NOVA LEI BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) E O IMPACTO NAS INSTITUIÇOES PÚBLICAS E PRIVADAS

Patricia Peck Garrido Pinheiro

Resumo

O presente estudo visa analisar os principais desdobramentos da sanção da Lei 13.709/18, a Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD). Para isso, pontuamos as transformações contextuais que resultaram no surgimento de um regulamento específico para a proteção de dados no país, como o amplo desenvolvimento tecnológico, o aumento da importância da informação dentro do contexto contemporâneo e a insegurança dos dados no mundo digital. Os principais impactos no ambiente jurídico e nas relações negociais também são analisados, sempre com o viés comparativo da lei nacional com o regulamento europeu, o General Data Protection Regulation (GDPR).

Palavras-chave

Direito digital – Proteção de dados – Privacidade – Dados pessoais – Sociedade digital – Lei de Proteção de Dados Pessoais

Sumário

Introdução

A Lei 13.709/18 (LGL\2018\7222), assinada pelo presidente Michel Temer no dia 14 de agosto de 2018, é o marco legal da proteção de Dados Pessoais do Brasil. Conhecida também pela sigla LGPD, a Lei Geral de Proteção de Dados, é originária do PLC 53/18, que por sua vez foi resultante da união de outros dois projetos, e estabeleceu um prazo de 18 meses de adaptação às novas

Patricia Peck Garrido Pinheiro

Doutora em Direito Internacional e Propriedade Intelectual pela USP, PhD

regras contados da data de sua publicação.

Criada como meio de fortalecer a proteção da privacidade dos usuários e de seus dados pessoais, a lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. Um dos grandes destaques trazidos com a novidade é que, a partir das novas regras, os cidadãos poderão ter acesso a informações de como seus dados são coletados, processados e armazenados. Ou seja, o objetivo é proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O surgimento dessa lei específica sobre proteção dos dados pessoais decorre das novas necessidades da sociedade digital que exige mais transparência das relações, considerando a sustentação do modelo atual de negócios onde a informação passou a ser a principal moeda de troca utilizada pelos usuários para ter acesso a determinados bens, serviços ou conveniências.

De acordo com a definição da LGPD, tratamento é compreendido como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

Assim como o *General Data Protection Regulation* (GDPR), o regulamento de proteção aos dados da União Europeia, a LGPD exige que toda e qualquer transação envolvendo dados que estejam em território nacional (do Brasil), independentemente de sua cidadania ou origem, sejam abarcadas pelas novas regras. Isso significa que todas as empresas que fazem operação de tratamento de dados – independentemente do meio de tratamento, do país de sua sede ou do país de origem dos dados, desde que estejam localizados no país – passem a ficar obrigadas à respeitar a LGPD.

Essa nova realidade pode modificar bastante o cenário mercadológico não só em âmbito nacional, mas também global, tendo em vista que os modelos de negócios desenvolvidos com base no uso de dados precisarão instituir novos procedimentos de tratamento que obedeçam às novas regras.

Evolução informacional: o aumento da importância da informação

Com o desenvolvimento social, a informação foi ganhando cada vez mais importância na sociedade, de modo que, a partir da Revolução Informacional ao fim do século XX, essa importância tornou-se bastante significativa culminando em um modelo econômico totalmente centrado nas bases de dados. Conforme já apontava Manuel Castells, em sua obra "Sociedade em Rede", faz parte da realidade da sociedade em rede a constante inovação tecnológica, sendo que as adaptações necessárias a tais inovações passam a seguir o mesmo ritmo acelerado das novidades técnicas[1].

É possível observar que a informação já era notada como um dos ativos de grande relevância da sociedade até antes mesmo do surgimento da Era Digital. Bruno Ricardo Bioni pontua esse fato em sua obra *Proteção de dados pessoais: a função e os limites do consentimento*:

Antes mesmo da criação da Internet, já

se havia constatado o papel de centralidade da informação para otimizar o desenvolvimento econômico. Com o *taylorismo*, passou-se a estudar o próprio processo de produção, investindo-se, por exemplo, em treinamento dos operários para se alcançar melhores taxas de produtividade. Portanto, desde a sociedade industrial, já se reconhecia a informação como um fator determinante para a geração de riquezas[2].

Apesar dessa notável constatação, o que não se imaginava é que a sociedade iria modificar tanto as suas relações em razão do desenvolvimento técnico-científico que as suas redes de relação se desfragmentariam em diversos grupos com possibilidade de comunicação e interação praticamente independentes de tempo e espaço.

Conforme afirma Hugo Moreira Lima Sauaia, em sua obra *A proteção dos dados pessoais no brasil*,

> [...] há um rompimento das redes de segurança, tecidas e sustentadas agora individualmente, o apoio oferecido anteriormente pela família, pelos amigos próximos [...] onde se poderia buscar auxílio para remediar as lesões provenientes do trabalho e das limitações humanas, parece não mais subsistir[3].

Esse rompimento é sentido também no que concerne à segurança e à estabilidade das relações, trazendo reflexos diretos ao funcionamento da sociedade. O que se observou foi que, com o advento da Internet e a disseminação de seu uso, a relações sociais se tornaram mais fluídas e instáveis, caracterizadas como relações líquidas, impalpáveis e imprevisíveis, na visão de Bauman[4].

Essa instabilidade foi transmitida aos meios digitais que, por sua própria natureza virtualizada, tornaram as noções de ação e reação inerentes ao comportamento humano menos identificáveis. Por outro lado, os riscos tornaram-se menos visíveis, dificultando assