente de qual tenha sido o fato inspirador para o artigo, os autores se propuseram a verificar se existia, no momento, arcabouço legal robusto o bastante para comportar a proteção da privacidade como direito autônomo, e, caso existisse, qual seria a natureza

de tal direito à privacidade e a extensão dos instrumentos de defesa atrelados a ele.

Num primeiro momento, ao confrontar as legislações pré-existentes referentes aos tipos de calúnia e de difamação, Warren e Brandeis concluíram que tais previsões se prestavam a proteger a honra imediata dos sujeitos de direito, mais especificamente no que diz respeito a atribuição inverídica de fatos vexatórios ou criminosos a indivíduos, configurando agressão moral direta, não necessariamente relacionando-se com o que já chamavam de direito de viver em paz, este, por sua vez, decorrência da interpretação moderna e abrangente do direito à vida.

Já no que tange às leis de propriedade intelectual, os autores também não observaram suficiência argumentativa que conferisse à privacidade autonomia capaz de fazer dela um direito autônomo.

No caso da propriedade intelectual, ficou evidente para eles que a maior preocupação da lei era com os frutos de publicação não autorizada de material cuja autoria pertencesse a terceiro, e não com a publicação em si. Isso afastaria da propriedade intelectual o condão de ser abrigo para o direito à privacidade que eles buscavam identificar.

Entretanto, foi na análise dos casos concretos julgados sob a ótica da propriedade intelectual que os autores finalmente conseguiram observar o fenômeno que tanto buscavam (e que deu notoriedade ao seu trabalho).

Dos vários casos elencados, um julgado pela Alta Corte de Chancelaria britânica, comumente conhecido como "Príncipe Alberto contra William Strange (Prince Albert v Strange)", chama a atenção por conter, nos fundamentos de sua decisão, as impressões necessárias à percepção de que algo, muito além da propriedade intelectual e seus frutos financeiros, estaria em voga.

3.1 Príncipe Alberto contra William Strange e a confidencialidade

Em 1849 a Alta Corte de Chancelaria britânica julgou favoravelmente um pedido formulado pelo então príncipe consorte do Reino Unido,

Alberto de Saxe-Coburgo-Gota, marido da Rainha Vitória, em desfavor do editor William Strange, cuja causa de pedir era a publicação não autorizada de gravuras criadas por ele e pela Rainha em seu momento de lazer e intimidade, em uma exposição organizada pelo editor e pelo escritor Jasper Tomsett Judge.

As gravuras haviam sido confiadas a um impressor de Windsor, chamado John Brown, que, por sua vez, as vendeu a Judge, que procedeu com a organização de uma exposição, junto a Strange, de cinquenta cópias das mencionadas gravuras, das quais duas foram enviadas ao Castelo de Windsor, para o profundo desagrado do Príncipe Alberto. Este prontamente ingressou com o pleito judicial pela proibição da exposição das gravuras, pela prevenção da sua publicação e sua imediata devolução, tendo seu pedido atendido.

Seria, talvez, um típico caso de violação de propriedade intelectual, não fosse a fundamentação adotada para conferir procedência ao pleito do príncipe. Nos argumentos que deram alicerce ao dispositivo decisório, Lorde Cottenham, julgador, apontou que o "caso de modo algum se debruça unicamente na questão da propriedade; pois uma quebra de confiança, confidência ou contrato, por si só, já daria direito ao requerente a uma liminar".

Isso significa que, apesar de reconhecer que a violação da propriedade intelectual das gravuras, por si só, configuraria fundamento suficiente para provimento ao pleito autoral, a mera quebra de confiança no que tange à confidencialidade dos itens cedidos ao impressor, denota, em si, uma violação imaterial que vai além dos possíveis prejuízos econômicos que poderiam se desdobrar da situação.

Em seu artigo "The Right to Privacy" os advogados Samuel Warren e Louis Brandeis enxergaram na fundamentação supramencionada a presença de direitos não explicitados, inominados até então. Ao reconhecer que a mera violabilidade da confidencialidade, em si, figurava como violação passível de retratação, o ilustre Lorde acabava por dar início

ao que viria a se tornar a primeira legislação de confidencialidade do Reino Unido.

3.2 O direito à privacidade e a legitimidade dos tratamentos de dados pessoais

Na conclusão de seu famoso artigo, Warren e Brandeis indicaram que apesar de restar evidente a existência deste direito à privacidade, mesmo que ocultamente presente em diversos julgados pelo mundo, inominado nas entrelinhas de outros direitos, ainda restava compreender a sua extensão, limitações e instrumentos que poderiam ser utilizados para garantir a sua aplicação.

Eles apontam, por exemplo, que o direito à privacidade não poderia ser fundamento para a proibição arbitrária de publicação de interesse público ou geral, ou mesmo que a publicitação de informação realizada na corte da lei, ou seja, dentro do escopo judiciário, ou quando decorrente de dever legal público ou privado, não poderia ser considerada violação de privacidade, de pronto.

Estes fundamentos parecem estranhamente familiares para quem estuda, hoje, legislações de privacidade como a GDPR ou a LGPD, e a similaridade fica ainda mais gritante quando chegamos a uma outra conclusão dos autores: "*O direito à privacidade cessa com a publicação dos fatos pelo indivíduo, ou com seu consentimento*" (WARREN e BRANDEIS, 1890, p.26)

Legítimo interesse, interesse público, exercício de atividade judicial, cumprimento de dever legal ou privado (contratual), fatos tornados públicos pelo próprio titular do direito, e, por último, é claro, o consentimento, todos fundamentos que hoje compõem o rol de bases legais para realização de tratamento de dados pessoais na LGPD (art. 7º, incisos I a X) ou na GDPR (art. 6, item 1 (a) a (f)), à exceção da publicitação voluntária do dado pelo próprio titular, que, por sua vez, é hipótese autônoma de dispensa de consentimento.

É interessante notar, hoje, diante das bases legais presentes na GDPR europeia e na LGPD brasileira, que a simples oposição do titular nunca poderia ser vista como impeditivo categórico ao tratamento de dados ou informações pessoais, já que, em diversas situações, o que fundamenta um tratamento é o interesse de terceiros, legítimo, mesmo que expressamente contrário aos interesses do titular.

Os autores concluem o artigo elencando remédios que consideram existentes para a aplicabilidade do direito à privacidade, reconhecendo que o método mais eficiente seria a judicialização individual mediante violação, de iniciativa do próprio titular. Entretanto, é fundamental destacar que os autores fazem um alerta para o fato de que o interesse social na criação de mecanismos penais que punam, de maneira regulatória, as violações de privacidade, não podia ser ignorado.

4. A privacidade como direito humano fundamental

A privacidade, especialmente quando observada sob a ótica do tratamento de dados pessoais, é comumente associada ao direito ao sossego, esquecimento e demais vieses que denotam a intenção do indivíduo de não ser perturbado ou ter seus dados explorados em detrimento de seu próprio gozo de vida.

O que de fato não é incorreto, uma vez que a preservação do sossego se conecta com a ciência da privacidade na medida em que nossas vidas privadas são devassadas, especialmente pela atividade econômica, que prospera por meio do tratamento e análise massivos de dados pessoais. Entretanto, é fundamental destacar que o tratamento de dados pessoais tem vertente muito mais sombria e potencialmente destrutiva.

Quando falamos, hoje, em tratamento de dados pessoais sensíveis, a exemplo daqueles listados no rol do art. 5º, inciso II, da Lei 13.809/18, no Brasil, uma palavra deve imediatamente vir às nossas mentes: discriminação.

A utilização do processamento de dados pessoais para fins discriminatórios é uma preocupação que permeia o debate há muito tempo, mas para que se possa compreender completamente a sua relevância, existe outro período histórico que precisa ser visitado.

4.1 O Holocausto e os dados pessoais sensíveis

A segunda grande guerra mundial dispensa maiores apresentações, e é de conhecimento notório que os horrores do holocausto e das armas nucleares deixaram cicatrizes permanentes na humanidade. A questão é, quanto disso tudo poderia ter tido resultado diferente se a privacidade individual tivesse sido levada em consideração desde o início do século passado?

Sabe-se que no curso da guerra foram incontáveis as quantidades e variedades de violações de privacidade cometidas contra os cidadãos de cada um dos países beligerantes, o que não é incomum dentro de um contexto de segurança natural.

Na verdade, em um passado muito menos longínquo tivemos o exemplo das medidas de segurança nacional adotadas pelos Estados Unidos da América em resposta ao trágico atentado terrorista cometido contra as torres gêmeas do World Trade Center, em setembro de 2001.

Na ocasião foram inúmeras as violações a direitos civis, incluindo a privacidade, que foram praticadas contra os cidadãos americanos e todos os aqueles que com eles se relacionavam, tudo sob o manto da segurança nacional.

De volta ao contexto da segunda guerra mundial, é fundamental se atentar ao fato de que boa parte das violações de privacidade ultrapassou, em muito, qualquer justificativa que poderia encontrar amparo na segurança. A situação se agrava ainda mais com a popularização da espionagem, que ainda viria a se aprimorar durante a Guerra Fria, e dos temores do desenvolvimento armamentista nuclear.

De toda sorte, além das violações às quais se espera dentro de um cenário bélico, o ponto mais importante de atenção é o tratamento massivo de dados pessoais dos cidadãos e residentes da Alemanha nazista, que tinha, por objeto, a trágica categorização do povo em grupos raciais, étnicos, políticos, religiosos e sexuais.

O que se desdobrou de tal prática não é novidade para qualquer um que tenha o mínimo de conhecimento histórico. Foram anos de segregação, tortura, massacre e atrocidades das mais perversas que nos marcaram para sempre, mas que, acima de tudo, marcaram aos próprios alemães.

Não é de se espantar que, no pós-guerra, a Alemanha tenha tomado fortíssima dianteira na criação de instrumentos normativos que proibissem a intrusão da vida privada de seus cidadãos sem que houvesse profunda e legítima justificativa para tanto.

Nos anos que se seguiram a Alemanha passou a ser vista como vanguardista na criação de salvaguardas que visaram a preservação da privacidade dos indivíduos, em especial no que dizia respeitos a dados sensíveis e passíveis de categorização discriminatória.

Este espírito viria, algumas décadas depois, a gerar umas das mais importantes jurisprudências de privacidade do século XX, que serviu de berço teórico para o que hoje encaramos como o que há de mais moderno no contexto da privacidade, mas voltaremos a isso mais tarde em tópico próprio.

4.2 A Declaração Universal dos Direitos Humanos

A segunda grande guerra mundial deixou feridas profundas e expostas na sociedade internacional que, em questão de meses após a publicitação dos horrores do holocausto e da detonação de duas bombas atômicas, decidiu que era hora de os povos se reunirem para além das suas próprias identidades nacionais em defesa da humanidade como grupo único.

Havia o recém surgido intuito de se criar uma comunidade internacional que teria como base ideologias que apoiassem o desenvolvimento sustentável e pacifista das nações signatárias; nascia a Organização das Nações Unidas, com objetivo principal de impedir que os terrores da segunda guerra mundial se repetissem.

Foi nesse contexto que um grupo liderado pelo advogado canadense John Peters Humphrey esboçou a carta de direitos que viria a ser adotada pela ONU como a Declaração Universal dos Direitos Humanos.

Em seu preâmbulo a carta expressava a motivação existente em afastar qualquer possibilidade de que as barbaridades cometidas na segunda guerra mundial encontrassem terreno fértil para proliferação num futuro que prezasse pela defesa da igualdade, liberdade, justiça e paz mundial.

Salienta que foi justamente o desprezo pelos direitos básicos do ser humano que deu causa aos atos bárbaros que ali se encerravam, e que isso ocorria em oposição a um mundo em que os todos gozassem de liberdade de palavra, de crença e da liberdade de vivessem a salvo do temor e da necessidade.

Evidentemente que nenhum desses direitos básicos poderia ser livremente exercido sem a garantia de que não haveria represália ou opressão ao gozo das liberdades, e é com isso mente que chamo a atenção para cinco itens específicos da Declaração Universal dos Direitos Humanos, quais sejam os artigos II, VII, XII, XVIII, XIX do referido diploma.

O Artigo II determina que o gozo dos direitos previstos na Declaração Universal dos Direitos Humanos não se dará mediante nenhuma distinção de raça, cor, sexo, idioma, religião, opinião política ou de outra natureza, origem nacional ou social, riqueza, nascimento ou qualquer outra condição, além de destacar, também, que não haverá distinção em razão de condição política, jurídica ou internacional do país ou território a que pertença uma pessoa.

O Artigo VII estabelece que todos serão iguais perante a lei e terão direito à igual proteção da mesma, inclusive contra qualquer tipo de discriminação que viole o diploma e contra qualquer incitação a tal discriminação.

A disposição prevista no Artigo XII é ainda mais direta no que tange ao estudo da privacidade, já que expressamente determina que ninguém será sujeito a interferências em sua vida privada, família, lar ou correspondência, nem a ataques desferidos contra a sua honra e reputação.

O Artigo XVIII estabelece as premissas de proteção à liberdade de pensamento, consciência e religião, e ao exercício livre e desembaraçado dessas liberdades, enquanto que o Artigo XIX tutela as liberdades de opinião e expressão, preocupando-se, inclusive, em explicitar que tais liberdades não são passíveis de interferência.

Como se observa, a Declaração Universal dos Direitos Humanos é recheada de princípios que permeiam a ideia de livre manifestação e integração, sem que haja nenhum tipo de discriminação nesse respeito.

Mesmo que num primeiro momento não fique clara a relação entre a privacidade e tais princípios, se nos mergulharmos no contexto histórico no qual a carta de insere, fica fácil de recordar que as mais graves violações a tais direitos cometidas na década anterior tiveram início justamente numa grande classificação do povo alemão, em categorias compostas justamente por elementos de constituem os direitos tutelados pela Declaração Universal de Direitos Humanos, como liberdade religiosa e não-discriminação étnica ou racial.

A verdade é que uma boa forma de se evitar a criação de sistemas inteiramente construídos sobre premissas discriminatórias é, desde o princípio, banir a realização de classificação das pessoas com bases e tais características sem que haja boa e legítima justificativa para tanto.

Se usamos como lente o contexto histórico descrito aqui, fica fácil perceber que os dados pessoais tidos como sensíveis pela Lei Geral de Proteção de Dados Pessoais, hoje, são justamente aqueles cujo

processamento pode dar causa a categorização discriminatória dos titulares, quais sejam: aqueles 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.

Ao elevar características pessoais à tutela de direito humano fundamental, a Declaração Universal dos Direitos Humanos reconheceu que o simples tratamento de tais dados pessoais representa risco quando não ocorrer dentro de um contexto legítimo, que justifique a sua realização, e isso tem profundo reflexo na forma como enxergamos o tratamento desses dados pessoais, hoje em dia.

4.3 Volkszählungsgesetz - A Lei de Censo Populacional Alemã de 1982

Como visto, a ideia de que a privacidade constitui sim direito humano fundamental cresceu e ganhou força nas décadas que se seguiram ao fim da segunda grande guerra mundial, em especial diante do forte ímpeto global em evitar, ao máximo, que os horrores do holocausto se repetissem.

Conforme mencionado anteriormente, a Alemanha assumiu posição de protagonismo no regramento da coleta e tratamento de dados pessoais no período pós-guerra, em especial no que diz respeito à criação de salvaguardas que objetivavam a preservação da privacidade dos indivíduos contra sistemas discriminatórios.

A Alemanha chegou a criar, em 1977, uma lei federal que regulamentava a proteção de dados pessoais, e isso sete anos após ver nascer no estado de Hesse, em seu território, o que hoje é tido como a primeira legislação especificamente voltada para a proteção de dados pessoais do mundo, a *Hessisches Datenschutzgesetz* (literalmente traduzido como Lei Hessiana de Proteção de Dados).

Mas foi em 1982 que a Alemanha foi palco de uma decisão judicial que viria a revolucionar a forma como o mundo enxerga a privacidade e a proteção aos dados pessoais de indivíduos.

Naquele ano o governo federal aprovou uma lei de censo populacional, assim chamada *Volkszählungsgesetz* (semanticamente traduzido como Lei de Censo Populacional), que previa uma gigantesca coleta de dados sobre os cidadãos alemães através de mais de cento e cinquenta perguntas que deveriam ser respondidas, dentre as quais haviam perguntas sobre gênero, estado civil, religião dentre outras.

Importante relembrar que, naquele período, o povo alemão ainda exibia notáveis marcas do período nazista, incluindo uma forte resistência a qualquer movimentação que pudesse ser associada, mesmo que indiretamente, ao regime Nacional-Socialista.

Diante disso, e em vistas do que o processamento em larga escala de dados pessoais sensíveis havia causado há quatro décadas, ocorreu uma explosiva reação negativa por parte do povo alemão à criação da *Volkszählungsgesetz*, não apenas diante de um questionário que consideravam devassante, composto por mais de 150 perguntas, mas também diante do fato de que as informações se prestavam, além da estatística, à atualização de um cadastro coletivo de residentes.

No contexto histórico da década em que a Alemanha viu nascer a primeira lei de proteção de dados pessoais do mundo, no estado de Hesse, bem como a sua própria lei federal de proteção de dados pessoais, que havia entrado em vigor dois anos antes, em 1978, houve profunda resistência por parte dos juristas à justificativa e estrutura apresentada pela nova lei de censo populacional, em especial por conta do mal uso que o país havia dado aos censos de larga escala no passado.

Essa turbulência terminou na suprema corte de justiça alemã, o Tribunal Constitucional, onde foi proferida a histórica decisão que acabou por inaugurar um dos mais importantes conceitos que existem na ciência da privacidade: a autodeterminação informacional.

A corte julgou que uma série de medidas de precaução e salvaguardas deveriam ser tomadas para que fosse legitima a realização do censo nos termos em que se pretendia, em especial ao restringir os escopos de compartilhamento dos dados pessoais coletados, proibindo, inclusive, que

fossem transferidos do governo nacional para os governos regionais com qualquer objetivo diverso daquele estatístico.

O julgado observou também que para que um individuo pudesse gozar livremente dos seus direitos basilares, era necessário garantir que ele tivesse autonomia e poder sobre a publicitação e divulgação de seus dados pessoais, devolvendo ao titular a voz ativa sobre as operações que envolvessem o tratamento de seus dados pessoais.

Esse direito de controle, ciência e transparência acerca da manipulação de dados pessoais passou a ser conhecido como autodeterminação informacional, ou autodeterminação informativa, como é chamado na LGPD brasileira.

A decisão ainda foi além, ao declarar que em épocas de processamento massivo de informações, a criação de medidas que visem proteger o titular do tratamento malicioso ou ilimitado de dados pessoais é medida que se impõe, sob pena de que o titular se veja tolhido de exercer livremente os direitos mais fundamentais.

A corte concluiu esclarecendo que o direito à proteção de dados pessoais não é ilimitado, e encontra teto no interesse público sobrepujante, desde que observada a segurança e a proteção dos dados, nos escopos de proporcionalidade e clareza, cuidando, inclusive, de mencionar a hipótese de que os dados sejam tratados de maneira anônima, para fins exclusivamente estatísticos.

Com o advento de jurisprudência tão revolucionária, surgiram várias das pedras de fundação sobre as quais hoje construímos o Direito à Privacidade e Proteção de Dados Pessoais, incluindo confidencialidade e anonimização para dados estatísticos, princípios da minimização de dados, estrita necessidade e adequação, necessidade de adoção de medidas satisfatórias de precaução e segurança quando do compartilhamento de dados pessoais entre entes públicos, dentre vários outros que futuramente vieram a ser incorporados à Diretiva de Proteção de Dados de 1995 e até à GDPR de 2018.

5. As Leis de Proteção de Dados

Como vimos até aqui, a privacidade trilhou um longo caminho antes que fosse reconhecida como direito autônomo. Observamos que os conceitos de segurança da informação sempre existiram na sociedade humana, e que nasceram praticamente junto com a ideia de registro de informação.

Ato contínuo, verifica-se foram necessários séculos e séculos para que se propusesse a conceituação da privacidade como conceito próprio, sendo primeiramente identificada por Sir Edward Coke em 1604 como a sacrossanta inviolabilidade do domicílio, na sua célebre frase "*a casa do homem inglês é, para ele, como seu castelo*".

Sequencialmente, quase duzentos anos depois, os advogados Samuel Warren e Louis Brandeis publicaram na revista Harvard Law Review o famoso artigo científico "*The Right to Privacy*" onde propuseram a existência de um direito autônomo e inominado à privacidade, observado principalmente no caso paradigma Príncipe Albert x Strange, no qual a tutela estatal se abrangeu para além dos frutos econômicos da produção artística em voga, adentrando em território imaterial, inerente à própria violação de confiança e confidencialidade existente entre as partes.

Com a catastrófica utilização de dados pessoais pela Alemanha nazista na primeira metade do século passado, surgiu fortíssimo ímpeto, a nível global, capitaneado, em vários aspectos, pela própria Alemanha pós-guerra, no sentido de reconhecer a importância de se preservar as características pessoais dos indivíduos de tratamentos discriminatórios e malignos.

Essa iniciativa culminou não apenas em diversas previsões internas à própria Declaração Universal dos Direitos Humanos e à criação da primeira lei de proteção de dados pessoais do mundo, no estado alemão de Hessa, e posteriormente, no país inteiro, como deu início a uma série de eventos que desaguaria no icônico julgamento da lei de censo alemã –

Volkszählungsgesetz – e posteriormente na criação da Diretiva de Proteção de Dados Europeia de 1995.

Diante disso, chegamos ao ponto final deste artigo, com a análise de algumas das legislações de proteção de dados pessoais que, em si, se prestaram como marcos históricos e teóricos para o atual estado da privacidade no Brasil e no mundo.

Como se verá a seguir, muito embora o conceito de privacidade como direito autônomo tenha surgido na doutrina norte-americana, a Europa assumiu a dianteira na normatização do tópico, começando em 1970, com a já mencionada legislação Hessiana de Proteção de Dados.

Entre os anos 70 e 2000 diversos estados europeus também criaram suas próprias leis de proteção de dados pessoais, como a Suécia em 1973, o próprio estado nacional alemão a Dinamarca e a França, os três em 1978, além das cartas magnas espanhola e portuguesa, que regulamentam a nível constitucional a matéria.

Entretanto, apesar da vasta pluralidade de legislações de privacidade surgidas no período, vamos nos ater apenas a um pequeno grupo que pode ser considerado como marco histórico para a matéria, por seu caráter inovador.

5.1 A Lei de Proteção de Dados de Hessa - 1970

Como fora exposto anteriormente, o estado alemão de Hessa foi o primeiro lugar do mundo a criar uma legislação que visasse especificamente a proteção de dados pessoais e, por consequência, a privacidade dos titulares.

O primeiro ponto a ser notado no que diz respeito à Lei Hessiana de Proteção de Dados é que ela foi criada visando a proteção dos dados dos titulares ante o Poder Público. A sua aplicabilidade é restrita aos entes da administração pública direta ou indireta, ou às empresas privadas na medida em que executem funções públicas mediante contrato público.

A lei também se preocupa em definir conceitos como “dado pessoal”, “parte terceira” e “processamento de dados”, sendo que neste última a lei já nasceu inovadora ao considerar que a mera coleta de dados já compõe o processo de tratamento de dados pessoais, quando destinado ao armazenamento, isso implica na necessidade de se observar os preceitos da lei desde o momento em que os dados são colhidos, na origem, e não apenas durante o trâmite da operação de tratamento ou do armazenamento definitivo.

Um ponto curioso e relevante sobre a Lei Hessiana de Proteção de Dados é que ela se encontra em vigor até os dias de hoje, havendo sido submetida a diversas alterações normativas desde a sua promulgação em 1970, ao ponto que hoje é recepcionada pela GDPR como norma complementar e vigente sobre o território em questão.

5.2 As diretrizes sobre a proteção da privacidade da OCDE de 1980

Em 1980 a OCDE (Organização para a Cooperação e Desenvolvimento Econômico) observou que aproximadamente metade dos seus países membros, incluindo Áustria, Canadá, Dinamarca, França, Alemanha, Luxemburgo, Noruega, Suécia e Estados Unidos, haviam aprovado legislação específica sobre a proteção de dados pessoais ou da privacidade.

Além disso, outros membros como Bélgica, Islândia, Holanda, Espanha e Suíça já possuíam projetos de lei preparados para votação.

Diante deste cenário a OCDE decidiu editar uma série de diretrizes concernentes à proteção da privacidade com um objetivo peculiar, porém de extrema relevância: mitigar o risco de que disparidades nas referidas legislações nacionais pudessem dificultar ou obstaculizar o livre fluxo de dados pessoais entre tais nações.

A ideia era evitar que os receios derivados do risco de violações pudessem retrair a criação de tecnologias de processamento e transmissão de informações, bem como interferir de maneira negativa em

determinados setores da economia mundial que dependem fortemente do tratamento de dados pessoais, como o bancário, por exemplo.

Neste contexto a OCDE decidiu desenvolvimento diretrizes que criassem um ambiente de harmonização das legislações individuais de cada uma das nações membros, garantindo a preservação dos direitos humanos em questão sem prejuízo dos importantes fluxos internacionais de dados.

Ficou estabelecido que as diretrizes em questão se prestariam como um consenso sobre os princípios básicos que permeiam a proteção da privacidade individual, e que poderiam ser incorporados às legislações particulares de cada estado-membro, quando pré-existentes, ou servirem de base teórica e filosófica para a sua criação nos países que esta ainda não foi desenvolvida.

O que diferencia as diretrizes das OCDE de 1980 das demais legislações de privacidade mencionadas é que estas se prestam não à criação de regras que visem à proteção daquele instituto em si, mas sim, à proteção da atividade econômica internacional no contexto da proteção de dados pessoais.

Isso não significa que os preceitos estabelecidos não tenham se construído sobre o alicerce da privacidade, mas que de fato o intuito normativo da OCDE com a criação das diretrizes foi oferecer balizas às normas de privacidade, garantindo uma espécie de segurança jurídica internacional para que o continuísmo das atividades econômicas desenvolvidas pelos estados-membros não fosse prejudicado.

Trata-se de normativa de imensa relevância por demonstrar que a criação e manutenção de instrumentos de controle e limitação da invocação da privacidade como direito autônomo devem ocorrer para se garantir que a proteção de dados não acabe por, efetivamente, resultar em atraso tecnológico ou econômico para o mundo como um todo.

É necessário que a privacidade seja preservada por meio do emprego de medidas criativas e razoáveis, não se atendo a preceitos antiquados e

ultrapassados que podem se inviabilizar no contexto de uma sociedade informacional.

É, inclusive, por esta razão que legislações modernas de privacidade, como a própria LGPD, trazem em sua lista de fundamentos basilares conceitos como "*o desenvolvimento econômico e tecnológico e a inovação*", listado no art. 2º, inciso V, do referido diploma.

5.3 O Tratado 108 do Conselho da Europa de 1981

O Conselho da Europa é uma organização internacional independente da União Europeia, apesar de ser costumeira a confusão, que tem por objeto defender os direitos humanos, a democracia e o Estado de direito na Europa.

Diferentemente da União Europeia, o Conselho da Europa não edita normas vinculantes para os estados membros, mas delibera e emite tratados sobre os mais diversos tópicos que se entrelacem com os objetivos supramencionados, aos quais os países podem ou não se submeter.

Um desses tratados, o de número 108, editado em 1981, tem especial relevância para o tema da privacidade, já que regulamenta a proteção dos indivíduos no contexto do processamento automático de dados pessoais.

Na ocasião de sua proposição, todos os países membros do Conselho da Europa foram signatários, vindo a contar ainda com a assinatura de países estranhos ao continente Europeu, como o México e o Uruguai.

A simples leitura do tratado já denuncia a sua forte relação com o que hoje observamos com cautela dentro do contexto das operações de tratamento de dados pessoais de forma automatizada.

O objetivo do tratado era, na literalidade, garantir, no território de cada signatário, para cada indivíduo de direito, independentemente de nacionalidade ou residência, o respeito por seus direitos e liberdades fundamentais e, em particular, seu direito à privacidade, no que diz respeito ao processamento automático de dados pessoais.

Na ocasião, observou-se a urgente necessidade de se criar balizas aos tratamentos automatizados de dados pessoais, crescentes à época, e medidas de segurança à privacidade dos titulares no contexto de tais tratamentos.

O texto normativo estabelecia que os signatários deveriam envidar esforços no sentido de atender aos princípios ali previstos, sempre que vislumbrada circunstância de tratamento automatizado de dados pessoais.

Dentre as previsões, uma que chama a atenção é aquela contida no Artigo 6, que estabelece que dados pessoais de categoria especial, quais sejam, aqueles que revelam origem racial, opiniões políticas, crenças religiosas ou não, bem como dados pessoais relativos à saúde ou vida sexual, ou relacionados a condenações penais, não poderiam ser objeto de processamento automatizado, a menos que o país signatário oferecesse legislação interna própria no sentido de garantir salvaguardas adequadas.

Em 28 de janeiro de 2019, em comemoração pelo Dia Mundial da Proteção de Dados, o Comitê Consultivo do Tratado 108 publicou suas diretrizes sobre o uso de Inteligência Artificial para o tratamento automatizado de dados pessoais.

O referido documento visa a constituição de guias para a criação de políticas e tecnologias que garantam que os aplicativos de IA não comprometam o direito à privacidade dos titulares de dados envolvidos nos tratamentos.

O Comitê Consultivo reconhece que a proteção dos direitos humanos, proteção esta que passa invariavelmente pelo direito à privacidade, como visto, deve ser considerada “by design” no desenvolvimento ou na adoção de tecnologias de inteligência artificial, mormente quando tais medidas se prestarem a tomada de decisão pautada na classificação de determinadas informações pautadas em dados pessoais.

5.4 A Diretiva de Proteção de Dados europeia de 1995

Diferentemente do Conselho da Europa, responsável pela edição do Tratado 108, o Parlamento Europeu possui, de fato, poder para sancionar

e fazer vigorar normas cogentes aos países membros da União Europeia e seus habitantes, inclusive com a previsão de punições por seu descumprimento.

Em pleno uso de tal poder, o referido corpo legislativo estabeleceu o instrumento normativo que viria a se tornar o mais moderno conjunto de regramentos concernentes à proteção de dados pessoais no mundo, até então.

Em meio aos instrumentos normativos referentes à privacidade e à proteção de dados pessoais nascidos na segunda metade do século XX, o que provavelmente mais se aproxima do que hoje utilizamos como escopo para regularização das operações de tratamento de dados pessoais no Brasil e no mundo é a Diretiva de Proteção de Dados europeia de 1995.

Apesar de sua aprovação em 1995, a diretiva só veio a vigorar em 1998, e previa, pela primeira vez na história, um vasto e detalhista arcabouço normativo no que tange à proteção de dados pessoais, em especial no que diz respeito à criação de medidas técnicas e requisitos objetivos para se reconhecer a legalidade dos tratamentos realizados, criando, inclusive, sanções pelo descumprimento de seus termos.

Dentre os principais avanços trazidos pela Diretiva, está a lista de definições referentes à matéria, criando uma necessária restrição à significação dos verbetes relacionados à privacidade e à proteção de dados pessoais.

Algumas das definições trazidas pela lei, inclusive, permanecem até os dias de hoje como sendo as formas oficiais de se encarar determinados conceitos na ciência da privacidade e da proteção de dados, como por exemplo no caso da definição de “dado pessoal”, como sendo “qualquer informação relativa a uma pessoa singular identificada ou identificável.”

Outros conceitos importantes presentes na Diretiva de Proteção de Dados de 95 que sobreviveram à prova do tempo são aqueles referentes a “controlador” e “processador”, respectivamente sendo “a pessoa singular ou coletiva, autoridade pública, agência ou qualquer outro órgão que, isoladamente ou em conjunto com outras pessoas, determine os objetivos

e os meios do tratamento de dados pessoais" e "pessoa singular ou coletiva, autoridade pública, agência ou qualquer outro organismo que processe dados pessoais em nome do controlador"; este último referenciado na LGPD como sendo o "operador de dados pessoais". É aqui que surge também a figura do *Data Protection Official*, precursor do atual *Data Protection Officer* e detentor de funções muito semelhantes àquelas deste último.

A Diretiva também inova ao criar requisitos legais objetivos para justificar a realização dos tratamentos de dados pessoais, o que chamamos de "bases legais" nas legislações modernas, os quais são profundamente familiares não apenas às bases utilizadas hoje em dia na GDPR e na LGPD, mas também aos limitadores de invocação do direito à privacidade listados por Warren e Brandeis no final do seu famoso artigo, como o consentimento expresso ou o cumprimento de obrigação legal ou regulatória.

Surge também a necessidade de que cada país membro da União Europeia tenha uma autoridade pública de proteção de dados que supervisione a aplicação dos princípios e leis de proteção à privacidade individual.

5.5 O Regulamento Geral de Proteção de Dados europeu de 2016 (GDPR)

Finalmente, após mais de séculos de profundos debates sobre as definições que orbitam o direito à privacidade, bem como suas limitações e regramentos, a União Europeia aprova, em 2016, a criação da *General Data Protection Regulation*, popularmente conhecida como GDPR.

Tida como uma evolução natural e orgânica da Diretiva de Proteção de Dados de 95, a GDPR aprimora várias das previsões já inauguradas naquele regramento, atualizando sua abrangência e eficácia às exigências de uma sociedade informacional digitalizada e focada no tratamento de dados pessoais (*data-driven*).

A princípio, um dos pontos mais dignos de nota é a ideia de que negócios e suas respectivas operações de tratamento de dados pessoais devem ser desenvolvidos levando em consideração os princípios de "*privacy by design*" e "*privacy by default*", que significam respectivamente "privacidade desde a concepção" e "privacidade por padrão".

Privacy by design implica na noção de todos os negócios que envolvam operacionalização de dados pessoais devem ser concebidas levando em consideração a privacidade dos titulares de dados. Isso significa que o questionamento quanto ao nível de devassa da privacidade deve ser etapa que constitui a jornada de desenvolvimento de negócios e produtos, de modo que tais negócios e produtos não se estabeleçam sobre premissas que violam a proteção dos dados dos titulares.

Por outro lado, *privacy by default* é a ideia de que qualquer serviço ou produto que envolva o tratamento de dados pessoais deve ter, por configuração padrão, coleta e tratamento dos dados estritamente necessários para o atingimento de sua finalidade, de modo que, caso a coleta e o tratamento de dados adicionais possa enriquecer a experiência buscada ou mesmo agregar valor à operação para o controlador dos dados, a coleta adicional deve ser ativamente acionada pelo titular, nunca automaticamente.

O que pode parecer simples, na verdade agrega imenso nível de segurança e proteção dos dados dos titulares, já que não apenas o processo de criação de desenvolvimento de negócios e produtos deve passar a considerar a privacidade como elemento primordial para a sua concepção, como também os tratamentos de dados necessários para o estrito funcionamento daqueles negócios e produtos terá como configuração padrão a coleta mínima de dados pessoais.

Adiante, outro ponto de imensa relevância no que tange à GDPR, é a internalização de requisitos objetivos para realização de transferência internacional de dados pessoais, o que veio a afetar não apenas os negócios dentro do Espaço Econômico Europeu (EEE), mas também em todo o mundo.

Ao estabelecer, em seu capítulo 5, critérios que devem ser atendidos para a legitimidade da internacionalização de dados pessoais, a GDPR acabou por dar início a uma "corrida mundial pela privacidade", na qual inúmeros países dispararam na direção da criação de legislações próprias de proteção de dados.

Isso se deve ao fato de que a GDPR estabelece as formalidades que devem ser observadas quando da realização de uma transferência internacional de dados pessoais, sendo que uma das mais objetivas é que o país terceiro em questão tenha recebido uma "decisão de adequação" concedida pela comissão da União da Europeia.

Os critérios para a obtenção da referida decisão envolvem o reconhecimento da nação como Estado de Direito, o seu nível de respeito pelos direitos humanos e liberdades fundamentais, a existência e rigor de legislações pertinentes, estrutura que favoreça a possibilidade de que um titular de dados lesado obtenha reparação civil, dentre muitos outros.

Para se atingir o nível de maturidade necessário para obtenção da decisão de adequação também é preciso que o país pretendente possua ao menos uma autoridade de supervisão com a responsabilidade de garantir e fazer cumprir as regras de proteção de dados, possuindo, inclusive, poder de aplicação de sanções administrativas no caso de seu descumprimento, além da função complementar de aconselhar os titulares de dados no exercício dos seus direitos.

Por fim, a GDPR exige ainda que o país pretendente honre com compromissos internacionais assumidos, em especial no que se refere à proteção de dados pessoais.

Como se pode perceber, tal exigência por parte da GDPR colocou as demais nações do mundo em situação de reconhecimento compulsório do direito à privacidade e instauração imediata de legislações que se prestem a viabilizar a obtenção das referidas decisões de adequação, já que, por óbvio, a interrupção dos fluxos de dados pessoais com a Europa seria economicamente fatal para qualquer nação, como de fato já havia sido notado desde as diretrizes da OCDE de 1980.

Ou seja, muito embora a GDPR se apresente como uma evolução orgânica da Diretiva de 95, inovando em pouco no que diz respeito aos conceitos de privacidade, e muito no que diz respeito aos instrumentos de controle e regramento das operações, a normativa atinge o patamar de diploma revolucionário na medida em que compele a evolução da privacidade em todo o mundo, para muito além do seu próprio território.

Diante disso temos que, por mais que a GDPR seja vista, hoje, como grande marco teórico para o regramento da privacidade no mundo, o grande abalo que o seu advento trouxe ao contexto normativo mais se deve ao fato de ter forçado a matéria a nível mundial do que pela próprias inovações materiais em si, já que grande parte delas já era presente na Diretriz de 95, incluindo o protótipo do DPO, como visto anteriormente.

De toda forma, fato é que a GDPR deu início um massivo processo legislativo mundial, voltado especialmente para a criação de instrumentos legais capazes de obter uma decisão de adequação pela Comissão Europeia, e o Brasil não é exceção à regra.

5.6 A Lei Geral de Proteção de Dados Pessoais brasileira de 2018 (LGPD)

Para se ter uma real compreensão da situação do nosso país dentro do contexto da história do direito à privacidade e proteção de dados pessoais, primeiro é preciso que se leve em consideração que, diferentemente da Europa, o Brasil são se encontrava na vanguarda de uma discussão sobre o direito à privacidade que já se estendia por quase 400 anos quando do surgimento da Lei Geral de Proteção de Dados Pessoais.

Na verdade, no que tange ao direito e preservação da intimidade e da vida privada, o Brasil é um infante no assunto, havendo inclusive sido palco de terríveis violações a tais direitos há menos de meio século atrás, no período dos governos militares.

A questão é que, até pouco tempo, o arcabouço legal brasileiro tangia de maneira muito superficial o tema da privacidade, sendo que o ordenamento jurídico basicamente preservava a inviolabilidade do lar e o respeito à preservação do sigilo de correspondência e comunicação telefônica.

Com o advento da Lei 12.737/2012, comumente conhecida como Lei Carolina Dieckmann, ou Lei dos Crimes Informáticos, vimos nascer o primeiro dispositivo legal especificamente voltado para as atuações digitais dos indivíduos, mas, mesmo assim, a lei é de extrema singeleza, e falha não apenas a nível conceitual mas na sua própria aplicabilidade, tão restrita pelas suas próprias definições.

Posteriormente tivemos o surgimento do Marco Civil de Internet, que inovou de certa forma ao prever em seus princípios, constantes do art. 3º, a proteção da privacidade.

O mesmo regramento também determina que a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet, o que interessantemente reverbera com o decisum proferido no famoso caso alemão da *Volkszählungsgesetz*, em que os julgadores reconheceram que o livre exercício das liberdades individuais estaria invariavelmente atrelado ao gozo da vida privada.

De fato foi somente com o surgimento da Lei 13.709/2018, assim chamada de Lei Geral de Proteção de Dados Pessoais, publicada em agosto de 2018, é que o Brasil viu emergir a primeira legislação especificamente voltada para a proteção da privacidade individual no contexto dos tratamentos de dados pessoais, seja qual for o meio de sua manipulação.

Profundamente inspirada na GDPR, a LGPD claramente surge como resposta ao dispositivo europeu na medida em que se presta a atender os requisitos presentes naquela, para obtenção da já mencionada decisão de adequação.

Não pode soar como novidade para qualquer um de nós que o tema da privacidade não estava mais ou menos em voga no país quando da

proposta da Lei no congresso nacional, e por óbvio que o ímpeto legislativo não partiu de uma súbita epifania normativa no sentido de passar a tutelar um direito que vinha sendo reiteradamente devassado.

Por mais que não pareça relevante, a natureza do motivador que serve de força motriz para o surgimento de uma legislação como a LGPD impacta profundamente na forma como o diploma é recebido pela sociedade. Numa realidade como a brasileira, sem qualquer contexto histórico que pudesse justificar a construção da LGPD, é natural que a Lei seja recebida com suspeita e resistência pelos setores mais afetados por suas determinações.

Quando LGPD foi publicada, em agosto de 2018, não levou muito tempo para que os mitos e os equívocos começassem a ser difundidos. E não é possível se esperar nada de diferente, já que, como dito, o Brasil não passou pela construção social que culminou na nominação do direito à privacidade e à proteção de dados pessoais como ocorreu na Europa, e isso faz com que a lei atinja a sociedade com caráter súbito e injustificado.

Por mais que se avalie positivamente os resultados práticos da implementação da LGPD no Brasil, muito além da mera adequação à GDPR, mas referenciando a própria emancipação da privacidade, é compreensível que o tema tenha sido recebido com dúvida e confusão, especialmente por parte da comunidade empresária, mais afetada pelo diploma.

A verdade é que enquanto o *vacatio legis* europeu se prestou a permitir tempo hábil para a adequação das empresas a um regramento que fazia referência a um direito já conhecido, no Brasil o mesmo período de tempo se presta também a educar quanto à existência daquele direito a princípio. Não é possível exigir que se compreenda a importância dos institutos de salvaguarda da privacidade e da proteção de dados se nem mesmo esses dois conceitos em si eram reconhecidos.

Para agravar a situação, no ímpeto de gerar oportunidades financeiras com a prestação de serviços de consultoria e venda de ferramentário de segurança, boa parte dos “especialistas” brasileiros deu

início a uma fortíssima campanha terrorista ao redor da LGPD, buscando a conquista de clientela pelo medo. Esse fator só fez piorar a receptividade à Lei, já que muitas vezes o discurso sustentado pelos mencionados consultores se equivocava na construção de uma imagem pouco realista das obrigações previstas pela LGPD, tornando-a inexequível.

Por mais que o prazo para implementação da lei seja deveras exíguo e isso possa causar, num primeiro momento, ansiedade para dar início ao processo de adequação em si, é fundamental compreender que o momento é, mais do que qualquer coisa, de aprendizado. Precisamos correr para sanar os séculos de atraso com relação ao debate acerca da privacidade, gerando conscientização real, e não mero senso de atendimento normativo.

A sociedade brasileira só vai atingir maturidade no campo da proteção de dados pessoais quando compreender de fato o seu valor, e isso independe de multas milionárias ou danos às marcas.

Obviamente que a instituição da LGPD se presta como forte motivador para o início desse trabalho, mas é fundamental que haja verdadeiro entendimento dos valores existentes por trás de cada dispositivo legal, pela via teleológica, para que, aí sim, possamos dizer que o Brasil está caminhando na direção de uma sociedade mais democrática do ponto de vista dos dados pessoais.

6. Conclusão

Diante de todo o exposto neste trabalho, fica evidente que o caminho percorrido pela privacidade, desde a sua existência como direito inominado e presente nas entrelinhas das jurisprudências e doutrinas, até o advento de normativas como a GDPR e a LGPD, foi trilhado de forma lógico-racional, e a construção da ideia de proteção de dados pessoais não surge como obstáculo ao desenvolvimento tecnológico, mas sim como incentivo para que este ocorra num escopo de criatividade voltada para o bem comum.

Do anonimato à autodeterminação informativa, a privacidade se apresentou de várias maneiras ao longo das eras, e hoje se comunica com a transparência e a boa-fé, dando alas aos avanços econômicos e tecnológicos sem que nenhum deles ocorra em detrimento da intimidade e do livre gozo de liberdades dos indivíduos de direito.

Quando da elaboração deste artigo, já eram dezenas de legislações de privacidade ao redor mundo, muitas das quais surgiram justamente em resposta às exigências da GDPR europeia. Isso importa em dizer que estamos diante de um momento de profunda virada paradigmática, e que somente será possível de fato observar o real impacto das mudanças ao final do processo global de adequação, que ainda deve se arrastar por mais alguns anos.

Até lá é de suma importância que todos os agentes dessa transformação, das áreas legais, de processos, de governança, de compliance além de tecnologia e segurança da informação, compreendam o seu valioso papel dentro da missão coletiva de tornar a privacidade um direito tão respeitado quanto aquele de ir e vir, e isso somente ocorrerá quando respeitarmos a complexidade e a relevância do tema, nos posicionando nas funções necessárias de difusão do conhecimento de qualidade e da conscientização coletiva, passando pela adequação dos agentes de tratamento e pelo empoderamento dos titulares de dados pessoais.

7. Referências

BRASIL. Congresso Nacional. Constituição Federal da República Federativa do Brasil. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 21 novembro de 2019.

BRASIL. Congresso Nacional. Lei Geral de Proteção de Dados Pessoais. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 21 novembro de 2019.

BRASIL. Congresso Nacional. Lei dos Crimes Informáticos. 2012. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 21 novembro de 2019.

BRASIL. Congresso Nacional. Marco Civil da Internet. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21 novembro de 2019.

WARREN & BRANDEIS. The Right to Privacy. 1890. Harvard Law Review. Vol. IV - No. 5

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

PECK. P. Direito Digital. Ed.6. São Paulo: Saraiva, 2016

Segunda seção

O impacto da Lei Geral de Proteção de Dados em modelos de negócio

12

A importância da governança digital na advocacia

Alexandre Atheniense [1]

1. Introdução

Em meados do século passado, a indústria automobilística discutia a necessidade de considerar se um cinto de segurança era um item essencial de segurança dos automóveis. Atualmente debatemos como funcionará e de quem será a responsabilidade civil sobre acidentes envolvendo os veículos autônomos ou como será regulamentado o uso de transporte via aplicativos.

Essas mudanças resultam do avanço contínuo da tecnologia que inova e impulsiona a criação de novos modelos de negócio e nos desafiam quanto aos impactos jurídicos que antes não eram objeto de estudo.

Tais mudanças também já ocorreram na advocacia, uma vez que diversos processos internos e externos nos escritórios tem suporte no tratamento de dados. As atividades operacionais precisam ser normatizadas pela sociedade de advogados, sobretudo para assegurar conformidade às recentes obrigações legais, quanto ao tratamento de dados pessoais, uma vez que este tema deixou de ser apenas uma boa prática e agora está sujeita a severas penalidades, sobretudo a reputação

[1] Alexandre Atheniense é um dos precursores do Direito Digital no Brasil, com experiência de 32 anos nesta área, Especialização em Internet Law na Harvard Law School, Sócio Fundador de Alexandre Atheniense Advogados e Co-Coordenador do Comitê de Direito Digital do CESA.

2. O que é Governança Digital ?

O termo governança digital resulta da rápida e vasta mudança na maneira pela qual advogados e sociedades de advogados devem, a partir de agora, repensar suas atividades, processos, sistemas, normas internas, competências e modelos de negócios.

Engana-se quem imagina que as inovações disruptivas trazidas pela transformação digital signifique que a governança deva ser deixada de lado. Muito pelo contrário. Se a cada dia usamos mais a tecnologia da informação para aumentar eficiência e produtividade, por conseguinte se torna necessário ampliar as melhores práticas de governança, gestão e inovação nas sociedades de advogados.

Uma boa governança corporativa digital traz mais agilidade, transparência e autonomia, portanto, está diretamente ligada a utilização da plataforma digital para fluxo de trabalho, preservação de conteúdo e tomada de decisões. Os advogados sócios que desejem fazer parte da transformação digital precisam como ponto de partida, exercer sua liderança para sensibilizar e engajar suas equipes para essa nova cultura e possam performar bem a “idéia” de ser digital e a clareza dos papéis que cada um deverá desempenhar.

Segundo a Endeavor, organização global voltada ao empreendedorismo, crescer com governança corporativa digital, entre outras coisas, significa aprimorar os processos de administração. Isso se aplica a tomadas de decisão estratégicas, como iniciar ou encerrar um projeto, e a definição de níveis e papéis de controle na organização. Mais uma vez, o conceito se destaca em meio à transformação digital, já que o processo de digitalização das diversas atividades operacionais tende a facilitar o acompanhamento, celeridade e rastreabilidade das práticas de gestão das sociedades de advogados.

É preciso enfatizar que esta transformação proporcionada pela Governança visa alcançar maturidade na tomada de decisões a partir do exame de várias referências que são geradas em formato digital.

Estas medidas se sustentam em alguns pilares essenciais tais como: normas internas, sistemas que permitam gerenciar as todas as atividades nas plataformas digitais, gerenciamento de processos e gestão de pessoas.

Governança diz respeito aos meios e processos que são utilizados para produzir resultados eficazes e mitigar riscos quanto a penalidades legais e riscos reputacionais.

Vale destacar a dimensão destas atividades, já que a governança tem a ver com atos propositais e não apenas comandos tácitos. A governança global está focada não apenas com decisões mas também com suas conseqüências – por exemplo, efeitos distributivos, programas e projetos, eficácia, consentimento, e implementação.

A expressão "governance" não é nova. Porém surgiu voltada a se relacionar com as atividades do Estado e suas políticas de gestão pública. Tais idéias emanaram do Banco Mundial tendo em vista aprofundar o conhecimento das condições que garantem um Estado eficiente.

Foram as instituições de Bretton Woods - Banco Mundial, Fundo Monetário Internacional - que a puseram na moda. O conceito englobava o conjunto dos poderes legislativo, executivo e judiciário, a administração, o governo, o parlamento, os tribunais, as coletividades locais, a administração do Estado, a Comissão Européia, o sistema das Nações Unidas. A capacidade governativa não seria avaliada apenas pelos resultados das políticas governamentais, e sim também pela forma pela qual o governo exerce o seu poder.

Segundo o Banco Mundial, em seu documento Governance and Development, de 1992, a definição geral de governança é "*o exercício da autoridade, controle, administração, poder de governo*".

Em outras palavras, "*é a maneira pela qual o poder é exercido na administração dos recursos sociais e econômicos de um país visando o desenvolvimento*", implicando ainda "*a capacidade dos governos de planejar, formular e implementar políticas e cumprir funções*". Duas questões merecem aqui destaque:

a) A idéia de que uma "boa" governança é um requisito fundamental para um desenvolvimento sustentado, que incorpora ao crescimento econômico equidade social e também direitos humanos ;

b) A questão dos procedimentos e práticas governamentais na consecução de suas metas adquire relevância, incluindo aspectos como o formato institucional do processo decisório, a articulação público-privado na formulação de políticas ou ainda a abertura maior ou menor para a participação dos setores interessados ou de distintas esferas de poder.

Ao longo dos anos, percebeu-se que estas práticas também deveriam ser aplicadas no âmbito corporativo, e, como o mundo dos negócios se converteu numa economia de dados, vivenciamos uma crescente mudança em busca da sustentação e convergência de atividades operacionais na plataforma digital com sustentabilidade.

Esta visão de ampliar o alcance da governança além da ótica de política pública e adentrar no mundo corporativo ganha notoriedade com os grandes escândalos financeiros, envolvendo diversas corporações nos Estados Unidos (EUA) como a Enron Corporation e Arthur Andersen, que causaram sérios prejuízos ao mercado e despertaram a atenção da sociedade em geral para a relevância desse assunto.

A partir daí, a governança corporativa se relacionou à gestão de uma organização, sua relação com os acionistas (shareholders) e demais partes interessadas (stakeholders): clientes, funcionários, fornecedores, comunidade, entre outros. Nos países anglo-saxões, sua essência está baseada em mecanismos de solução para o conflito de agência, decorrente da assimetria informacional e conflito de interesses entre as partes envolvidas (proprietários e administradores).

O movimento pela governança corporativa ganhou força em meados da década iniciada em 1980 nos EUA. Os grandes investidores institucionais passaram a se mobilizar contra algumas corporações que eram administradas de maneira irregular, em detrimento dos acionistas.

Esse movimento foi se alastrando pelo mundo, chegando à Inglaterra, inicialmente, e depois se estendendo pelo restante da Europa, chegando ao

Brasil na última década com a sanção da Lei Anticorrupção que foi o advento para que várias organizações se submeter a programas de *compliance*.

No âmbito corporativo é o conjunto de processos, regulamentos, decisões, costumes, idéias que mostram a maneira pela qual aquela empresa ou sociedade é dirigida ou administrada.

Já a Governança Digital na Advocacia é um conjunto de práticas normas internas, padrões definidos por sócios, com o objetivo de garantir controles efetivos, ampliando os processos de segurança cibernética, proteção de dados e riscos reputacionais por meio do tratamento de dados na plataforma digital.

Estas medidas visam buscar benefícios como melhoria dos processos de tomadas de decisões, ambientes de controle mais eficazes, redução do custo em suas atividades e diferencial de mercado.

Daí percebemos que qualquer sociedade de advogados precisa refletir que a inovação precisa de um propósito, de modo a provocar mudanças consideráveis na forma como se organizam, prestam serviços de qualidade, mantendo seus objetivos éticos, porém, com uma necessária mudança de visão sobre os impactos da tecnologia sobre o seu ramo de atividade.

A definição de propósito não é só uma afirmação dos valores das sociedades de advogado . O propósito define de forma mais clara os objetivos estratégicos, cria uma conexão mais forte entre os parceiros de negócio, seus colaboradores e clientes. Os meios digitais potencializam a comunicação sobre o valor gerado pelos serviços, e, por isso, a cada dia tornam-se uma parte fundamental da estratégia do negócio.

Ninguém discute que as práticas organizacionais da advocacia vem numa linha crescente, acelerada e irreversível no sentido de explorar e implantar novas tecnologias de forma holística, com foco na convergência das tecnologias disruptivas para gerar maior valor aos serviços prestados e com isto reconfigurando o modelo de negócios.

3. O futuro da governança digital

Nas próximas décadas, as megatendências que impactarão de forma contundente as empresas em todo o mundo, direcionam para o fomento à tecnologia e à inovação voltadas para a solução dos principais desafios enfrentados pela humanidade.

Em razão disto, um dos campos de inovação mais promissores, qual seja a transformação digital, compreende a computação em nuvem, a internet das coisas (IoT), a indústria 4.0 / internet industrial e a inteligência artificial (AI). O progresso na área de inteligência artificial resultará em avanços como carros autônomos, robôs e outras aplicações que terão um impacto de grande alcance.

Finalmente, para além dos desafios que terão de ser enfrentados, observa-se também a formação de uma nova sociedade que clama por mudanças significativas no relacionamento entre pessoas e organizações.

Neste particular, a busca por ações cada dia mais éticas e transparentes entre as organizações e todos aqueles que direta ou indiretamente se relacionam com as mesmas torna-se quase que uma constante. No sentido de mapear e estruturar tais ações para aplicabilidade por parte das organizações surge então, com muita ênfase o conceito de governança, agora aplicado ao mundo corporativo.

4. Os pilares da governança digital

No âmbito da implantação de um projeto de governança digital na advocacia, baseia em quatro pilares: Proteção de dados pessoais, Segurança da Informação, Reputação Digital e Compliance.

Os sócios necessitam entender que governança digital não é mais um novo projeto na área de Tecnologia da Informação, mas sim uma decisão “top down” que demanda um protagonismo que lhes pertence

Caso os sócios não participem nestes assuntos e exerçam efetivamente o seu poder decisório, os resultados a serem alcançados jamais acontecerão.

Um dos maiores equívocos que poderá ocorrer, será delegar e exercer a implantação e sustentabilidade da Governança Digital apenas aos responsáveis dos setores operacionais.

A implantação do projeto de Governança Digital na Advocacia deve ter o enfoque visando a sensibilização e alinhamento estratégico, jurídico e tecnológico com a participação de membros do poder decisório e com os colaboradores se setores estratégicos como jurídico, controladoria, recursos humanos, comunicação, financeiro

5. As frentes de trabalho da Governança Digital

As frentes de trabalho para implantar e exercer a governança digital nas sociedades de advogados são:

Jurídica - Se relaciona com a criação de normas internas quanto a segurança da informação e privacidade, revisão de contratos em decorrência das lacunas quanto às obrigações legais no tratamento de dados pessoais e outros documentos que se tornaram exigência após o advento da LGPD.

Estas medidas se destinam a estabelecer limites ou definir condutas para os colaboradores quanto ao uso da infraestrutura digital e dados pessoais tratados pela sociedade de advogados.

Estratégica - Se relaciona a necessidade de criação ou revisão dos processos operacionais internos e externos, para adequá-los também às obrigações legais impostas pela Lei Geral de Proteção de Dados Pessoais.

> Sistêmica - Implantação ou adequação dos softwares que tratam dados estratégicos das sociedades de advogados para dar suporte tecnológico aos mecanismos de controle para eficácia do governança.
> Pessoas - Capacitação da equipe e formalizar a ciência quanto às normas e processos adotados após a implantação das mudanças.

Estas adequações não podem ser consideradas como uma tarefa eventual ou que devem ser cumpridas uma única vez. Muito pelo contrário, o exercício da governança demanda a necessidade de verificações periódicas destas mudanças, para evitar que venham a perder sua eficácia com o tempo.

6. As etapas essenciais para o exercício da governança digital

As etapas essenciais para a execução do projeto de governança digital são:

1ª. Identificar quem são as partes envolvidas que deve ser alvo das medidas de governança
2ª. Coletar Informações via questionários, entrevistas presenciais ou remotas com as lideranças operacionais da sociedade de advogados, visando a mapear as lacunas existentes quanto ao aspecto normativo, estratégico e sistêmico
3ª. Uma vez mapeados estes *gaps*, será necessário avaliar os riscos jurídicos envolvidos, as medidas corretivas necessárias e o grau de complexidade para efetivação das mesmas. Caberá aos sócios neste momento, avaliar e aprovar as mudanças operacionais ou até mesmo institucionais que serão colocadas em prática.
4ª. Partir para o plano de ação visando a implantação das medidas corretivas nas frentes retro mencionadas
5ª. Criação ou revisão de processos internos que permitirão verificações periódicas para controle da eficiência dos mecanismos de controle.
6ª. Treinamento e formalização das normas internas correlatas perante os colaboradores e fornecedores.

7. A relevância da governança da reputação digital

A reputação é um dos ativos mais valiosos e ameaçados nesses tempos. Atualmente os advogados e escritório de advocacia tem cada vez mais dificuldade para serem vistas na internet como desejam ser.

Além disso é preciso ter em mente que nas plataformas digitais o currículo profissional não se limita mais às informações que cada pessoa

revela sobre o seu perfil. Por isso é necessário ficar atento à movimentação de ex funcionários, colaboradores, fornecedores, clientes insatisfeitos, pois estas são as principais fontes de risco que demandam monitoramento dos conteúdos que são veiculadas a seu respeito na web.

Porém não basta apenas monitorar, mas sim ter um plano de contingenciamento pré definido capaz de abreviar o enfrentamento de um incidente reputacional para evitar que um fato se transforme numa crise.

Temos que ter em mente a dificuldade de exercer o controle sobre a publicação de conteúdos de terceiros sobre a nossa reputação profissional. Nos dias atuais, qualquer pessoa é a própria mídia na internet, bem como um paparazzo em potencial.

Estas pessoas visão chamar atenção pública com alcance global, fazendo denúncias, reclamando, dizendo boas verdades ou grandes mentiras. Com o Google, tudo que existe na internet pode ser revelado em poucos clicks.

Como já presenciamos, estes conteúdos podem fechar sociedades de advogados como ocorreu no escândalo Panama Papers, influenciar na decisão de voto como ocorreu no Brexit, na compra de produtos e na contratação de serviços profissionais de advocacia.

A minha experiência profissional em lidar com estes incidentes com advogados ou sociedades de advogados revela que quanto menor o tempo de reação menor será a possibilidade de dano reputacional.

A reputação e a imagem são os bens a serem tutelados na mídia digital no século digital XXI. É cada vez mais relevante que advogados e as sociedades saibam o que estão falando na internet seu respeito.

Manter sempre a governança da reputação e se manter informado sobre eventuais excessos na liberdade de expressão do pensamento ou *fake news* é um recurso extremamente valioso para estar preparado para possíveis repercussões legais e nunca ser pego de surpresa.

A todo instante, milhões de registros são deixados em conversas no Facebook, Twitter, vídeos no YouTube e outras redes sociais. Tais registros já vem sendo aceitos pela Justiça brasileira como provas.

A gestão da reputação digital prevê desde o monitoramento de informações na internet e nas redes sociais, até ações de enfrentamento extrajudiciais ou judiciais de agressores online. Estas estratégias vêm se transformando numa ferramenta indispensável para gestão de risco e compliance.

Por este motivo é necessário que os advogados monitorem continuamente, previnam e respondam imediatamente aos incidentes no mundo digital, associando estratégias de enfrentamento, pesquisa, comunicação e medidas jurídicas que poderão ser tomadas sempre que houver alguma divulgação de conteúdo negativo relativo ao escritório ou um de seus sócios.

Não existe uma bala de prata que garanta uma única solução dos problemas reputacionais. Em regra devem ser tomadas várias alternativas em frentes diversas para lidar com agressores, nos casos em que existam abusos, notícias falsas ou incorretas, infrações ou delitos A legislação brasileira garante a liberdade de expressão, veda o anonimato e define o rito jurídico para conter e punir os eventuais excessos.

É possível remover os conteúdos negativos, por ações de relações públicas, pela via administrativa, ou judicial, entre outras. Porém, é preciso ter em mente que o somatório dessas soluções não se aplicam a todos os casos.

As pesquisas realizadas na ferramenta de busca do Google revelam as referências indexadas a partir da geração de conteúdos de outros sites contra os quais devem ser ser tomadas medidas.

Algumas vezes o agente é anônimo, o que demanda desdobramentos judiciais perante provedores de aplicações e de conexão à internet antes para identificação de autoria antes do ajuizamento da medida judicial para punir o infrator. Nos casos de anonimato, dependendo do caso é viável que o pedido de remoção seja movido contra o provedor de aplicativo apenas, caso esta atividade seja o suficiente para sanar um incidente.

Em alguns casos quando o conteúdo se caracterizar por uma remoção inviável será possível escondê-lo, tirando-o da primeira página do Google.

Esta estratégia não é tão fácil ou imediata quanto parece, mas com persistência e muita experiência sobre como criar conteúdos e escolher os melhores critérios de indexação com o tempo os resultados poderão ser bastante satisfatórios.

Para um enfrentamento eficiente, o primeiro passo necessário é conhecer quem são os agentes envolvidos e seus relacionamentos. Quem é o gerador ou repassador de conteúdos. Qual o alcance do acesso de terceiros ao conteúdo gerado por cada um destes ?

Neste sentido é necessária a realização de uma pesquisa de gestão de presença online, monitoramento de reputação digital e influência digital de modo a gerar um diagnóstico e desenvolver estratégias mais eficazes a partir de várias referências de comunicação detalhadas bem como análise dos riscos.

O enfrentamento mais eficiente deve contar com o somatório dos talentos jurídico e de comunicação, pois várias vezes a resposta pode vir por uma alternativa ou outra, ou mesmo ambas simultâneamente.

8. A importância do *compliance* para as sociedades de advogados

Nos últimos anos tivemos três fatores de destaque que impulsionaram a necessidade das sociedades de advogados a implantarem projetos de governança digital e de compliance. Me refiro a lei anticorrupção (lei 12846/13), a operação lava jato e a sanção da Lei de Proteção de Dados Pessoais.

Esta última abarcou em seu artigo 42, a jurisprudência em vigor do STJ, confirmando a responsabilidade solidária daqueles responsáveis por armazenar dados e informações que venham causar prejuízo a alguém.

Percebe-se portanto que a implantação de um programa de compliance numa sociedade de advogados também deixou de ser uma boa prática e para se tornar uma obrigação legal sujeita a sanções pesadas.

Antes da sanção da lei de proteção de dados, a preocupação mais relevante que motivava a implantação de um programa de *compliance* no escritório resultava do risco e prevenção a fraudes e corrupção.

Desde então, o cuidado com a segurança da informação e proteção de dados pessoais, a gestão de risco e de pessoas no tocante ao tratamento de dados pessoais, a necessidade de ampliar as normas internas sobre estes temas, a revisão de procedimentos internos, o atendimento a auditorias internas e externas cada vez mais abrangentes e minuciosas passaram a ser também alvo de preocupação dos sócios diante dos riscos jurídicos e de mercado envolvidos.

Do outro lado do negócio as empresas têm realizado e ampliado *due diligence* sobre as sociedades de advogados, buscando por qualquer tipo de informação negativa seja por pesquisas que são conduzidas internamente ou ampliando e detalhando o escopo dos seus relatórios periódicos de auditoria sobre a estrutura de tecnologia da informação, buscando informações sobre como o escritório toma medidas sistêmicas para proteger os dados de seus clientes, as *legal opinions* dadas aos seus clientes e orientando sua equipe contra o vazamento de dados ou qualquer outro incidente de segurança da informação, que venha causar danos à imagem e reputação de seus clientes como do próprio escritório de advocacia.

Talvez a maioria gestores das sociedades de advogados ainda não sabem, é que no Brasil existem empresas que oferecem serviços de buscas de informações advindas de centenas de bases de dados que desnudam diversas referências todo o perfil do escritório e seus sócios. Tais informações revelam de forma apurada tudo o que se queira saber sobre a banca que será contratada.

Por este motivo, tais temas se tornaram cada vez mais relevantes ao ponto de diferenciar e ser motivo preferencial para a contratação de um escritório de advocacia dependendo da natureza do negócio envolvido.

Como efeito direto desses riscos, cada vez mais se torna relevante um monitoramento em tempo real e medidas corretivas breves para sanar

quaisquer problemas que afetem informações inconsistentes, desatualizadas ou equivocadas que estejam divulgadas na internet sobre o escritório, seus sócios, seus clientes, as demandas em que atuam para evitar que tal fato se caracterize como uma *fake news*. Se tais medidas não forem executadas o mais breve possível após a ciência este fato poderá converter em crise em pouco tempo, causando danos ainda maiores.

9. Conclusão

Ao longo deste estudo, foi possível destacar como é importante para as sociedades de advogados exercerem a governança digital corporativa diante dos potenciais riscos envolvidos.

Os sócios devem repensar que o alcance de suas atividades na condução dos negócios foi ampliado demandando competência para se tornar mais planejador, indutor, coordenador de políticas, além do controle sobre todas as informações que são tratadas relativo ao negócio tanto no ambiente interno quanto externo.

A boa notícia é que cada vez mais que se torna possível migrar as atividades diárias para a plataforma digital, este controle poderá ser performado com mais eficiência do que antigamente.

Nós advogados devemos ter razão de sobra para nos preocuparmos sobre os conteúdos que são divulgados na internet de modo geral, sobretudo diante das sanções aplicadas pela Lei de Proteção de Dados, os danos à reputação ou mesmo a eventual perda de um cliente por descuido com a informação digital que é tratada no escritório de advocacia.

Inobstante os desafios apresentados, é preciso salientar que com a premência de um novo ciclo de geração de tecnologias disruptivas é importante estar preparado desde já, pois cada vez mais, os dados tratados pelas sociedades de advogados terão significado relevante para o exercício da advocacia.

Isso significa dizer que uma ação articulada de investimentos, estratégias e engajamento dos sócios no exercício da governança digital

corporativa na advocacia, vai abrir espaços para posicionar o escritório de forma diferenciado no mercado, bem como criar um diferencial competitivo, de modo a revelar ao mercado, uma visão inovadora que permitirão acompanhar o dinamismo das atuais transformações tecnológicas e marcos legislativos.

Portanto, mais do que nunca a governança digital corporativa nas sociedades de advogados deve alcançar os sócios, advogados , estagiários, paralegais, fornecedores e membros da equipe administrativa.

Esta mudança deve ser encarada como um fator de eficiência, segurança, integridade e diferencial de mercado, capaz de gerar uma verdadeira mudança dentro do ambiente profissional em consonância com critérios éticos e profissionais.

Os mais bem adaptados a este meio estarão sujeitos a um menor risco de penalidades e ataques à reputação. Sabemos que qualquer mudança assusta, inclusive as boas. Porém a inércia das sociedades de advogados quanto a adoção imediata das medidas de governança digital pode ter um custo muito mais significativo em situações de enfrentamento a um incidente se comparadas com as atividades preventivas alertas neste estudo. É preciso refletir sobre este tema.

13

LGPD e *Legal Design*

Felipe Soares de Magalhães [1]
Thiago Thomaz Siuves Pessoa [2]

1. Introdução

O mundo em que vivemos passou por profundas transformações ao longo dos séculos e a partir da década de 1990, com a criação e facilitação de acesso à internet, bem como com a revolução digital que já experimentamos desde a segunda década do século XXI, novas formas de relacionamento entre as pessoas e destas com as corporações foram consideravelmente alteradas, com repercussão em todas as áreas do conhecimento humano, inclusive no Direito.

E justamente neste cenário de "admirável mundo novo" que vivemos é que nos deparamos com uma crescente demanda de tratamento de dados

---

[1] Bacharel em Direito pela Faculdade de Direito Milton Campos. Sócio da Magalhães, Perfeito e Soares Sociedade de Advogados. Co-Founder da *Edutech* de Proteção e Privacidade de Dados *SECRETUM*. Advogado inscrito na Ordem dos Advogados do Brasil, Seção Minas Gerais. Pós-graduado em Direito de Empresa pela Universidade Gama Filho/RJ, Pós-graduado em Processo Civil pela Universidade FUMEC, Pós-Graduando em Direito da Proteção e Uso de Dados pela PUCMINAS. Curso de Direito Imobiliário pela Fundação Getúlio Vargas (FGV). Curso de Incorporação de Edifício do Prof. Jamil Rahme. Técnico em Transação Imobiliária pelo Sindimóveis do Rio de Janeiro/RJ. Curso de Aprofundamento em Proteção de Dados e Privacidade pelo DTI BR – Centro de Pesquisa em Direito, Tecnologia e Inovação. Membro da Comissão de Ética e Disciplina da OAB/MG (2012/2015). Membro da Comissão Especial de Proteção de Dados da OAB/MG (2019/2021). Atuante nas áreas de Direito Digital (com ênfase em Proteção de Dados/LGPD), Direito Civil (com ênfase em D. Imobiliário e D. Consumidor) e Direito Empresarial.

[2] Bacharel em Direito pela Faculdade de Direito Milton Campos. Sócio Fundador do escritório Pessoa Advocacia. *Chief Legal Officer (CLO)* da Fintech de Negócios e Educação Financeira VALE OURO. Co-Founder da *Edutech* de Proteção e Privacidade de Dados *SECRETUM*. Advogado inscrito na Ordem dos Advogados do Brasil, Seção Minas Gerais. Pós-graduado em Direito Público pela ANAMAGES / Unicentro Newton Paiva. Pós-graduado em Regime Jurídico dos Recursos Minerais pela Faculdade de Direito Milton Campos. Curso de Atualização em Direito, Tecnologia e Inovação pelo DTI BR – Centro de Pesquisa em Direito, Tecnologia e Inovação. Curso *Legal Creatives Design* pela *Legal Creatives,* em parceria com a Edevo. Membro da Comissão Especial de Proteção de Dados da OAB/MG (2019/2021). Advogado corporativo. Consultoria estratégica sobre negócios jurídicos de empresas e serviços de consultoria jurídica.

pessoais, seja para cumprimento de obrigações legais ou para obtenção de vantagens comerciais por algumas empresas, estas com o objetivo de fornecer produtos e/ou serviços que sejam úteis, agradáveis, desejáveis ao destinatário, bem como interativos e intuitivos, com aplicação do já contemporâneo conceito da "era da experiência" e gerando como uma de suas consequências a necessidade de utilização das ferramentas de *Design Thinking* para solucionar os desafios decorrentes de tal realidade posta, somado à uma crescente regulamentação legal.

Foi neste contexto que fora promulgada a Lei Geral de Proteção de Dados Pessoas (LGPD), no Brasil, Lei nº. 13.709/2018, a qual tem por objeto a regulamentação das atividades de tratamento de dados pessoais e que acaba por conter premissas legais que devem ser observadas para o desenvolvimento de uma cultura de proteção e privacidade de dados pessoais até o momento ainda em desenvolvimento no Brasil.

Dentro desse contexto, é que entra o *Design Thinking* como uma abordagem que busca a solução de problemas de forma coletiva e colaborativa, em uma perspectiva de empatia máxima com os destinatários da norma: as pessoas são colocadas no centro de desenvolvimento dos trabalhos de ensino e implantação de conformidade com a LGPD.

As ferramentas do *Design Thinking* buscam implementar um processo que consiste em tentar mapear e mesclar a experiência cultural, a visão de mundo e os processos inseridos na vida dos indivíduos, no intuito de obter uma visão mais completa para a solução de problemas e, dessa forma, melhor identificar as barreiras e gerar alternativas viáveis para transpô-las. Parte-se do levantamento das reais necessidades do ser humano destinatário e emprega-se uma abordagem preponderantemente "humana", que pode ser usada em qualquer área de negócio, inclusive para se buscar uma criação de cultura de proteção e privacidade de dados.

Em virtude dessa realidade atual projetada para esfera jurídica, torna-se necessária a adaptação do profissional do Direito à realidade de buscar novos conhecimentos e dar forma à prestação de seus serviços

exatamente como a "era da experiência" preceitua, com visão sistêmica e assertiva das necessidades de seus clientes e atuação eficaz, de forma a permitir um entendimento mais facilitado e próximo do cliente, inclusive no tocante aos aspectos da LGPD.

Para tanto, é proposto ao operador do direito um novo modelo mental de aplicação do direito para solução dos problemas de interface jurídica no tocante aos procedimentos de implantação e conformidade com a LGPD, através de uma metodologia de aplicação de ferramentas do *Design Thinking* no pensamento jurídico ou aplicação do chamado *Legal Design,* de forma a permitir que sejam alcançadas soluções legais cada vez mais precisas para as necessidades dos clientes, bem como mais compreensíveis e intuitivas, com o escopo de auxiliar na melhor compreensão da LGPD e interfaces desta normativa com as operações das empresas pelos diversos membros componentes destas.

É no cenário acima delimitado que propomos a análise do *Legal Design* e sua aplicação pelos operadores do Direito como forma de facilitar a obtenção de melhores resultados em trabalhos de implantação e conformidade com a LGPD.

2. Contornos gerais da Lei Geral de Proteção de Dados pessoais (LGPD) e o desafio da implantação de uma cultura de proteção de dados

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº. 13.709/2018, criou um novo regramento para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores privados e públicos.

Importante salientar que o Brasil já dispunha de mais de 30 normas que direta e indiretamente tratavam da proteção à privacidade e aos dados pessoais, dentre as quais podemos citar Código de Defesa do Consumidor, Marco Civil da Internet, Lei do Cadastro Positivo, dentre outras.

Todavia, a LGPD vem substituir e/ou complementar esse arcabouço regulatório setorial, que por vezes era conflituoso e obscuro e que trazia

insegurança jurídica e tornava o País menos competitivo no contexto de uma sociedade cada vez mais movida a dados.

A LGPD visa não somente garantir direitos individuais, mas também fomentar o desenvolvimento econômico, tecnológico e a inovação por meio de regras claras, transparentes e seguras para o uso adequado de dados pessoais. Neste sentido, importante destacarmos os contornos gerais da norma invocada, o que nos permitirá entender os desafios implícitos para adequação à referida normativa.

Podemos afirmar que dos principais objetivos da LGPD são: a) assegurar o direito à privacidade e à proteção de dados pessoais de todas as pessoas naturais cujos os dados sejam coletados e/ou tratados em território nacional; b) estabelecer regras claras sobre o tratamento de dados pessoais em território nacional e criar um padrão para tanto; c) fomentar o desenvolvimento econômico e tecnológico; e d) fortalecer a segurança das relações jurídicas que impliquem em coleta e/ou tratamento de dados pessoais.

São destinatários da norma toda a pessoa natural ou pessoa jurídica de direito público ou privado que de alguma forma colete e/ou trate dados pessoais em território nacional, tanto em ambiente *off-line* quanto *online*.

Ganham destaque nesse cenário as pessoas jurídicas de direito privado, uma vez que, em razão de várias determinações legais e de estratégias comerciais, acabam por coletar e/ou tratar um grande volume de dados pessoais.

A LGPD apresenta como conceito de dados pessoais qualquer informação relacionada à uma pessoa natural que possa ser identificada ou identificável a partir dos dados coletados, sendo que ainda existe a classificação de dados sensíveis, sendo estes os relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, saúde, vida sexual, dado genético ou biométrico, que só poderão ser submetidos a tratamento mediante consentimento específico e destacado do titular para finalidades específicas ou para cumprimento de obrigação legal ou regulatória pelo

controlador; tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral; proteção da vida ou da incolumidade física do titular ou de terceiros; tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou, garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Importante destacar que o tratamento dos dados pessoais de crianças e adolescentes deverá ser realizado em seu melhor interesse e somente mediante o necessário consentimento específico e em destaque de pelo menos um dos pais ou responsável legal.

A lei ainda apresenta o conceito de dados anonimizados, que são os dados pessoais relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

O Titular dos Dados é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. O tratamento é toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

A LGPD ainda nos apresenta a figura do Controlador de Dados, que é a pessoa natural ou jurídica a quem competem as decisões referentes ao tratamento de dados pessoais. Por sua vez, ainda nos é apresentada a figura do Operador de Dados, que é a pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do Controlador.

A LGPD cria a Autoridade Nacional de Proteção de Dados Pessoais (ANPD), cujas principais funções serão zelar pela proteção dos dados pessoais; elaborar as diretrizes para a política nacional de proteção de dados pessoais e da privacidade; fiscalizar o cumprimento da Lei e aplicar as sanções previstas na LGPD; bem como editar regulamentos e procedimentos sobre a proteção de dados pessoais.

A lei também cria a figura do Encarregado pelo tratamento de dados pessoais, que deve atuar como canal de comunicação entre o controlador, a ANPD e os titulares de dados, inclusive sendo o responsável a comunicar ao órgão competente e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares; receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, receber comunicações das autoridades competentes, orientar colaboradores e contratados do operador acerca das práticas a serem adotadas em relação à proteção de dados, entre outras atividades que venham a ser estabelecidas pelas autoridades competentes. A identidade e as informações de contato do Encarregado devem ser públicas, claras e objetivas, de preferência no site do controlador.

A LGPD ainda nos apresenta requisitos para o tratamento de dados pessoais, que constituem verdadeiras premissas para que o tratamento seja efetuado de acordo com as disposições legais. São princípios da atividade de tratamento de dados:

a) Finalidade: para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
b) Adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
c) Necessidade: limitação do tratamento ao mínimo necessário para a realização das suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
d) Transparência: informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

e) Não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e
f) Segurança: utilização de medidas 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 difusão;
g) Prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
h) Responsabilização e prestação de contas: demonstração pelo agente da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, inclusive da eficácia das medidas;
i) Livre acesso: consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade dos seus dados pessoais;
j) Qualidade dos dados: exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

Tendo por premissa os princípios acima destacados, a LGPD autoriza o tratamento de dados nas seguintes hipóteses: mediante consentimento do titular; para cumprimento de obrigação legal ou regulatória do Controlador; quando necessário para execução de contrato ou procedimentos preliminares a um contrato do qual seja parte o titular, a pedido do titular; para exercício regular de direitos em processos judiciais, administrativos ou arbitrais; para a proteção da vida ou da incolumidade física do titular ou de terceiro; para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; quando necessário para atender aos interesses legítimos do controlador ou de terceiro, salvo quando prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção de seus dados pessoais; para proteção do crédito; pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

Neste ponto, importante destacar que ao falar em consentimento, a LGPD está se referindo à uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais, devendo ser esta por escrito, de forma destacada, ou por outro meio que

demonstre a manifestação de vontade do titular. Deverá referir-se a finalidades determinadas e serão nulas as autorizações genéricas para o tratamento de dados pessoais. Ocorrendo mudanças da finalidade para o tratamento de dados pessoais não compatível com o consentimento original, o titular deverá ser informado sobre as mudanças de finalidade, podendo revogar o consentimento, caso discorde das alterações.

Quando o tratamento for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre esse fato e sobre os meios pelos quais poderá exercer seus direitos.

Por fim, o consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob o amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, sendo dispensada a exigência do consentimento para os dados tornados manifestamente públicos pelo titular.

No tocante ao legítimo interesse, a LGPD preceitua que somente poderá ser fundamentado para finalidades legítimas, consideradas a partir de situações concretas, que incluem o apoio e a promoção de atividades do controlador e, em relação ao titular, a proteção do exercício regular de seus direitos ou a prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele; somente o tratamento de dados pessoais estritamente necessários para a finalidade pretendida; mediante a adoção de medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse.

A transferência de dados pessoais para um país estrangeiro ou organização internacional da qual o país seja membro é permitida nos seguintes casos: para países ou organizações internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na Lei, mediante avaliação pelo órgão competente, que levará em consideração as normas gerais e setoriais da legislação em vigor no país

de destino ou na organização internacional; a natureza dos dados; a observância dos princípios gerais de proteção de dados; a adoção de medidas de segurança previstas em regulamento; a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados; e as outras circunstâncias específicas relativas à transferência; quando comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na lei, com definição do seu conteúdo por órgão competente, na forma de cláusulas contratuais específicas para uma determinada transferência; cláusulas-padrão contratuais; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos; para cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; para a proteção da vida ou da incolumidade física do titular ou de terceiros; quando o órgão competente autorizar a transferência; quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; para a execução de política pública ou atribuição legal do serviço público; e por fim, com consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades.

Ainda no tocante ao tratamento, cumpridas as finalidades para as quais os dados pessoais foram coletados, constatado que deixaram de ser necessários, havendo revogação do consentimento ou por determinação das autoridades competentes, os dados devem ser eliminados, isto é, excluídos dos bancos de dados do controlador e do operador. Fica autorizada a conservação de dados pessoais para cumprimento de obrigação legal ou regulatória ou para uso exclusivo do controlador, vedado o acesso por terceiros e desde que anonimizados.

A ANPD poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais referente a suas operações de tratamento de dados. O relatório de impacto à proteção de dados pessoais é a documentação do responsável que contém a descrição dos processos

de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A legislação ainda estabelece os seguintes direitos dos titulares: confirmar a existência de tratamento de seus dados pessoais; acessar seus dados pessoais; corrigir dados pessoais incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados pessoais desnecessários, excessivos ou tratados em desconformidade com a LGPD; portabilidade de dados pessoais a outro fornecedor de produto ou serviço; eliminação de dados tratados com o seu consentimento; obtenção de informações sobre as entidades públicas e privadas com as quais o controlador realizou o compartilhamento de dados pessoais; obtenção de informações sobre a possibilidade de não consentir com o tratamento de dados pessoais e sobre as consequências da negativa; revogação do consentimento dado para o tratamento de dados pessoais.

No contexto, devemos destacar que a LGPD recomenda aos controladores e operadores formularem 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 de dados pessoais, 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.

A LGPD estabelece penalidades bastante rigorosas quais sejam: advertência; observação de divulgação do incidente; eliminação de dados pessoais; bloqueio, suspensão e/ou proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados pessoais; multa de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos e limitada, no total, a R$50.000.000,00 (cinquenta milhões de reais) por infração.

As referidas penalidades não substituem a aplicação de sanções administrativas, civis ou penais previstas em legislação específica. A inobservância ao princípio da segurança pode, em caso de dano ao titular, gerar responsabilidade civil e criminal solidária entre controlador e operador e o dever de reparar os danos, sem prejuízo das sanções administrativas, existindo, inclusive, a possibilidade de inversão do ônus da prova a favor do titular dos dados pessoais quando for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular dos dados pessoais for excessivamente onerosa para o mesmo.

Esses, em linhas gerais, são os contornos da LGPD, que se apresenta como uma normativa detalhada no tocante a proteção e privacidade de dados no Brasil, o que comprova a relevância da temática de tratamento de dados pessoais no cenário atual.

Importante destacar neste contexto que a Lei Geral de Proteção de Dados Pessoais impacta diretamente no dia a dia das empresas brasileiras, pois implica na necessidade de implementação de procedimentos de conformidade com a referida lei, com revisão de processos internos de fluxo de dados pessoais, criação ou revisão de programas de governança, com políticas de segurança e proteção da informação e gestão de crises, revisão de contratos comerciais, contratos com fornecedores, contratos de trabalho e contratos com prestadores de serviços, treinamento de colaboradores e tantas outras providências que se fizerem necessárias ao atendimento da normativa legal.

E dado o momento atual de amadurecimento da sociedade brasileira quanto a temática em foco, podemos afirmar que a LGPD propõe um desafio cultural, que exigirá não só aos destinatários da norma, mas principalmente, em um primeiro momento, aos profissionais que se propõem a trabalhar com a implantação de medidas de conformidade com a referida normativa, um grande esforço para a promoção de quebras de paradigmas e mudanças de comportamento, com desenvolvimento de uma nova mentalidade.

Neste sentido, Diego de Lima Gualda[3] já destacou:

> "O Brasil não detém uma cultura de proteção de dados pessoais e isso repercute nas práticas corporativas. Continua corriqueira a existência de bases de clientes em planilhas sem controle de acesso, trocas de e-mails com essas bases, uso de dados pessoais de clientes para fins distintos do propósito da coleta, manutenção de dados pessoais por períodos indefinidos e sem controle de segurança, atividades de marketing não regulares, etc.
> As organizações devem investir em revisitar cada uma de suas linhas de negócio e práticas a elas inerentes, além de treinamento contínuo para colaboradores. A grande maioria dos problemas de violação de dados pessoais e segurança da informação têm por causa condutas inadequadas e a mudança de cultura corporativa é muito mais lenta e muito mais difícil que a troca ou implantação de um software. Não devemos subestimar a importância e o desafio cultural que a LGPD traz consigo."

Assim, em um primeiro momento, de igual maneira o profissional do direito que quiser se dedicar à temática a LGPD, deverá ser criativo e recorrer às ferramentas que possam auxiliar na melhor compreensão do novo cenário que se descortina pelos destinatários dos serviços de implantação de conformidade com a LGPD.

Aqui podemos afirmar que entender o momento de amadurecimento e a experiência do cliente quanto à temática de proteção de dados pessoais será fundamental para que se construam caminhos de aprendizado e fixação de conteúdo a partir de uma premissa próxima à realidade vivenciada pelo cliente.

É justamente neste contexto que o *Legal Design* poderá se extremamente útil e até mesmo fundamental para que efetivamente se obtenha um resultado eficaz de uma verdadeira implantação de uma cultura de proteção de dados pessoais.

---

[3]GUALDA, Diego de Lima. **Desafio Cultural da Proteção de Dados.** Disponível em:
< https://www.aarb.org.br/desafio-cultural-da-protecao-de-dados/ > Acesso em: 03 de fevereiro de 2020

3. *Legal Design* e aplicação para melhor adaptação aos preceitos da LGPD

Como destacado acima, com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) no Brasil, fica latente o grande desafio cultural da proteção de dados, o que deve ser objeto de atenção de todos os profissionais que se propõem a dedicar esforços na área de proteção de dados e segurança da informação, até mesmo em razão da atual realidade de grande volume de tratamento de dados pessoais para fins legais ou diversos, como obtenção de vantagens comerciais para fornecimento de serviços ou produtos de forma mais adequada ao perfil do cliente.

Neste contexto, o operador do direito deve recorrer às ferramentas e técnicas que possibilitem que o trabalho de interface jurídica de adequação aos preceitos da LGPD seja mais acessível do ponto de vista do destinatário, de forma a permitir à este uma melhor compreensão e conscientização quanto as disposições legais de proteção de dados pessoais e as vantagens inseridas na legislação e em uma cultura de proteção de dados.

É neste contexto que se propõe a utilização do *Legal Design* como um facilitador na compreensão pelas instituições e seus membros quanto as disposições legais de proteção de dados pessoais, tornando tais normativas mais inteligíveis aos seus diversos agentes destinatários, funcionando assim como um catalizador da adoção de uma cultura de proteção de dados.

Sobre o *Legal Design,* já fora destacado:

> "O Legal Design é a disciplina cruzada do pensamento jurídico, design thinking e design de experiência do usuário (UX). Usamos essas disciplinas para melhorar a cordialidade humana de entender e aplicar a lei, uma vez que a lei visa criar ordem na sociedade e criar um ambiente de vida e trabalho pacífico para todos.
>
> Trata-se de compreender as necessidades humanas para desenhar as soluções adequadas, ao mesmo tempo em que se conquista engajamento e proximidade dos clientes com o sistema jurídico.

> *Em suma, o Legal Design é uma metodologia que busca entender o contexto e a necessidade das pessoas em sua relação com a lei, e através de uma visão ampla decorrente desta análise, entregar a melhor solução jurídica para o caso concreto." (MACHADO, Matheus Parreira; PESSOA, Thiago Thomaz Siuves, 2019).*

Em interface com as questões legais, podemos afirmar que o *Design Thinking* busca se concentrar na melhoria da qualidade de vida das pessoas no tocante à assertividade do suporte jurídico para o provimento de serviços, experiências e produtos, o que afeta sobremaneira o comportamento humano. Utiliza técnicas de pesquisa de empatia e *design* para obter as necessidades latentes dos usuários, a fim de criar novas soluções, inovações e melhorias nos produtos e serviços existentes.

Além disso, o *Design Thinking* é um método amplamente aplicado no pensamento de *design* ou na abordagem de *design* de serviço. Pode tornar histórias complexas mais tangíveis e fáceis de entender. Além disso, o *design* de experiência do usuário (UX) é usado para criar experiências envolventes, engajando o destinatário ou cliente a participar da construção da solução de um problema.

Legal Design é a aplicação do *design* centrado no ser humano no mundo do Direito, para tornar os sistemas e serviços jurídicos nele focados utilizáveis e satisfatórios, buscando atender as necessidades do ser humano enquanto usuário do sistema legal.

Para tanto, traz uma cultura de *Design Thinking*, pesquisa de usuários e métodos de *design* focados na relação do ser humano com o mundo do direito e no processo, estabelece novas métricas chave para a forma como se opera no mundo jurídico, tendo como objetivo fornecer serviços que são (1) utilizáveis, (2) úteis e (3) envolventes.

Assim, uma abordagem de *design* para serviços jurídicos coloca as pessoas e seus contextos como foco, questiona como seu *status quo* poderia ser melhorado e, em seguida, considera o potencial da criatividade, da inovação e da tecnologia como intervenções.

Portanto, parte da premissa de que os advogados devem desenvolver visão sistêmica focada nas necessidades do cliente para criar serviços

jurídicos verdadeiramente amigáveis, envolventes, interativos e de qualidade, tendo, assim, três ordens de objetivos: ajudar o leigo e o profissional legal, criar uma melhor interação entre advogado e cliente dentro do sistema legal e promover uma aplicação das leis mais assertiva às soluções dos problemas do cliente, inclusive trabalhando para melhorias de curto prazo e mudanças inovadoras a longo prazo.

Relacionados com estes objetivos, existem dois principais destinatários estratégicos, separados, mas interligados: o leigo (cliente) e o profissional legal (advogado). Com a aplicação das ferramentas do *Legal Design,* surgem questões fundamentais. Para o leigo no sistema legal: como podemos torná-lo mais inteligente, mais capacitado e no controle das complexidades de seus assuntos legais e das leis que se aplicam a ele? Para o profissional legal: como podemos apoiá-lo para praticar melhor a lei, para atender seus clientes de maneiras mais assertivas e eficazes de forma a envolver o cliente ativamente na solução dos problemas?

O *Legal Design* pergunta ainda sobre como podemos aumentar a sabedoria, o empoderamento e a tomada de decisões estratégicas. Seu objetivo é melhorar a compreensão dos clientes sobre as regras e sistemas que se aplicam a eles e lhes oferecer o poder de navegar pelo sistema legal da maneira mais estratégica, inteligente e intuitiva. Isto, em um ecossistema inovador, até pela mentalidade atual, é de grande valia ao empreendedor.

Neste sentido, ele usa o poder dos processos de conscientização mental e dos processos de *design* para criar melhores interfaces e ferramentas com as quais os clientes podem navegar pelo sistema legal, bem como busca criar sistemas e regras mais intuitivos, com o objetivo de priorizar no sistema legal a facilitação do entendimento e de sua utilização mais assertiva, de acordo com as necessidades atuais do destinatário da norma legal.

Assim, ele pode ser usado como mais uma ferramenta para o advogado ter em seu repertório na solução dos desafios legais apresentados por seus clientes, ou pode ser usado como um processo de

inovação e implementação, para transformar novas ideias em novos serviços, que podem ser implementados de forma ágil.

Para tanto, importante a lição que destaca as metas estabelecidas pelo *Legal Design:*

> "Neste sentido, o Legal Design estabelece algumas metas mais concretas para os projetos a serem implementados, a saber:
> a) Solução de problemas aprimorada: ser mais inovador e criativo na geração de soluções para os desafios legais propostos pelos clientes.
> b) Serviços centrados no cliente: colocar o foco no cliente e conquistar clientes de maneiras melhores, fornecendo-lhes melhores serviços adaptados às suas necessidades explícitas (e ocultas) – e para comunicar-lhe informações de maneiras mais claras, mais atraentes e mais intuitivas.
> c) Melhor Comunicação: comunicar informações – particularmente informações jurídicas complexas – de uma maneira mais didática, mais atraente e mais intuitiva." (MACHADO, Matheus Parreira; PESSOA, Thiago Thomaz Siuves, 2019).

O principal equívoco dos advogados em relação ao *design* é pensar que isso significa apenas fazer algo parecer mais bonito, mais nítido e melhor. A maioria das pessoas reduz o *design* à estética, como escolha de fonte, cor ou modelos de slides do *PowerPoint*. Tudo isso se resume à aparência superficial, "como algo parece". Aparência é certamente um fator importante, mas não é tudo o que o *design* tem para oferecer – e certamente não é o coração do que ele representa atualmente.

Não se ignora que dentro do *Legal Design* existe uma sub-área de *Visual Law,* a qual é conceituada por muitos como a materialização do pensamento decorrente do *Legal Design,* de forma que o *Visual Law* se concentra na produção de materiais mais explicativos e criativos sobre o Direito, ou seja, é a manifestação física do *Legal Design* centrada na melhor compreensão dos aspectos legais que envolvem o destinatário da mesma.

Mas como dito acima, não se trata apenas de um "documento mais bonito", mas de um trabalho realizado por uma equipe multidisciplinar focada nas necessidades do usuário (cliente), utilizando-se de técnicas de *Design*, com o objetivo de trazer novos conceitos de interação com os

usuários no que diz respeito aos documentos jurídicos da sua empresa, como, por exemplo, em contratos, pareceres, normas de condutas internas, etc.

Assim, em verdade, o uso da técnica de *Design* é sobre fazer coisas que são intuitivas, envolventes, valiosas e amadas para as pessoas que as usam. Trazer isto para o universo do direito e aplicar tal pensamento para atuação profissional que pretende se dedicar à área de segurança da informação e proteção de dados pessoais parece-nos ser o caminho mais adequado e necessário a ser percorrido pelo operador de direito que deseje obter resultados satisfatórios na implantação de procedimentos de conformidade e atendimento às disposições legais da LPGD.

Usando a linha de raciocínio de empregar ferramentas e métodos para criar empatia, o *Legal Design* pode criar a ponte entre o mundo legal (técnico) e as pessoas, permitindo que os advogados tenham um contato com o cliente mais eficaz e com melhor comunicação, em um ambiente empático. Isso ajuda a trazer seus conhecimentos e habilidades de uma forma que seja acessível para os leigos, preservando o delicado valor legal de forma assertiva e específica focada na necessidade do cliente, sempre se pautando em uma visão sistêmica.

O processo de *Legal Design* não é uma receita pronta – embora possa ser útil aprendê-lo através de um conjunto de etapas já estabelecidas. À medida que o advogado passa por mais ciclos, encontra as próprias preferências e percebe os diferentes valores e atividades de cada etapa, de forma que poderá construir o processo do seu jeito. Cada desafio pode exigir uma variação diferente do processo de *Legal Design*, de acordo com suas próprias habilidades, com as necessidades do cliente e com o tipo de problema que se objetiva resolver.

Entretanto, o fluxo principal de todos esses processos é o mesmo: o começo passa por entender as necessidades dos clientes e a área de desafios, entender quais são as suas dores em seus negócios inovadores e, em seguida, apresentar ideias, limitando-se às mais promissoras para

dimensionar para uma implementação mais assertiva e adequada à realidade específica.

É justamente aqui que verificamos o processo de empatia, que é a capacidade de nos colocarmos no lugar do outro e de entendermos algo, no caso do *Legal Design,* o problema jurídico, segundo o ponto de vista do cliente. Este tipo de abordagem busca primeiramente uma imersão no problema, à procura de um entendimento que só pode ser obtido próximo ao cliente para o qual se pretende apresentar uma solução. Essa elucidação é bem diferente de outros modos de trabalho tradicionais, em que o advogado recebe o cliente em seu escritório, faz um resumo padrão do caso e após isso senta à mesa para buscar uma solução, nem sempre se aproximando da realidade e da dor do cliente e muitas vezes até alienando este da construção da solução mais adequada ao caso.

Neste sentido, ferramentas do *Design Thinking* devem ser úteis na formatação do fluxo dos processos acima destacados. Recomenda-se, de início, a utilização do conhecido Canvas de Proposta de Valor, criado por Alexander Osterwalder[4], que pode facilmente ser utilizada por advogados para melhor compreenderem as dores de seus clientes, os ganhos por eles esperados e como os seus serviços e produtos podem se encaixar em suas necessidades.

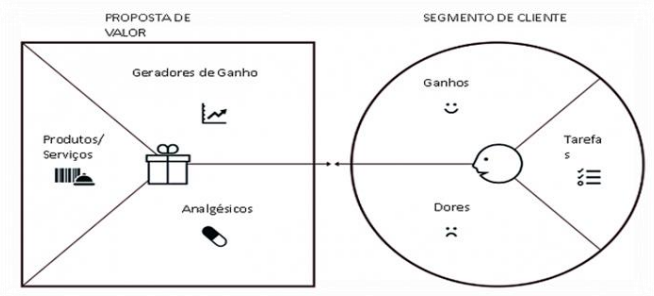

Figura 1 – Canvas de Proposta de Valor.[5]

[4] OSTERWALDER, Alexander; PIGNEUR, Yves; BERNARDA, Greg; SMITH, Alan; PAPADAKOS, Patricia. **Value Proposition Design: How to Create Products and Services Customers Want**. Published by John Wiley & Sons, INC, Hoboken, New Jersey, 2014.

[5] Fonte: https://canaltech.com.br/gestao/proposta-de-valor-por-onde-todo-empreendedor-deveria-comecar/

No contexto da LGPD, a utilização do Canvas de Proposta de Valor poderá ser muito útil e eficaz quando no momento da implementação de procedimentos de conformidade com a LGPD pelas corporações, sendo uma ferramenta estratégica para a implantação de uma cultura de proteção de dados tendo como premissa de partida o destinatário do referido trabalho de implementação, podendo ser este o cliente, o fornecedor de produtos e serviços e terceirizados destes, o empregado da corporação, ou seja, todos aqueles que estiverem envolvidos no tratamento de dados pessoais de alguma forma.

Aqui outra ferramenta útil é o mapa de empatia, ferramenta colaborativa que permite conhecer a fundo seu público-alvo e se colocar no lugar de cada persona para identificar suas dores e necessidades, no caso, dores e necessidades daqueles destinatários da implantação de uma cultura de proteção de dados pessoais e conformidade com a LGPD.

O mapa de empatia oferece uma visão real dos comportamentos, desejos e percepções do destinatário, usuário ou cliente, sendo um recurso que cria uma personagem imaginária representada em um gráfico simples, revelando os reais interesses do destinatário – e não o que se imagina sobre ele.

Basicamente, sua estrutura mostra alguns questionamentos centrais sobre os pensamentos, sentimentos e experiências do indivíduo, que juntos oferecem um panorama detalhado de seu perfil e estilo de vida.

O termo "empatia" diz tudo sobre a ferramenta, pois indica a capacidade de se colocar no lugar do outro e experimentar sua visão de mundo.

O mapa de empatia foi criado pela consultoria de design XPLANE, como parte da Metodologia Canvas para modelos de negócios.

Segundo o fundador da XPLANE, Dave Gray[6], o instrumento visual foi criado para ajudar as equipes a compreender profundamente seus clientes e aprimorar a experiência do usuário.

[6]Fonte: https://medium.com/the-xplane-collection/updated-empathy-map-canvas-46df22df3c8a

O objetivo é capturar o ponto de vista do cliente a partir do *Design Thinking*, que foca nas necessidades do público-alvo para projetar soluções sob medida, ou seja, o mapa de empatia é centrado em pessoas e suas motivações.

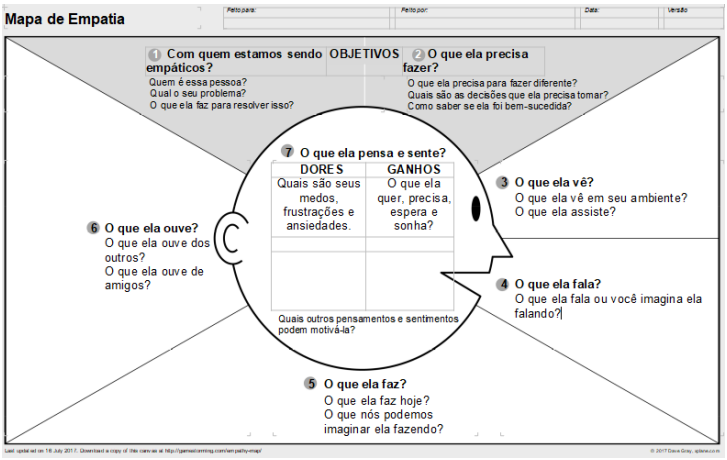

Figura 2 – Mapa de Empatia[7]

Assim, a utilização das ferramentas acima destacadas, dentre outras, será de grande valia ao profissional do direito que se dedicar à área de proteção e segurança de dados pessoais, pois auxiliará na adoção de providências e medidas concretas que tornarão mais fácil a compreensão à LGPD na prática pelos seus destinatários, o que poderá ser um instrumento catalizador de implantação de um cultura de proteção de dados.

A utilização de elementos visuais dentro de um contexto de melhor experiência do destinatário a quem se comunica algo constitui um poderoso instrumento de comunicação e no contexto de educação quanto a aplicação da LGPD e de seus preceitos não poderia ser diferente.

A utilização de vídeos, infográficos (peça visual utilizada para apresentar informações e dados de maneira facilitada, o que ajuda na compreensão do leitor mesmo quando o conteúdo tem maior

[7]Fonte: https://www.voitto.com.br/blog/artigo/mapa-de-empatia

complexidade), *storyboard* (construção gráfica que revela quadro a quadro o conteúdo de um conteúdo audiovisual), *story mapping (*técnica para criar um entendimento de um assunto contando estórias a partir do ponto de vista do destinatário do assunto), *storytelling* (uso de recursos audiovisuais em conexão com palavras através de uma narrativa que crie um vínculo emocional com o destinatário do assunto), fluxogramas (representação esquemática de um processo, muitas vezes feito através de gráficos que ilustram de forma descomplicada a transição de informações entre os elementos que o compõem), e até gamificação (uso de técnicas de jogos para cativar pessoas por intermédio de desafios constantes e bonificações) poderá revolucionar a forma como o profissional do direito que pretende trabalhar com a LGPD e assim obter melhores resultados com os trabalhos de implantação de procedimentos de conformidade com a LGPD e desenvolvimento de uma cultura de proteção de dados pessoais junto aos clientes e a todos os destinatários da norma.

A entrada em vigor da Lei Geral de Proteção de Dados Pessoais — LGPD, prevista para agosto de 2020, traz uma série de novos direitos relacionados a transparência no uso de dados pessoais e sensíveis e é uma ótima oportunidade para aplicação do *Legal Design*, visto que o tema pode contribuir muito para responder aos questionamentos sobre como podemos adequar esse tipo de informação para atendermos aos requisitos da lei.

Neste sentido, entendemos ser importante trazermos alguns exemplos práticos. Sabemos que tradicionalmente os contratos e as políticas de privacidade criados para melhor informar e orientar o usuário (destinatário de tais documentos), nas mais diversas plataformas, digitais ou não, não são transmitidos de forma transparente, clara e de fácil entendimento.

Neste contexto, com a entrada em vigor da *GDPR – General Data Protection Regulation* na Europa, muitas das empresas do velho continente se depararam com a necessidade de adequações e com a oportunidade de redigir contratos e políticas de privacidade que ao mesmo

tempo atendessem ao disposto na lei e fossem de mais fácil entendimento ao público em geral.

Neste sentido, Priscilla Brito[8], destaca a experiência da empresa europeia Juro:

> "Uma empresa europeia, Juro, ao analisar sua política de privacidade, identificou vários problemas que tornavam essa política inacessível e inutilizável. Com o objetivo de transformá-la em algo que as pessoas pudessem se envolver, a Juro aplicou o Legal Design em conformidade com a GDPR – General Data Protection Regulation (lei de proteção de dados em vigor na Europa, que foi base para nossa LGPD), com o intuito de traduzir a informação e adequar a apresentação para usuários leigos.
>
> A parte mais interessante disso tudo, foi que a Juro, após duas semanas de lançamento da nova política, percebeu um aumento de 1.352,94% de usuários que visualizaram sua política completa.
>
> A ação da Juro, além de demonstrar preocupação com o usuário, ajudou a empresa a transmitir seus valores. A disponibilização dos termos contratuais e políticas de privacidade, com fácil entendimento e com leitura agradável, é a melhor forma de transmitir a mensagem de que o cliente é o centro do seu negócio. E o Legal Design está aí para isso."

Veja que no exemplo acima destacado, a utilização do *Legal Design* para adequação de uma política de privacidade foi tão bem sucedida na missão de transparência da informação e adequação da informação ao destinatário que ocasionou até um aumento de pessoas que efetivamente acessaram o documento e tomaram ciência de seu teor, seu principal objetivo.

Outros exemplos são pertinentes. A Europol, agência da União Europeia (UE) responsável por garantir o cumprimento da lei e com foco de atuação na segurança e combate à criminalidade, fez um excelente trabalho ao criar um encarte de folha, de forma objetiva e com elementos visuais, destaca em um esquema uma diretiva sobre proteção de dados pessoais quando estes são utilizados pelas autoridades policiais e

[8]BRITO, Priscilla. **LGPD e UX com uma pitada de Legal Design**. Disponível em: <https://brasil.uxdesign.cc/lgpd-x-ux-legal-design-7515b347e666> Acesso em 01 de fevereiro de 2020.

judiciárias na Europa, apresentando o objetivo central da GDPR – *General Data Protection Regulation,* seus princípios chaves, definição de dado pessoal, titularidade de dados, direitos dos titulares de dados e novidades decorrentes da norma legal.

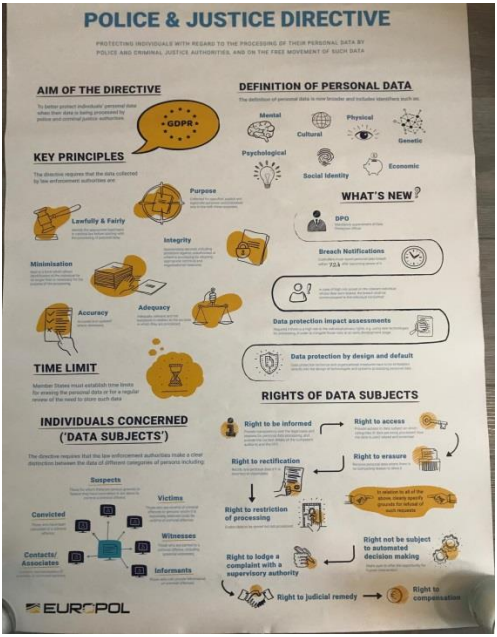

Figura 3 – Diretiva da Europol[9]

O documento acima destacado serve de inspiração para os operadores do direito que se propuserem a doutrinação de desenvolvimento do conhecimento sobre a LGPD e criação de uma cultura de proteção de dados, traduzindo bem o verdadeiro espírito do *Visual Law* e sua adequada aplicação.

No Brasil, já vemos algumas iniciativas semelhantes, como este encarte digital que trata de um perfil do Encarregado de Proteção de dados, com informações bem objetivas e elementos visuais para facilitação do entendimento.

[9] Fonte: https://www.linkedin.com/posts/n%C3%BAria-baxauli-1b0698107_a-lgpd-prev%C3%AA-a-cria%C3%A7%C3%A3o-de-uma-legisla%C3%A7%C3%A3o-activity-6605812526426931200-dHDa

Figura 4 – Encarte Digital sobre o Encarregado de Dados[10]

A própria Administração Pública também tem apresentado iniciativas, como um portal na *web* do Serviço Federal de Processamento

[10]Fonte: https://www.instagram.com/motaalves.fabricio

de Dados (Serpro), empresa pública de prestação de serviços em tecnologia da informação do Brasil, que apresenta uma série de informações sobre a LGPD, com vídeo tratando da norma em 2 (dois) minutos e um infográfico, que permitem ao destinatário da comunicação uma compreensão melhor da temática.

Figura 5 – Infográfico sobre a LGPD pelo Serpro[11]

De igual maneira, a prática dos profissionais que se dedicam ao trabalho de proteção de dados pessoais demonstra uma série de providências que devem ser adotadas para uma implantação eficaz dos procedimentos de conformidade com a LGPD e de fato a utilização da criatividade de forma adequada pode se constituir em instrumento de grande valia para o sucesso do trabalho.

No Brasil, sabemos que algumas empresas apresentam uma variedade de pessoas em níveis de escolaridade e cultural dos mais

[11]Fonte: https://www.serpro.gov.br/lgpd/menu/arquivos/infografico-lgpd-em-um-giro

diversos. Não podemos negar que a forma como deve ser comunicada as obrigações da LGPD para os colaboradores de uma empresa deve estar atenta à realidade fática de cada colaborador, ou seja, a abordagem deve ter como premissa a realidade que é vivenciada por cada um, sendo inteligível que uma transmissão de informações e treinamento mais formal pode gerar fixação de conteúdo e engajamento para pessoas com um nível de escolaridade maior, mas para outras, com escolaridade menor, por exemplo, pode chegar a gerar até um desinteresse pelo tema.

Exemplo prático de solução adequada no cenário acima apontado é relatado pelo professor Cláudio Roberto Magalhães Pessoa, Pós-Doutor em Gestão e segurança da informação na Universidade do Porto (Portugal) e membro certificado *Exin Privacy & Data Protection – Essentials* (LGPD), que em conversa com os autores deste artigo sobre um trabalho desenvolvido para criação de fluxos de segurança da informação e conformidade com a LGPD para uma empresa de grande porte com desnivelamento de nível de escolaridade entre seus colaboradores, narrou ser necessário entender a realidade dos colaboradores de menor grau de instrução e desenvolver uma forma de aprendizado e treinamento lúdico, através de um teatro abordando a temática da LGPD dentro de uma realidade da empresa e na vida daqueles colaboradores, para lançar o tema de forma próxima ao dia a dia daquelas pessoas e assim atingir o objetivo de maior conscientização, fixação de conteúdo e engajamento quanto a necessidade de maior proteção aos dados pessoais e respeito aos ditames legais da LGPD.

Assim, por tudo acima exposto, podemos afirmar que *Legal Design* tornará a aplicação do arcabouço da LGPD mais acessível, mais utilizável e mais envolvente, buscando redesenhar como todos podem usar a lei e criar ferramentas legais que sejam fáceis de usar e compreender. Isso capacita as pessoas para obter o controle de seus direitos e deveres, bem como reitera a premissa atual de que o operador do direito, no exercício de suas funções, tenha uma visão sistêmica da legislação aplicável às

corporações e postura participativa na construção de soluções que sejam mais acessíveis ao entendimento médio.

4. Considerações Finais

Atualmente nos deparamos com uma crescente demanda de tratamento de dados pessoais, seja para cumprimento de obrigações legais ou para obtenção de vantagens comerciais por algumas empresas, estas com o objetivo de fornecer produtos e/ou serviços que sejam úteis, agradáveis e, principalmente, desejáveis ao destinatário.

Foi neste contexto que fora promulgada no Brasil a Lei Geral de Proteção de Dados Pessoas (LGPD) sob o nº. 13.709/2018, a qual tem por objeto a regulamentação das atividades de tratamento de dados pessoais e que deixou latente o grande desafio de inserção da cultura da proteção de dados, o que deve ser objeto de atenção de todos os profissionais que se propõem a dedicar esforços na àrea de proteção e privacidade de dados e segurança da informação.

Neste contexto, o operador do direito deve recorrer às ferramentas e técnicas que possibilitem que o trabalho de interface jurídica de adequação aos preceitos da LGPD seja mais acessível do ponto de vista do destinatário da norma, aplicando assim o *Legal Design,* de forma a permitir uma melhor compreensão e conscientização quanto as disposições legais acerca da proteção de dados pessoais e as vantagens inseridas na legislação e em uma cultura de proteção de dados, capacitando assim o destinatário da norma para obter o controle de seus direitos e deveres, bem como possibilitando uma postura participativa na construção de soluções de conformidade com a LGPD que sejam mais acessíveis ao entendimento médio.

5. Referências:

BRASIL, **Lei nº. 13.709 de 14 de agosto de 2018.** Diário Oficial da República, Poder Executivo, Brasília, DF.

BRITO, Priscilla. **LGPD e UX com uma pitada de Legal Design**. Disponível em: <https://brasil.uxdesign.cc/lgpd-x-ux-legal-design-7515b347e666> Acesso em: 01 de fevereiro de 2020.

BROWN, Tim. **Design Thinking: uma metodologia poderosa para decretar o fim das velhas ideias.** Rio de Janeiro: Alta Books, 2017.

GUALDA, Diego de Lima. **Desafio Cultural da Proteção de Dados.** Disponível em: < https://www.aarb.org.br/desafio-cultural-da-protecao-de-dados/ > Acesso em: 03 de fevereiro de 2020

Leonel, Guilherme; Miyazaki, Natalia. **Legal Design – Uma nova Forma de pensar o Direito.** Disponível em: <https://medium.com/@legalhackerscampinas/legal-design-uma-nova-forma-de-pensar-o-direito-c2618acbfd99 > Acesso em: 10 de março de 2019.

LIMA, Fabricio Alves de; LOEWEM, Eduardo Vianna. **Legal Design Thinking aplicado ao Direito.** Disponível em: <https://fabriciolima92.jusbrasil.com.br/artigos/557928225/legal-design-design thinking-aplicado-ao-direito > Acesso em: 10 de março de 2019.

MACHADO, Matheus Parreira; PESSOA, Thiago Thomaz Siuves. **Legal Design para Startups.** Revista de Direito das Startups, nº2. São Paulo: Enlaw, 2019.

OSTERWALDER, Alexander; PIGNEUR, Yves; BERNARDA, Greg; SMITH, Alan; PAPADAKOS, Patricia. **Value Proposition Design: How to Create Products and Services Customers Want**. Published by John Wiley & Sons, INC, Hoboken, New Jersey, 2014.

PINHEIRO, Tennyson; ALT, Luis. **Design Thinking Brasil: empatia, colaboração e experimentação para pessoas, negócios e sociedade.** Rio de Janeiro: Elsevier, 2012.

WHAT is Legal Design Thinking?. **Visual Contratcs.** Disponível em:<https://www.visualcontracts.eu/community/what-is-legal-design-thinking> Acesso em: 10 de março de 2019

14

LGPD e a privacidade desde a concepção [1]

Lucas Sávio Oliveira [2]

1. Introdução

A Lei Geral de Proteção de Dados[3] ("LGPD") impõe um desafio claro a todos os agentes de tratamento[4]: garantir que a privacidade e a proteção de dados pessoais sejam elementos basilares de sua operação.

O disposto no artigo 46, *caput* e §2º da LGPD evidencia que a privacidade e a proteção de dados precisam fazer parte da cultura dos agentes de tratamento a ponto de que seus produtos e serviços sejam concebidos e executados com a observância 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 forma de tratamento inadequado ou ilícito"[5].

---

[1] Agradeço ao Marcus Drumond, meu amigo e sócio, pelo apoio durante a elaboração deste artigo e, principalmente, por sua cuidadosa revisão.

[2] *Bacharel e Mestre em Direito pela Universidade Federal de Minas Gerais – UFMG e Mestre em Direito Comercial Internacional e Resolução de Litígios pela Swiss International Law School (SiLS). Sócio de Oliveira Drumond Advogados.*

[3] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da União*, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 dez. 2019.

[4] De acordo com o Artigo 5º, VI, VII e IX da LGPD, os agentes de tratamento de dados são tanto o controlador, "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", quanto o operador "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".

[5] *Idem*, artigo 46.

Além disso, de acordo com o artigo 49 da referida lei, "os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares." [6] Tal obrigação é complementada pela necessidade da "adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais"[7], o que será estimulado pela Autoridade Nacional de Proteção de Dados[8], conforme estabelecem os artigos 51 e 55-J, inciso VIII da LGPD.

Esses e outros dispositivos da LGPD são a materialização em nosso ordenamento do conceito de *privacy by design*, que, traduzindo para o português, significa privacidade desde a concepção.

Partindo dessa constatação, este artigo tem como objetivo ampliar a compreensão sobre o que significa o referido conceito, além de oferecer exemplos de medidas que significam, na prática, o cumprimento, pelas corporações, públicas ou privadas, das obrigações legais dele advindas. Para tanto, inicia-se por um resgate histórico da construção do conceito de *privacy by design*, passando a analisar seus 7 princípios fundamentais e terminando com 8 estratégias para implementar a privacidade desde a concepção, apresentado as ligações existentes com a LGPD.

2. Origem e evolução do conceito de *privacy by design*

Conforme explica Peter Hustinx, "o conceito de *'privacy by design'* está intimamente relacionado com o conceito de *'privacy enhancing technologies'* [tecnologias de aprimoramento da privacidade] ou PET. Esse termo foi utilizado pela primeira vez no relatório: '*Privacy-enhancing*

[6] *Idem*, artigo 49.

[7] *Idem*, artigo 51.

[8] Trata-se do órgão da administração pública federal, integrante da Presidência da República, ainda em formação, responsável por editar instruções complementares para facilitar a interpretação da LGPD e fiscalizar os agentes de tratamento.

technologies: o caminho para o anonimato" que foi publicado em 1995."[9] O referido documento foi um trabalho conjunto entre a Autoridade Holandesa de Proteção de Dados, à época presidida pelo próprio Peter Hustinx, e o então Comissário de Informações e Privacidade da Província de Ontário, no Canadá, Tom Wright. Merece destaque o fato de que da equipe de Tom Wright fazia parte, como Comissária Assistente, Ann Cavoukian, uma das mais influentes autoridades na construção e expansão do *privacy by design*, tendo sucedido Tom Wright entre 1997 e 2014 como Comissária de Informações e Privacidade da Província de Ontário.

O trabalho desenvolvido em 1995 trazia reflexões sobre o uso de dados pessoais que, somente agora, com a LGPD, começa-se a fazer no Brasil:

> Ao avaliar a necessidade de dados identificáveis durante o curso de uma transação, a questão principal com a qual devemos começar é: quanta informação / dados pessoais são realmente necessários para o bom funcionamento do sistema de informação que envolve essa transação? Esta pergunta deve ser feita desde o início - antes do design e desenvolvimento de qualquer novo sistema.
>
> (...)
>
> O que é necessário é uma mudança de paradigma de uma mentalidade segundo a qual "mais é melhor" para uma mentalidade minimalista. É possível minimizar a quantidade de dados identificáveis atualmente coletados e armazenados nos sistemas de informação, mas ainda atender às necessidades daqueles que coletam as informações? Acreditamos que sim.[10]

---

[9] No original: "The concept of "Privacy by Design" is closely related to the concept of "privacy enhancing technologies" or PET. This term was used for the first time in the report "Privacy-enhancing technologies: the path to anonymity" that was published in 1995." (HUSTINX, Peter. *Privacy by design: delivering the promises. In.* Identity in the Information Society. Volume 3, Issue 2, 2010, p. 253. Disponível em: <https://link.springer.com/article/10.1007/s12394-010-0061-z>. Acesso em: 2 dec. 2019.) (tradução nossa).

[10] No original: "When assessing the need for identifiable data during the course of a transaction, the key question one must start with is: how much personal information/data is truly required for the proper functioning of the information system involving this transaction? This question must be asked at the outset — prior to the design and development of any new system. (...) What is needed is a paradigm shift away from a "more is better" mindset to a minimalist one. Is it possible to minimize the amount of identifiable data presently collected and stored in information systems, but still meet the needs of those collecting the information? We believe that it is." (BORKING,

Tais reflexões demonstram o início da compreensão de que, para salvaguardar a privacidade e a proteção de dados pessoais, a legislação por si só não é suficiente, o que traz a necessidade de que tais conceitos façam parte dos próprios sistemas de informação, uma compreensão que levou ao desenvolvimento da noção de *privacy by design.*[11]

Antes, porém, de tratar do conceito, se faz necessário esclarecer o que significa uma *privacy enhancing technology*. Ainda que não exista consenso, pode-se dizer que, em linhas gerais, se trata de uma tecnologia que:

> 1. reduz ou elimina o risco de violar os princípios e a legislação de privacidade;
> 2. minimiza a quantidade de dados mantidos sobre indivíduos; e
> 3. capacita os indivíduos a manter o controle das informações sobre si mesmos o tempo todo.[12]

A fim de exemplificar "estratégias das PETs quanto atributos específicos e dimensões que elas devem preservar para cumprir seu objetivo de garantir a privacidade do usuário", Jonas Valente[13] apresenta uma série de mecanismos que podem ser utilizados nas mais diversas tecnologias, tais como: limitação da coleta de dados, propósito específico, autenticação e autorização, anonimização, pseudo-identidade, criptografia, biometria, possibilidade de auditagem, desagregação e controle pelo usuário.

John; CAVOUKIAN, Ann; *et al. Privacy-enhancing technologies: the path to anonymity*. Volume 1. Technical report. Haia, 1995.) (tradução nossa).

[11] CAVOUKIAN, Ann. *Privacy by design – Leading Edge. In.* IEEE Technology and Society Magazine, Volume 31, Issue 4, winter, 2012. Disponível em: <https://ieeexplore.ieee.org/document/6387956/authors#authors>. Acesso em: 2 dec. 2019.

[12] No original: "1. Reduces or eliminates the risk of contravening privacy principles and legislation. 2. minimises the amount of data held about individuals. 3. Empowers individuals to retain control of information about themselves at all times." (ENTERPRISE PRIVACY GROUP. *Privacy by Design: An Overview of Privacy Enhancing Technologies*. 2008. Disponível em: <http://www.dsp.utoronto.ca/projects/surveillance/docs/pbd_pets_paper.pdf>. Acesso em: 2 dec. 2019.) (tradução nossa).

[13] VALENTE, Jonas. *Promovendo a prvacidade e a proteção de dados pela tecnologia: privacy by design e privacy enhancing-technologies. In.* Privacidade em perspectivas. Organizadores Sérgio Branco, Chiara de Teffé. – Rio de Janeiro: Lumen Juris, 2018. pp. 121, ss. Disponível em: <https://itsrio.org/wp-content/uploads/2018/06/Privacidade-em-perspectivas_DTP.pdf> Acesso em: 2 dec. 2019.

Ou seja, em uma estratégia de *privacy by design* as PETs são mecanismos que podem ser utilizados para a proteção dos usuários. Conforme explica Valente, muitas vezes esses conceitos se confundem, mas podem ser trabalhos separadamente,

> sendo o primeiro relacionado à prática global de orientação de todo o processo de desenvolvimento e fabricação com o objetivo de assegurar a privacidade e a proteção de dados do usuário e de coletividades e o segundo a denominação de toda sorte de solução tecnológica que tem esta orientação em seu design.[14]

Ann Cavoukian explica que o *privacy by design* é, em verdade, um *framework*, para que, de forma proativa, a privacidade seja embutida diretamente não somente nas tecnologias da informação, mas também nas práticas de negócio, no *design* físico e em infraestruturas de rede, fazendo com que ela se torne um padrão.[15] Trata-se de uma expansão da noção de proteção da privacidade.

Nas palavras de Daniel Le Métayer:

> privacy by design é algo diferente do uso de ferramentas de aprimoramento de privacidade ou ferramentas de segurança: privacy by design tem a ver com os requisitos gerais de um sistema e a definição de sua arquitetura. Como tal, **privacy by design é uma questão de escolha**: geralmente há várias opções disponíveis para atingir um determinado conjunto de funcionalidades, algumas delas favoráveis à privacidade e outras menos. [16] (Grifou-se).

Ou seja, desde a concepção dos sistemas e soluções é necessário decidir o caminho a se seguir para se chegar a um equilíbrio entre os

---

[14] VALENTE, Jonas. *Promovendo a prvacidade e a proteção de dados pela tecnologia: privacy by design e privacy enhancing-technologies. In.* Privacidade em perspectivas. Organizadores Sérgio Branco, Chiara de Teffé. – Rio de Janeiro: Lumen Juris, 2018. p. 111. Disponível em: <https://itsrio.org/wp-content/uploads/2018/06/Privacidade-em-perspectivas_DTP.pdf> Acesso em: 2 dec. 2019.

[15] CAVOUKIAN, Ann. *Privacy by design – Leading Edge. In.* IEEE Technology and Society Magazine, Volume 31, Issue 4, winter, 2012. Disponível em: <https://ieeexplore.ieee.org/document/6387956/authors#authors>. Acesso em: 2 dec. 2019.

[16] No original: "privacy by design is different from the use of privacy enhancing tools or security tools: privacy by design has to do with the general requirements of a system and definition of its architecture. As such, privacy by design is a matter of choice: multiple options are generally available to achieve a given set of functionalities, some of them being privacy friendly, others less." (MÉTAYER, Daniel Le. *Privacy by Design: A Matter of Choice. In. Data Protection in a Profiled World*. Editores Serge Gutwirth, Yves Poullet, Paul de Hert. Springer, 2010. p. 325.).

objetivos de quem está desenvolvendo o sistema e os direitos dos indivíduos cujos dados serão utilizados para que tais objetivos sejam alcançados.

Segue Le Métayer esclarerendo que,

> em um segundo estágio, ferramentas apropriadas de aprimoramento da privacidade e segurança devem ser identificadas para implementar a arquitetura. Mas, da mesma forma que o uso da criptografia não é de forma alguma uma garantia de segurança, **o uso de ferramentas de aprimoramento ou segurança da privacidade não é, por si só, uma garantia de privacidade**: a questão mais importante é ter uma visão clara da situação geral do sistema, os atores envolvidos, seus níveis de confiança ou autoridade, suas interações, o que eles precisam saber e a informação flui entre eles, a fim de garantir que a escolha das ferramentas seja consistente com os requisitos de privacidade. [17] (Grifou-se).

O *privacy by design* foi, ao longo do tempo, ganhando espaço, a ponto de se tornar requisito de legislações avançadas de proteção de dados, como é o caso do Regulamento Geral de Proteção de Dados da União Europeia, conhecido por sua sigla em inglês GDPR, que deixa expresso em seu Artigo 25 que a proteção de dados deve ser desde a concepção e como padrão.[18]

---

[17] No original: "In a second stage, appropriate privacy enhancing and security tools have to be identified to implement the architecture. But, in the same way as the use of cryptography is by no means a guarantee of security, the use of privacy enhancing or security tools is not in itself a guarantee of privacy: the most important issue is to have a clear view of the overall system, the actors involved, their levels of trust or authority, their interactions, what they need to know and the information flows between them, in order to ensure that the choice of tools is consistent with the privacy requirements."(MÉTAYER, Daniel Le. *Privacy by Design: A Matter of Choice*. *In. Data Protection in a Profiled World*. Editores Serge Gutwirth, Yves Poullet, Paul de Hert. Springer, 2010. pp. 325 e 326.).

[18] "Artigo 25. Proteção de dados desde a concepção e por defeito (SIC). 1. Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os riscos decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica, tanto no momento de definição dos meios de tratamento como no momento do próprio tratamento, as medidas técnicas e organizativas adequadas, como a pseudonimização, destinadas a aplicar com eficácia os princípios da proteção de dados, tais como a minimização, e a incluir as garantias necessárias no tratamento, de uma forma que este cumpra os requisitos do presente regulamento e proteja os direitos dos titulares dos dados. 2. O responsável pelo tratamento aplica medidas técnicas e organizativas para assegurar que, por defeito, só sejam tratados os dados pessoais que forem necessários para cada finalidade específica do tratamento. Essa obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao seu prazo de conservação e à sua acessibilidade. Em especial, essas medidas asseguram que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares. 3. Pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas nos n.ºs 1 e 2 do presente artigo, um procedimento de certificação aprovado nos termos do artigo 42. (UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares

O principal objetivo, perseguido desde a época em que o conceito começou a ser gestado, é o de que a privacidade faça parte da cultura organizacional das corporações, sejam elas privadas ou públicas, de tal forma que, desde a concepção de serviços e produtos, não apenas a preocupação com ela, mas a ocupação efetiva e prática, seja uma realidade. É sobre o que se passa a tratar.

3. Os 7 princípios fundamentais

A fim de que o *privacy by design* seja uma realidade nas organizações em geral, Ann Cavoukian destrinchou o conceito em 7 princípios. Eles oferecem chaves para que se possa compreender as dimensões e alcance da visão que preconiza a privacidade desde a concepção como caminho para garantir a autodeterminação informacional dos titulares de dados e, ao mesmo tempo, oferecer vantagem competitiva às organizações. Passa-se, a seguir, a analisar cada um desses princípios.[19]

3.1 Proativo, não reativo; preventivo, não corretivo

Para que se possa garantir, de fato, a privacidade do usuário, é preciso, antes de mais nada, prever os eventos que sejam invasivos à privacidade e tomar as medidas adequadas para prevenir que tais eventos se materializem. A ideia, portanto, é agir antes que o fato aconteça, e não esperar que isso ocorra e, só então, tomar medidas corretivas. Trata-se do

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). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=pt>. Acesso em: 5 dez. 2019.).

[19] A análise que segue tem como base os seguintes artigos: (i) CAVOUKIAN, Ann. *Privacy by design: the definitive workshop. A foreword. In.* Identity in the Information Society. Volume 3, Issue 2, 2010. pp 247–251 Disponível em: <https://link.springer.com/article/10.1007/s12394-010-0062-y>. Acesso em: 3 dec. 2019. (ii) CAVOUKIAN, Ann. *Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices.* Disponível em: <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>. Acesso em: 3 dec. 2019. (iii) CAVOUKIAN, Ann; TAYLOR, Scott; ABRAMS, Martin E. *Privacy by Design: essential for organizational accountability and strong business practices. In.* Identity in the Information Society. Volume 3, Issue 2, 2010. pp 405–413. Disponível em: <https://link.springer.com/article/10.1007/s12394-010-0053-z>. Acesso em: 3 dec. 2019.

reconhecimento do valor e dos benefícios de se adotar práticas de proteção à privacidade de forma antecipada e consistente.

Tal compreensão deve fazer parte da cultura da organização, a qual deve se comprometer de forma clara com altos níveis de proteção da privacidade. Tal comprometimento deve ser demonstrável, estando expresso em suas políticas e sendo, de fato, imposto em todas as ações da corporação, de forma que todos os envolvidos – usuários, colaboradores e todos os demais *stakeholders* – compreendam que a privacidade é um valor inegociável.

Para tanto, além das políticas, são necessários o aprimoramento e o treinamento contínuos de todos os colaboradores da organização, de forma que os mecanismos existentes para a proteção da privacidade sejam utilizados para fazer com que possíveis incidentes sejam resolvidos antes mesmo de se tornarem problemas reais.

3.2 Privacidade como padrão

Para que exista um nível máximo de privacidade é necessário que os dados pessoais sejam automaticamente protegidos pelos sistemas de informação e pelas práticas de negócios. Na prática, a ideia é a de que, mesmo que o titular não tome nenhuma atitude proativa para a proteção de seus dados, sua privacidade seja mantida. Para tanto, a privacidade deve estar embutida no sistema como um padrão. Caso não esteja claro a necessidade ou o uso que será feito de uma informação pessoal, a regra geral deve ser a presunção da privacidade. É o que se chama de *privacy by default*.

Ann Cavoukian explica que determinadas práticas são corolários desse princípio, quais sejam:

> **Especificação de finalidade** - os propósitos para os quais as informações pessoais são coletadas, usadas, mantidas e divulgadas devem ser comunicadas ao indivíduo (titular dos dados) antes ou no momento em que as informações

são coletadas. Os propósitos especificados devem ser claros, limitados e relevantes para as circunstâncias.

Limitação de coleta - a coleta de informações pessoais deve ser justa, lícita e limitada àquela necessária para os fins especificados.

Minimização de dados - a coleta de informações de identificação pessoal deve ser mantida em um mínimo estrito. O design de programas, tecnologias de informação e comunicação e de sistemas deve começar com interações e transações não identificáveis, como padrão. Sempre que possível, a identificação, observabilidade e vinculação de informações pessoais devem ser minimizadas.

Limitação de uso, retenção e divulgação - o uso, retenção e divulgação de informações pessoais devem ser limitados aos objetivos relevantes identificados para o indivíduo, pelos quais ele consentiu, exceto quando exigido por lei. As informações pessoais devem ser retidas apenas pelo tempo necessário para cumprir os propósitos declarados e depois destruídas com segurança.[20]

Tais práticas estão intimamente relacionadas aos princípios que devem ser observados nas atividades de tratamento de dados pessoais dispostos no artigo 6º da LGPD[21], estando, da mesma forma, inter-

[20] No original: "**Purpose Specification** – the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances. **Collection Limitation** – the collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes. **Data Minimization** – the collection of personally identifiable information should be kept to a strict minimum. The design of programs, information and communications technologies, and systems should begin with non-identifiable interactions and transactions, as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized. **Use, Retention, and Disclosure Limitation** – the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed. (CAVOUKIAN, Ann. *Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices.* Disponível em: <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>. Acesso em: 3 dec. 2019.).

[21] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados; IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais; V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza,

relacionados com os demais princípios fundamentais do *privacy by design* ora analisados.

3.3 Privacidade incorporada ao design

A privacidade deve ser incorporada ao desenho e à arquitetura tanto dos sistemas de informação, quanto das práticas de negócio de forma: (i) holística – considerando contextos mais amplos; integrativa – a fim de abarcar todos os *stakeholders* e interesses envolvidos; e (ii) criativa – já que embutir privacidade pode, muitas vezes, significar a necessidade de alterar escolhas feitas previamente, as quais não respondam ao valor. Assim, a privacidade passa a ser parte dos próprios mecanismos como um componente essencial, uma funcionalidade central a ser entregue ao usuário, e não um mero apêndice.

A ideia central é a de minimizar ao máximo os possíveis impactos na privacidade que possam ser causados pela tecnologia, operação ou arquitetura de informações da corporação, garantindo que a proteção da privacidade não seja facilmente comprometida por qualquer uso, configuração incorreta ou erro. Aqui entra a necessidade de realizar e publicar, de forma contínua e sistemática, avaliações de impacto e risco de privacidade, a fim de que não apenas os riscos, mas as medidas para mitiga-los, estejam documentados, sejam demonstráveis e auditáveis.

---

relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento; VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial; VII - **segurança**: utilização de medidas 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 difusão; VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."(Grifou-se) (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da União*, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 dez. 2019.).

3.4 Funcionalidade total: soma positiva, não soma zero

Determinadas visões sobre a privacidade e a proteção de dados tendem a colocar esses objetivos como impeditivos para o alcance de outros interesses legítimos ou mesmo para a existência de funcionalidades técnicas. É como se a proteção da privacidade significasse, por exemplo, a perda de ganhos econômicos, numa soma zero, na qual um anula o outro.

O *privacy by design* vem quebrar essa falsa dicotomia ao defender que todos os objetivos devem ser alcançados, incluindo a proteção à privacidade. Para tanto, convida a buscar soluções criativas que possam acomodar, na maior extensão possível, os variados interesses envolvidos e as funcionalidades esperadas em um contexto de ganha-ganha e, portanto, numa soma positiva.

Ao incorporar a privacidade em suas operações, as corporações acabam aprendendo a gerar ainda mais valor econômico ao proteger a privacidade individual. Tanto é assim que a própria LGPD estabelece como um de seus fundamentos "o desenvolvimento econômico e tecnológico e a inovação"[22].

Cabe, quanto a isso, refletir sobre o fato de que o respeito à privacidade irá significar, dentro de pouco tempo, um ativo importante para manter e captar clientes, sejam eles os próprios titulares ou empresas com as quais as corporações se relacionam, os quais estarão cada vez mais conscientes e ocupados com a proteção de dados pessoais.

3.5 Segurança de ponta a ponta e proteção total do ciclo de vida

Sem segurança não é possível garantir a privacidade. Não apenas a segurança da informação digitalmente armazenada, mas também, em determinados casos, medidas de segurança física, já que nem todos os

[22] BRASIL. Artigo 2º, V. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da União*, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 dez. 2019.

dados pessoais são digitalizados. E, para que seja efetiva, a segurança deve estar presente em todo o ciclo de vida do dado pessoal na organização, desde sua coleta até sua devida, apropriada e tempestiva eliminação, incluindo, por exemplo, criptografia, controles e níveis de acesso aos dados e mecanismos de autenticação.

Seguindo o disposto na LGPD, segurança deve ser um atributo entendido como a "utilização de medidas 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 difusão"[23], sendo este um dos princípios norteadores da legislação. Tal aspecto é um dos que justifica o fato de que o trabalho de adequação e manutenção da conformidade à LGPD deve ser feito em conjunto, no mínimo, por profissionais do campo do direito e da ciência da informação.

Reitera-se, quanto a esse princípio, o disposto nos artigos 46, §2º, e 49 da LGPD, os quais evidenciam a necessidade de se considerar a segurança dos dados desde a concepção e estruturar os sistemas de forma a atender os requisitos de segurança e as boas práticas de governança.

Vale frisar que a segurança também deve ser demonstrável, estando não apenas escrita na necessária política de segurança da informação, mas efetivamente colocada em prática por todos na corporação. Para tanto, a conscientização constante da equipe, das mais variadas formas e estratégias, é um elemento essencial para que as falhas não ocorram, justamente, por ações ou omissões humanas.

3.6 Visibilidade e Transparência

As corporações precisam estar abertas e ser honestas com os titulares dos dados com os quais opera. Nesse sentido, elas precisam estar preparadas para prestar contas e gerar confiança nos indivíduos dando

[23] Idem. Artigo 6º, VII.

visibilidade às suas políticas e práticas de proteção de dados, bem como sendo transparentes com os usos efetivamente feitos dos dados.

Ann Cavoukian destaca como práticas essenciais para o cumprimento desse princípio as seguintes:

> **Responsabilização** - A coleta de informações pessoais implica um dever de cuidar de sua proteção. A responsabilidade por todas as políticas e procedimentos relacionados à privacidade deve ser documentada e comunicada conforme apropriado e atribuída a um indivíduo especificado. Ao transferir informações pessoais para terceiros, uma proteção de privacidade equivalente por meios contratuais ou outros deve ser garantida.
>
> **Abertura** - Abertura e transparência são essenciais para a prestação de contas. As informações sobre as políticas e práticas relacionadas ao gerenciamento de informações pessoais devem ser prontamente disponibilizadas aos indivíduos.
>
> **Conformidade** - Devem ser estabelecidos mecanismos de reclamação e reparação, e as informações comunicadas sobre eles a indivíduos, incluindo como acessar o próximo nível de recurso. As etapas necessárias para monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade devem ser tomadas.[24]

Ou seja, todos as políticas e procedimentos adotados pela corporação para a proteção de dados devem estar devidamente documentados, o que vai desde o relatório de impacto à proteção de dados ao plano em caso de incidente de segurança, passando pelas avaliações de legítimo interesse, política de proteção de dados e cláusulas contratuais.

---

[24] No original: "**Accountabilty** – The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured. **Openness** – Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals. **Compliance** – Complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken. (CAVOUKIAN, Ann. *Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices*. Disponível em: <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>. Acesso em: 3 dec. 2019.).

Não à toa, portanto, o fato de "a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados" e "a adoção de política de boas práticas e governança" [25] serem parâmetros para a definição das sanções em caso de infrações à LGPD. Mais que isso, a transparência é um dos princípios de nossa lei, conforme expresso no artigo 6º, VI: "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial".

3.7 Respeito à privacidade e foco no usuário

O último e talvez mais importante princípio de *privacy by design* está refletido justamente nos dois primeiros fundamentos da proteção de dados em nosso ordenamento: respeito à privacidade e autodeterminação informativa[26].

Para que haja o respeito à privacidade é preciso que o usuário, ou seja, o titular dos dados seja colocado no centro, de tal forma que os resultados do processo de *privacy by design* venham do legítimo reconhecimento dos interesses desses usuários. Como consequência, deve ser dado a eles o poder de decidir sobre seus próprios dados e exercer, no caso brasileiro, todos os direitos estabelecidos no artigo 18 da LGPD.[27]

---

[25] BRASIL. Artigo 52, §1º, VIII e IX. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da União*, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 dez. 2019.

[26] *Idem*. Artigo 2º, I e II.

[27] "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; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei." (BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da União*, 15 ago. 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 dez. 2019.).

Nas palavras de Ann Cavoukian,

> O respeito à privacidade do usuário (...) se estende à necessidade de que as interfaces homem-máquina sejam centradas no ser humano, centradas no usuário e amigáveis a ele, a fim de que decisões informadas sobre privacidade possam ser exercidas com segurança. Da mesma forma, as operações de negócios e as arquiteturas físicas também devem demonstrar o mesmo grau de consideração para com o indivíduo, que deve aparecer com destaque no centro das operações que envolvem coleta de dados pessoais.[28]

É preciso compreender o comportamento do titular e, até mesmo, sua percepção quanto à privacidade. Os responsáveis por esses desenhos, como os desenvolvedores, por exemplo, devem ser capazes de compreender possíveis vulnerabilidades, assim como o significado de eventuais violações de dados, não apenas sob a perspectiva das corporações, mas sim, e principalmente, do ponto de vista dos titulares de dados.[29]

4. Estratégias para se considerar

Além dos princípios acima descritos, existem 8 estratégias concretas de privacidade que auxiliam na tomada de decisões quanto ao desenho de processos e sistemas. Conforme explica Jaap-Henk Hoepman, elas podem ser divididas em estratégias orientadas aos dados (minimizar, separar, abstrair e esconder) e estratégias orientadas a processos (informar, controlar, dar cumprimento e demonstrar).[30]

---

[28] No original: "Respect for User Privacy (...) extends to the need for human-machine interfaces to be human-centered, user-centric and user-friendly so that informed privacy decisions may be reliably exercised. Similarly, business operations and physical architectures should also demonstrate the same degree of consideration for the individual, who should feature prominently at the centre of operations involving collections of personal data." (CAVOUKIAN, Ann. *Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices*. Disponível em: <https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>. Acesso em: 3 dec. 2019.).

[29] SENARATH, Awanthika; ARACHCHILAGE, Nalin A.G.; SLAY, Jill. Designing. *Privacy for You: A Practical Approach for User-Centric Privacy*. *In*. Human Aspects of Information Security, Privacy and Trust. Editor Theo Tryfonas. Springer, 2017. p.746.

[30] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 3 Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

A figura abaixo, de autoria do próprio Jaap-Henk Hoepman[31] e aqui traduzida, deixa claro que, pensando nas fases de desenvolvimento de um software, as estratégias apresentadas devem ser utilizadas desde o início do processo, nas fases de desenvolvimento do conceito e análise. Já os padrões de desenho de privacidade devem vir na fase de *design*. As tecnologias de aprimoramento da privacidade, por sua vez, vêm na fase de implementação.

Passa-se, então, a apresentar cada uma das 8 estratégias.

4.1 Minimizar

"Limite, ao máximo possível, o processamento de dados pessoais."[32]

Essa é, sem dúvidas, a melhor – e mais óbvia – das estratégias. Ora, quanto menos dados pessoais, menores são as possibilidades de abuso, de vazamento ou de uso inadequado. Por isso, é preciso pensar muito bem se os dados pessoais são realmente necessários para atingir os fins pretendidos: uma mudança de estratégia pode fazer com que bem menos dados sejam necessários ou menos evitar que eles tenham que ser coletados. É preciso ser específico com os propósitos.

Verifica-se que que na LGPD a minimização aparece na forma do princípio da necessidade, expresso no artigo 6º, III: "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados."[33]

---

[31] HOEPMAN, Jaap-Henk. *Making Privacy by Design Concrete. In.* European Cyber Security Perspectives. 2018. p. 26. Disponível em <https://overons.kpn/content/downloads/news/Brochure_Cyber_security_2018

_web.pdf> Acesso em: 4 dec. 2019.

[32] No original: "Limit as much as possible the processing of personal data." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 5. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.)

[33] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da União*, 15 ago. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 dez. 2019.

Hoepman indica algumas táticas relacionadas a essa estratégia:[34]

a. selecionar as pessoas relevantes e os dados relevantes dessas pessoas;
b. excluir os dados irrelevantes antes mesmo da coleta;
c. remover os dados assim que eles deixarem de ser necessários; e
d. destruir completamente os dados quando eles não forem mais necessários.

4.2 Separar

"Separe o processamento de dados o máximo possível."[35]

A estratégia consiste em separar, de forma lógica e física, o processamento de dados a fim de fazer com que seja mais difícil combinar e fazer correlações com diferentes tipos de dados e garantir integridade contextual.

As duas táticas para tanto são:[36]

a. isolar, coletando e processando dados pessoais em bases de dados ou aplicações distintas; e
b. distribuir a coleta e o processamento de dados em diferentes localizações físicas, utilizando bases de dados que não estejam sob o controle de uma mesma entidade.

4.3 Abstrair

"Limite ao máximo os detalhes em que os dados pessoais são processados."[37]

---

[34] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 5. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

[35] No original: "Separate the processing of personal data as much as possible." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 8. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.).

[36] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 5. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

[37] No original: "Limit as much as possible the detail in which personal data is processed." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 10. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.).

Enquanto a estratégia da minimização faz com que nos perguntemos que dados são necessários, a abstração nos faz questionar o nível de detalhes que de fato são necessários para alcançar determinada finalidade. Quanto menos detalhado o dado, menor o risco.

Para que a estratégia seja efetiva, o recomentado é adotar as seguintes táticas:[38]

a. resumir, ou seja, preferir dados mais genéricos, tais como a idade ao invés data de nascimento, ou o nome da cidade no lugar de um endereço completo, por exemplo;
b. agrupar, agregando informações genéricas sobre um grupo de pessoas ao invés de manter dados pessoais; e
c. alterar, de propósito e com um critério aleatório, determinados dados, de modo que o resultado permaneça relevante, mas sem revelar a realidade sobre o titular do dado, como, por exemplo, alterar um a localização real de uma pessoa.

4.4 Esconder

"Proteja os dados pessoais ou torne-os impossíveis de serem "linkados" ou vistos. Certifique-se de que não se tornem públicos ou conhecidos."[39]

A ideia central desta estratégia é fazer com que os dados pessoais sejam protegidos de tal forma que seu acesso não seja possível, que seja impossível ligá-los a uma determinada pessoa (utilizando técnicas de anonimização, por exemplo) ou até mesmo fazer com que seja impossível saber de sua existência.

As táticas relacionadas a essa estratégia são:[40]

[38] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 10. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

[39] No original: "Protect personal data, or make it unlinkable or unobservable. Make sure it does not become public or known." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 12. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.).

[40] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 12. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

a. restringir o acesso aos dados apenas a quem, de fato, precisa, tomando medidas para que seja difícil que, acidentalmente, tais dados sejam vazados ou compartilhados;
b. ofuscar as informações de tal forma que elas não sejam inteligíveis para quem não souber como decifrá-las ou não tiver a chave para tanto;
c. dissociar as informações, retirando as ligações e correlações entre elas e removendo dados que tornem uma pessoa diretamente identificável; e
d. mesclar os dados pessoais de tal forma que sua fonte e suas inter-relações não fiquem claras.

4.5 Informar

"Informar os titulares dos dados sobre o processamento de seus dados pessoais dados de maneira oportuna e adequada."[41]

Uma vez mais, a transparência aparece como ponto central do *privacy by design*. Os titulares de dados devem ser informados sobre quais dados estão sendo processados, de que forma o são e com qual finalidade. Isso gera confiança nos titulares de dados, que poderão tomar decisões informadas, e demonstrará o grau de responsabilidade da corporação quanto ao uso de dados.

Para tanto, algumas táticas podem ser adotadas:[42]

a. suprir os titulares de dados com informações claras sobre o processamento de dados, sobre a retenção de dados e sobre os parceiros com quem eles são compartilhados, dando acesso livre e fácil à política de privacidade e deixando claro como as pessoas podem entrar em contato para tirar dúvidas ou exercer direitos;
b. explicar que dados são processados e os motivos para tanto, tudo de forma didática e simples para que os titulares dos dados realmente entendam o que é feito; e
c. notificar os titulares de dados sobre o tratamento que é realizado, sobre o compartilhamento com terceiros e, tão logo a corporação tomar conhecimento,

[41] No original: "Inform data subjects about the processing of their personal data in a timely and adequate manner." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 14. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.).

[42] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 14. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

quando um vazamento ocorrer, prezando sempre pela objetividade e clareza das informações e dando ao titular a possibilidade de escolher sobre o que quer ser notificado.

4.6 Controlar

"Forneça aos titulares dos dados controle adequado sobre o processamento de seus dados pessoais."[43]

Esta é uma estratégia fundamental, já que permite aos titulares de dados ter algo que eles de fato querem: voz sobre como seus dados são utilizados. Isso sem comprometer que o uso e o compartilhamento necessários para que os serviços sejam fornecidos a eles.

O controle sobre os dados pessoais pode ser garantido aos titulares de várias maneiras:[44]

a. em determinados casos, pedir o consentimento do titular será uma forma de controle, desde que o consentimento seja informado e possa ser facilmente retirado;
b. oferecer alternativas ao titular, fazendo com que determinadas funcionalidades só possam usufruídas mediante consentimento para o processamento de dados;
c. informar aos titulares que dados foram e são coletados e dar aos titulares a possibilidade de revisão e atualização de tais dados, usando um *dashboard* de privacidade, por exemplo; e
d. dar aos usuários a possibilidade de excluir seus próprios dados, o que também pode ser feito por um *dashboard*.

4.7 Dar cumprimento

"Comprometa-se a processar dados pessoais de maneira amigável à privacidade e dê cumprimento a isso adequadamente."[45]

---

[43] No original: "Provide data subjects adequate control over the processing of their personal data." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 16. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.).

[44] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 16. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

[45] No original: "Commit to processing personal data in a privacy-friendly way, and adequately enforce this." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 18. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.).

É preciso ter políticas claras de privacidade e segurança da informação e dar cumprimento a elas, começando pela alta administração, de forma que todos na corporação se sintam responsáveis por garantir a privacidade dos titulares de dados. Trata-se, portanto, de uma estratégia organizacional.

A efetividade virá do cumprimento de algumas táticas:[46]

a. a primeira delas é construir uma política de privacidade e segurança da informação e tomar para si a responsabilidade de que ela seja cumprida;
b. depois, será necessário manter a política, sustentar sua existência não apenas com controles técnicos e organizacionais, mas com a atribuição de responsabilidades, o treinamento de todo o pessoal interno e com medidas para garantir que terceiros, como operadores de dados, também cumpram com a política; e
c. considerando que as circunstâncias e contextos mudam, será necessário rever a política e fazer e implementar alterações sempre que necessário, mantendo-a de forma efetiva.

4.8 Demonstrar

"Demonstre que você está processando dados pessoais de maneira amigável à privacidade."[47]

Não basta ser: é preciso demonstrar que se é. As corporações devem ser capazes de demonstrar, não apenas para os titulares de dados, mas para as autoridades, que dão cumprimento à legislação de proteção à privacidade.

Para tanto, as táticas são as seguintes:[48]

[46] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 18. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

[47] No original: "Demonstrate you are processing personal data in a privacy-friendly way." (HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 20. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.).

[48] HOEPMAN, Jaap-Henk. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 20. Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

a. documentar todos os passos importantes tomados para que a adequação à legislação, incluindo *logs,* certificando-se de que a documentação condiz com a realidade;
b. auditar constantemente os procedimentos organizacionais em geral, em especial como os dados pessoais estão sendo processados; e
c. reporte os dados para a autoridade de proteção de dados e, sempre que necessário e possível, a consulte.

5. Conclusão

A LGPD veio trazendo a necessidade de que as corporações, sejam elas privadas ou públicas, reavaliem, de forma profunda, suas práticas, processos e procedimentos que envolvem a coleta e tratamento de dados pessoais. Isso se justifica pelo fato de que a privacidade e os interesses titulares de dados devem passar a figurar como elementos essenciais para a tomada de decisões estratégicas, que influenciam, inclusive, modelos de negócios.

Uma das medidas mais efetivas para que a proteção à privacidade e aos dados pessoais seja colocada em prática, desenvolvida ao longo de anos de pesquisa e comprovação prática partindo da ideia de que as tecnologias devem aprimorar a privacidade, é a adoção do conceito de *privacy by design*, ou seja, o de considerar a privacidade desde a concepção de produtos e serviços.

Como visto, tal adoção depende de medidas efetivas baseadas nos princípios que informam o conceito. Foram apresentadas, ainda, 8 estratégias práticas para que a privacidade seja considerada desde o início dos processos, já fase de desenvolvimento do conceito.

6. Referências

BORKING, John; CAVOUKIAN, Ann; *et al. Privacy-enhancing technologies: the path to anonymity*. Volume 1. Technical report. Haia, 1995.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. *Diário Oficial da União*, 15 ago. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 1 dez. 2019.

CAVOUKIAN, Ann. *Privacy by design – Leading Edge. In.* IEEE Technology and Society Magazine, Volume 31, Issue 4, winter, 2012. Disponível em: <https://ieeexplore.ieee.org/document/6387956/authors#authors>. Acesso em: 2 dec. 2019.

_____. *Privacy by Design: The 7 Foundational Principles - Implementation and Mapping of Fair Information Practices.* Disponível em: < https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf>. Acesso em: 3 dec. 2019.

_____. *Privacy by design: the definitive workshop. A foreword. In.* Identity in the Information Society. Volume 3, Issue 2, 2010. pp 247–251 Disponível em: <https://link.springer.com/article/10.1007/s12394-010-0062-y>. Acesso em: 3 dec. 2019.

CAVOUKIAN, Ann; TAYLOR, Scott; ABRAMS, Martin E. *Privacy by Design: essential for organizational accountability and strong business practices. In.* Identity in the Information Society. Volume 3, Issue 2, 2010. pp 405–413. Disponível em: < https://link.springer.com/article/10.1007/s12394-010-0053-z>. Acesso em: 3 dec. 2019.

D´ ACQUISTO, Giuseppe. DOMINGO -FERRER, Josep. KIKIRAS, Panayotis, TORRA, Vicenç. DE MONTOJYE, Ives-Alexandre. BOURKA, Athena. *Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics*. ENISA (European Union Agency for Network and Information Security), 2015.

ENTERPRISE PRIVACY GROUP. *Privacy by Design: An Overview of Privacy Enhancing Technologies*. 2008. Disponível em: <http://www.dsp.utoronto.ca/projects/surveillance/docs/pbd_pets_paper.pdf>. Acesso em: 2 dec. 2019.

HOEPMAN, Jaap-Henk. *Making Privacy by Design Concrete. In.* European Cyber Security Perspectives. 2018. Disponível em <https://overons.kpn/content/downloads/news/Brochure_Cyber_security_2018_web.pdf> Acesso em: 4 dec. 2019.

_____. *Privacy Design Strategies (The Little Blue Book)*. Publicação independente. 2019. p. 3 Disponível em: <https://www.cs.ru.nl/~jhh/publications/pds-booklet.pdf> Acesso em: 4 dec. 2019.

HUSTINX, Peter. *Privacy by design: delivering the promises. In.* Identity in the Information Society. Volume 3, Issue 2, 2010. Disponível em: <https://link.springer.com/article/10.1007/s12394-010-0061-z>. Acesso em: 2 dec. 2019.

MÉTAYER, Daniel Le. *Privacy by Design: A Matter of Choice. In. Data Protection in a Profiled World*. Editores Serge Gutwirth, Yves Poullet, Paul de Hert. Springer, 2010.

SENARATH, Awanthika; ARACHCHILAGE, Nalin A.G.; SLAY, Jill. Designing. *Privacy for You: A Practical Approach for User-Centric Privacy. In.* Human Aspects of Information Security, Privacy and Trust. Editor Theo Tryfonas. Springer, 2017. p.746.

VALENTE, Jonas. *Promovendo a prvacidade e a proteção de dados pela tecnologia: privacy by design e privacy enhancing-technologies. In.* Privacidade em perspectivas. Organizadores Sérgio Branco, Chiara de Teffé. – Rio de Janeiro: Lumen Juris, 2018. Disponível em: <https://itsrio.org/wp-content/uploads/2018/06/Privacidade-em-perspectivas_DTP.pdf> Acesso em: 2 dec. 2019.

15

Análise jurídica dos incidentes de segurança e a responsabilidade civil no Brasil

Vitor Eduardo Lacerda de Araújo [1]
Douglas Dias Vieira de Figueredo [2]

1. Introdução

Partindo-se do conceito formulado pelo Regulamento Geral de Proteção de Dados Europeu, uma vez que a legislação nacional não o definiu, um incidente de segurança é (UNIÃO EUROPEIA, 2016):

> "uma violação que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento".

Incidentes de segurança são muito diversificados, podendo ser *scans*, notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles; *worms* notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede; ataques *web*, que visam o comprometimento de

[1] *Mestrando em Direito Digital e Bacharel em Direito - UFMG. Especialista em Direito Processual Penal - Faculdade Internacional Signorelli. Estagiário Docente na disciplina Direito Penal II - UFMG. Supervisor Jurídico de Instituição Financeira. Membro da Comissão de Proteção de Dados - OAB/MG*

[2] *Advogado e Professor Universitário (Graduação e Pós-Graduação. Mestre em Direito – Escola Superior Dom Helder Câmara. Especialista em Direito Tributário - CEAJUFE. Especialista em Direito e Processo Civil - FADIPA. Certificate in Business Analytics, Financial Accounting and Economics for Managers - HARVARD BUSINESS SCHOOL. Gerente Jurídico de Instituição Financeira*

servidores ou desfigurações de páginas na Internet; invasões, ou acesso não autorizado a computadores e redes; *denial of service (DoS)*; e fraudes, tendo sido reportados quase 2 milhões de incidentes ao Núcleo de Informação e Coordenação do Ponto BR nos últimos dois anos. Assim, além da violação da privacidade e acesso não autorizado a dados pessoais de pessoas naturais, fatos como esses são capazes de resultar em danos patrimoniais, morais e até mesmo colocar em risco a vida de pessoas.

Somente no ano de 2018 no Brasil, tivemos inúmeros casos relevantes de falhas e tratamentos inadequados em segurança da informação, destacando-se o ocorrido com a Uber, com comunicação de vazamento de dados de mais de 156 mil pessoas, em 2016, mas apenas relatado no último ano; a Netshoes, com exposição de dados de mais de 2 milhões de clientes ao final de 2017; o Facebook, que no escândalo "Cambridge Analytica" comprometeu dados de quase 500 mil brasileiros (GRANVILLE, 2019); o Banco Inter, com vazamento de dados de 19 mil correntistas, em que houve acordo com o Ministério Público do Distrito Federal e Territórios para o pagamento de quantia de R$ 1,5 milhão de reais a instituições de combate ao crime cibernético e também de caridade; e, por último a C&A, que sofreu ciberataque em sistema de vale-presente e trocas, que resultou em mais de 2 milhões de clientes afetados (LOTT, 2019).

Devido aos números e os famosos casos de empresas líderes de mercado, foi atraída a atenção da comunidade jurídica em torno da criação de uma legislação nacional que garantisse segurança aos titulares de dados pessoais. Assim, com o intuito de auxiliar na criação uma cultura de proteção de dados no Brasil, foi promulgada a Lei nº 13.709 em agosto de 2018, com prazo de entrada em vigor em dois anos após sua publicação.

Sob a ótica das empresas, preocupam-nas os custos que serão dispendidos para adequações sistêmicas e procedimentais para estarem em conformidade com a norma, mas principalmente os relacionados a potenciais indenizações a que serão condenadas em processos administrativos e judiciais. Os orçamentos das organizações deverão estar

preparados para ações judiciais individuais e coletivas, ajuizadas por clientes, funcionários e demais pessoas físicas relacionadas, cooperação com investigações administrativas e judiciais, auditorias, multas, respostas à incidentes, remodelagem da infraestrutura de segurança da informação, seguros cibernéticos, danos à imagem e reputação empresarial, dentre outros.

Preocupa-nos que o aplicador da lei não estará familiarizado com a matéria quando à comunidade acadêmica, que há tempos se debruça sobre doutrinas estrangeiras e observa os comportamentos do judiciário europeu e norte-americano. Portanto, não é interesse do presente artigo a investigação de casos de incidente de segurança da legislação alienígena, ou o aprofundamento nas compreensões europeias sobre a matéria de privacidade e proteção de dados, devido ao objetivo de aproximar o jurista brasileiro da situação nacional. Nesse sentido, será realizada uma abordagem vinculativa entre a nova legislação de proteção de dados e as já consagradas hipóteses de responsabilidade civil, visando-se predizer a atuação dos magistrados nacionais quando da aplicação do novo diploma legal à situação brasileira.

Desse modo, na primeira parte do artigo explicaremos o que são incidentes de segurança, com enfoque no vazamento de dados, o mais comumente causador de danos a titulares pessoas naturais; em um segundo momento estudaremos as hipóteses de responsabilidade civil no ordenamento jurídico brasileiro, com o intuito de facilitar a compreensão de como se dará a sua configuração a partir da entrada em vigor da lei; e, por último, trataremos acerca da ausência de responsabilidade civil dos agentes de tratamento de dados, por instrumentos já previstos na legislação nacional Não é interesse do presente trabalho a explanação de conceitos básicos da matéria, a diferenciação entre direito à privacidade e proteção de dados pessoais, bem como a retomada histórica do surgimento de leis protetivas.

O nosso intuito maior é seguir as discussões acerca da aplicação dos diplomas legais relacionados, sobretudo a Lei nº 13.709/2018, devendo ser

analisados especificamente as disposições normativas concernentes à ocorrência de incidentes de segurança, atribuição de responsabilidades sob o aspecto civil e a possibilidade de mitigação de riscos.

2. Incidentes de segurança e vazamento de dados

Antes de tratarmos especificamente acerca da responsabilidade do agente de tratamento de dados, deve-se conceituar pela doutrina e legislação o que é um incidente de segurança da informação categorizado como vazamento de dados, também chamado de *data breach*.

Um incidente de segurança ocorre quando algum indivíduo obtém, de forma não autorizada, acesso a sistemas e dados protegidos de uma organização, sendo esse um estágio inicial de violação que podem levar a danos em sistema e exposição de dados (SYMANOVICH, 2019). Ou, segundo entendimento do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, "*qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores*", citando, como exemplo, tentativas de ganhar acesso não autorizado a sistemas ou dados, ataques de negação de serviço, uso ou acesso não autorizado a um sistema, modificações em um sistema, sem o conhecimento, instruções ou consentimento prévio do dono do sistema e desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso.

Nesse sentido, um incidente de vazamento de dados pessoais ocorre quando a violação da segurança acaba por expor informações de pessoas naturais, protegidos ou confidenciais, que são copiados, transmitidos, vistos, roubados ou utilizados por indivíduo não autorizado a fazê-lo (U.S. DEPARTAMENTO OF HEALTH AND HUMAN SERVICES, 2019).

O *data breach* poderá ocorrer de forma ativa/intencional ou passiva/negligente. A primeira, quando um *cracker*, com o intuito de obter proveito econômico em conduta ilícita, obtém acesso não autorizado a uma base de dados, podendo exigir o resgate mediante pagamento em dinheiro

ou até mesmo criptomoedas; ou, de forma negligente por parte do agente de tratamento de dados, quando um *hacker*, com o objetivo de detectar vulnerabilidades em sistemas e aplicações de empresas identifica uma falha de segurança com exposição de informações, sujeito ao acesso de agente mal-intencionados. Nesse segundo caso, o *hacker* que identifica a falha de segurança não pratica crime, somente informa a empresa acerca dos dados expostos, que, deverá, então, identificar a ocorrência de coleta por outros agentes, por meio de parecer técnico emitido por profissional de segurança da informação.

No Brasil, até o advento da Lei Geral de Proteção aos Dados Pessoais, ainda não havia disposições legais específicas quanto à incidentes de segurança. No entanto, o art. 48 do referido diploma dispõe que "*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*" (BRASIL, 2018), sem conceituar o que seria tal ocorrência. Já o Decreto nº 8.771/2016, que regulamento o Marco Civil da Internet, trata tão somente da responsabilidade pelos danos causados em falhas de guarda de registros de conexão, acesso e conteúdo, conforme artigos 13, §6º;15, §4º; 17; e 18 (BRASIL, 2018), conforme falaremos em seção específica. Por outro lado, no âmbito do Regulamento Europeu de Proteção de Dados Pessoais há conceituação precisa expressa no art. 4º, item 12 (UNIÃO EUROPEIA, 2016):

> *"o vazamento de dados pessoais significa uma falha na segurança que resulta em destruição acidental ou ilícita, perda, alteração, divulgação não autorizada de, ou acesso a, dados pessoais transmitidos, armazenados ou processados de outra forma".*

A preocupação recente expressada via previsões legais deve-se pelo fato de que, dentre as falhas de segurança em sistemas de rede existentes, o vazamento de dados é aquele que potencialmente gera maiores danos aos titulares. Isto porque, quando decorre de invasão, acesso indevido, roubo ou sequestro de informações pessoais, com o enfoque direto em

obter registros de uma base de dados robusta, compromete uma significativa massa de dados, em comparação a uma ocorrência de fraude, que visa diretamente vantagem econômica, por meio da extração de dados individualmente, gerando menores riscos a um coletivo de titulares.

Nesse sentido, entendendo a gravidade potencial de um vazamento de dados, alerta o considerando 85 do Regulamento Geral de Proteção de Dados Europeu (UNIÃO EUROPEIA, 2016):

> Uma violação de dados pessoais pode, se não tratada de maneira apropriada e oportuna, resultar em danos morais a pessoas naturais, tais como a perda de controle dos seus dados pessoais ou a limitação direitos, discriminação, roubo ou fraude de identidade, perda financeira, reversão não autorizada de pseudonimização, à reputação, perda de confidencialidade dos dados pessoais protegidos pelo sigilo profissional ou por qualquer outra desvantagem econômica ou social para a pessoa natural em causa.

Assim, para aferição do dano ocasionado a partir de um incidente de segurança que exponha dados pessoais, é necessário se verificar as especificidades do vazamento. Ou seja, a natureza da infração à norma, número de pessoas afetadas, tipos de dados, o propósito de seu processamento, a duração do incidente, se a ocorrência foi intencional ou negligente, ações da organização para mitigação do dano e, conforme veremos em seção a seguir, como se dá a organização da infraestrutura de segurança para prevenção a incidentes.

Logo mais trataremos a respeito da necessidade de respeito ao princípio da prevenção, visando-se evitar todo e qualquer incidente, no entanto, ato primeiro, será compreendermos como as empresas poderão ser responsabilizadas civilmente em caso de *data breach*.

3. Responsabilidade Civil no Brasil em casos de incidente de segurança

Conforme doutrina de Cavalieri Filho, responsabilidade é um dever jurídico sucessivo, consequente à violação de uma obrigação (CAVALIERI

FILHO, 2012, p. 2), ou, nos dizeres de Karl Larenz, "*a responsabilidade é a sombra da obrigação*" (LARENZ, 1958, p. 34). O Código de Defesa do Consumidor, o Marco Civil da Internet e a Lei Geral de Proteção de Dados dispõem uma série de obrigações para que as empresas, enquanto agente de tratamento de dados, cumpram, caso contrário, haverá violação de dever jurídico originário, surgindo, então, o dever de reparar o prejuízo causado na esfera civil, com o intuito de recompor o equilíbrio econômico-jurídico provocado pelo dano.

A responsabilidade civil ocorre a partir do cometimento do ato ilícito, ou seja, da violação de uma obrigação, podendo ela ser contratual ou extracontratual, e tem por objetivo tornar indene o prejudicado, reestabelecer à vítima situação em que estaria sem a ocorrência do fato danoso. No tocante à presente análise, importa-nos não as obrigações com natureza voluntária, mas tão somente as legais, impostas pelas normas que protegem dados pessoais, determinações vivas pelos pressupostos estatuídos em leis, com conteúdo definido, ressalvada a necessidade de alinhamento de entendimentos por parte da Autoridade Nacional de Proteção de Dados, "*órgão da administração pública responsável por zelar, implementar e fiscalizar*" (BRASIL, 2018) o cumprimento da Lei nº 13.709/18, vinculado à Presidência da República, que deverá ser criado até agosto de 2020.

Só haverá responsabilidade civil em caso de vazamento de dados, em qualquer das modalidades que serão apresentadas, por violação de dever jurídico preexistente nas leis de proteção de dados pessoais, sobretudo na Lei Geral de Proteção de Dados, pressupondo o dever de indenizar ao descumprimento de uma obrigação, já que, conforme previsto no art. 927, do Código Civil, aquele que, por ato ilícito, causar dano a outrem, fica obrigado a repará-lo (BRASIL, 2018). Ou seja, a causa jurídica que gera obrigação de indenizar em uma relação entre agentes de tratamento e titulares é o cometimento de ato ilícito stricto sensu, uma lesão antijurídica e culposa dos comandos que devem ser observados por todos (CAVALIERI FILHO, 2012, p. 6), na forma do exposto no art. 186 do Código Civil,

"aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" (BRASIL, 2002).

Em análise do mencionado item, depreende-se a ideia de culpa, que está essencialmente ligada à responsabilidade, nesse contexto, a de natureza subjetiva. Desse modo, sob essa modalidade, para que um agente de tratamento de dados seja responsabilizado por um incidente de segurança, caberá ao prejudicado comprovar a existência de dano; culpa lato sensu, ou seja, ação ou omissão negligente, imprudente ou imperita, incluindo ainda o dolo; e por último o nexo causal (CAVALIERI FILHO, 2012, p. 18).

De forma mais especificada, dentre os pressupostos da responsabilidade subjetiva estão previstos elementos para que se constitua o ônus de indenizar. O primeiro, formal, é a violação de um dever jurídico mediante conduta voluntária; depois, o subjetivo, podendo ser o dolo ou a culpa; e, por último, o causal material, sendo este o dano e a relação de causalidade (CAVALIERI FILHO, 2012, p. 19). E por violação de direito deve-se compreender todo e qualquer direito subjetivo, na hipótese de incidentes de segurança, os fundamentais, absolutos e não patrimoniais personalíssimos, tais quais a intimidade, a privacidade e a proteção de dados pessoais, conforme já se discute na proposta de emenda à Constituição nº 17/2019.

Todavia, essa concepção clássica dos elementos da responsabilidade civil foi revista ao longo do século XX, para abarcar além do conceito tradicional de culpa, também hipóteses em que se é dispensada a sua prova para ensejo da reparação. Nesse sentido, a teoria do risco desenvolvida em países como Itália, Bélgica e, principalmente, na França, foi adotada pelo direito brasileiro, estando presente no Código Civil em artigos como o 927, parágrafo único, que trata da obrigação de indenização pelos danos causados, independente da 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, sendo esta a

chamada responsabilidade objetiva. Nesse sentido, cabe-nos verificar a aplicação do Código de Defesa do Consumidor nas relações de tratamento de dados pessoais.

3.1 Código de Defesa do Consumidor e a Teoria Objetiva

Tratando de forma cronológica, a primeira hipótese de responsabilidade objetiva que se cabe tratar é a prevista no Código de Defesa do Consumidor. A edição da lei reflete discussão em torno da evolução da responsabilidade civil no século XX, passando pela flexibilização do conceito e da prova da culpa, após pela culpa presumida, a contratual, a anônima e então a teoria objetiva, com o intuito de se proteger o consumidor (CAVALIERI FILHO, 2012, p. 511). Desse modo, o que se verificou foi a alteração do enfoque na conduta do autor do dano, para o fato causador do dano, pelo que se concluiu pela importância de prever objetivamente um dever de segurança e garantia de idoneidade pelos serviços e produtos lançados no mercado, por parte dos fornecedores (CAVALIEIRI FILHO, 2012, p. 513).

Em seu âmbito restou superada a distinção dualista entre responsabilidade contratual e extracontratual, para se materializar na relação jurídica de consumo, contratual ou não. Desse modo, deve o fornecedor observar o dever de segurança a todos os indivíduos relacionados aos produtos e ou serviços ofertados no mercado, por meio de vínculo direto, sob pena de cometer um acidente de consumo pelo dano que a coisa vier a causar. Nesse contexto, o incidente de vazamento de dados pode configurar defeito no tratamento de informações pessoais, ou seja, no produto ou prestação de serviços, por violação do dever de qualidade e segurança, em razão de vulnerabilidade do sistema operacional do fornecedor. Conforme se depreende dos artigos 12 e 14, respectivamente (BRASIL, 1990):

> Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela

> reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos.
> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

Ambos os artigos preveem em seu § 1º, II, que o produto ou o serviço são defeituosos quando não oferece a segurança que deles legitimamente se espera, levando-se em conta seu uso e os riscos razoáveis. Portanto, ao contratar um serviço ou comprar um produto que pressupõe o compartilhamento de seus dados pessoais, o consumidor deposita sua confiança em um fornecedor, que deverá observar os seus direitos fundamentais a liberdade, privacidade, livre desenvolvimento da personalidade e sobretudo de proteção de seus dados como titular.

Destaca-se ainda que, apesar de utilizar o termo "consumidor", este conceito é maximizado em caso de defeito na prestação de serviços, na forma do art. 17, equiparando-se, então, todos os indivíduos prejudicados pelo incidente ocorrido, em faceta expansiva da responsabilidade objetiva.

Assim, responderá a empresa tanto pelos danos materiais, quanto os morais, senão pelos potenciais, uma vez que se tornará difícil comprovar o número de agentes que tiveram acesso às informações expostas, tornando-se complexa a concreta apuração do prejuízo causado. Desse modo, o direito consumerista soma a prescindibilidade da prova de culpa do agente causador do dano, à disposição para inversão do ônus da prova, quando demonstrada a verossimilhança das alegações e a hipossuficiência do indivíduo lesado, na forma de seu art. 6 (BRASIL, 1990).

O Código de Defesa do Consumidor apresenta, ainda, a potencialidade de a mera exposição ilícita do dado pessoal configurar dever de indenizar, por violação de obrigação da empresa em assegurar a proteção do consumidor, uma vez que houve risco de coleta e utilização indevida de informações pessoais por agentes mal-intencionados, dano

que dificilmente será mensurável. É o chamado dano *in re ipsa*, em que não é necessária a comprovação da extensão material ou moral do dano ocasionado, em uma alusão ao artigo 944 do Código Civil, para que reste demonstrados os prejuízos gerados para o indivíduo.

3.2 Código Civil e a Teoria Objetiva

Por sua vez, o próprio Código Civil prevê a modalidade de responsabilidade objetiva em algumas hipóteses, sendo-nos relevante tratar acerca do abuso de direito como ato ilícito. Conceituado como exercício antissocial, o abuso de direito nada mais é do que o desvio da finalidade social ou econômica do direito, é a atuação antiética por parte do indivíduo (DANTAS, 1977, p. 372). Também compreendido pela doutrina como ato contrário à destinação econômica ou social do direito subjetivo, que, reprovado pela consciência pública ou social, excede, por consequência, o conteúdo do direito (GUSMÃO, 1977, p. 53).

Nesse viés, percebe-se a intersecção com o princípio da finalidade previsto na Lei Geral de Proteção de Dados, disposto como *"realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"* (BRASIL, 2018). Assim, tal qual o princípio da finalidade, mas também da necessidade e adequação, o fundamento principal do abuso de direito é obstar que o direito seja utilizado como forma de opressão (CAVALIERI FILHO, 2012, p. 173), ou seja, que o agente de tratamento, em nosso caso, utilize seu poder com destinação distinta daquela que o titular espera.

Assim, da leitura do mencionado art. 187, depreende-se que não é necessária à empresa a consciência da alteração da finalidade, ou seja, não há que se comprovar a culpa ou dolo, basta o excesso à boa-fé, os bons costumes, o fim social ou econômico do direito. Vejamos: "*também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente*

os limites impostos pelo seu fim econômico social, pela boa-fé ou pelos bons costumes" (BRASIL, 2002).

Aliado ao artigo 187, o abuso de direito encontra previsão no artigo 927 do Código Civil, dispondo que será gerada a obrigação de indenizar quando houver conflito entre a finalidade própria do direito e a atuação no caso concreto. Com isso, tem-se que o controlador deverá informar ao titular a exata finalidade de tratamento do dado pessoal a ser compartilhado.

Caso contrário, ou seja, na hipótese de desvio do propósito informado, sem transparência da alteração por parte do titular, ressalvada a necessidade de revalidação da base legal que constitui seu escopo jurídico, deverá este agente de tratamento ser responsabilizado pelos danos causados, na forma do previsto na legislação civil. Nesse sentido, decisão do Superior Tribunal de Justiça configurou abuso no exercício de direito por parte de empresa de *credit scoring*, decidindo no seguinte sentido (SUPERIOR TRIBUNAL DE JUSTIÇA, 2014):

> O desrespeito aos limites legais na utilização do sistema "credit scoring", configurando abuso no exercício desse direito (art. 187 do CC), pode ensejar a responsabilidade objetiva e solidária do fornecedor do serviço, do responsável pelo banco de dados, da fonte e do consulente (art. 16 da Lei n. 12.414/2011) pela ocorrência de danos morais nas hipóteses de utilização de informações excessivas ou sensíveis (art. 3º, § 3º, I e II, da Lei n. 12.414/2011), bem como nos casos de comprovada recusa indevida de crédito pelo uso de dados incorretos ou desatualizados.

Diante de todas estas circunstâncias, considerando a teoria subjetiva e a objetiva do Código Civil, a aplicação de responsabilidade no Código de Defesa do Consumidor, bem como o comportamento da jurisprudência, reforça-se a necessidade de o controlador de dados estar em conformidade com as recentes legislações protetivas, visando-se evitar infrações às obrigações previstas para proteção da privacidade e dos dados pessoais, bem como se prevenir de sujeição à responsabilidade civil.

4. Ausência de responsabilidade civil por danos causados a titulares de dados pessoais

Para emergência do dever de indenizar, necessário se faz que exista um dano, uma ação ou omissão para sua origem e ainda o nexo de causalidade, conforme visto anteriormente. Assim, Aguiar Dias defende que é preciso demonstrar, para intentar a ação de reparação, que sem o fato alegado, o dano não se teria produzido (DIAS, 1983, p. 314). Além disso, em matéria de direito digital, conclui-se que a complexidade da matéria compromete o entendimento sobre o agente realmente responsável por parte do autor, titular dos dados pessoais infringidos, sendo comum a ocorrência de ilegitimidade passiva do réu que responde na ação judicial, seja ele controlador ou operador.

4.1 Fato de terceiro como excludente de responsabilidade civil em casos de incidente de segurança

Prevê o art. 43, III, que os agentes de tratamento de dados não serão responsabilizados quando provarem que o dano causado é decorrente de culpa exclusiva de terceiro (BRASIL, 2018). Terceiro, conforme definição de Aguiar Dias, é qualquer pessoa além da vítima e o responsável, alguém que não tem qualquer ligação com o causador aparente do dano e o lesado (DIAS, 2006, p. 399).

Desse modo, em caso de um incidente de vazamento de dados, facultar-se-á ao agente de tratamento romper o nexo causal entre sua conduta e o dano sofrido pelo titular, a vítima, visando demonstrar que não contribuiu para o resultado. Ou seja, poderá o controlador ou o operador provarem que houve violação da segurança por parte de um hacker, um ataque a seus sistemas operacionais, por exemplo, que, por si só, destruiu a relação causal entre a vítima e a ele mesmo, o aparente causador do dano, desde que seja algo irresistível e desligado de ambos.

Equipara-se, então, o fato de terceiro, ao caso fortuito e força maior, em razão de ser origem do dano uma causa estranha à ação ou omissão do agente aparente (CAVALIERI FILHO, 2012, p. 70). A culpa exclusiva de terceiro também se encontra no Código de Defesa do Consumidor, no rol de causas excludentes de responsabilidade do fornecedor, em seus arts. 12 §3, III e 14, §3, II.

No entanto, em caso de alegação de fato de terceiro, o magistrado deverá analisar se a conduta do agente concorreu de algum modo para o resultado danoso, e, caso confirmado, não haverá mais exclusão de causalidade. Desse modo, caberá aos agentes de tratamento de dados observar o princípio da segurança constante no Código de Defesa do Consumidor, bem como o princípio da prevenção previsto na Lei Geral de Proteção de Dados e ainda adotar as boas práticas de governança de dados pessoais listadas em seu capítulo VII, para o fim de conseguirem se resguardar contra acessos não autorizados, fraudes e demais crimes cibernéticos. A comprovação de excludente de fato de terceiro em processos judiciais é tema que será melhor tratado em próximo artigo.

4.2 "Fato do Operador" como excludente de responsabilidade de Controlador

Apesar do tema por si só poder ser tratado em artigo específico, cumpre-nos explicar brevemente acerca da relação entre os agentes de tratamento de dados e a responsabilidade. A Lei Geral de Proteção de Dados, inspirada pelo Regulamento Geral de Proteção de Dados Pessoais europeu, criou diferenças no tratamento de dados entre os chamados controladores e operadores.

Em seu artigo 4º, o regulamento europeu define controlador como *"pessoa natural ou jurídica, autoridade pública, agência ou outros tipos que, em conjunto ou separadamente, determinam o propósito e meios do processamento dos dados pessoais*" e o operador *"significa pessoa natural ou jurídica, autoridade pública, agência ou outros tipos que processam*

dados pessoais a pedido do controlador" (UNIÃO EUROPEIA, 2016). A título comparativo, percebe-se a semelhança das definições presentes no art. 5 da lei nacional, em que controlador é *"pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referente ao tratamento de dados pessoais"*, e o operador *"pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"* (BRASIL, 2018).

Compreende-se que a relevante diferença entre os agentes de tratamento está na capacidade decisória. O operador procederá às ordens de um controlador, sendo, então, este último o responsável pelas decisões acerca do tratamento, enquanto ao primeiro caberá tão somente executar as atividades que lhe são mandadas, na forma do art. 39 da LGPD: *"O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria"* (BRASIL, 2018).

Causa certa confusão em um estudante que recém inicia seus conhecimentos na legislação de proteção de dados, principalmente quando se percebe que o termo "controlador" surge sessenta e duas vezes, enquanto "operador" é mencionado apenas onze vezes, deixando a entender que não há qualquer responsabilidade para este último. No entanto, não é o que o art. 42 dispõe quando prevê que tanto o controlador e o operador serão responsáveis pelos danos patrimoniais, morais, individuais e coletivos que causarem a outrem no tratamento de dados pessoais, em violação à legislação de proteção de dados pessoais (BRASIL, 2018).

Para tanto, para que haja responsabilidade solidária e, após, direito ao regresso, caberá ao controlador provar que o operador realizou tratamento em descumprimento às suas obrigações de proteção de dados previstas na lei, ou que não seguiu as instruções lícitas por ele concedidas, hipótese em que será equiparado ao próprio controlador, na forma do art. 42, I, da mencionada lei. Já o direito de regresso, também ficou previsto

no art. 42, em seu parágrafo quarto, dispondo que o controlador deverá ser recompensado, na medida de sua participação no evento danoso.

Ou seja, caso o aparente responsável, controlador, realize prova de que não concorreu para o evento, valendo-se da segurança garantida pelas boas práticas de proteção, sendo os danos causados culpa exclusiva do operador, deverá ser integralmente reembolsado, ou até mesmo declarado ilegítimo passivo, dependendo da interpretação que os Tribunais farão no judiciário brasileiro, ao passo em que a lei entrar em vigor e decisões começarem a forma jurisprudência na matéria de proteção de dados, tendo por base a nova legislação.

4.3 Outras situações de ausência de responsabilidade: culpa concorrente e exclusão de corresponsabilidade entre controladores

Cabe-nos ainda investigar o art. 43 da Lei Geral de Proteção de Dados. De forma inversa em nossa análise, retornando ao inciso III, este diz que os agentes de tratamento só não serão responsabilizados quando provarem que o dano é decorrente de culpa exclusiva do titular dos dados (BRASIL, 2002), caso de culpa concorrente, conforme previsto no art. 945 do Código Civil: *"Se a vítima tiver concorrido culposamente para o evento danoso, a sua indenização será fixada tendo-se em conta a gravidade de sua culpa em confronto com a do autor do dano"*.

Nas palavras de Sílvio Cavalieri, *"fala-se em culpa concorrente quando, paralelamente à conduta do agente causador do dano, há também conduta culposa da vítima, de modo que o evento danoso decorre do comportamento culposo de ambos"* (CAVALIERI FILHO, 2012, p. 45). Entanto, esclarece ainda o autor que a doutrina recente prefere tratar como concorrência de causas ou de responsabilidade, pois, como no caso de incidentes de vazamento de dados, poderá ser hipótese de aplicação de teoria objetiva da responsabilidade civil.

Assim, caso na ocorrência de incidente de segurança a vítima também concorra para o dano que foi por ela sofrido, deverá ser responsabilizada

em conjunto com o agente de tratamento de dados pessoais. Para tanto, deverá o magistrado analisar se mesmo diante da conduta equivocada do agente de tratamento, o dano poderia ter sido evitado pela conduta da própria vítima, titular, ou seja, se há presença de erro injustificável de sua parte.

Desse modo, analisa-se o grau de importância e intensidade para a ocorrência do resultado, de ambas as condutas, de sorte que o agente não teria condições de produzir o resultado danoso por si só, devendo contar, portanto, com o efetivo auxílio do titular dos dados (CAVALIERI FILHO, 2012, p. 45). A responsabilidade de cada qual ocorrerá na medida de sua participação, não necessariamente pela metade, mas sim proporcionalmente ao grau de culpabilidade de cada um dos indivíduos envolvidos, conforme defendido por Aguiar Dias "*a culpa da vítima, quando concorre para a produção do dano, influi na indenização, contribuindo para a repartição proporcional dos prejuízos"* (DIAS, 2006, p. 314). Lembrando-se que, sem embargo tratar sob o termo "culpa", a concorrência de condutas deverá ser abrangida por causas tangenciais, também aplicável na responsabilidade objetiva, conforme a jurisprudência tem admitido no ordenamento brasileiro.

Por último, o art. 42, II, dispõe que *"os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente"* (BRASIL, 2018). Todavia, visando proteger os agentes em conformidade com a lei, os incisos I e II do art. 43 resguardam aqueles que agiram em conjunto com outros responsáveis, mas que não realizaram o tratamento que gerou o incidente de segurança ou que, embora o tenham realizado, não violaram legislação protetiva de dados, mas sim outrem.

Nesse caso, caberá ao controlador comprovar judicialmente que não realizou o tratamento, ou realizou em conformidade com a legislação, ou seja, de acordo com as políticas de segurança, de privacidade e com todo o programa de governança e proteção de dados pessoais. Desse modo, a Lei

Geral de Proteção de Dados traz mais uma salvaguarda aos bons agentes de tratamento.

Considerações finais

O recente fortalecimento e surgimento de normas de proteção de dados, sobretudo a promulgação Lei nº 13.709/18, com entrada em vigor programada para agosto de 2020, emerge a preocupação da sociedade civil em garantir maior proteção às informações transacionadas entre cidadãos e empresas. Estas, por sua vez, tardiamente têm se preparado para a adoção de medidas de conformidade, podendo-se predizer que à data da entrada em vigência não será suficiente para que agente de tratamento se conscientizem acerca da necessidade de cumprirem a legislação federal.

Nesse sentido, discutimos a responsabilização sob o aspecto civil, predizendo à interpretação de magistrados acerca do novo diploma legal, considerando que a legislação e doutrina estrangeira não serão de conhecimento geral do judiciário, cabendo-nos investigar a situação brasileira sob a própria legislação e produção científica nacional. Há relevante desconhecimento por parte dos aplicadores da lei sob a matéria de privacidade e proteção de dados, valendo-se citar decisão do Tribunal de Justiça do Rio Grande do Sul, que sugeriu à consumidora que se mudasse "*para a floresta, deserto, meio do oceano ou para outro planeta*", pois só assim conseguiria fazer valer *"seus direitos à privacidade na forma ou amplitude como defende"*, em caso de negativa de pedido de comercialização de dados pessoais da autora para terceiros, com o objetivo publicitário de produtos e serviços (TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL, 2014).

Desse modo, os principais obstáculos estão na compreensão da matéria por parte de magistrados e órgãos da administração pública, bem como na aplicação da responsabilização civil de acordo com as leis de proteção de dados, com determinação entre abrangência da teoria subjetiva e objetiva, estabelecimento de indenização compensatórias e

identificação de agentes de tratamentos de dados responsáveis pelos danos causados. Nesse sentido, revisamos a doutrina brasileira de responsabilidade civil, com o enfoque na aplicação em leis protetivas de dados, verificamos as diferentes teorias de responsabilização e, por último, hipóteses de excludente de imputação de responsabilidade a controladores, considerando a concorrência de sua conduta para o dano.

Concluímos que, em que pese a frustração do titular na exposição de suas informações, não há responsabilização civil automática em caso de incidente de segurança, sendo obrigatória a comprovação dos elementos, dano, nexo causal e, no mínimo, conduta concorrente para o evento, senão a culpa *lato sensu*. No entanto, conforme tratado, é crescente o número de incidentes de segurança ocorridos no Brasil, sendo 676.514 incidentes de segurança reportados ao Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança somente em 2018 no Brasil.

Portanto, é de suma importância que as empresas que tratem esse tipo de informação estejam em conformidade com a Lei Geral de Proteção de Dados Pessoais, sobretudo com os princípios previstos em seu artigo 6º, aqui destacando o princípio da segurança e da prevenção, também presentes no art. 4º do Código de Defesa do Consumidor. Uma boa estratégia de defesa é também uma estratégia ofensiva, ou seja, ter um efetivo programa de governança em proteção de dados pessoais é a chave para evitar responsabilidades civis e administrativas.

Para tanto, os agentes de tratamento de dados deverão adotar diversas medidas previstas na legislação federal, além de exceder o rol taxativo, caso queiram mitigar riscos e se tornar referência em experiência do cliente, em relação à proteção de suas informações e privacidade. Tais medidas serão melhor tratadas em artigo específico, mas dentre elas, as organizações deverão estabelecer um completo inventário dos dados armazenados e manipulados em sua função, com devida categorização com relação à sensibilidade, gerir o acesso aos dados e atendimentos dos titulares no exercício de seus direitos, definir políticas de segurança da informação, respostas à incidentes com plano de ação e elaborar relatórios

de impacto sempre que solicitados pela Agência Nacional de Proteção de Dados.

Diferente do argumento alarmista que operadores do direito têm defendido para adoção de políticas de conformidade à nova legislação, com enfoque em sanções administrativas, multas e responsabilidade civil, acreditamos que a emergência do diploma é uma oportunidade. Cabe as empresas que são agentes de tratamento de dados interpretar a legislação em sua forma positiva, visando a melhoria da experiência do cliente, bem como a própria organização de suas informações, sistemas e processos, que garantirão cada vez mais proteção destes, de seus funcionários, *stakeholders* e demais pessoas naturais com as quais se relaciona. Simultaneamente, poderão se defender de possíveis incidentes de segurança, ou, pelo menos, não praticar condutas que contribuam para a sua ocorrência, mote para evicção de qualquer responsabilidade.

Referências

BRASIL. *Código de Defesa do Consumidor*. Congresso Nacional. Brasília, 11 de setembro de 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078.htm >. Acesso em 28 de junho de 2019.

_____. *Código Civil*. Congresso Nacional. Brasília, 10 de janeiro de 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm >. Acesso em 28 de junho de 2019.

_____. *Lei nº 13.709/2018*. Congresso Nacional, Brasília, 14 de agosto de 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em 28 de junho de 2019.

CAMARGOS, Daniel. *Vazamento da Uber expôs nome, telefone e e-mail de 156 mil usuários brasileiros*. São Paulo, 12 de abril de 2018. Disponível em: < https://www1.folha.uol.com.br/mercado/2018/04/vazamento-da-uber-expos-nome-telefone-e-email-de-156-mil-usuarios-brasileiros.shtml >. Acesso em 29 de junho de 2019.

CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. São Paulo: Atlas, 2012.

COSTA, Judith Martins. *Os fundamentos da responsabilidade civil*. São Paulo: Jurid Vellenich, 1991. p. 29-52.

DANTAS, Santiago. *Programa de Direito Civil*. Rio de Janeiro: Editora Rio, 1977.

DIAS, José de Aguiar. *Responsabilidade Civil em Debate*. Rio de Janeiro: Forense, 1983.

GRANVILLE, Kevin. *Como a Cambridge Analytica recolheu dados do Facebook*. São Paulo, 21 de março de 2018. Disponível em: < https://www1.folha.uol.com.br/mercado/2018/03/como-a-cambridge-analytica-recolheu-dados-do-facebook.shtml >. Acesso em 29 de junho de 2019.

GUSMÃO, Paulo Dourado. *Abuso do direito, velho tema, sempre atual*. Rio de Janeiro: Revista de Direito do Ministério Público do Estado da Guanabara, nº 20.

Núcleo de Informação e Coordenação do Ponto BR. Estatísticas dos Incidentes Reportados ao CERT.BR. Disponível em: < https://www.cert.br/stats/incidentes/2018-jan-dec/tipos-ataque.html >. Acesso em 29 de junho de 2019.

_____. *Estatísticas dos Incidentes Reportados ao CERT.BR*. Disponível em: < https://www.cert.br/stats/incidentes/ >. Acesso em 29 de junho de 2019.

_____. *FAQ: Perguntas Frequentes ao CERT.BR*. Disponível em: < https://www.cert.br/docs/certbr-faq.html#6 >. Acesso em 28 de junho de 2019.

LARENZ, Karl. Derecho de Obligaciones. Madrid: Editorial Revista de Derecho Privado, 1958.

LOTT, Diana. *Relembre os principais vazamentos de dados de brasileiros em 2018*. São Paulo, 04 de janeiro de 2019. Disponível em: < https://www1.folha.uol.com.br/tec/2019/01/relembre-os-principais-vazamentos-de-dados-de-brasileiros-em-2018.shtml >. Acesso em 29 de junho de 2019.

Superior Tribunal de Justiça. Recurso Especial: REsp 1419697 RS 2013/0386285-0. Relator Ministro Paulo de Tarso Sanseverino. DJe: 17 nov. 2014. Disponível em: < https://stj.jusbrasil.com.br/jurisprudencia/152068666/recurso-especial-resp-1419697-rs-2013-0386285-0 >. Acesso em 29 de junho de 2019.

SYMANOVICH, Steve. *What is a security breach?*. Disponível em: < https://us.norton.com/internetsecurity-privacy-security-breach.html >. Acesso em 28 de junho de 2019

Tribunal de Justiça do Rio Grande do Sul. Processo de conhecimento: Autos nº 0103154-84.2014.8.21.0001. Juiz de Direito: Luiz Augusto Guimarães de Souza. DJE nº 5320, 16 mai. 2014. Disponível em: < https://www.jusbrasil.com.br/processos/174012158/processo-n-0103154-84201482100001-do-tjrs >. Acesso em 29 de junho de 2019.

UNIÃO EUROPEIA. *General Data Protection Regulation*. Parlamento Europeu. Bélgica, 27 de abril de 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em 29 de junho de 2019.

U.S. Departamento of Health and Human Services. *Information Memorandum*. 1 de julho de 2015. Disponível em: < https://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf >. Acesso em 28 de junho de 2019.

16

LGPD:
a proteção de dados e o consentimento granular

Gustavo Batista Guimarães

1. Boas Novas

Com o advento da Lei Geral de Proteção de Dados (Lei 13.709/18) no Brasil, a privacidade do titular dos dados toma novos rumos. Rumos de empoderamento, uma vez que agora temos uma legislação específica sobre o assunto. Trata-se de uma grande evolução jurídica e até econômica para o país, pois muitos outros países já possuem regulamentações sobre a proteção de dados há alguns anos, o que ajuda nos acordos das empresas brasileiras com as de outros países, por exemplo, empresas europeias, pois a LGPD, além de ser inspirada na General Data Protection Regulation da União Europeia (GDPR), traz uma segurança jurídica nas negociações, pelo fato de o Brasil possuir uma legislação específica.

2. Proteção de dados e o consentimento

De forma ampla, a proteção de dados pessoais pode ser entendida como mecanismos que buscam efetivar o direito humano de proteção à privacidade.

2.1 Consentimento

A LGPD traz, no corpo do seu texto, dez (10) bases legais que permitem realizar o tratamento desses dados, uma delas é o consentimento. Tratados por muitos como um dos pilares da proteção de dados pessoais, o consentimento é uma ferramenta existente em todas as leis que versam sobre o referido assunto. Entretanto, falar sobre consentimento sob o olhar do Direito, não é um assunto novo, pois o Direito Civil sempre buscou qualificar o que seria uma declaração de vontade válida entre particulares. No campo do Direito do Consumidor, essa questão tomou ares mais protetivos, principalmente nas questões contratuais, por exemplo, nos contratos de adesão, onde geralmente não há discussão sobre as bases desses contratos. O consumidor sempre se vê obrigado a aceitar o que lhe é imposto para usufruir um produto ou um serviço.

E é principalmente baseado em um viés de proteção ao consumidor que o consentimento relativo a uso de dados pessoais buscará se desenvolver, sendo esse um dos destaques que a Lei Geral de Proteção de Dados Pessoais nos traz. De fato, a LGPD e a GDPR dão uma especial proteção, diante da importância que representam hoje na economia, do valor que representam essas informações e, principalmente, os riscos das informações que esse tratamento proporciona. Afinal, dependendo do conjunto de informações, pode-se prever o comportamento do consumidor e montar até um perfil psicológico, como posicionamento político, orientação sexual e religiosa. Imaginemos o valor disso para um empregador ou para um fornecedor de plano de saúde que ao precificar o valor do mesmo ao cliente, sabe do seu histórico de doenças. São dados muito sensíveis e que não podem ficar à mercê de qualquer pessoa. É um assunto que requer uma reflexão de todos, não só do ponto de vista legal, mas principalmente do ponto vista ético e moral.

Mas vamos deixar esse assunto para uma outra oportunidade e focar no assunto que trata o artigo proposto.

Como mencionado anteriormente, o consentimento é uma das 10 bases legais que a lei permite o tratamento desses dados pelo controlador, que pelo texto da lei 13.709/18 é "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Segundo a LGPD, o consentimento será considerado válido se for expressado de forma evidente e inequívoca, por escrito ou não. Tendo o controlador ou até mesmo o operador que segundo a Lei 13.709/18 é "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador"; cuidados adicionais em casos de dados sensíveis ou dados de crianças e adolescentes. Nessas circunstâncias, prescreve a lei que o consentimento deve ser manifestado "de forma específica e destacada", sendo obrigatório, na última hipótese, o consentimento expresso dos pais.

Não podemos deixar de mencionar que, segundo a Lei Geral de Proteção de Dados, esse consentimento tem que ser ainda livre e espontâneo, sob pena de configurar vício de vontade, sendo todo consentimento dado nulo. Por isso, a figura do encarregado ou Data Protection Officer (DPO), nomenclatura trazida pela GDPR, se torna tão importante dentro das empresas, pois cabe a ele estudos e análises cautelosas de como deve ser realizado esse consentimento e desenvolver meios para que seja realizado de acordo com a lei, e acompanhar para que o tratamento desses dados, no ambiente interno, possa ser feito com segurança e com a maior transparência para o titular dos dados.

Por isso, os produtos ou serviços que realizam tratamento de dados pessoais devem adequar-se ao códex normativo da LGPD, integrando aos seus sistemas soluções que criem possibilidades do titular dos dados dar seu consentimento de maneira informada. Sistemas que estejam totalmente de acordo com a privacy by design ou by default.

3. Privacy by design e default

Trata-se de um conceito em que todos os sistemas ou serviços são projetados, construídos e implementados, tendo observado a segurança e

a privacidade dos dados pessoais. Como explica a Doutora Ann Cavoukian, criadora deste conceito:

> *"Privacy by Design é uma metodologia na qual a proteção de dados pessoais é pensada desde a concepção de sistemas, práticas comerciais, projetos, produtos ou qualquer outra solução que envolva o manuseio de dados pessoais. "*

Sistemas que desde a sua concepção estão em acordo com a proteção de dados pessoais e com a segurança, sistemas claros, que respeitam os direitos dos usuários à privacidade. Neste sentido, a privacidade não pode ser assegurada somente pelo cumprimento de textos regulatórios e sim ser a cultura de operação de uma organização.

3.1 Princípios

Este conceito possui sete (7) princípios:

1. Proativo não reativo; preventiva não corretiva;
2. Proteção de dados como configuração padrão;
3. Privacidade Incorporada ao Design;
4. Funcionalidade Total -Soma Positiva, Não Soma Zero;
5. Segurança de ponta a ponta -proteção total do ciclo de vida;
6. Visibilidade e transparência;
7. Respeito à privacidade do usuário

3.1.1 Proativo não reativo; preventiva não corretiva

A proteção de dados by design deve ser proativa, ao invés de reativa, onde deve-se antecipar e evitar eventos invasivos à privacidade. Ela visa impedir que esses eventos aconteçam.

3.1.2 Proteção de dados como configuração padrão

Visa oferecer o mais alto grau de segurança aos dados, proporcionando aos dados pessoais uma proteção "automática", assim, nenhuma ação é necessária para que pessoa tenha seus dados protegidos. É incorporada ao sistema por padrão.

3.1.3 Privacidade Incorporada ao Design

Privacidade presente no design e no sistema como um todo, sem atrapalhar a funcionalidade do mesmo.

3.1.4 Funcionalidade Total -Soma Positiva, Não Soma Zero

Objetiva ter em harmonia todos os interesses e objetivos que cercam o sistema ou serviço, de maneira positiva para todos os envolvidos, evitando uma "disputa", por exemplo, privacidade versus segurança, demonstrando que é possível ter ambas, equilibrando custos e construindo um sistema seguro.

3.1.5 Segurança de ponta a ponta -proteção total do ciclo de vida

Garante que o dado em todo seu ciclo de vida esteja seguro, desde a coleta até o descarte do mesmo. Gerenciamento seguro das informações de ponta a ponta no processo.

3.1.6 Visibilidade e transparência

Tem como objetivo assegurar a todos os titulares dos dados que independente da prática ou tecnologia usada, ela está de acordo com as premissas estabelecidas e objetivos declarados na captação dos dados e na conquista do consentimento.

3.1.7 Respeito à privacidade do usuário

Exige que todos envolvidos no processo de criação do sistema ofereçam medidas que assegurem a privacidade, mantendo os interesses do indivíduo sempre em primeiro lugar.

Assim, adotar uma abordagem de Proteção de Dados “by design” é uma ferramenta essencial para minimizar os riscos de privacidade e criar confiança, facilitando a obtenção do consentimento, pois tudo é feito de forma clara e sem gerar dúvidas nos titulares dos dados.

4. Consentimento granular

Neste contexto que traz a LGPD, as corporações não podem mais somente informar que os dados poderão ser captados, tem que mostrar o porquê, a forma que será feita, duração do tratamento destes dados, finalidade proposta, mostrar as suas responsabilidades e riscos do titular ao dar este consentimento, quais as possibilidades de revogação. Tudo de maneira transparente, dando a possibilidade ao titular dos dados de optar ou não por usar o produto ou serviço de seu interesse, podendo manifestar consentimento específico para determinado tipo de tratamento e não para os outros visados pelo controlador ou operador, além de revogar tal consentimento a qualquer momento. É o que se chama de consentimento granular ou fatiado.

5. Conclusão

Em um mundo cada vez mais tecnológico, onde cada vez a manipulação dos dados são realizadas em grande escala, é importante garantir a segurança de um princípio cada vez mais caro em nossa sociedade: o da privacidade.

6. Referências

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019

VENTURA, Leonardo Henrique de Carvalho. Disponível em: https://jus.com.br/artigos/69585/privacy-by-design-e-compliance-na-lgpd

SOARES, Pedro Silveira Campos. Disponível em: https://www.anoreg.org.br/site/2019/05/13/artigo-a-questao-do-consentimento-na-lei-geral-de-protecao-de-dados-por-pedro-silveira-campos-soares/

EXIN Privacy & Data Protection Foundation Privacidade, Dados Pessoais e GDPR (White Paper Leo Besemer)

17

A escolha subjetiva de várias bases legais para o tratamento de dados pessoais

Marcos Souza [1]

1. Introdução

Todo o tratamento de dados pessoais demanda a escolha de uma base legal. Apenas uma dentre as dez é necessária para que o tratamento seja legítimo, todavia, a questão essencial reside na escolha de qual base utilizar ou quais.

Vale lembrar que as bases legais são as justificativas que a LGPD apresenta para que o tratamento possa ser realizado, as quais estão definidas no seu artigo 7º, conforme destacado a seguir:

I. O consentimento;
II. O cumprimento de obrigação legal (ou regulatória);
III. A execução de contrato ou de procedimentos preliminares a um contrato (desde que solicitado pelo titular);
IV. A proteção da vida ou da incolumidade física do titular (ou de terceiro);
V. A tutela da saúde;
VI. O legítimo interesse;
VII. A proteção do crédito;
VIII. O exercício regular de direitos;

[1] Marcos Souza é Advogado do Sistema do Sistema FIEMG, membro do Programa de Proteção de Dados FIEMG, membro da ANPPD® - Associação Nacional dos Profissionais de Privacidade de Dados, membro da Comissão de Proteção de Dados da OAB/MG e Especialista em Direito Público pela PUC Minas. Atuou como auditor e gestor na áreas de corregedoria e compliance no serviço público estadual e como gestor na área de ciência da informação no setor privado.

IX. A realização de estudos e pesquisas;
X. E, no caso do poder público, a execução de políticas públicas.

Dito isso, qual seria o melhor a se fazer, escolher uma única base legal para uma finalidade ou finalidades específicas, ou escolher várias bases para uma única finalidade ou finalidades ou tratamentos variados?

2. A individualização das bases legais

Essa tarefa não é das mais fáceis, em verdade, é das mais complexas que se apresenta para qualquer profissional de privacidade, a uma, porquê, uma vez escolhida a base legal e oficialmente informada ao titular, e já tendo se iniciado o tratamento, pouquíssima ou nenhuma margem existe para que se adote outra base para aquela mesma finalidade inicialmente declarada.

Tal condição é que torna ainda mais difícil a escolha da base legal, contudo, essa tarefa possui outro aspecto que se mostra fundamental para seu sucesso ou fracasso. A ponderação sistemática e completa acerca da imprescindibilidade do tratamento dos dados pessoais para alcance de determinada(s) finalidade(s), é etapa essencial para um balizamento adequado e eficiente dos itens que compõem os aspectos de privacidade, base legal, tratamento e finalidade.

Por ponderação sistemática e completa, entenda-se:

I. Verificar amplamente se o tratamento dos dados é essencial ao atingimento da(s) finalidade(s) pretendida(s). Sem tratamento de dados pessoais, não há necessidade de indicação de base legal. Nesse caso a anonimização deve ser considerada sempre como alternativa ao tratamento de dados pessoais;
II. Identificar exaustivamente para qual(is) finalidade(s) os dados serão tratados e que tipos de tratamento serão utilizados. Conhecer todas as possíveis finalidades que poderão ser atribuídas ao tratamento dos dados, bem como as variações de tratamento que poderão potencialmente ser utilizadas. Nesse caso, é fundamental que o diagnóstico do fluxo desses dados seja realizado de forma mais fidedigna e ampla possível.

Se não há dado pessoal a ser tratado, consequentemente, não haverá necessidade de indicação de uma base legal. Entretanto, embora tal aspecto seja significativamente relevante, este tema demanda uma discussão mais aprofundada, e, portanto, será tratado em outra ocasião.

Ultrapassadas essas questões, deve-se então avaliar as implicações envolvidas na operacionalização do tratamento dos dados decorrentes da(s) base(s) legal(is) adotadas. Essas implicações dizem respeito à compatibilização do tratamento dos dados com a observância e viabilização dos direitos dos titulares.

Ora, se a base legal escolhida para todas as finalidades de tratamento de um determinado dado for somente o consentimento, o controlador deverá estar ciente que a qualquer momento poderá ser obrigado a cessar o tratamento e excluir definitivamente os dados, uma vez que nesse caso, como se optou pelo consentimento, obrigatoriamente deverá ser franqueado ao titular uma forma simples e acessível de se revogar esse consentimento.

Por outro lado, se foram adotadas bases legais diferentes para finalidades diferentes de tratamento, no caso de uma revogação de consentimento, o controlador, a depender das outras bases utilizadas, poderá manter o tratamento dos dados para as demais finalidades que não foram alcançadas pelo direito de revogação.

Há vários casos em que essa indicação de mais de uma base legal para finalidades distintas ocorrerá de forma totalmente dissociada da vontade do Controlador, como é o caso do tratamento realizado para cumprimento de obrigação legal ou regulatória, hipótese em que, mesmo que tenham sido adotadas outras bases legais, numa eventual revogação do consentimento pelo titular, esta não repercutirá no tratamento dos dados realizados para cumprimento de obrigação legal ou regulatória.

Descortinando o “dilema” inicialmente posto, percebe então que a questão referente à utilização de mais de uma base legal para tratamentos e finalidades distintas, em alguns casos é até natural e esperada, ficando o

"dilema" apenas acerca da utilização de mais de uma base legal para uma mesma finalidade e tratamento.

Poderia o controlador coletar o consentimento dos titulares e ao mesmo tempo indicar o legítimo interesse como base legal para a mesma finalidade? Sendo afirmativa a resposta, não estaria a se falsear o consentimento, uma vez que, nesse caso, mesmo revogando o consentimento, poderia o controlador continuar o tratamento fundado no legítimo interesse, como se fosse uma espécie de backup legal.

Embora esse artifício pareça tentador em um primeiro momento, a interpretação teleológica da LGPD, principalmente por conta do Princípio da Transparência, indica que tal artifício deverá ser analisado com reservas, haja vista que poderá não ser visto com bons olhos pelo Judiciário, pela Autoridade Nacional de Proteção de Dados (ANPD) e demais autoridades que irão ou já estão atuando nessa seara.

Em outros casos os aspectos negativos notados na situação anterior não estão presentes, havendo até mesmo certa naturalidade na indicação de mais de uma base legal. Isso pode ser notado em situações em que se possa optar por uma pluralidade de bases legais para uma mesma finalidade, e que não haja necessidade do consentimento, como por exemplo o cumprimento de obrigação legal e a execução de contrato ou de procedimentos preliminares a um contrato, as quais também podem ser conjugadas com o exercício regular de direitos.

Todas essas questões propiciam a compreensão de que o dilema da base legal única, assim como vários outros dilemas do direito, é algo que, possivelmente, não possui uma resposta única e absoluta.

Pode se dizer que cada situação vai demandar soluções específicas e que deverão ser balizadas de acordo com o contexto próprio de cada cenário, ora será utilizada apenas uma base legal para um único tratamento e uma única finalidade, ora será demandada a utilização de várias bases legais para um mesmo tratamento e múltiplas finalidades, da mesma forma, também haverá situações em que poderão sim ser adotadas várias bases legais para uma única finalidade.

O ponto é que a medida da legalidade nesses casos será determinada caso a caso, e a implementação de uma ou várias bases legais para a realização do tratamento certamente deverá ser avaliada tendo por base o Princípio da Transparência harmonizado com todos os demais princípios e regras dispostos no atual "micro ordenamento" já instituído.

3. Conclusão

Por mais propicia e relativa que pareça essa conclusão, a análise de toda a sistemática e caráter teleológico da LGDP conduzem à ideia de que tal conclusão é de fato adequada, primeiro porque a LGPD foi instituída não como forma de entrave à utilização dos dados pessoais, mas, sim como verdadeira viabilizadora das atividades que contemplam o tratamento de dados pessoais, de modo a agregar mais valor aos dados, segundo porque a LGPD, como norma geral que é, foi concebido como norma de caráter mais programático, deixando espaço para que as necessárias adaptações interpretativas sejam realizadas de acordo com o caso concreto, aspectos esses que não se compatibilizam com a adoção de interpretações fechadas e limitadas.

Portanto, é forçoso concluir que a adoção de uma ou várias bases legais para uma mesma ou variadas finalidades e tratamentos, deverá ser definida em cada caso e consideradas todas as regras e princípios vigentes sobre a matéria, sendo apenas a partir da atuação de todas as autoridades envolvidas, e a consolidação de entendimentos sobre o tema que se terá um horizonte mais definido e claro.

4. Referências

BRASIL. Constituição da República Federativa do Brasil de 1988. Palácio do Planalto, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso: 20 fev. 2020.

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Palácio do Planalto, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso: 20 fev. 2020.

Terceira seção

Cases de implantação

18

Cases de implantação LGPD: a evangelização dos colaboradores

Tatiana Alves de Castro [1]

1. Introdução

A tecnologia conectou o mundo e possibilitou mudanças drásticas na forma de consumir produtos e serviços. Ao usufruir e interagir através do uso de ferramentas eletrônicas, acabamos por expor nossa privacidade e dados, fato que desencadeou a interveção pública através, dentre outras, da Lei Geral de Proteção de Dados – LGPD.

Não que essa exposição já não acontecesse fora do mundo virtual, mas o advento da internet automatizou a coleta, o compartilhamento e a aplicação de inteligência sobre os dados, escancarando, por conseguinte, a invasão que seus titulares vinham, há muito, sofrendo.

A desconfiança de estar sendo vigiado e ouvido por equipamentos eletrônicos, o bombardeio de conteúdo em consonância com consultas realizadas na internet e a avalanche de propaganda e marketing de acordo com as preferências de consumo mostraram-se difíceis de serem resolvidas que não por meio de uma legislação protetiva.

---

[1] Advogada do Banco Semear S/A, atuando há mais de 15 anos em jurídico corporativo de instituição financeira. Formada pela PUC Minas, pós-graduada em Direito Público (Newton Paiva) e com MBA em Direito Civil e Processual Civil pela Fundação Getúlio Vargas. É certificada em Privacy and Data Protection Officer pela EXIN e em Compliance pela KPMG. Atual secretaria geral adjunta da Comissão Especial de Proteção de Dados da OAB/MG e membra da Comissão de Assuntos Jurídicos da ABBC e da ACREFI e das Subcomissões de Assuntos Jurídicos e Compliance de Dados e de Negócio, Tecnologia e Governança de Dados da FEBRABAN.

Ainda que a culpa por tal exposição e invasão não seja exclusiva das pessoas jurídicas para as quais a LGPD é dirigida, uma vez que os próprios titulares dos dados descuidaram de sua privacidade e de seus dados pessoais no desejo de usufruirem com mais agilidade dos produtos e serviços que lhes interessavam, ressoa evidente que algo precisava ser feito, como de fato foi.

Assim, estamos diante de uma lei protetiva que exige não apenas o cumprimento e a observância de seu conteúdo, mas, também e principalmente, uma mudança cultural.

Essa mudança cultural depende, e muito, do fornecimento de treinamento pelas empresas aos colaboradores, atividade, inclusive, prevista na LGPD. Vejamos o que dispõe a Seção II - Do Encarregado pelo Tratamento de Dados Pessoais, mais precisamente o inciso III, §2º, do artigo 41:

> "Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais.
>
> § 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
>
> § 2º **As atividades do encarregado consistem em**:
>
> I - aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
>
> II - receber comunicações da autoridade nacional e adotar providências;
>
> III - **orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais**; e
>
> IV - executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

> § 3º A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados." - destacado

Como se vê, o treinamento é mandatório. Trata-se de um mecanismo essencial para a instituição de uma cultura de proteção à privacidade e aos dados pessoais na corporação e, por conseguinte, para o sucesso do projeto e o cumprimento da lei.

Isso porque, ainda que sejam adotados os mais eficientes controles e medidas de segurança, são os funcionários e os contratados o elo mais frágil, capazes de expor a empresa, mesmo que de forma inconsciente, a riscos acentuados. Os colaboradores precisam saber e entender o comportamento que deles se espera, o que somente será atingido por meio de educação e conscientização.

De nada adianta a estruturação de um projeto de adequação cuidadoso, com investimento em tecnologia e melhoria dos processos de gestão e de governança corporativa, sem incorporar à cultura de negócios da empresa os temas de privacidade e proteção de dados pessoais, de modo que não seja possível dissociar o cumprimento da legislação da observância das normas internas.

É vital o treinamento periódico para o engajamento e sensibilização de toda a corporação no cumprimento da LGPD, que não deve ser visto como um entrave para o desenvolvimento comercial, mas sim como uma regra fundamental, que assegura a segurança e a estabilidade ao negócio.

A seguir serão apresentados *cases* de implantação da Lei Geral de Proteção de Dados, com foco no treinamento/conscientização dos colaboradores, em diferentes segmentos de negócio.

Vale mencionar que a colaboração feita pelas empresas e profissionais não esgota o tema, até porque o projeto de adequação à LGPD é contínuo e sofrerá, paulatinamente, melhorias, inclusive em decorrência das regulamentações que estão por vir.

2. Banco Semear S.A.

O Banco Semear originou-se em 2006 da fusão da Seculus CFI (Crédito, Financiamento e Investimento) e Banco Emblema, com o propósito de contribuir com o cenário econômico de Minas Gerais, oferecendo serviços financeiros aos clientes e parceiros. Ao longo dos anos, ampliou sua participação no mercado nacional, aumentando a carteira de produtos e serviços, tornando-se, assim, um banco múltiplo e inovador, com foco em inclusão e educação financeira.

Recebeu esse ano (2019) o prêmio de segundo banco mais inovador do Brasil, após criteriosa avaliação técnica da Fundação Dom Cabral.

Os preparativos para adequação à LGPD pela instituição financeira iniciaram-se ainda no ano de 2018, ano de promulgação da lei, e desde então os colaboradores, parceiros e prestadores de serviços vivenciam a preocupação e o engajamento do Banco Semear para alcançar o sucesso na proteção da privacidade e dos dados de seus clientes e colaboradores.

Em abril de 2019, como vistas a introduzir os conceitos e as noções básicas da legislação, o Banco Semear convocou todos os funcionários e contratados para participar de workshops de conscientização obrigatórios.

Tais workshops se mostraram altamente produtivos na fase seguinte, de mapeamento do ciclo de vida dos dados na empresa, quando os colaboradores, novamente chamados, demonstraram nas entrevistas desenvoltura e facilidade para indicar e discorrer sobre os fluxos, processos, atividades e recursos utilizados no tratamento de dados pessoais.

Com vistas a não perder o engajamento dos colaboradores, já que algumas etapas do projeto de adequação à Lei Geral de Proteção de Dados não depende da atuação de todos eles, foram produzidos conteúdos para divulgação na intranet e nos televisores espalhados pela sede do Banco Semear, bem como realizada a GRC Week, evento de Governança, Riscos e Compliance, que contou com uma palestra de LGPD ministrada pela experiente Data Protection Officer – DPO, Daniela Hansson.

As recentes interações com os colaboradores sobre o tema foram realizadas pelo time de segurança da informação, com rápidas apresentações sobre engenharia social, phishing, ataques, blindagens, etc.

Ressalte-se que após a revisão e aperfeiçoamento das políticas internas, os colaboradores serão novamente convocados para conhecer as novas diretrizes e nortear o comportamento coeso, disseminando, assim, as normas corporativas decorrentes do *compliance* à LGPD.

Está no *roadmap* do Banco Semear, ainda, o uso de plataforma de ensino à distância – EAD, confecção de revistas com linguagem informal associada à imagens/desenhos/cenas do dia a dia corporativo, descanso de tela temático, jogos de diferentes tipos (como de tabuleiro, memória e outros), além de quiz e testes surpresas, com vistas a sensibilizar os funcionários e os contratados sobre a importância do cumprimento da Lei Geral de Proteção de Dados.

E, assim, a evangelização dos colaboradores será periódica e contínua, inclusive para atualizá-los sobre a futuras exigências da Agência Nacional de Proteção de Dados – ANPD, do Banco Central do Brasil – BACEN e outros.

3. SYMPLA

A Sympla é uma empresa de tecnologia que oferece uma plataforma para gestão de eventos e venda de ingressos, facilitando a interação entre público e organizadores. Atualmente, atende aproximadamente 6 milhões de usuários.

Foi eleita a "Startup do Ano" no Spark Awards 2015, prêmio realizado pela Microsoft e ABStartups, atraindo, assim, investimentos financeiros.

Tais investimentos, inevitavelmente, trouxeram novas responsabilidades, como por exemplo, o atendimento a novos níveis de Compliance Global, em diferentes áreas. Uma dessas áreas foi justamente a privacidade e proteção de dados pessoais.

A Sympla adota uma metodologia de *compliance* em privacidade e proteção de dados pessoais que tem, como um dos pilares, o treinamento dos colaboradores.

Segundo Frederico Felix (2019), atual *Privacy & Data Protection Coordinator* da Sympla, o treinamento é muito importante, pois grande parte das vulnerabilidades advém do comportamento de pessoas e não, necessariamente, de softwares ou hardwares.

Nesse contexto, entende-se que devem ser adotadas diversas medidas para conscientizar e treinar os funcionários. Vejamos:

> Todo novo colaborador realiza um treinamento em vídeo sobre privacidade e proteção de dados, com questões a serem respondidas ao final.
>
> Além disso, o novo funcionário participa, na primeira semana, do onboarding, onde cada área apresenta suas frentes de trabalho, incluindo a área de privacidade e proteção de dados.
>
> São realizadas ações especiais, como uma semana de segurança da informação e privacidade, convidando palestrantes externos para falar sobre os temas. Também são produzidos adesivos e ministrados workshops específicos e personalizados para cada área, como por exemplo, ao time de suporte ao cliente, que precisa identificar e tratar requisições relacionadas ao exercício dos direitos dos titulares, ou ao time de marketing, sobre como lidar com perfilização, ações de mail marketing, etc..
>
> Ainda, são elaborados flyers temáticos ("pills virais"), fazendo uso de personagens conhecidos da "cultura pop", com conteúdo relacionado à privacidade, de forma a aumentar o nível de conscientização. Por ser uma empresa de cultura jovem e mais dinâmica, esse tipo de artifício funciona, o que, talvez, pode não ocorrer em uma empresa mais "tradicional".
>
> Todo material é produzido internamente, havendo um esforço conjunto das áreas para dar efetividade à entrega planejada.
> Logo após a divulgação dos conteúdos e treinamentos percebe-se que os colaboradores ficam mais alertas e cautelosos, validando ações com o time de privacidade e proteção de dados antes de adotá-las.

> Por essa razão, o trabalho de treinamento e conscientização deve ser constante. O projeto de adequação à LGPD não é uma corrida que terminará em 2020, mas sim uma maratona que não terá linha de chegada, inclusive diante da possibilidade de novas regulamentações e exigências por parte da autoridade reguladora. (Frederico Felix, 2019).

4. Atos

A Atos é uma empresa multinacional, de origem francesa, cuja principal atividade é suportar a transformação digital de seus clientes, projetando, integrando, operando soluções específicas em todos os setores de negócios com base na tecnologia de seus parceiros (Siemens, Worldline, Google Cloud, Vmware, SAP, Microsoft, Oracle, AWS, Cisco, etc.) e desenvolvendo tecnologias e produtos de ponta.

Conta com 120.000 (cento e vinte mil) colaboradores, distribuídos entre 73 (setenta e três) países. Na América do Sul tem suas principais unidades em São Paulo, com presença na Colômbia, Argentina, Peru, Uruguai, Venezuela e Chile, contando com aproximadamente 4.000 (quatro mil) colaboradores nesse continente.

Atualmente, os maiores supercomputadores da América Latina estão no Brasil e foram fabricados e implementados pela Atos, como o caso do Santos Dumont, no Laboratório Nacional de Computação Científica.

Segundo Américo Alonso (2019), atual Chief Security Officer – CSO para América do Sul, por ser a Atos uma empresa de DNA Francês, o processo de adequação às leis protetivas de privacidade e dados pessoais é maduro, estabilizado, repetitivo e multidisciplinar, sendo que todas as aplicações globais da Atos são validadas não somente por DPOs (Data Protection Officers) de países dentro da União Europeia, como também por DPOs das demais regiões, de forma a garantir que o acesso à dados pessoais (inclusive de colaboradores) não fere a legislação aplicável a cada unidade da Atos no mundo.

Quanto à evangelização dos colaboradores, assim discorre:

> A conscientização é fundamental.
> Em Proteção de Dados, o colaborador sempre é o elo mais frágil. Se não temos eles conscientes da importância do assunto, e de seus direitos como cidadãos, não podemos esperar que eles sejam atores ativos no processo.
>
> Utilizamos várias formas de difundir a mensagem.
> Primeiramente, é politica da Atos (global) que todos os colaboradores, durante o onboarding (e em forma anual) devem realizar 4 (quatro) cursos mandatórios online de aproximadamente 30 (trinta) minutos, com exame final, sendo que 2 (dois) desses cursos têm como tema segurança e proteção de dados.
> Se o colaborador não finaliza ou não é aprovado, não recebe acessos à rede, sendo responsabilidade do gestor facilitar tempo necessário para que o colaborador realize os treinamentos.
> Em forma mensal, existem calls regionais com o time do escritório de proteção de dados de forma a responder dúvidas, tratar assuntos relacionados, etc.
>
> Ainda, contamos com TVs em todas as unidades, onde passamos vídeos de diferentes assuntos, sendo um deles de proteção de dados. No caso do Brasil, com foco na LGPD.
>
> Por último, temos campanhas de gamification, de forma a brincar com os colaboradores e validar o nível de concientização do assunto. (Américo Alonso, 2019).

5. Cisco

A Cisco é líder mundial em tecnologia, oferecendo soluções que propiciam conexão, computação e colaboração com segurança. Tem como premissa ajudar a sociedade, através de seus colaboradores, produtos e parceiros, a se conectar com segurança e a aproveitar hoje as oportunidades da transformação digital do futuro. Foi fundada em 1984 em São Francisco, na Califórnia, e acaba de completar 25 anos no Brasil.

Para Márcia Muniz (2019), atual Diretora Jurídica e *sponsor* do projeto de adequação à LGPD, "os colaboradores precisam viver a cultura de proteção de dados e entender como vai funcionar o programa e como a

companhia se posiciona sobre o assunto, ou seja, ter a verdade da corporação".

Como se vê, a etapa de evangelização dos colaboradores é de extrema importância para a organização e não está adstrita à fase inicial, devendo ser contínua. Vejamos o entendimento exposto ao discorrer sobre a gestão de crise em incidentes de segurança envolvendo os titulares de dados:

> *Gerir a crise começa no envolvimento de todos os colaboradores, cientificando-os da existência de um Comitê e um plano de crise, evitando uma "crise de nervos" pois, essa sim, instaura um caos. (Márcia Muniz, 2019).*

Ainda, segundo Márcia Muniz (2019), é importante orientar os colaboradores da existência de um responsável por comunicar formalmente o incidente em nome da instituição (porta voz), o que só é possível através de reiterados treinamentos e impregnação da cultura de privacidade e proteção de dados na cultura organizacional.

7. Whirlpool

A Whirlpool é fabricante de eletrodomésticos, presente no Brasil com as marcas Brastemp, Consul e KitchenAid.

Segundo Gustavo Godinho (2019), Gerente Jurídico e atual PMO do Programa de Adequação à LGPD na Whirlpool, deve-se pensar em treinamentos para os colaboradores, áreas funcionais, fornecedores e, inclusive, desde que possível, para as famílias dos colaboradores, já que a Lei Geral de Proteção de Dados não é apenas uma lei com foco consumerista.

O projeto de adequação na empresa faz uso de Provas de Conceito "Proof of Concept – PoC", realizado com o propósito de verificar se determinado conceito / processo / software é suscetível de ser explorado de uma maneira útil e que, efetivamente, sua usabilidade possa trazer benefícios reais para a empresa; "Privacy Champions" (campeões / embaixadores da privacidade), tema este tropicalizado da GDPR (General

Data Protection Regulation), onde colaboradores representam e defendem o programa de privacidade e proteção de dados nas principais áreas funcionais, ajudando a incorporar e reforçar o conhecimento, práticas seguras e atitudes necessárias. Além disso, ações como "Gamification", "Quiz", etc., são passíveis de uso visando a vinculação do público interno com este assunto de grande preocupação, não só para as empresas, como ao país como um todo.

Quanto à conscientização dos colaboradores e, até mesmo, de seus familiares, assim finaliza:

> Por dar um caráter social ao programa / jornada pois, frisando, é algo que não há término e que deverá ser cíclico e constantemente renovado, havendo de ser estendido a outros stakeholders como os mencionados acima. (Gustavo Godinho, 2019).

8. Ford

A Ford Motor Company é uma empresa global com sede em Dearborn, Michigan (Estados Unidos). A empresa projeta, fabrica, comercializa e presta serviços de pós-venda a uma linha completa de carros, picapes, SUVs, veículos eletrificados e veículos de luxo da Lincoln. A Ford emprega aproximadamente 191.000 pessoas em todo o mundo. No Brasil, a empresa está estabelecida desde 1919 e mantém as marcas automotivas Ford e Troller, além de uma estrutura de três fábricas, além do Campo de Provas de Tatuí.

Para Adriana Tocchet Wagatsuma (2019), atual Legal e Compliance Executive da Ford, cada empregado deve ser engajado e entender seu papel no projeto de implementação e cumprimento da Lei Geral de Proteção de Dados.

A Ford tem trabalhado para disseminar a cultura de privacidade e proteção de dados em todas as áreas da empresa, acreditando que os conceitos da nova lei deverão permear todos os níveis da organização, para então multiplicarem-se e depois solidificarem-se.

9. Uber

A Uber é uma multinacional americana, prestadora de serviços eletrônicos de intermediação por meio de aplicativos que permitem a conexão entre motoristas e passageiros, entregadores e restaurantes. A Uber está no Brasil desde 2014.

Para Flávia Mitri (2019), atual Privacy Legal Director Latin America da Uber, devem ser promovidos, exaustivamente, educação, treinamento e comunicação para os colaboradores fixarem a política de privacidade e proteção de dados da empresa.

Para tanto, entende que a jornada de adequação à Lei Geral de Proteção de Dados deve contar que com:

> (a) treinamentos sobre privacidade: explicação do que é um dado pessoal e o impacto que cada colaborador tem no tema;
>
> (b) criação de políticas internas de acesso a dados pessoais;
>
> (c) criação de comitê de privacidade e segurança, que podem ser usados para tirar dúvidas e gerenciar crise;
>
> (d) criação de programas de engajamento de privacidade - como privacy champions - que engaja pessoas de diferentes times para atuar como "olheiros" para proteção de dados em suas respectivas organizações;
>
> (e) ter um sponsor na gerência sênior da empresa, como o CEO ou CFO, que ajude a abraçar a causa e remover a ideia de que é uma preocupação exclusiva do jurídico;
>
> (f) ter o apadrinhamento do tema dos principais heads de cada área, para que os seus funcionários entendam a seriedade do assunto. (Flávia Mitri, 2019).

Como se vê, há consenso sobre a relevância da evangelização dos colaboradores no tema da privacidade e proteção de dados, já que a

mudança de cultura é decisiva e carece ser praticada, repraticada, re-repraticada incansavelmente, até que se estabeleça um novo *mindset*.

Muito se tem dito sobre "abrir a caixinha da LGPD", assim como foi com os direitos trabalhistas e do consumidor. Se bem reparar, temos impregnado em nossa mente tais direitos, que, assim como a privacidade e proteção de dados, decorrem de lei e foram, paulatinamente, incorporando na nossa cultura.

Deve-se, então, usar e abusar de apresentações, workshops, reuniões, cursos, palestras, videoconferências, campanhas, comunicados, cartilhas, revistas, ensino à distância (EAD), dentre outros, preferencialmente personalizados ao segmento empresarial, a fim de disseminar a cultura e reforçar comportamentos positivos.

Com efeito, o incentivo à privacidade e proteção e dados depende do fortalecimento do ambiente institucional, isto é, das regras do jogo que deverão ser obedecidas pelos funcionários e contratados, o que não inclui apenas as normas jurídicas, mas também sociais e culturais.

Quarta seção

A LGPD e o Poder Público

19

Desafios da LGPD na adminstração pública e a (des)continuidade das políticas públicas

Ricardo Gomes Figueiroa [1]

1. Introdução

Nos dias atuais, cada vez mais, o aparato tecnológico agregado à prestação dos serviços público se constitui como uma vontade da sociedade e uma necessidade de efetivação do interesse público.

A internet e os serviços inteligentes, assim como as ferramentas hoje disponíveis, se prestam como instrumentos indispensáveis à efetiva implementação da função administrativa.

O aumento da necessidade de utilização de dispositivos tecnológicos que coletam dados sobre os cidadãos, tratando esses dados de várias maneiras, faz surgir questionamentos importantes acerca da questão da privacidade dos usuários, notadamente quanto ao compartilhamento dessas informações sem a devida autorização.

A Lei geral de proteção de dados (LGPD), lei 13.709/2018, dedica capítulo específico para a Administração Pública, e, não obstante as tentativas políticas para a retirada dos artigos do seu escopo, destaca-se que a força imperativa desta lei se revela imprescindível e se sobreleva

[1] Graduado em Direito pela Pontifícia Universidade Católica de Minas Gerais (2004). Pós graduação em Direito Público (2006). Mestrando em Propriedade Intelectual e Inovação tecnológica pela UFMG. Procurador do Município da Prefeitura Municipal de Ribeirão das Neves. Advogados atuante nas Direito Empresarial, Imobiliário, Administrativo e Direito Digital.

justamente para garantir maior transparência no uso e nas "trocas de informações" pelo Poder Público com os dados dos seus administrados.

Para uma melhor compreensão, importante uma análise sobre o foco que a LGPD pretende dar à Administração, no qual importante relembrar alguns conceitos de direito administrativo para que possa aclarar os seus objetivos desta legislação.

Pois bem. Maria Sylvia Zanella di Pietro citando Oswaldo Aranha Bandeira de Mello diz que "a palavra administrar significa não só prestar serviço, executá-lo, como, outrossim, dirigir, governar, exercer a vontade com o objetivo de obter um resultado útil; e que até, em sentido vulgar, administrar quer dizer traçar programa de ação e executá-lo". (31ª edição. Editora forense direito administrativo. Pag 117.)[2]

Ainda, de acordo com a renomada autora, o conceito de administração pública divide-se em dois sentidos: **1) sentido objetivo, material ou funcional**; **2) sentido subjetivo, formal ou orgânico; 3) ampla; e 4) estrita.**

> "Em sentido objetivo, material ou funcional, a administração pública pode ser definida como a atividade concreta e imediata que o Estado desenvolve, sob regime jurídico de direito público, para a consecução dos interesses coletivos. Em sentido subjetivo, formal ou orgânico, pode-se definir Administração Pública, como sendo o conjunto de órgãos e de pessoas jurídicas aos quais a lei atribui o exercício da função administrativa do Estado".31ª edição. Editora forense direito administrativo. Pag 118.

Nesse sentido, subjetivamente, podemos definir **Administração Pública** como sendo o conjunto de órgãos, pessoas jurídicas e seus respectivos agente, que realizam as atividades públicas, em conformidade com os princípios e normas de direito público, visando os fins desejados pelo Estado.

Deste modo, a Administração Pública, é representada tanto pelos os órgãos integrantes das pessoas jurídicas políticas (União, Estados,

[2] DI PIETRO, Maria Sylvia Zanella. Direito administrativo. 31ª edição. Editora forense. 2018.

Municípios e Distrito Federal), aos quais a lei confere o exercício de funções administrativas, Administração direta, como também pela Administração Indireta responsáveis pela execução indireta da atividade administrativa e dotadas de personalidade jurídica própria.

Neste desiderato, o estabelecido no artigo 23[3] da lei 13.709/2018 nos indica quem são as pessoas jurídicas de direito público que podem tratar dados fazendo expressa menção ao parágrafo único[4] da lei de acesso à informação, lei 12.527/2011, subordinando, assim estas pessoas ao escopo da LGPD e que melhor será apresentado à frente.

Em sequência destaca-se o conceito de função administrativa que nos dizeres de José dos Santos Carvalho Filho, citando Diogo de Figueiredo Moreira Neto, defini como sendo "a atividade do Estado para realizar seus fins, debaixo da ordem jurídica". (Carvalho, pag. 4, 25ª edição).[5]

O ponto central da função administrativa reside na forma como o Estado geri os interesses coletivos, sendo certo que os fins pretendidos pela Administração devem, sempre, estar em consonância com os princípios constitucionais, bem como à legislação.

Nesse tocante, sem aprofundar na discussão, o exercício da função administrativa se torna um importante instrumento ao desenvolvimento das políticas públicas, na medida em que prescreve a forma que o Estado deve agir para cumprir o seu mister.

---

[3] Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , 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, desde que: I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos; II -(VETADO); e III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e (Redação dada pela Lei nº 13.853, de 2019) Vigência

[4] Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.

Parágrafo único. Subordinam-se ao regime desta Lei:I – os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público; II – as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.(grifei)

[5] FILHO, José dos Santos Carvalho. Manual de direito Administrativo. São Paulo. Editora Atlas. 2012.

Noutra esteira, José dos Santos Carvalho Filho apresenta o conceito de serviço público descrevendo que "é toda atividade prestada pelos Estado ou por seus delegados, basicamente sob o regime de direito público, com vistas à satisfação de necessidades essenciais e secundárias da coletividade". (CARVALHO pag. 321, 25 edição).[6]

Assevera-se que os serviços públicos somente podem ser prestados caso exista norma regulamentadora que defina os meios e a forma que aquele serviço será prestado, sempre visando o interesse público, em observância do princípio da legalidade.

Importante destacar também o princípio da continuidade dos serviços públicos que se torna a chave para a manutenção dos serviços públicos e garantia dos cidadãos de que o Estado não frustrará os seus direitos, na medida que eventual interrupção (descontinuidade das políticas públicas) poderá prejudicar o bom funcionamento do Estado.

O assunto se revela de extrema importância e merece destaque no presente estudo, haja vista que este princípio determina que o Estado deve ser estimulado a aperfeiçoar os seus serviços e se adaptar aos adventos das novas tecnologias adequando sua prestação às novas realidades social.

Com efeito, é neste desiderato que o atendimento das exigências da LGPD pelo Poder Público deverá ser construído não somente por se tratar de uma obrigação legal, mas como uma metodologia para a implementação dos conceitos e mudanças de cultura, tornando a legislação de proteção de dados mais efetiva e ao mesmo tempo promovendo o avanço tecnológico e econômico do Estado.

A metodologia utilizada no presente artigo é a pesquisa descritiva e exploratória, baseados na doutrina, em análise histórica e análise da legislação. As principais fontes de pesquisa foram a doutrina especializada. site planalto.gov (LGPD), artigos sobre o tema e as palavras chaves usadas foram LGPD e Administração Pública, no qual se buscou estabelecer uma

[6] FILHO, José dos Santos Carvalho. Manual de direito Administrativo. São Paulo. Editora Atlas. 2012.

relação entre a continuidade dos serviços públicos com a implementação da LGDP no contexto da administração pública.

2. A inclusão do setor público no escopo da LGPD

Traçado esse brevíssimo comentário acerca do conceito de Administração Pública, nos deparamos com o seguinte questionamento, a quem se destina, no âmbito da Administração Pública, as normas da LGPD?

Os artigos 23 e seguintes do Capítulo IV, Seção I, da Lei Geral de Proteção de Dados que dispõe sobre as regras de tratamento de dados pessoais pelo Poder Público assim preceitua:[7]

> Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , 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, desde que:
>
> Art. 1º Esta Lei dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal.
> Parágrafo único. Subordinam-se ao regime desta Lei:
> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Como já assinalado, o aludido artigo, ao dispor sobre as regras de tratamento de dados pessoais pelo Poder Público faz expressa menção ao

[7] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >, acesso em: 22 nov. 2019.

artigo 1º da Lei de Acesso à Informação, determinando que os órgãos públicos integrantes das respectivas administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público no âmbito da União, Estados, Distrito Federal e Municípios, bem como as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

Aplicam-se, da mesma forma, às entidades privadas sem fins lucrativos (OSCIP, OS, OSC, Sistema S, etc.) que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres, nos termos do artigo 2º[8] da lei de acesso à informação.

A interpretação destes dispositivos da Lei de acesso à informação e da LGPD reafirma a ideia de que a Administração Pública está obrigada a se adequar e investir em questões de segurança da informação e atuar de forma preventiva, visando, assim, resguardar o tratamento dos dados pessoais coletados para fins diversos do interesse público.

Constitui dever do Estado assegurar a proteção da informação, porém, a despeito disso, podemos afirmar que não existe uma relação dicotômica entre a LGPD e o tratamento de dados pelo Poder Público, mesmo porque, a informação constitui atividade imprescindível ao exercício da função administrativa.

Assim, a formação dessa complexa rede de informações e processamento de dados pelas pessoas jurídicas de direito público, aqui destacadas, deverão estar devidamente adequadas, mesmo antes da vigência da lei, sob pena de violação do interesse público.

[8] Art. 2º Aplicam-se as disposições desta Lei, no que couber, às entidades privadas sem fins lucrativos que recebam, para realização de ações de interesse público, recursos públicos diretamente do orçamento ou mediante subvenções sociais, contrato de gestão, termo de parceria, convênios, acordo, ajustes ou outros instrumentos congêneres. Parágrafo único. A publicidade a que estão submetidas as entidades citadas no **caput** refere-se à parcela dos recursos públicos recebidos e à sua destinação, sem prejuízo das prestações de contas a que estejam legalmente obrigadas.

O Poder Público também poderá tratar dados pessoais, no caso de segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais, conforme legislação específica, que contenha medidas proporcionais e necessárias para que o tratamento de dados pessoais atenda ao interesse público, mas todos estes caso encontram fora do escopo da lei geral de proteção, haja vista as especificidades destas atividades.

3. Princípios da administração pública e sua correlação com a LGDP

A Lei Geral de Proteção de Dados define os princípios especiais à proteção de dados, quais sejam: finalidade; adequação; necessidade; livre acesso; qualidade dos dados, transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas.[9]

A Lei Geral de proteção de dados pessoais, LGPD, tem como fundamentos, o respeito à privacidade, a honra, a imagem e a vida privada, também à autodeterminação informativa, ao determinar o direito do cidadão ao controle dos seus dados, a liberdade de expressão, de informação, de comunicação e de opinião, que são direitos previstos na Constituição brasileira, o desenvolvimento econômico e tecnológico e a inovação, com fundamento na livre iniciativa e na livre concorrência e a defesa do consumidor, o livre desenvolvimento da personalidade e a dignidade humana.[10]

Um dos grandes desafios da Administração Pública se insere na dicotomia da transparência x privacidade, sendo certo que os modelos atuais de segurança da informação, a priori, permeiam a precariedade (pelo menos no âmbito público) e elevam o risco de vazamento de dados.

Segundo Miguel Reale "(....,) princípios gerais de direito são enunciações normativas de valor genérico, que condicionam e orientam a

[9] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >, acesso em: 22 nov. 2019.

[10]Disponível em: < https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/objetivo-e-abrangencia-da-lgpd >, acesso em: 22 nov. 2019.

compreensão do ordenamento jurídico, quer para a sua aplicação e integração, quer para a elaboração de novas normas". (REALE JÚNIOR, Lições preliminares de direito, pag. 285, 25º ed.)[11]

Imperiosa a premissa de que o interesse público deve sobrepujar ao interesse privado, contudo, até que ponto a administração pública pode se valer dessa prerrogativa? Quais são seus limites?

A resposta, a meu ver, pode parecer simples, aprioristicamente, na medida que a administração pública deve respeitar os princípios que são modelos dogmáticos a serem cumpridos por expressa determinação constitucional, artigo 37, ou seja, existe um balizamento para a Administração, senão vejamos:[12]

> Art. 37. A administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte: (Redação dada pela Emenda Constitucional nº 19, de 1998)

Segundo Roberto Alexy, em sua Teoria dos direitos fundamentais afirma que princípios são "comandos de otimização", ou seja, podem ser cumpridos em graus diferentes e realizados da melhor forma possível e seguindo critérios de proporcionalidade e razoabilidade.[13]

Destaca-se ainda, nesse sentido, o referencial trazido por Bruno Bioni (2019, pag.101) acerca da decisão da Corte Constitucional alemã sobre a lei do censo de 1983 que obrigou seus cidadãos a fornecerem dados pessoais para informação ao governo sobre a distribuição geográfica e espacial da população.[14]

Naquele julgado destacou-se a possibilidade do governo de cruzar informações com outras dados públicos disponíveis para fins não específicos.

---

[11] REALE, MIGUEL. Proteção de Dados Pessoais a função e os limites do consentimento. Rio de Janeiro. Editora forense, 2019.

[12] Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm >, acesso em: 22 nov. 2019.

[13] ALEXY, Robert. Teoria discursiva do direito. Organização, tradução e estudo introdutório Alexandre Travessoni Gomes Trivisonno. Forense Universitária. Rio de Janeiro. 2015

[14] BIONI, Bruno Ricardo. Proteção de Dados Pessoais a função e os limites do consentimento. Rio de Janeiro. Editora forense, 2019.

Resumidamente, a corte reconheceu a inconstitucionalidade da lei e reafirmou o direito fundamental do indivíduo em autodeterminar sua informação, impondo limites ao Estado para o processamento dos dados. (BIONI, pág. 103)[15]

No Brasil, por exemplo, destacamos a lei de acesso à informação (LAI) que estabelece a obrigação de informação, em razão dos princípios da publicidade e transparência, sendo certo que a disponibilização de dados considerados públicos deve sempre se curva às regras estabelecidas, mas fundamentalmente aos princípios balizadores o caso requeira, sempre respeitado a legalidade, a finalidade e o melhor interesse público, dentre outros princípios.[16]

Certo é que, casuisticamente, as questões mais críticas merecem uma análise mais minuciosa e devem sempre ser submetidas ao crivo da proporcionalidade e à razoabilidade, para que não exista violações decorrente de eventuais contradições na legislação.

4. (Des)continuidade das políticas públicas

A estruturação do Estado se transformou ao longo da história de acordo com a realidade e as necessidades da sociedade. Nos primórdios, o cultivo de alimentos foi determinante para a ficção dos indivíduos à terra e a partir daí é que surgiu o desenvolvimento de técnicas de plantio, caça, busca por água potável, fazendo, pois, proliferar a produção, o que também fez aumentar a concentração de pessoas em um determinado local (*polis*).[17]

Dado o aumento de pessoas em um mesmo local, surgiu também a necessidade de organização, devido à complexidade de tarefas necessárias a suprir as necessidades daqueles indivíduos.

---

[15] Idem 9.

[16] Disponível em: <http://www.scielo.br/pdf/rdgv/v14n2/1808-2432-rdgv-14-02-0513.pdf >, acesso em: 22 nov. 2019.

[17] Disponível em: <https://pt.wikipedia.org/wiki/Hist%C3%B3ria_das_cidades>, acesso em: 22 nov. 2019.

O crescimento desordenado do Estado é gatilho para o baixo desenvolvimento econômico e social, sobretudo aqueles com carência de infraestruturas e recursos naturais.

Diante desse cenário, e na atual conjectura, as "Políticas Públicas conceituada como a totalidade de ações, metas e planos que os governos (nacionais, estaduais ou municipais) traçam para alcançar o bem-estar da sociedade e o interesse público."[18]

A implementação de políticas públicas se dá através do exame das estruturas, da prática, da realidade social vivenciada pela administração e que sua efetividade se alcança com a aceitação política da sociedade.

Os administradores públicos, responsáveis pelas decisões, devem selecionar as prioridades em consonância com as expectativas da sociedade da melhor forma possível ao interesse público. O bem-estar social, até certa medida, é dever do Estado e a escolha e manutenção das boas políticas públicas deve ser mantida por todas as gestões que representam determinada sociedade.[19]

O planejamento público é uma realidade imprescindível ao desenvolvimento econômico do Estado e o avanço tecnológico é fundamental neste processo, sendo inegável sua essencialidade ao livre desenvolvimento da personalidade.

Nesse contexto, o Estado deve dedicar tempo deste planejamento não somente ao seu desenvolvimento, mas também à privacidade dos cidadãos, pois esta deve ser encarada como prioridade, haja vista que o eventual antagonismo entre avanço tecnológico-privacidade pode causar sérios entraves ao seu desenvolvimento.

A legislação sobre proteção de dados traz uma série de garantias aos cidadãos, sendo dever do Estado a escorreita implementação destas garantias através dos seus processo e procedimentos.

---

[18] Formulação, Implementação e Avaliação de Políticas Públicas – Fundação Centro de formação de Servidor Público-FUNCEP- 1986.

[19]Disponívelem:<http://www.mp.ce.gov.br/nespeciais/promulher/manuais/MANUAL%20DE%20POLITICAS%20P%C3%9ABLICAS.pdf >, acesso em: 22 nov. 2019.

Nos termos do artigo 23 da lei de proteção de dados, a Administração Pública poderá tratar dados pessoais pelos seus órgãos e entidades do Poder Público para a atender sua finalidade pública, a persecução do interesse público e com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, desde que:

> a) sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sites;
> b) seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

Destarte, identifica-se assim a necessidade de melhor aprimoração dos usos dos dados, transformado a informação em conhecimento, adequando, a Administração Pública, este conhecimento, às suas finalidades específicas e inerentes à prestação dos serviços públicos, sempre com observância dos princípios da minimização dos dados, boa-fé e interesse público, atentando-se que os desvios de finalidade serão tratados, pelas autoridades competentes, como ato de improbidade administrativa.

5. Bases legais e poder público

O Estado é um dos maiores concentradores de dados do mundo, controlando informações sobre saúde, dados financeiros, de educação, de processos judiciais, relativos à segurança, dentre outros dados, além de processar uma enorme quantidade de dados de seus servidores nas três esferas, federal, estadual e municipal.

Com o vertiginoso aumento de dispositivos tecnológicos que são capazes de coletar dados sobre os indivíduos, monitorar suas atividades, descobrir suas preferências e traçar seu perfil comportamental traz à tona questões atinentes à proteção da privacidade. A vigilância em massa e o

uso e compartilhamento não autorizado de dados pessoais, são um desafio e um grande risco para os cidadãos.[20]

Em razão desses riscos a criação de alternativas tecnológicas pelo Poder Público deve ter, desde a sua concepção (*privacy by design*), a proteção da privacidade como fundamento prioritário.

A administração pública está sujeita a balizas legais que delimitam como deverá ocorrer a coleta, o uso e o compartilhamento de dados pessoais, o que deve ser feito com a devida cautela, para tanto o administrador público deve observar os fundamentos daquela coleta e determinar a respectiva base legal.

A lei de Proteção de dados prevê, em seu artigo 7º, as hipóteses em que os dados pessoais podem ser tratados, como podemos abaixo observar:

> *Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
> *I - mediante o fornecimento de consentimento pelo titular;*
> *II - para o cumprimento de obrigação legal ou regulatória pelo controlador;*
> *III - pela 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, observadas as disposições do Capítulo IV desta Lei;*
> *IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;*
> *V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;*
> *VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*
> *VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;*
> *VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência*

[20] Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/dados-administracao-publica-14052018 >, acesso em: 25 nov. 2019.

> *IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou*
> *X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.*

Conforme acima evidenciado, a Administração Pública tem o poder-dever de tratar, usar e compartilhar os dados necessários para a execução de suas políticas públicas, previstas em lei e regulamentos ou ainda respaldadas em contratos, convênios ou instrumentos congêneres, independentemente do consentimento do titular dos dados e, nos termos do mencionado artigo 23 da LGPD 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, desde que, sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos e seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais.

A escolha da base legal dependerá do tipo de prestação de serviço e também dos dados que estão sendo processados pela Administração Pública. Para cada compromisso da administração, cujo fim se processe dados, deverá o responsável (encarregado de dados/DPO) apresentar o fundamento legal daquele processamento.[21]

Diante desse contexto a Administração Pública deve adotar, gradativamente, o uso de aplicações das informações como estratégia para aproximar os cidadãos da Administração facilitando, assim, o acesso aos serviços públicos.

[21] Idem 16

6. Dados públicos x dados privados; a base legal do consentimento

De um lado temos o tratamento de dados pessoais elevado à condição de ativo mais valioso da atual economia e de outro a autodeterminação informacional como garantia do direito de personalidade do indivíduo e em uma leitura descuidada, tais informações, podem gerar intepretações totalmente paradoxais.

Esta interpretação, historicamente, relaciona-se na perspectiva de um direito de privacidade, no qual decorre a dualidade entre o público e o privado, e, nos dizeres de Bruno Bioni "O que é público e privado é o que normatiza o conteúdo do direito à privacidade, sendo a sua lógica centrada na liberdade negativa de o indivíduo não sofrer interferência alheia". (BIONI, 2019, pag 96).[22]

Para o este autor, "a "evolução" do direito à privacidade que sobrelevaria o direito à proteção de dados pessoais consistiria em uma proteção *dinâmica* e em uma *liberdade positiva* do controle sobre as informações pessoais".(BIONI, 2019, pag 97).[23]

Os §§ 3º e 4º, artigo 7 da lei Geral de Proteção de Dados deixa claro que esta dicotomia (público x privado) parece ter sido mitigada ou mesmo eliminada, na medida que a lei autoriza o acesso aos dados públicos que podem ser tratados, desde que, se considere a finalidade para o tratamento, a boa-fé do agente e notadamente o interesse público do tratamento do dado.[24]

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
> I - mediante o fornecimento de consentimento pelo titular;
> § 3º O tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

[22] Idem 9

[23] Idem 9

[24] Idem 7

> § 4º É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, resguardados os direitos do titular e os princípios previstos nesta Lei.

O consentimento é uma das bases legais estabelecidas no artigo 7º da lei de proteção de dados e é definido como a manifestação inequívoca, informada e livre em que o titular deste direito autoriza o tratamento de seus dados pessoais para uma finalidade determinada específica.

Nesse contexto, o poder público ao tratar dados pessoais deverá verificar a base legal para tal tratamento e uma vez identificada a necessidade de consentimento deverá submeter ao crivo do titular a expressa autorização, devendo, este processo estar devidamente integrado ao processos que legitimou o tratamento de dados, visando, minimizar eventuais efeitos negativos do tratamento de dados dos cidadãos.

Por exemplo, um determinado aplicativo público que coleta informações para determinado serviço de utilidade público pode processar seus dados, contudo, para caso esse mesmo aplicativo queira traçar o perfil do usuário para fim diverso daquele inicial, deverá solicitar o expresso consentimento do usuário, sob pena de violação de direitos.

Para Bruno Bioni o consentimento do titular deve, no meio da indústria da informação, é um "sujeito vulnerável", na medida que a incerteza da utilização de seus dados é a tônica deste processo. Nesse quadro de incertezas o uso dos dados, com parcimônia, por aqueles que os processam, pode se tornar o diferencial para o cidadão. (BRUNO BIONI, PAG 165).[25]

Outro aspecto relevante neste são os questionamentos sobre as possibilidades de compartilhamento de bancos de dados pessoais entre órgãos e autoridades no âmbito da Administração Pública. Como resposta, ainda que sem profundidade no debate, observa-se a imperiosa necessidade de previsão legal e ainda a Administração deve se ater ao fim público específico.

[25] Idem 9

Assim, a finalidade especificada para o tratamento de dados e sua utilização deve ser pertinente, direcionada, proporcional e com o menor impacto possível ao titular, ou seja, a minimização dos dados deve ser a regra do tratamento, salvaguardando os direitos dos cidadãos.

Por derradeiro, a provisão de serviços público e o tratamento de dados pelo Poder Público devem ser o mais transparente possível e adequados com suas políticas públicas, evitando o tratamento para fins diversos daqueles especificados e sempre aliado aos fins públicos.

7. Considerações finais

A abordagem destacada no presente estudo refere-se a forma como o Poder público, uma vez inserido no contexto da lei Geral de Proteção de Dados, deve tratar o direito dos titulares.

A potencialização de tecnologias que expõe os cidadãos é enorme sendo dever do Estado a proteção em todas suas esferas, executiva, legislativa e judiciária cumprindo seu papel de promotor do bem-estar público.[26]

Os desafios para a efetiva utilização dos dados são de extrema importância para a tomada de decisão pelos gestores públicos e a qualidade dessa prestação é dependente da forma como os dados são processados para gerar a informação adequada.

De forma geral, o processo de conhecimento pelo uso dos dados, visa atender as expectativas do futuro dos entes públicos, sendo a análise das realidades locais e suas características, os problemas e as oportunidades das regiões, as demandas de determinados nichos da população, indicadores de emprego e desemprego, as desigualdades etc, os fatos que irão alimentar este processo para que, então, os entes definam sua melhor estratégia

[26] PINHEIRO, Patricia Peck. #DIREITODIGITAL. 6ª edição. Saraiva. 2019.

Uma avaliação dos impactos da proteção de dados no cotidiano é imperiosa para aprimorar o monitoramento, a qualidade dos dados e a tomada de decisões, na medida que age preventivamente na proteção da privacidade gerando maior confiança da população.

Os programas e ações do governo são a forma que se desenvolvem as políticas públicas, e na busca por alcançar um determinado objetivo, por exemplo, como a implantação de um posto de saúde ou uma escola em uma determinada região, o gestor público buscará dados para a solução deste problema.

Por isso é notória a necessidade do uso dos dados pelo Poder Público, sempre em conformidade com a legislação, como forma de se alcançar as melhores políticas públicas para os cidadãos. O mapeamento dos dados se torna imprescindível para gerar informação pois é através da informação é que se gera o conhecimento necessários para uma boa política pública.

8. Referências

ALEXY, Robert. **Teoria discursiva do direito**. Organização, tradução e estudo introdutório Alexandre Travessoni Gomes Trivisonno. Forense Universitária. Rio de Janeiro. 2015

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais a função e os limites do consentimento**. Rio de Janeiro. Editora forense, 2019.

DI PIETRO, Maria Sylvia Zanella. **Direito administrativo,** 31ª ed. Rio de Janeiro: Editora forense. 2018.

FILHO, José dos Santos Carvalho. **Manual de direito administrativo**. São Paulo. Editora Atlas. 2012.

PINHEIRO, Patricia Peck. **Direito digital,** 6ª ed. Saraiva. 2019.

REALE, MIGUEL. **Proteção de Dados Pessoais a função e os limites do consentimento**. Rio de Janeiro. Editora forense, 2019.

20

Aplicação da Lei Geral de Proteção de Dados ao poder público

Zilda A. Goncalves de Sousa
Igor da Silveira Franco

Na sociedade atual, a informação converte-se em poder a partir do momento em que a informática permite transformar informações parciais e dispersas em informações em massa e organizadas, o que torna imperativa a regulamentação jurídica dessas técnicas para a proteção da privacidade dos cidadãos (Perez Luño)

1. Introdução

Um dos pontos mais relevantes na Lei Geral de Proteção de Dados Pessoais (LGPD) é sua aplicação às práticas de tratamento de dados também no setor público, isso porque em seus diversos poderes (Executivo, Legislativo e Judiciário) e entes federativos (União, Estados, Distrito Federal e Municípios), utilizam-se do tratamento de dados pessoais dos cidadãos, não somente para a elaboração e execução de políticas públicas, mas para a oferta dos mais diversos serviços. O uso da tecnologia da informação e de técnicas de tratamento de dados pessoais tem sido cada vez mais explorados pela administração pública como indispensável instrumento para a condução pública, por esse motivo, uma atenção especial deve ser dada ao tratamento de dados pessoais pelo setor público.

A transparência dos dados em posse do Poder Público é princípio constitucional que foi regulamentado no Brasil pela Lei de Acesso à

Informação (Lei nº 12.527 de 2011) e encontra um dos seus limites na vedação ao fornecimento de dados pessoais pelo Poder Público. A junção entre os princípios da proteção da privacidade (e de dados pessoais) e da transparência é assunto que perpassa a regulamentação dos assuntos, que são, deste modo, interligados e com limitações sujeitas a discussão.

Tem-se ainda interligado ao tema, o Marco Civil da Internet (Lei nº 12.965/2014), que demonstra, ao longo de sua redação, a preocupação do legislador para com a privacidade e a proteção dos dados pessoais dos usuários da internet. O decreto regulador do Marco Civil (Decreto nº 8.771/2016), contudo, teve a competência de definir o conceito de dado pessoal e estabeleceu certas diretrizes para a regulação de sua proteção, enumerando alguns entes públicos para tanto.

Frisa-se que a Lei Geral de Proteção de Dados destinou todo um capítulo (IV) ao tratamento de dados pessoais pelo Poder Público, e foi precisamente neste capítulo onde se procurou criar um equilíbrio entre acesso à informação em posse da administração pública e a proteção dos dados pessoais dos cidadãos, trazendo claras menções à Lei de Acesso à Informação. O presente diploma tem por objetivo a contribuição a complicada tarefa do gestor público, por intermédio da exposição de algumas linhas de raciocínio sobre os dispositivos da LGPD no panorama da aplicação pelo poder público. Várias são as regras criadas de modo específico para o poder público, como as relativas a compartilhamento de dados pessoais, transparência e bases autorizativas dos tratamentos de dados pessoais exclusivas para órgãos e entidades públicas.

Recorrentes são as citações da frase: "Dados são o novo petróleo", em tradução livre para a original "*Data is the new oil*", criada por Clive Humby, um matemático londrino especializado em ciência de dados. Expressão esta, que ficou "famosa" quando o assunto gira em torno de dados pessoais e as questões envoltas ao seu tratamento, uma vez que se defende a ideia de que os dados são tão valiosos quanto o petróleo – o que sugere, que quem aprender como fazer bom uso deles e tirar proveito de todo seu potencial, só tem a ganhar.

No entanto, embora se tratem de "um mineral tecnológico valiosíssimo", os dados pessoais são altamente radioativos haja visto os riscos que ostentam. Neste cenário é que se percebe, uma vez mais, que o tratamento de dados pessoais deve se dar de forma cirúrgica e com as ferramentas adequadas apontadas pela LGPD.

Assim, com a crescente utilização de dispositivos tecnológicos espalhados por todas as zonas urbanas, capazes de coletar dados que digam respeito aos cidadãos, monitorar suas atividades e até identificá-los, resta claro o quão delicadas são as questões que cercam a privacidade dos indivíduos, por isso, os órgãos e as entidades públicas, assim como as empresas privadas, também precisam adequar-se a LGPD, vinculando sua adequação a uma transformação cultural que deve avançar com a maior brevidade possível.

2. A Lei Geral de Proteção de Dados (Lei Federal n. 13.709/2018)

Dados pessoais são o estímulo para a atual economia, que é baseada no compartilhamento de conhecimento, de informações e de dados pessoais. Com a sua inevitável utilização e sem uma regulamentação específica, abusos recorrentes são cometidos. A evolução da ideia de privacidade conduziu a sociedade a perceber que o uso incorreto desses dados poderia violar a dignidade da pessoa humana abrindo na sociedade uma ponte que leva à discriminação e à falência dos mais fundamentais direitos humanos. Este novo contexto social provocou em todo o mundo a urgente e necessária discussão sobre o tema.

Mais de 100 (cem) países ao redor do mundo já adotaram uma lei geral para regular o tratamento de dados pessoais em seus diversos setores. Uma Lei Geral de Proteção de Dados pode ser entendida, de forma geral, como um marco regulatório que estabelece direitos e garantias para os cidadãos em relação aos seus dados pessoais, independentemente de quem ou de que forma estes sejam tratados.

O termo “proteção” visa assegurar que o cidadão tenha a seu dispor ferramentas para exercer o efetivo controle sobre seus dados e, ainda que o tratamento de dados pessoais tenha contrapesos e incentivos para que danos aos cidadãos sejam evitados, sem impedir a inovação a partir do tratamento de tais dados, elemento fundamental e indispensável da sociedade da informação.

A Lei Geral de Proteção de Dados justamente esse propósito: direciona-se aos setores público e privado com a pretensão de constituir um equilíbrio entre a proteção dos dados dos cidadãos e, no caso do setor público, a utilização desses dados para a elaboração e execução de políticas públicas e a correta prestação de serviços públicos.

Por derradeiro, importante frisar que a LGPD que foi publicada em 14 de agosto de 2018 e entra em vigor em 16 de agosto de 2020. Relevante nesse contexto é ainda a Medida Provisória 869/2018 ("MP"), aprovada pelo Senado Federal em, 29 de maio de 2019, que traz diversas alterações à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018).

Além das alterações já promovidas pelo então presidente Michel Temer em dezembro de 2018, destacam-se no novo texto (i) a possibilidade de proibição definitiva das atividades de tratamento de dados para entidades infratoras; (ii) a necessidade de o encarregado (DPO) ter conhecimento jurídico regulatório na matéria; (iii) a flexibilização no tratamento de dados de saúde e dados pessoais publicamente acessíveis; e (iv) a efetiva criação da Autoridade Nacional de Proteção de Dados (ANPD) como órgão de natureza jurídica transitória ligado à Presidência da República.

3. Disposições preliminares

O artigo 1º da LGPD traz a garantia da proteção de dados no enfoque dos direitos fundamentais da liberdade, da privacidade e do livre desenvolvimento da personalidade, sendo importantes preceitos

constitucionais e que devem ser observados pelas entidades empresariais e governamentais:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018)[1]

A Lei Geral de Proteção de Dados dispõe apenas sobre o tratamento de dados pessoais. Deste modo, não alcança diretamente dados de pessoas jurídicas, documentos sigilosos ou confidenciais, segredos de negócio, planos estratégicos, algoritmos, fórmulas, softwares, patentes, documentos ou informações que não sejam ligados à pessoa natural ou identificável. Essas outras informações encontram amparo em outros diplomas legais, tais como a Lei de Propriedade Industrial (Lei n.9279/1996), a Lei de Direitos Autorais (Lei 9.610/1998) e a Lei de Software (Lei n.9.609/1998), por exemplo.

Importante mencionar que a LGPD alcança pessoas físicas ou jurídicas de direito público ou privado que procedam com o tratamento de dados pessoais. Denota-se que não há que se falar na existência de direitos absolutos, no entanto limitações a direitos fundamentais devem se dar com moderação, de forma necessária e atendendo ao princípio da proporcionalidade.

A LGPD disciplina princípios correlatos à privacidade que possuem alicerce no artigo 5º, inciso X, da Constituição Federal: "[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988)2.

Segundo Bastos (2000, p. 56), o inciso X, do artigo 5º, da Constituição Federal, demonstra que a privacidade é:

---

[1] <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

2 <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>.

> A faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

Conforme lição de Lafer (1988, p. 239), o direito à privacidade deve ser protegido sendo que esse direito: "[...]do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que só se refere a ela, que diz respeito ao seu modo de ser no âmbito da vida privada". Em complemento, Silva (2009, p. 206) discorre:

> Toma-se, pois, a privacidade como o conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito. A esfera de inviolabilidade, assim, é ampla, abrange o 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.

Nesta esteira, a Lei Geral de Proteção de Dados se adequa em dois preceitos básicos previstos na Constituição Federal, que se refere ao princípio da dignidade da pessoa humana e ao princípio da autonomia da vontade. Na concepção de Ramos (apud ARAÚJO, 2017)3:

> A dignidade da pessoa humana é uma qualidade inerente a cada ser humano, e que na qualidade de princípio fundamental possui como principal característica o fato de serem elemento e medida dos direitos fundamentais. Deste modo, observa-se que em regra a violação a um dos direitos fundamentais à privacidade estará sempre vinculada a uma ofensa à dignidade da pessoa humana. O princípio da dignidade da pessoa impõe limites ao poder estatal, visando impedir que o poder público venha a violar a dignidade

3 <https://jus.com.br/artigos/60812/a-privacidade-da-pessoa-humana-como-direito-constitucional>.

> pessoal, mas igualmente implica em que este mesmo Estado venha a promover a proteção e promoção de uma vida com dignidade para todos.

E sobre o princípio da autonomia da vontade, Diniz (2011, p. 40) ensina que é: "[...] o poder de estipular livremente, como melhor lhes convier, mediante acordo de vontade, a disciplina de seus interesses, suscitando efeitos tutelados pela ordem jurídica".

Desta forma, a LGPD busca a proteção de direitos e garantias fundamentais da pessoa natural titular de dados pessoais, um equilíbrio necessário de forma a diminuir riscos e disciplinar regras bem delimitadas sobre o tratamento de dados pessoais.

Organizações públicas e privadas devem visualizar a proteção de dados como direitos precípuos aos cidadãos, objetivando a proteção dos direitos fundamentais da liberdade e da privacidade; e do livre desenvolvimento da personalidade da pessoa natural titular dos dados pessoais.

4. Fundamentos da Lei Geral de Proteção de Dados

A LGPD possui fundamentos constitucionais baseados na proteção, que incluem também princípios fundamentais da dignidade da pessoa humana e da autonomia da vontade. Logo, o legislador inseriu como fundamento no art. 2º da Lei os seguintes preceitos:

> 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. (BRASIL, 2018)[4]

[4] <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

I - O respeito à privacidade

A privacidade é um dos fundamentos mais importantes da LGPD, tendo sido listada inicialmente pelo legislador. Consoante garantia trazida pela Declaração Universal dos Direitos Humanos (art. 12), bem como nossa Carta Magna (art. 5º, X), o direito à privacidade é garantia fundamental do ser humano, sendo assim condição essencial para o livre desenvolvimento da personalidade humana.

Desse modo, a proteção da privacidade nos termos da LGPD, tem como finalidade a garantia ao titular dos dados pessoais o controle sobre o acesso de terceiros à sua vida privada, motivo pela qual a lei versa sobre os requisitos e hipóteses para o tratamento dos dados pessoais.

II- autodeterminação informativa

Trata-se da garantia dada ao titular dos dados pessoais o controle de seus dados pessoais. Desdobramento advindo do direito à privacidade.

Reconhecido originariamente pelo Tribunal Constitucional Alemão em 1982, quando do julgamento da Lei do Censo Alemã, a autodeterminação informativa traz a garantia ao titular dos dados pessoais a liberdade de decisão sobre as condições de tratamento de seus dados pessoais, ou seja, o controle sobre como os dados serão tratados, assim como sobre as finalidades do tratamento e a identificação do responsável pela atividade, assegurando, assim, um dos objetivo da LGPD (proteção à liberdade do titular de dados pessoais).

III- Liberdade de expressão, de informação, de comunicação e de opinião

A liberdade de expressão é garantia essencial para o livre desenvolvimento da personalidade humana, sendo uma das finalidades da Lei Geral de Proteção de Dados.

Garantia fundamental da Constituição Federal (art. 5º, IX), a liberdade de expressão, e as liberdades de informação, comunicação e opinião são fundamentos da LGPD por serem condições necessárias para o livre desenvolvimento da pessoa humana, vez que são representantes da expressão da personalidade das pessoas.

Com a previsão de tais garantias como fundamentos da Lei Geral de Proteção de Dados, o legislador deixa claro a necessidade de equilibrar sua existência com o respeito à privacidade, devendo ser reprimidos eventuais excessos, de acordo com a garantia dada pela legislação pátria (injúria, difamação e calúnia).Assim, em situações de excessos da liberdade de expressão com violação das normas relativas ao tratamento dos dados pessoais, haverá a prevalência ao respeito à privacidade, objetivo e fundamento da LGPD.

IV – Inviolabilidade da intimidade, da honra e da imagem

A Lei Geral de Proteção de Dados enfatiza a inviolabilidade da intimidade, da honra e da imagem, como direitos igualmente fundamentais previstos na Carta Magna (art. 5º, IX, da CF/88).

Marcel Leonardi traz a reunião de doutrinas acerca do assunto, sendo importante a citação de algumas delas:

> " é o direito de o indivíduo ser deixado em paz para viver sua própria vida com um grau mínimo de interferência", "direito de subtrair-se à publicidade para recolher-se na própria reserva", "o direito a intimidade é o direito de o indivíduo não ser arrastado para a ribalta contra sua vontade, de subtrair-se à publicidade e de permanecer recolhido na sua intimidade, o direito de manter olhos e ouvidos indiscretos afastados dessa esfera de reserva, bem como o direito de impedir a divulgação de palavras, escritos e atos realizados nessa esfera de intimidade, e espaço íntimo intransponível por intromissões ilícitas externas".

Assim, a inviolabilidade da intimidade, da honra e da imagem são fundamentos basilares da LGPD, gerando as mais variadas obrigações de

proteção e gerando uma mudança na cultura do tratamento de dados pessoais.

V – Desenvolvimento econômico e tecnológico e a inovação

Como dever do Estado, estão assegurados, pela Constituição Federal em seus artigos 218 e 219, a promoção e o incentivo ao desenvolvimento econômico e científico, devendo ser interpretados como princípios fundamentais da Constituição Federal quanto ao desenvolvimento nacional.

Desta forma, a inclusão do desenvolvimento econômico e tecnológico e da inovação dentre os fundamentos da Lei Geral de Proteção de Dados deixa claro que a norma que regula a proteção de dados pessoais não foi elaborada a fim de impor obstáculos ao livre avanço da tecnologia e de suas utilidades, mas tão somente para garantir que o seu desenvolvimento esteja em conformidade com proteção dos dados pessoais.

A LGPD, para tanto, é uma resposta aos anseios sociais com vistas a trazer mais segurança jurídica para o ambiente digital com o tratamento dos dados pessoais, bem como com a criação da ANPD. Assim, o desenvolvimento econômico e tecnológico dialoga intimamente com o progresso social e com a inovação.

VI – A livre iniciativa, a livre concorrência e a defesa do consumidor;

O legislador optou por incluir como fundamentos da Lei Geral de Proteção de Dados relevantes matérias constitucionais, visto que a livre iniciativa é fundamento da República Federativa do Brasil (art. 1º, IV, da CF), enquanto a livre concorrência e a defesa do consumidor são princípios da ordem econômica (art. 170, caput e I, da CF).

Como bem pontua Rony Vainzof: “dados pessoais deixaram de ser insumos para a criação e o desenvolvimento de qualquer negócio, para servirem de *commodities* ao possuírem grande valor comercial e

estratégico de acordo com a quantidade, qualidade e capacidade de tratamento."

Desta forma, o mercado de tratamento de dados pessoais deve abrir-se a todos os empreendedores e assegurar-lhes o livre exercício de qualquer atividade econômica nos termos do artigo 170 CF/88, que disciplina que a ordem econômica, fundada na valorização do trabalho humano e na livre-iniciativa, tem por fim assegurar a todos uma existência digna, conforme os ditames da justiça social, observados os princípios da livre concorrência e o da defesa do consumidor.

VII– Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais;

À luz do art.1º, inciso III, da Constituição Federal, a proteção da pessoa humana deve ser entendida como valor máximo do ordenamento jurídico. Desta forma, todos os cidadãos têm direito à proteção de dados, ao controle sobre sua coleta, retenção, tratamento, eliminação e divulgação dos seus dados pessoais.

Ao embasar sua existência no livre desenvolvimento da personalidade e na dignidade da pessoa humana, a LGPD reforça o compromisso e a sensibilidade do tema, evidenciando-o como pressuposto para um Estado democrático.

Assim, citando Philip Agre: "ao controlar informação pessoal é controlar a identidade do seu próprio projeto de mundo. É a liberdade de que a construção da própria identidade não sofrerá coação de forma injusta."

5. Princípios norteadores da LGPD

A Lei Geral de Proteção de Dados (LGPD) estabelece em seu artigo 6º princípios que, junto com a boa fé, devem guiar a atividade de tratamento de dados pessoais no Brasil, são eles:

*** Princípio da Finalidade:** temos por este princípio que para a realização do tratamento de dados pessoais, os propósitos deverão ser legítimos, específicos, explícitos e deverão ser informados ao titular, não havendo a possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I, da Lei 13.709/2018);

*** Princípio da Adequação:** o tratamento de dados pessoais deverá ser compatível com as finalidades informadas aos seus titulares, de acordo com o contexto do tratamento (art. 6º, II, da Lei 13.709/2018);

*** Princípio da Necessidade:** esse princípio impõe que há limitações do tratamento de dados pessoais ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados (art. 6º, III, da Lei 13.709/2018);

*** Princípio do Livre Acesso:** é a garantia dada aos titulares dos dados pessoais para que haja a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (art. 6º, IV, da Lei 13.709/2018);

*** Princípio da Qualidade dos Dados:** deve ser garantido aos titulares dos dados pessoais objetos de tratamento, exatidão, clareza, relevância e atualização dos dados de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento (art. 6º, V, da Lei 13.709/2018);

*** Princípio da Transparência:** por esse princípio é garantido aos titulares dos dados pessoais, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (art. 6º, VI, da Lei 13.709/2018);

*** Princípio da Segurança:** princípio muito importante que impõe a utilização de medidas 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 difusão ((art. 6º, VII, da Lei 13.709/2018);

> * **Princípio da Prevenção:** é a adoção de medidas aptas a prevenir a ocorrência de danos em virtude do tratamento de dados pessoais (art. 6º, VIII, da Lei 13.709/2018);
>
> * **Princípio da Não-Discriminação:** esse princípio garante que não será permitida a realização de tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos (art. 6º, IX, da Lei 13.709/2018);
> * **Princípio da Responsabilização e Prestação de Contas:** por esse princípio fica o agente que tratar dados pessoais obrigados a demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, e inclusive, da eficácia destas medidas (art. 6º, X, da Lei 13.709/2018).

Assim, a LGPD traz o rol de princípios que devem nortear o tratamento de dados pessoais e devem ser seguidos na aplicação da lei. Estes princípios garantem a homogeneidade, a eficácia e a aplicabilidade correta das normas.

6. LGPD e poder público

Para entender o impacto que a Lei Geral de Proteção de Dados terá no âmbito da Administração Pública é necessário recorrer aos conceitos fornecidos pelo Direito Administrativo em relação a sua constituição: "o ordenamento jurídico brasileiro submete as variadas hipóteses de atuação da administração pública, nos três poderes e em todos os níveis da Federação, ora a um regime jurídico tipicamente de direito público, ora a normas oriundas predominantemente do direito privado" (ALEXANDRINO; PAULO, 2017, p. 11).

A LGPD destina um capítulo inteiro (Capítulo IV) tão somente para abordar o tema "Tratamento de Dados Pessoais pelo Setor Público" e aponta que a integração com a Lei de Acesso à Informação se faz necessária.

Sem a intenção de esgotar o assunto, abordaremos artigo por artigo aos quais transcrevemos:

> Art.23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , 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, desde que:
>
> I - sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos;
> II - (VETADO); e
> III - seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art. 39 desta Lei; e
> IV - (VETADO).
> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.
> § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
> § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .
> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.
> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

Este artigo traz a definição de quais são as pessoas jurídicas de direito público interno que se subordinam aos termos da Lei quando realizarem o tratamento de dados pessoais, sendo necessário atrelar esta atividade a uma finalidade e a objetivos específicos.

Necessário se faz ressalvar que a LGPD deixa clara sua relação de complementar-se com a Lei de Acesso à Informação, ao mencionar expressamente as pessoas jurídicas de direito público elencadas no art.1º, parágrafo único, da LAI.

Frisa-se que tanto a LGPD quanto a LAI são legislações voltadas ao valor da transparência da atividade pública, pelo qual o cidadão, pessoa natural, está possibilitado de exercer a defesa de seus direitos e garantias constitucionais em desfavor do Estado e exercendo o efetivo controle das atividades públicas como modo de equilibrar a relação entre Estado e indivíduo.

7. Destinatários da norma

Os destinatários da lei são os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, Cortes de Contas, Judiciário e Ministério Público nos três níveis federativos.

Já no que diz respeito à administração indireta, estão submetidas à LGPD as autarquias, fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios.

8. Princípios administrativos

O "caput" do artigo 37 da Constituição Federal de 1988 remete expressamente sobre os princípios administrativos da legalidade, impessoalidade, moralidade, publicidade e eficiência, e os implícitos, no artigo 2º da Lei Federal 9.784/99 que são: a legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência.

Os princípios existem para orientarem e conduzirem as normas> São as bases e os guias para que leis e normas sejam entendidas e cumpridas.

Por intermédio dos princípios podemos entender o alcance e o sentido das regras jurídicas.

9. Pressupostos de legitimidade para o tratamento de dados pessoais pelo poder público

De acordo com o artigo 23, caput, da LGPD, o tratamento de dados pessoais pelo Poder Público tem por requisitos o atendimento de uma finalidade pública, a busca de um interesse público e a execução, pelo poder público, de suas competências legais ou cumprimento de suas atribuições.

10. Atendimento de uma finalidade pública

Expresso no artigo 37 da Constituição Federal, o principio da impessoalidade obriga o agente público a praticar um ato administrativo somente para o seu fim legal de forma impessoal (Art.5 º, II, da CF/88).

O princípio da finalidade pública determina que o ato público seja praticado sempre com finalidade pública, impedindo assim, que o agente público busque outro objetivo que não seja este, estando impedido também de praticá-lo para atender interesses próprios ou de terceiros.

Assim, para a LGPD, a finalidade pública é atendida pelo Poder Público no tratamento de dados pessoais quando há estreita obediência aos termos da lei, aliando o atendimento a finalidade pública ao interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

11. Persecução de um interesse público

O interesse público encontra-se ligado umbilicalmente com o atendimento do bem comum da coletividade. Sobre o item, citamos Antônio Bandeira de Mello:

> "(...) interesse público deve ser conceituado como interesse resultante do conjunto de interesses que os indivíduos pessoalmente têm quando considerados em sua qualidade de membros da sociedade e pelo simples fato de o serem. "

Há de se reconhecer que os indivíduos possuem interesse legítimo de que seus direitos e garantias constitucionais sejam observados e assegurados pelo Estado através do tratamento correto dos dados pessoais que lhes são entregues, não se aceitando que haja benefício exclusivo do órgão público representado.

Assim, a finalidade pública determina ao Poder Público que o tratamento de dados pessoais se dê em atendimento a execução de uma política pública ou interesses institucionais assegurados pela norma, já o interesse público deve-se pautar pela preservação dos direitos e garantias constitucionais do administrado, pessoa natural, obedecendo o bem comum da coletividade.

12. Transparência no tratamento de dados pessoais

O inciso I, do art.23, da LGPD dispõe que deve haver transparência no tratamento dos dados pessoais pelo Poder Público, estabelecendo as hipóteses de tratamento que devem ser obedecidas em estreita conformidade com a norma. Tal determinação legal esbarra no princípio constitucional da legalidade administrativa.

Os requisitos legais impõem que as informações sejam disponibilizadas de forma clara, atualizada e de fácil acesso em sítios eletrônicos dos entes da Administração Pública.

13. Encarregado ou *Data Protection Officer* (DPO)

O inciso III, do art.23, da LGPD, determina que seja indicado um encarregado quando realizarem operações de tratamento de dados pessoais, nos termos do art.39 desta Lei.

Para a efetivação das determinações legais expostas na LGPD, norma baseada no arcabouço legal europeu (GDPR), foi criada a figura do "Encarregado pelo Tratamento de Dados Pessoais", também conhecido como Data Protection Officer (DPO).

O DPO, de acordo com a lei, deveria ser uma pessoa natural, característica que foi flexibilizada pela MP 869/18 que excluiu a palavra "natural". O encarregado será indicado pelo controlador, que atuará como canal de comunicação entre controlador e titulares de dados pessoais e com a Autoridade Nacional de Proteção de Dados.

14. Autoridade Nacional de Proteção de Dados (ANPD) - atribuições

> § 1º A autoridade nacional poderá dispor sobre as formas de publicidade das operações de tratamento.

Dentre as atribuições da ANPD elencadas no artigo 55-J da LGPD, merecem destaque a elaboração de diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade; a fiscalização e a aplicação de sanções; a difusão das normas e das políticas públicas sobre proteção de dados pessoais e sobre medidas de segurança; e ainda, a promoção de ações de cooperação com autoridades de proteção de dados pessoais de outros países, sejam de natureza internacional ou transacional.

Importante mencionar que, o compromisso legal com a transparência nas operações de tratamento de dados pessoais, deve se dar em estreito respeito ao princípio da publicidade assegurado pelo art. 37 da Constituição Federal aliado ao princípio da transparência previsto no artigo 6 º, inciso VI, da Lei Geral de Proteção de Dados.

> § 2º O disposto nesta Lei não dispensa as pessoas jurídicas mencionadas no caput deste artigo de instituir as autoridades de que trata a Lei 12.527...

A Lei de Acesso à Informação (LAI) dispõe que as informações solicitadas pelo cidadão ao Poder Público sejam fornecidas pelo órgão ou

entidade pública titular da informação e, em eventual recurso, seja direcionado à autoridade hierárquica superior.

Já a figura do encarregado disposta na LGPD, se trata de pessoa indicada pelo controlador para atuar como canal de comunicação entre controladores, titulares de dados e Autoridade Nacional de Proteção de Dados.

Há, portanto, uma relação de complementariedade entre o Encarregado (DPO) disposto na LGPD e o órgão ou entidade pública responsável pela custódia da informação nos termos da LAI.

Como bem cita Antônio Fernando Tasso, "enquanto a autoridade de acesso a informação tem por investidura legal dar acesso ao cidadão a toda informação passível de publicidade sob custódia da Administração Pública, observadas a matriz do sigilo, ao encarregado cabe, entre outras atribuições, justamente o oposto, qual seja a preservação de dados pessoais e dados sensíveis que estejam em bases públicas. "

Portanto, há interdependência das atividades públicas que estas suas pessoas desenvolvem, devendo-se dar vasta publicidade as suas deliberações conjuntas.

> § 3º Os prazos e procedimentos para exercício dos direitos do titular perante o Poder Público observarão o disposto em legislação específica, em especial as disposições constantes da Lei nº 9.507, de 12 de novembro de 1997 (Lei do Habeas Data) , da Lei nº 9.784, de 29 de janeiro de 1999 (Lei Geral do Processo Administrativo) , e da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) .

A LGPD faz parte de um sistema de proteção de dados, que passa a centralizar todas as disposições referentes ao tema de proteção de dados que estavam abarcados de forma descentralizadas em outras normas.

> § 4º Os serviços notariais e de registro exercidos em caráter privado, por delegação do Poder Público, terão o mesmo tratamento dispensado às pessoas jurídicas referidas no caput deste artigo, nos termos desta Lei.

> § 5º Os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a administração pública, tendo em vista as finalidades de que trata o caput deste artigo.

A Lei Geral de Proteção de Dados confere aos serviços notarias, de registro e de protesto, o mesmo tratamento legal dado as pessoas jurídicas de direito público, em consonância com os artigos 173 da CF/88 e artigo 24 da LGPD.

A LGPD determina aos órgãos notariais e de registros o dever legal de fornecimento de acesso aos dados do Poder Público, que devem estar necessariamente unidos ao atendimento à finalidade pública da atividade registral, e pelo qual seja assegurada a garantia da autenticidade, segurança e eficácia dos atos jurídicos, assim como do órgão ou ente público que postula o acesso.

Os serviços notariais e de registro exercidos em caráter privado, por delegação da Administração Pública, terão o mesmo tratamento dispensado às pessoas jurídicas de direito público. Deste modo os órgãos notariais e de registro devem fornecer acesso aos dados por meio eletrônico para a Administração Pública.

15. Empresas públicas e sociedades de economia mista na exploração de atividade econômica

> Art. 24. As empresas públicas e as sociedades de economia mista que atuam em regime de concorrência, sujeitas ao disposto no Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.
> Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos deste Capítulo.

É sabido que o Estado pode prestar serviços públicos ou atuar na exploração da atividade econômica, excepcionalmente por meio de empresas de direito privado, quando autorizado por lei.

A LGPD em atendimento às normas constitucionais, assegura que as empresas estatais que atuem em regime de concorrência atentem-se para as regras do tratamento de dados destinadas as pessoas jurídicas de direito privado. Desta forma, empresas estatais que exercem atividade de forma de monopolista, subordinam-se à Lei Geral de Proteção de Dados.

Do mesmo modo que as empresas estatais atuam na exploração de atividade econômica em modelo de monopólio, terão também o mesmo tratamento garantido pela LGPD ao Poder Público aquelas que exerçam atividade pública.

> Art. 25. Os dados deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

O artigo 25 trata apenas de dados pessoais e dados sensíveis, conforme definições legais constantes no artigo 5 º, incisos I e II, da LGPD.

Para Fernando Antônio Tasso, "a LGPD prescreve que dados pessoais e sensíveis sejam armazenados de forma estruturada e em formato aberto (interoperável), de modo a permitir seu consumo por outros órgãos ou entes públicos, inclusive mediante a integração de sistemas, desde que observadas determinadas premissas técnicas e, desta forma, viabilizar a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública, a disseminação e o acesso das informações pelo público em geral."

> Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.

O artigo 26 deixa claro que o uso compartilhado de dados pessoais pelos órgãos públicos deve pautar-se na observância aos princípios de proteção de dados pessoais expostos no artigo 6º da Lei. São eles, os

princípios da finalidade, da adequação, da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas.

Esses princípios elencados na Lei Geral de Proteção de Dados garantem validade e legitimidade às regras de proteção de dados pessoais, consolidando-se quando a execução das políticas públicas está em igualdade com as liberdades dos cidadãos, titulares dos dados pessoais.

> Art. 27. A comunicação ou o uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado dependerá de consentimento do titular, exceto:
> I - nas hipóteses de dispensa de consentimento previstas nesta Lei;
> II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do inciso I do caput do art. 23 desta Lei; ou
> III - nas exceções constantes do § 1º do art. 26 desta Lei.
> Parágrafo único. A informação à autoridade nacional de que trata o caput deste artigo será objeto de regulamentação.

Têm-se por esse artigo que o consentimento é a base legal que tem a finalidade de trazer legitimidade ao acesso dos dados pessoais nos bancos de dados públicos por entes privados.

Em síntese, o Poder Público está legalmente fundamentado para proceder com o tratamento de dados pessoais quando está executando políticas públicas, e ao compartilhar esses dados pessoais com entes privados, o faça mediante obtenção de consentimento dos titulares desses dados.

> **Art. 28.VETADO.**

16. Solicitação da ANPD ao poder público

> Art. 29. A autoridade nacional poderá solicitar, a qualquer momento, aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado e poderá emitir parecer técnico complementar para garantir o cumprimento desta Lei.

A Autoridade Nacional de Proteção de Dados poderá solicitar aos órgãos e às entidades do poder público a realização de operações de tratamento de dados pessoais, fornecimento de informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado.

Em relação as outras atividades a serem desenvolvidas pela ANPD, valemo-nos da citação de Fernando Antônio Tasso em sua contribuição à obra Lei Geral de Proteção de Dados Comentada: "No que concerne às demais atividades, quais sejam, a de solicitar informações específicas sobre o âmbito e a natureza dos dados e outros detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei, não há qualquer ressalva em assim proceder, porquanto consistem em ações que guardam estreita relação com a missão institucional da ANPD."

16.1. A Autoridade Nacional de Proteção de Dados (ANPD)

> Art. 30. A autoridade nacional poderá estabelecer normas complementares para as atividades de comunicação e de uso compartilhado de dados pessoais.

A ANPD possui amplo poder normativo para exercer sua função pública de implementação da LGPD, conforme disposição expressa do art.55-J, inciso II, da Lei.

De uma análise detida do art.30, acima citado, evidenciou-se que a Autoridade Nacional de Proteção de Dados exerce atividades de comunicação e uso compartilhado de dados pessoais na esfera da Administração Pública ao emitir normas complementares já existentes.

Deste modo, dentre as atribuições do órgão, destacam-se a elaboração de diretrizes para a Política Nacional de Proteção de Dados Pessoais e Privacidade; a fiscalização e aplicação de sanções; a divulgação para a população do conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; e promoção

de ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional.

Não restam dúvidas da importância da Autoridade Nacional de Proteção de Dados – vista como crucial para o funcionamento adequado da Lei Geral de Proteção de Dados. Neste cenário, as funções institucionais a serem desempenhadas pela ANPD devem estar em conformidade com uma adequada interpretação e implementação da Lei estabelecendo um processo de segurança jurídica para as questões envoltas à proteção de dados pessoais.

16.2. Responsabilização do Poder Público

> Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, a autoridade nacional poderá enviar informe com medidas cabíveis para fazer cessar a violação.

O artigo 31 dispõe acerca da possibilidade (poder/dever) de a Autoridade Nacional de Proteção de Dados enviar informes com medidas adequadas para pôr fim a violações por órgãos ou entes da Administração Pública.

Frisa-se que o ato de informar/recomendar ao Poder Público as medidas cabíveis para fazer cessar a violação por este praticada, não retira ou mitiga o caráter ou o poder sancionatório da ANPD e deixa claro que os entes públicos não estão imunes as sanções em caso de desídia e displicência pelos entes administrados.

As sanções administrativas a que estão sujeitos os entes públicos são mais serenas daquelas a que se submetem os entes privados e estão estabelecidas no §3º do artigo 52, sendo elas:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

> VI - eliminação dos dados pessoais a que se refere a infração;

No artigo 52, § 1º, inciso II, há a disposição da Lei em se levar em consideração o quesito da boa-fé pelo infrator quando da prática da violação. Assim, se o administrado tem ciência do ato praticado, há clara violação desse princípio.

Ademais, ocorrendo o tratamento indevido de dados pessoais, deverá ser comunicada à Agência Nacional de Proteção de Dados e aos titulares dos dados atingidos em um prazo razoável. Em caso de incidentes envolvendo dados pessoais, deverão ser tomadas medidas corretivas, podendo inclusive, tornar pública a infração, o bloqueio dos dados pessoais dos envolvidos no tratamento indevido e até a eliminação dos dados.

Outras medidas poderão ser aplicadas, como por exemplo, o que dispõe a Lei nº. 8.112/90, que trata do regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais, sendo que os artigos 121 e 122 assim discorrem acerca das responsabilidades dos agentes públicos:

> Art. 121. O servidor responde civil, penal e administrativamente pelo exercício irregular de suas atribuições.
>
> Art. 122. A responsabilidade civil decorre de ato omissivo ou comissivo, doloso ou culposo, que resulte em prejuízo ao erário ou a terceiros.
> § 1º A indenização de prejuízo dolosamente causado ao erário somente será liquidada na forma prevista no art. 46, na falta de outros bens que assegurem a execução do débito pela via judicial.
> § 2º Tratando-se de dano causado a terceiros, responderá o servidor perante a Fazenda Pública, em ação regressiva.
> § 3º A obrigação de reparar o dano estende-se aos sucessores e contra eles será executada, até o limite do valor da herança recebida.

Apesar de não haver punição de multa para entes públicos, sanções como o bloqueio dos dados pessoais podem gerar grande impacto na atuação pública e, mais uma vez, é necessário ressaltar que as empresas públicas e sociedades de economia mista que atuem em regime de

concorrência conforme a determinação constitucional se submetam também a sanção pecuniária.

Assim o legislador deixa explícito que além da Lei Geral de Proteção de Dados o setor público se submete a outros ditames legais, quais sejam, a Lei de Improbidade Administrativa, o Estatuto do Servidor Público Federal e a Lei de Acesso à Informação.

17. Elaboração e publicação de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)

> Art. 32. A autoridade nacional poderá solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

O relatório de impacto à proteção de dados pessoais (RIPD), também conhecido como DPIA – Data Protection Impact Assessment, é o documento gerado pelo controlador, que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais. Este relatório deve apresentar as medidas, salvaguardas e mecanismos de mitigação de riscos, conforme o artigo 5º, inciso XVII da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018). Citando Marcilio Braz, "O propósito de um Data Protection Impact Assessment não é eliminar todos os riscos, mas minimizar a existência destes".

O relatório de impacto à proteção de dados pessoais encontra-se disposto no artigo 5º, XVII da lei, senão, vejamos:

> Art. 5º Para os fins desta Lei, considera-se:
> XVII – relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Faz-se ainda, imperiosa a citação do artigo 38 da LGPD, deixando claro, no âmbito de aplicação do relatório, quais são os elementos básicos que devem compô-lo:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

Citando novamente Marcílio Braz, acertadamente sobre o tema, conclui que, "considerando que o mens legis no tocante a necessidade, abrangência (parcialmente) e elementos constitutivos deste relatório inspira-se no GDPR (General Data Protection Regulation) da União Europeia, em nossa opinião o diploma legal pátrio findou por carecer de maiores esclarecimentos e definições quanto a ao escopo e formatação do referido relatório, em contraposição ao diploma legal europeu".

Em análise detida do art. 38 da LGPD tem-se que a ANPD tem o poder de imposição ao determinar a elaboração de um DPIA a um controlador que ainda não o tenha realizado. Levando em consideração que está expressa na Lei, através do verbo "determinar", a obrigatoriedade de realização de relatórios de impacto à proteção de dados pessoais para operações de tratamento, a sua ausência é capaz de ensejar a aplicação de multas ou processos administrativos ou processos judiciais em desfavor do controlador por não se atentar para o tratamento de dados de forma correta, conforme dispõe a Lei Geral de Proteção de Dados.

Corroborando com o entendimento acima esposado, segue o artigo 10, § 3º, que se segue:

> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como

> fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Ao esmiuçar os artigos 32 e 38 da LGPD, nota-se que na letra fria da Lei, embora com nítidos desencontros na redação, os verbos "determinar" e "solicitar" não se tratam de meras liberalidades do controlador, mesmo no âmbito do poder público. No artigo 32, o texto da Lei se utiliza do verbo "solicitar" ao requerer que o agente público publique o relatório de impacto de dados pessoais, enquanto que no artigo 38, de outra forma, se utiliza do verbo "determinar" para requerer a elaboração do mesmo relatório. Reforçando esta posição, desta monta, no artigo 10, §3, da mesma Lei, utiliza-se o mesmo verbo "solicitar" ao – novamente - requerer o RIPD do controlador nas hipóteses lá descritas. Portanto, pode-se concluir de forma lógica que não haveria motivo ao legislador para se utilizar do mesmo verbo "solicitar" (no artigo 10, §3 e artigo 32) para determinações distintas, provocando o entendimento de que o sentido do verbo é o mesmo, qual seja, da exigência do relatório de impacto de dados pessoais nos casos estabelecidos.

Assim, os termos se "confundem" e se "completam", levando à conclusão que os órgãos públicos dispõem da mesma obrigatoriedade que os entes privados, na elaboração de relatórios de impacto à proteção de dados pessoais para suas operações de tratamento.

18. Outras considerações

18.1 Abrangência da Lei Geral de Proteção de Dados ao setor público

O Poder Público é um dos maiores concentradores de dados pessoais, pois está no controle, ainda que indiretamente, da vida financeira, do acesso à saúde, dos processos judiciais, de dados educacionais, de dados trabalhistas dos cidadãos e assim por diante. Deste modo, excluir o poder público da égide da Lei Geral de Proteção de Dados seria uma quebra dos

direitos constitucionais dos cidadãos e o início de uma longa insegurança jurídica.

O Poder Público vem se tornando cada vez mais digital, desde aplicativos que possibilitam acessar faturas de consumo de energia elétrica, água e impostos, a aplicativos de recuperação de créditos, notas fiscais, acesso a bancos públicos, a agências reguladoras e serviços como INSS e FGTS, dentre outros.

Conforme pesquisa realizada pelo Internetlab "a Administração Pública também passa a adotar gradativamente o uso de aplicações de internet como estratégia para se aproximar de cidadãos e facilitar o acesso à informação e a prestação de determinados serviços".

Como o Estado é um grande controlador de dados pessoais é de suma importância sua necessidade de submissão à Lei Geral de Proteção de Dados, sendo inimaginável um cenário onde isso fosse diferente sem afrontar diretamente direitos basilares dos cidadãos.

18.2 Não aplicação da LGPD ao poder público

Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

> III - 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;

O Art. 4º, inciso III, enumera os casos em que as atividades envolvendo o tratamento de dados pessoais se revestem de caráter unicamente estatal e blinda o Poder Público de qualquer responsabilidade quanto aos tratamentos realizados, assim, o legislador excepcionou a aplicação da Lei Geral de Proteção de Dados para as finalidades acima listadas.

O Regulamento Europeu de Proteção de Dados em seu art.2º (2) d também excepciona sua aplicabilidade a autoridades competentes para

efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais, incluindo a prevenção de ameaças à segurança pública.

Lembrando que os tratamentos dos dados pessoais realizados para os fins que estão fora do escopo da LGPD deverão obedecer a regência de legislação específica, que prevê que as medidas a serem tomadas para esses tratamentos sejam proporcionais e estritamente necessárias ao atendimento do interesse público, garantindo-se assim, o devido processo legal, os princípios gerais de proteção e os direitos do titular, a fim de evitar excessos e abusos pelos entes públicos.

Por fim, vale ressaltar ainda, que o tratamento de dados para as finalidades acima mencionadas, só poderão se dar por pessoa jurídica de direito privado em procedimentos sob a tutela de pessoa jurídica de direito público, sendo certo que os dados pessoais constantes de bancos de dados constituídos para tais fins não podem ser tratados por pessoas jurídicas de direito privado, com exceção das controladas pelo Poder Público.

18.3 Transferência internacional de dados realizada pelo administração pública

A Lei Geral de Proteção de Dados traz alguns casos em que a Administração Pública poderá realizar operações de transferência internacional de dados, vez que um dos objetivos da norma regulatória é facilitar o fluxo de dados pessoais desde que protegidos, estes casos estão previstas no artigo 33, nos incisos I, III, IV, VI, VII.

Frisa-se que para a operação de transferência internacional de dados deverá haver o cumprimento de acordos de cooperação internacional, execução de políticas públicas ou atribuições do serviço público, quando a transferência tiver por objetivo proteger a vida ou a incolumidade física do titular ou de terceiros ou quando estiverem acordadas em instrumentos de direito de internacional com fins de cooperação jurídica e ocorrer entre órgãos públicos de inteligência, investigação e persecução.

Contudo, havendo a necessidade de realização de tais transferências e existindo dúvida acerca do grau de proteção fornecido pelo país destinatário dos dados pessoais, a União, Estados, Distrito Federal e Municípios poderão requisitar parecer da Autoridade Nacional de Proteção de Dados.

19. Considerações finais

Com o rápido crescimento da tecnologia da informação no século XX, surge a expressão "morte da privacidade", que tem por fim evidenciar que é impossível blindar eventos e elementos da vida privada frente ao vasto fluxo de informações ofertado pelas novas tecnologias.

Sabe-se que há séculos o controle de informações pelas instituições sociais, tais como a Igreja e o Estado, esteve associado ao controle do poder na sociedade. No entanto, a partir de meados do século XX, o desenvolvimento tecnológico acarretou a intensificação dos fluxos de informação e, no início do século XXI, de uma forma nunca antes vista levou à denominação da sociedade atual como "sociedade da informação" ou "era da informação".

Manuel Castells afirma que: "está em curso uma verdadeira revolução tecnológica, cujo núcleo se refere às tecnologias da informação, processamento e comunicação", e o Poder Público se insere diretamente nessa "revolução tecnológica", visto que é o maior detentor e controlador de dados pessoais de uma sociedade.

Insta salientar que no escoar do século XXI, a mudança da função do Estado, atrelada à revolução tecnológica, colaborou para as mudanças no alcance do direito à privacidade, tornando-o direito basilar dos cidadãos em todo o contexto social. Nessa seara, a violação da privacidade não é problema apenas de grandes celebridades, e sim, passa a atingir cidadãos e se torna um problema social a ser contornado pelo Estado.

Tem-se que o direito à privacidade não se trata de um direito absoluto, pois possui limitações fundadas em outros direitos individuais

ou coletivos, fundamentais para a vida em sociedade. Corroborando com o tema, citemos Alan Westin: "O desejo do indivíduo por privacidade nunca é absoluto, uma vez que a participação em sociedade é igualmente importante. ". Assim, cada indivíduo está continuamente envolvido em um processo pessoal de equilíbrio entre o desejo de privacidade e o desejo de exposição e comunicação com os outros, à luz de condições do ambiente e de normas sociais na sociedade em que vive. O indivíduo o faz em face das pressões da curiosidade dos outros e dos processos de vigilância que toda sociedade necessita para a implementação de normas sociais."

Para Jorge Reis Novais, "É interessante observar que ao mesmo tempo em que o princípio da dignidade humana é o fundamento da autonomia do titular do direito, é ela também o seu limite", assim um dos maiores desafios da Administração Pública será atender às regras trazidas pela LGPD, respeitando as necessárias restrições quanto ao tratamento dos dados pessoais de cidadãos brasileiros.

A acertada inclusão do poder público no escopo da Lei Geral de Proteção de Dados obriga-o a adequar-se e investir em segurança que por tantas vezes são deixadas de lado, e ainda, faz com que o Poder Público tenha o dever de atuar de forma a evitar o comércio de dados pessoais para fins estranhos aos quais foram coletados e confiados pelos seus titulares.

Como "nem tudo são flores ", assim como "nem tudo são espinhos", a LGPD trará um importante e necessário equilíbrio aos interesses sociais e econômicos para todos os setores públicos e privados, assim como para as liberdades e garantias fundamentais. Trará ainda mais proteção e segurança para os titulares de dados pessoais, tutelando de forma necessária a proteção de dados em conformidade com a dignidade da pessoa humana, combinada com os limites da privacidade, da honra e da imagem individual de cada pessoa. Por fim irá tutelar a livre iniciativa e os fins econômicos, frutos do tratamento de dados pessoais, de forma legítima, com responsabilidade, proporcionalidade e razoabilidade.

Finalmente haverá mais aprimoramento para o desenvolvimento tecnológico no país, implementação de boas práticas de negócios em todas

as áreas, impulsionamento do mercado digital e ao mesmo tempo proteção dos dados pessoais dos cidadãos. O Estado reúne todas as ferramentas necessárias para dar bons exemplos e iniciar o processo de boas práticas e *compliance*.

20. Referências

ALEXANDRINO M.; PAULO V. Direito Administrativo Descomplicado. 27 ed. São Paulo: Método, 2017.

ARAÚJO, Lucimara Brandão Reis. A privacidade da pessoa humana como Direito Constitucional. Jus, 2017. Disponível em: <http://jus.com.br/artigos/60812/a-privacidade-da-pessoa-humana-como-direito-constitucional>. Acesso em: 15 out. 2019.

BRASIL. Constituição da República Federativa do Brasil de 1988. Palácio do Planalto, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 20 out. 2019.

BRASIL. Decreto-lei nº. 200, de 25 de fevereiro de 1967. Dispõe sobre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Palácio do Planalto, 1967. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del0200.htm>. Acesso em: 20 out. 2019.

BRASIL. Lei nº. 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Palácio do Planalto, 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>. Acesso em: 20 out. 2019.

Disponível em: <https://baptistaluz.com.br/institucional/aprovada-pelo-congresso-a-medida-provisoria-869-que-altera-a-lei-geral-de-protecao-de-dados/>. Acesso em 20 out.2019

Disponível em: <https://itsrio.org/pt/publicacoes/lei-geral-de-protecao-de-dados-pessoais-lgpd-e-setor-publico/>. Acesso em 20 out.2019

BRASIL. Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Palácio do Planalto, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 out. 2019.

BRASIL. Lei nº. 13.853, de 08 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. Palácio do Planalto, 2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1>. Acesso em: 20 out. 2019.

BRASIL. Lei nº. 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Palácio do Planalto, 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm>. Acesso em: 14 out. 2019.

DINIZ, Maria Helena. Curso de Direito Civil Brasileiro: teoria das obrigações contratuais e extracontratuais. 27 ed. São Paulo: Saraiva, 2011.

GOMES, Helton Simões. Vazamento de dados cresce e já é 2º maior ataque digital ao governo federal. Uol, 2019. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2019/06/16/vazamento-de-dados-cresce-e-ja-e-2-maior-ataque-digital-ao-governo-federal.htm>. Acesso em: 20 out. 2019.

LAFER, Celso. A reconstrução dos direitos humanos: um diálogo com o pensamento de Hannah Arendt. São Paulo: Companhia das Letras, 1998.

MAGRANI, E. A Internet das coisas. Rio de Janeiro: FGV Editora, 2018.

MARCOS, Marcela. Recém-aposentados recebem ligações para contratar consignado. Folha de São Paulo, 2019. Disponível em: <https://www1.folha.uol.com.br/mercado/2019/02/recem-aposentados-recebem-ligacoes-para-contratar-consignado.shtml>. Acesso em: 20 out. 2019.

PIETRO, M. S. Direito Administrativo. Rio de Janeiro: Forense, 2018.

RIBEIRO, Bastos Celso. Curso de Direto Constitucional. São Paulo: Saraiva, 2000.

SILVA, José Afonso da. Curso de direito constitucional positivo. 32 ed. São Paulo: Malheiros, 2009.

LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2011

DONEDA, Danilo. Da privacidade a proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.p.101.

Tribunal Europeu de Direitos Humanos da União Europeia, Niemietz v. Alemanha, 72/1991/324/396, seção 29, j. 16.12.1992.

CUPIS, Adriano de. Os direitos da personalidade. Trad. Adriano Vera Jardim e Antônio Miguel Caeiro. Lisboa: Morais, 1961. p. 15.

COSTA Júnior, Paulo José da. O direito de estar só: tutela penal da intimidade. 4. Ed. São Paulo: Revista dos Tribunais, 2007. p. 49.

MORAES, Alexandre de. Direitos humanos fundamentais: teoria geral, comentários aos arts. 1º a 5º da Constituição da República Federativa do Brasil. 8 . ed. São Paulo: Atlas, 2007. p.128.

LGPD: Lei Geral de Proteção de Dados comentada/Viviane Nóbrega Maldonado, Renato Ópice Blum, coordenadores. - São Paulo: Thomson Reuters Brasil, 2019. Vários autores.

VAINZOF, Rony (LGPD: Lei Geral de Proteção de Dados comentada/Viviane Nóbrega Maldonado, Renato Ópice Blum, coordenadores. - São Paulo: Thomson Reuters Brasil, 2019. Vários autores. P.40)

TASSO, Fernando Antônio (LGPD: Lei Geral de Proteção de Dados comentada/Viviane Nóbrega Maldonado, Renato Ópice Blum, coordenadores. - São Paulo: Thomson Reuters Brasil, 2019. Vários autores. P.261)

TASSO, Fernando Antônio (LGPD: Lei Geral de Proteção de Dados comentada/Viviane Nóbrega Maldonado, Renato Ópice Blum, coordenadores. - São Paulo: Thomson Reuters Brasil, 2019. Vários autores. P.276)

TASSO, Fernando Antônio (LGPD: Lei Geral de Proteção de Dados comentada/Viviane Nóbrega Maldonado, Renato Ópice Blum, coordenadores. - São Paulo: Thomson Reuters Brasil, 2019. Vários autores. P.282) Disponível em: <https://www.juridoc.com.br/blog/noticias/11452-o-que-e-a-autoridade-nacional-de-protecao-de-dados-anpd/> Acesso em: 25 out. 2019.

GDPR - General Data Protection Regulation

LGPD - Lei nº 13.709/2018

LAI - Lei nº 12.527/2012 Lei de Acesso à Informação - art. 1º, Parágrafo Único.

Lei de Improbidade Administrativa - Lei nº 8.429 de 2 jun. 1992

Estatuto do servidor público - Lei nº 8.112 de 11 dez. 1990/Disponível em: <https://brasilpaisdigital.com.br/> Acesso em 20/11/2019

Relatório de Impacto. Disponível em: <https://blog.sanderecella.com.br/2019/08/29/adequacao-a-lgpd-o-que-e-o-relatorio-de-impacto-a-protecao-de-dados-pessoais/>. Acesso em 21/11/2019

BRANCO S. O Estado quer seus dados pessoais, mas sem transparências nem direitos. Acesso em: 21 nov. 2019.

BRASIL. Constituição, 1988. Diário Oficial da União, Brasília, DF, 5 out. 1988. Acesso em: 21 nov. 2019.

LUCCA, C. Manobra no Senado tenta retirar o setor público da Lei de Proteção de Dados.

MAGRANI, E. A Internet das coisas. Rio de Janeiro: FGV Editora, 2018.

ROSSO, Ângela Maria, LGPD e setor público: aspectos gerais e desafios. Disponível em:<https://www.migalhas.com.br/dePeso/16,MI300585,31047-LGPD+e+setor+publico+aspectos+gerais+e+desafios>. Acesso em 29 nov.2019.

CF: GARFINKEL, Simson. Database Nation: The Death of Privacy in the 21th Century. O'Reilly Media: California, 2000; SMITH, Robert Ellis. Privacy. How to protect. What´s left of it. Garden City: Anchor Press/Doubleday, 1979; SOLOVE, Daniel J.. The digital person: technology and privacy in the information age. New York: New York University Press, 2004.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. Vol. 1. A sociedade em rede. Trad: Roneide Venâncio Majer. São Paulo: Paz e Terra, 1999, p. 50.

WESTIN, Alan. Privacy and Freedom. Op. Cit., p. 7 (tradução livre).

NOVAIS, Jorge Reis. Renúncia a Direitos Fundamentais. In: MIRANDA, Jorge. (org.) Perspectivas Constitucionais nos 20 anos da Constituição de 1976. Volume I. Coimbra: Coimbra Editora, 1996, p. 287.

PÉREZ LUÑO, Antônio-Enrique. Manual de Informática e Derecho. Barcelona: Editorial Ariel, 1996, p. 43.

SUMNER, Stuart. You: for sale – protecting your personal data and privacy online. Waltham: Elsevier, 2016. p. 4

SUMNER, op. cit., p. 6

21

Proteção de dados dos trabalhadores e a competência da autoridade nacional de proteção de dados

Duarte Moura

1. Autoridade Nacional de Proteção de Dados – ANDP

A criação da ANPD tem como objetivo a adequação da legislação brasileira, para a nova regulamentação de proteção de dados, buscando adequação aos mais evoluídos padrões internacionais.

Em meados de agosto de 2018, houve a promulgação da Lei nº 13.709, que foi denominada de Lei Geral de Proteção de Dados Pessoais ou LGPD. Nesse mesmo período, o ex-presidente Michel Temer vetou os artigos que tratavam da criação da Autoridade Nacional de Proteção de Dados (ANPD) e, em seu âmbito, do Conselho Nacional de Proteção de Dados, justificando tal ato, sob a alegação de que havia um vício formal de iniciativa no processo legislativo para a criação da ANPD, na medida em que ela deveria emanar do Poder Executivo e não do Poder Legislativo.

Independentemente das razões do veto, a discussão sobre a criação de uma autoridade controladora passava por um ponto essencial. Se a ANPD não fosse criada, ou se criada sem que tivesse uma independência necessária para à sua atuação na promoção da proteção de dados pessoais, será que seriam estabelecidas diretrizes relacionadas, a sua fiscalização e a aplicação de sanções, caso houvesse alguma violação aos direitos dos titulares de dados pessoais, e, será que a eficácia da LGPD não seria

substancialmente prejudicada, tendo em vista que a lei foi criada considerando a existência de uma autoridade investida de tais funções?

Além disso, tal situação iria de encontro às propensões internacionais em matéria de proteção de dados, verificadas, não somente, mas em especial no quadro da Organização para Cooperação e Desenvolvimento Econômico, bem como em países da União Europeia, onde já existem órgãos semelhantes e que já estão em operação, com grandes consequências advindas de uma inapropriada anuência às diretrizes até então elaboradas para um sistema internacional de proteção de dados, que hoje está em um continuo e rápido processo de construção.

De qualquer forma, seja pela pressão externa ou pela própria necessidade da existência de um órgão como a ANPD, no final de dezembro de 2018, quase acabando o mandato de Temer, houve a edição, pela Presidência da República, da Medida Provisória de nº 869/2018, que, finalmente, fomentou a criação da ANPD e também gerou algumas alterações em outros pontos da LGPD.

Mesmo que o modelo adotado na MP não seja o mesmo adotado pela LGPD, a criação desse órgão ajuda, certamente, ao interesse inicial de adequação da legislação brasileira, na matéria de proteção de dados, aos mais evoluídos padrões internacionais e tenta suprir a falha gerada pelo veto presidencial de agosto de 2018.

Originalmente, o modelo institucional que foi sugerido para a ANPD era de que fosse uma autarquia especial, tendo seu vínculo ao Ministério da Justiça, possuindo independência administrativa, autonomia financeira e ausência de subordinação hierárquica. Mas o modelo aprovado pela MP 869/2018, transformou a ANPD em um órgão da administração pública federal que é vinculado à Presidência da República, garantindo a autoridade a sua autonomia técnica, sendo-lhe designada a responsabilidade por zelar, implementar e fiscalizar o cumprimento da LGPD.

2. A proteção de dados do empregado

Com a LGPD, foram dadas mais responsabilidades a todos que processam os dados de qualquer indivíduo. E, adentrando esse assunto para as relações de trabalho, não há dúvidas de que empregadores, bem como os tomadores de serviços, deverão realizar de maneira correta a coleta, armazenamento e tratamento de dados daqueles que lhes prestam serviços.

Sabemos que é uma prática bem comum as empresas utilizarem os dados de seus empregados, como por exemplo, ao serem elaboradas as políticas internas, bem como na avaliação de benefícios concedidos aos seus empregados.

Isto é, desde a fase de inscrição para a vaga de emprego ou do processo seletivo que será realizado pela empresa, o indivíduo fornece uma grande quantidade de dados, passando pelo processo de admissão, onde diversos documentos serão fornecidos, devendo ser feito o prévio consentimento para o tratamento de dados, como, por exemplo, através de cláusula expressa no contrato de trabalho, com validade até o momento da rescisão.

Após o término do contrato de trabalho, a guarda dos dados pelas empresas é legitimada e respaldada pela LGPD, estando esta em conformidade com a legislação trabalhista, uma vez que tais dados podem ser necessários para cumprimento de obrigações legais ou mesmo para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

Não se pode esquecer da prescrição trabalhista, quando falamos de guarda de dados, pois, sabe-se, que o direito de ação, na seara trabalhista, tem sua prescrição em 2 anos após o término do contrato de trabalho, podendo os empregados pleitearem seus direitos relativos aos últimos 5 anos do contrato de trabalho a contar da data do ajuizamento da ação.

Pode acontecer de as empresas compartilharem os dados de seus empregados com terceiros, mas, somente no caso desse compartilhamento

estar exclusivamente vinculado aos limites estabelecidos, como por exemplo, para a abertura de conta em bancos, a adesão a planos de saúde, etc., correndo o risco de violar a LGPD e as leis trabalhistas, por potencial abuso de direito.

Devemos falar dos dados pessoais considerados como "dados sensíveis", que somente devem ser processados quando estritamente necessários. Esses dados são protegidos pela legislação e pela jurisprudência brasileira no âmbito trabalhista, passando agora a serem contemplados com uma máxima proteção pela LGPD. Haverá uma maior restrição ao processamento de quaisquer informações do tipo, dificultando ainda mais que estes dados sejam usados pelo empregador, em exemplo nos processos trabalhistas, mesmo sabendo que boa parte da jurisprudência trabalhista tem entendido como abusiva o uso de dados pessoais confidenciais para suas defesas.

Com a entrada em vigor da LGPD, as práticas abusivas utilizadas pelas empresas na relação de trabalho deverão ser revistas, pois, além de estarem violando a Constituição Federal e a legislação trabalhista, também estarão violando a proteção dos dados sensíveis dos empregados, quando não houver nenhuma hipótese que legitime seu processamento, para seu uso ou utilização.

Devendo assim, as empresas reavaliarem suas práticas de segurança, políticas internas, códigos de ética, dentre outros, ponderando inclusive a real necessidade de tratamento de certos dados sensíveis.

Não se pode esquecer que deve ser avaliada a real necessidade de fazer o tratamento de dados pessoais sensíveis pela empresa. E que não sendo estritamente necessário à sua utilização, esta assumirá os riscos dispensáveis, que podem atingir a esfera cível, trabalhista e até mesmo criminal.

3. Autoridade nacional de proteção de dados e reglamentação na area trabalhista

A ANPD possui autonomia técnica e decisória, e lhe foi dada atribuições, conforme dispõe o art. 55-J, da Lei nº 13.709/19, valendo destacar algumas dessas atribuições:

- Zelar pela proteção de dados pessoais, dos segredos comerciais e industriais;
- Fiscalizar e aplicar sanções no caso de descumprimento da LGPD;
- Apreciar petições de indivíduos contra controladores de dados;
- Dispor sobre as formas de publicidade das operações de tratamento de dados pessoais;
- Editar regulamentos e procedimentos sobre a proteção de dados pessoais e privacidade.

Em outras palavras, a ANPD é o órgão nacional de fiscalização e aplicação da LGPD, de forma que ela examinará como controladores e subcontratantes executam o tratamento de dados pessoais, aplicando as punições necessárias, ajudará os titulares de dados pessoais a obterem informações claras e precisas, além de receber as reclamações dos indivíduos.

A ANPD é responsável por executar as regras e estabelecer diretrizes para prática do tratamento de dados pessoais no Brasil. Este órgão é responsável por fazer com que a LGPD fique mais clara e acessível para os titulares de dados quanto para os agentes de tratamento, garantindo segurança jurídica às transações que envolvem informações pessoais.

Existem inúmeros pontos sobre a atuação desse órgão em abertos, pontos estes que devem ser estudados e refletidos. Sendo, talvez, o principal, em saber se os direitos elencados pela LGPD em relação aos Empregados-Titulares são de natureza do direito trabalhista ou não. Pode considerar tal resposta afirmativa se for considerado que os dados do titular somente estão sendo objeto de aplicação da lei, devido a existência

do contrato de trabalho, sendo, portanto, um direito que decorre do contrato de trabalho.

Talvez essa resposta pode ser diferente do que falamos, pois, se aplicarmos por analogia a razão de decidir do STF no RE 586.453, recurso este que se pautou na questão da competência da Justiça do Trabalho em julgar pedidos de complementação de aposentadoria, decidindo que na relação jurídica tais entidades se baseavam em seus regulamentos e não no contrato de trabalho. Podendo concluir que possivelmente a relação do Titular-Controlador, que se dá a partir da LGPD, mesmo que no âmbito do contrato de trabalho, não seria idêntico, em sua natureza, na relação Empregado-Empregador, sob o entendimento de que os direitos abordados pela LGPD ultrapassariam o contrato de trabalho.

Uma resposta correta para tal questionamento dependerá, por exemplo, de saber quanto à competência da Justiça do Trabalho para manifestar em ações versando sobre multas que podem ser aplicadas a Controladores quando se tratar de violações a LGPD, no tratamento de dados dos titulares que sejam empregados. Ainda podemos ponderar que essa resposta vai depender de saber se a haverá a aplicação de normas internas de compliance do Empregador-Controlador, a aplicação do princípio da inalterabilidade *in pejus* das condições de trabalho.

Certamente há outros pontos que devem ser tidos como objetos de reflexão sobre esse assunto, podemos citar a possibilidade ou não de a empresa solicitar dados do candidato a emprego, na fase inicial de seleção para o emprego, ou do empregado, ao longo do contrato de trabalho, considerando os termos do art. 7º, V, da LGPD, que expressamente condiciona o tratamento desses dados a pedido do titular dos dados e não a pedido do Controlador.

Temos também a possível aplicação ou não do conceito de "legítimo interesse" do Controlador pelo empregador, para efeito da dispensa de consentimento, nos termos do art. 7º, IX, e 10 da LGPD.

Outro ponto, seria a aplicação ou não do disposto no art. 8º §2º da LGPD, que declara ser do controlador o ônus da prova da validade de

consentimento ao processo do trabalho; e mais especificamente a aplicação ou não dessa regra no caso dos empregados chamados autossuficientes, conforme art. 444, parágrafo único da CLT.

Pode se falar de uma possível normatização de maneira coletiva da proteção de dados por meio de Acordo ou Convenção Coletiva, ou, individualmente, por termo aditivo no caso dos empregados autossuficientes, considerando os limites dos arts. 611 A e 611 B da CLT.

As obrigações previstas em Acordo ou Convenção Coletiva autorizariam o tratamento de dados sem consentimento, nos termos do art. 7º V, da LGPD, já que referida norma faz menção a "execução do contrato", e sendo certo que Acordos e Convenções coletivas, que muitas vezes demandam o tratamento de dados pessoais, não são, a rigor, "contratos".

Talvez o estudo e normatização da viabilidade de conservação de dados pessoais dos empregados, que não impliquem cumprimento de obrigações legais, após o seu desligamento, e especialmente se o empregado solicitar a eliminação desse dado, conforme art. 15, III, e art. 16 da LGPD.

A responsabilidade do Controlador e do Operador prevista nos arts. 42, e 44, parágrafo único da LGPD, especialmente a responsabilidade solidária entre ambos, se aplicaria à pessoa do Operador no caso de ele ser empregado do Controlador?

Então podemos dizer que a ANPD pode regulamentar o tratamento de dados nas relações de trabalho, mas somente quando envolver o manuseio de dados pessoais, pois qualquer violação à LGPD nessa esfera poderá ser objeto de ação judicial ou administrativa, bem como sujeitar-se à fiscalização aplicada pela da Autoridade Nacional de Proteção de Dados e suas sanções, que estão previstas no art. 52 da Lei Geral de Proteção de Dados, onde as multas podem chegar a 50 milhões de reais.

4. Referências

BIONI, Bruno Ricardo. **De 2010 a 2018: a discussão brasileira sobre uma Lei Geral de Proteção de Dados pessoais**. Disponível em: https://www.jota.info/opiniao-eanalise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-adiscussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018. Acesso em: 20 nov. 2019.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoas** – A Função e os Limites do Consentimento. São Paulo: Editora Forense, 2018.

BRASIL, DECRETO-LEI Nº 5.452, DE 1º DE MAIO DE 1943. **Aprova a Consolidação das Leis do Trabalho**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452compilado.htm. Acesso em: 21 Nov. 2019.

DONEDA, Danilo. **A proteção de dados pessoais como direito fundamental**. Revista Espaço Jurídico 12/103. Joaçaba: Unoese, 2011.

OLIVIERI, Nicolau. **LGPD**: impactos nas rotinas trabalhistas e no contrato de trabalho. Disponível em: https:// www.granadeiro.adv.br/clipping/2019/05/14/46729. Acesso em: 23 nov. 2019.

TEFFÉ, Chiara Spadaccini de. MAGRANI. Eduardo. **Artigo "Proposta para a criação da Autoridade Brasileira de Proteção aos Dados Pessoais**. Disponível em: <https://itsrio.org/wp-content/uploads/2018/12/autoridade-protecao-de-dados.pdf>. Acesso em: 27 Nov. 2019.

Sobre os autores

Alexandre Rodrigues Atheniense
Alexandre Atheniense é um dos precursores do Direito Digital no Brasil, com experiência de 32 anos nesta área. Especialização em Internet Law na Harvard Law School. Sócio Fundador de Alexandre Atheniense Advogados e Co-Coordenador do Comitê de Direito Digital do CESA.

Bernardo Menicucci Grossi
Advogado, Doutorando em Direito Privado pela PUC Minas, Mestre em Direito Privado, com distinção *cum laude*, também pela PUC Minas, Especialista em Direito Processual Civil pelo CAD. É Presidente da Comissão de Proteção de Dados da OAB/MG, Membro da Coordenação de Tecnologia e Inovação do Conselho Federal da OAB, Membro do Comitê Gestor do PJE do Tribunal de Justiça do Estado de Minas Gerais, Membro Fundador do Instituto de Direito e Inteligência Artificial - IDEIA e Membro Efetivo do Instituto dos Advogados de Minas Gerais - IAMG. Cursou extensão em *Internet Law* pela *Harvard Law School*, em *Compliance and Data* Protection pela *University of Pennsylvania,* em *New Models of Business in Society* pela *University of Virginia*, e em Proteção de Dados pela FGV, pela Data Privacy Brasil e em Novas Tecnologias pela UFMG. Professor da Pós-Graduação do IEC / PUC Minas e do CEDIN. Contato: bernardo@grossi.law | @grossilaw

Bruna Cardoso Nunes
Acadêmica de Direito da Faculdade Dom Helder Câmara, Membro da Comissão de Proteção de Dados da OAB/MG.

Camila de Oliveira
Acadêmica de Direito da Faculdade Dom Helder Câmara, Membro da Comissão de Proteção de Dados da OAB/MG.

Daniel Evangelista Vasconcelos de Almeida
Doutorando em Direito pela UFMG, Mestre em Direito Privado pela PUC Minas, Professor de Direito Civil da FAMIG. Professor da Pós-Graduação *lato sensu* da PUC Minas e CEDIN. Advogado especialista em Direito Digital. Membro da Comissão de Proteção de Dados da OAB/MG. Contato: danielevangelista@gmail.com

Douglas Dias Vieira de Figueiredo
Advogado e Professor Universitário (Graduação e Pós-Graduação). Mestre em Direito pela Escola Superior Dom Helder Câmara, Especialista em Direito Tributário pelo CEAJUFE, Especialista em Direito e Processo Civil pela FADIPA, *Certificate in Business Analytics, Financial Accounting and Economics for Managers* pela *Harvard Business School*. Gerente Jurídico de Instituição Financeira.

Duarte Moura
Mestrando em Instituições Sociais, Direito e Democracia pela Universidade FUMEC (2019-2021). Advogado com atuação nas áreas de Direito Civil, Digital, Previdenciário, Família e Sucessões. Consultor Jurídico para implementação e adequação das normas, conforme determina a Lei Geral de Proteção de Dados. Membro da Comissão de Proteção de Dados da OAB/MG. Integra o Núcleo de Pesquisa do Programa de Pós-Graduação *Stricto Sensu* em Direito da Universidade FUMEC. Atuou, quando estudante, como assistente jurídico por mais de 3 anos, realizando o acompanhamento e o peticionamento em processos bancários. Experiência de 2 anos em Direito Militar como estagiário na secretaria de 2a instância do Tribunal de Justiça Militar de MG.

Felipe Soares de Magalhães
Bacharel em Direito pela Faculdade de Direito Milton Campos. Sócio da Magalhães, Perfeito e Soares Sociedade de Advogados. Co-Founder da *Edutech* de Proteção de Dados *SECRETUM*. Advogado inscrito na Ordem dos Advogados do Brasil, Seção Minas Gerais. Pós-Graduado em Direito de Empresa pela Universidade Gama Filho/RJ, Pós-Graduado em Processo Civil pela Universidade FUMEC, Pós-Graduando em Direito da Proteção e Uso de Dados pela PUC Minas. Curso de Direito Imobiliário pela Fundação Getúlio Vargas, Curso de Incorporação de Edifício do Prof. Jamil Rahme, Técnico em Transação Imobiliária pelo Sindimóveis do Rio de Janeiro, Curso de Aprofundamento em Proteção de Dados pelo DTI BR. Membro da Comissão de Ética e Disciplina da OAB/MG (2012/2015), Membro da Comissão Especial de Proteção de Dados da OAB/MG (2019/2021). Atuante nas áreas de Direito Digital (com ênfase em Proteção de Dados/LGPD), Direito Civil (com ênfase em Direito Imobiliário e Direito do Consumidor) e Direito Empresarial.

Fernanda Araújo Couto e Melo Nogueira
Sócia do escritório João Bosco Leopoldino Advocacia e Consultoria, Graduada em Direito pela Universidade FUMEC em 2008, Mestre em Ciências Jurídico-Empresariais pela Faculdade de Direito da Universidade de Lisboa, em 2013, Especialista em Contratos pela Fundação Getúlio Vargas, em 2015, MBA em Gestão Estratégica de Negócios pela Universidade FUMEC, em 2017. Membro da Comissão de Proteção de Dados da OAB/MG.

Guilherme Henrique Gualtieri de Oliveira
Advogado, Especialista em Direito Tributário pela PUC-MG e Certificado em *Privacy & Data Protection e Information Security* pela *Exin,* Holanda. Membro da Comissão de Proteção de Dados da OAB/MG.

Gustavo Batista Guimarães
Bacharel em Direito pela Universidade FUMEC. Advogado atuante em Minas Gerais em Direito Digital com foco em Proteção de Dados, Direito Previdenciário e é sócio da 4 Server Soluções em TI. Possui cursos em Proteção de Dados e Certificações como *Privacy and Data Protection Practitioner (Exin/AdaptNow), Information Security Management Foundation based ISO/IEC 27001 (Exin/AdaptNow), Privacy and Data Protection Foundation (Exin/AdaptNow), Privacy e Data Protection Essentials (Exin/AdaptNow). Trabalhou no setor de tecnologia da informação da Universidade FUMEC por 09 anos.*

Igor da Silveira Franco
Bacharel em Ciência da Computação na Universidade Federal de Minas Gerais (UFMG), Pós-Graduado em TI Bancária pela Universidade de São Paulo (USP), Consultor Especialista em Integração, Qualidade de Dados, Governança e Adequação da TI à LGPD, além de *Business Intelligence, Analytics* e Arquitetura de sistemas. Membro da *Mensa International*.

João Lucas Vieira Saldanha
Advogado, especialista em Proteção de Dados, Direito Digital e Compliance. Sócio Fundador do escritório Saldanha & Gualtieri Advogados Associados, Sócio e Data Protection Officer da empresa "Tripla", Membro da Comissão de Proteção de Dados da OAB/MG, do ISACA - Information Systems Audit and Control Association, ISFS, PDPF, PDPP e DPO pela Exin, Holanda. Consultor de privacidade e proteção de dados, pesquisador e autor de diversos artigos sobre o tema.

Lucas Sávio Oliveira
Bacharel e Mestre em Direito pela Universidade Federal de Minas Gerais - UFMG e Mestre em Direito Comercial Internacional e Resolução de Litígios pela *Swiss International Law School - SiLS*. Sócio de Oliveira Drumond Advogados. Membro da Comissão de Proteção da Dados da OAB/MG.

Marcos Souza
Advogado do Sistema FIEMG, Membro do Programa de Proteção de Dados FIEMG, Membro da ANPPD® - Associação Nacional dos Profissionais de Privacidade de Dados, Membro da Comissão de Proteção de Dados da OAB/MG e Especialista em Direito Público

pela PUC Minas. Atuou como auditor e gestor das áreas de corregedoria e *compliance* no serviço público estadual e como gestor na área de ciência da informação no setor privado.

Maurício Leopoldino da Fonseca
Sócio Fundador do João Bosco Leopoldino Advocacia e Consultoria, Graduado em Direito pela Universidade Federal de Minas Gerais, em 1990, Mestre pela Faculdade de Direito da Universidade Federal de Minas Gerais, em 2001, Especialista em Direito Administrativo pela UFMG, em 1992. Procurador do Estado de Minas Gerais, desde 1993.

Paulo Roberto Godoy Perilli
Professor de Direito Empresarial da Pontifícia Universidade Católica de Minas Gerais, Vice-Presidente da Comissão de Proteção de Dados da OAB/MG. Eleito pelo *ranking* independente da *Acritas* como um dos 55 *Star Lawyers* da América do Sul, pelos anos consecutivos de 2018 e 2019. Mestre em Direito Empresarial pela Faculdade de Direito Milton Campos, Pós-Graduado em Direito Processual Civil pela Pontifícia Universidade Católica de Minas Gerais e Graduado em Direito pela Pontifícia Universidade Católica de Minas Gerais. Palestrante pelo Centro Industrial e Empresarial de Minas Gerais - CIEMG. Autor e co-autor de livro jurídico e de diversos artigos científicos publicados em revistas e livros jurídicos. Membro do grupo de pesquisa Constituição e Processo.

Pedro Henrique Rocha Silva Fialho
Advogado, Pós-Graduado em Direito Empresarial pela PUC Minas, Professor substituto do Pré-Concursos, Membro da Comissão de Proteção de Dados da OAB/MG e da Comissão de Direito Empresarial da OAB/MG. Membro do grupo de estudos de Direito Empresarial da UFMG. Contato: pedro.fialho@mourasiqueira.com

Ricardo Gomes Figueiroa
Graduado em Direito pela Pontifícia Universidade Católica de Minas Gerais (2004) e Pós-Graduado em Direito Público (2006). Mestrando em Propriedade Intelectual e Inovação Tecnológica pela UFMG. Procurador do Município de Ribeirão das Neves. Advogado atuante nas áreas de Direito Empresarial, Imobiliário, Administrativo e Direito Digital.Direito Empresarial, Imobiliário, Administrativo e Direito Digital.

Sidney Cássio Alves Rocha
Advogado graduado pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas), Mestrando em Direito Penal pela PUC Minas, Especialista em Ciências Criminais pela PUC Minas. Engenheiro Eletricista pela PUC Minas e MBA em Gestão Empresarial pela FGV. Contato: contato@sidneyrocha.com.br

Tatiana Alves de Castro

Advogada com mais de 15 anos de experiência em jurídico corporativo de instituição financeira. Formada pela PUC Minas, pós-graduada em Direito Público (Newton Paiva) e com MBA em Direito Civil e Processual Civil pela Fundação Getúlio Vargas. É certificada em Privacy and Data Protection Officer pela EXIN e em Compliance pela KPMG.

Thiago Thomaz Siuves Pessoa

Bacharel em Direito pela Faculdade de Direito Milton Campos. Sócio Fundador do escritório Pessoa Advocacia, *Chief Legal Officer* (*CLO*) da *Fintech* de Negócios e Educação Financeira Vale Ouro, Co-Founder da *Edutech* de Proteção e Privacidade de Dados *SECRETUM*. Advogado inscrito na Ordem dos Advogados do Brasil, Seção Minas Gerais, Pós-Graduado em Direito Público pela ANAMAGES / Unicentro Newton Paiva, Pós-Graduado em Regime Jurídico dos Recursos Minerais pela Faculdade de Direito Milton Campos. Curso de Atualização em Direito, Tecnologia e Inovação pelo DTI BR. Curso *Legal Creatives Design* pela *Legal Creatives* em parceria com a Edevo. Membro da Comissão de Proteção de Dados da OAB/MG (2019/2021). Advogado corporativo. Consultoria estratégica sobre negócios jurídicos de empresas e serviços de consultoria jurídica.

Vitor Eduardo Lacerda de Araújo

Mestrando em Direito Digital e Bacharel em Direito pela UFMG. Especialista em Direito Processual Penal pela Faculdade Internacional Signorelli. Estagiário Docente na disciplina Direito Penal II na UFMG, Supervisor Jurídico de Instituição Financeira. Membro da Comissão de Proteção de Dados da OAB/MG.

Wallace Almeida de Freitas

Advogado, Especialista em Direito Imobiliário pela Escola Paulista de Direito - EPD. Presidente da Comissão de Direito e Tecnologia da Informação da OAB, Subseção Contagem/MG, Membro da Comissão de Proteção de Dados da OAB/MG.

Zilda A. Gonçalves de Sousa

Bacharel em Direito pela Universidade de Itaúna. Advogada de Direito Digital. Autora de artigos jurídicos. Membro da Comissão de Proteção de Dados da OAB/MG.

A Editora Fi é especializada na editoração, publicação e divulgação de pesquisa acadêmica/científica das humanidades, sob acesso aberto, produzida em parceria das mais diversas instituições de ensino superior no Brasil. Conheça nosso catálogo e siga as páginas oficiais nas principais redes sociais para acompanhar novos lançamentos e eventos.

www.editorafi.org
contato@editorafi.org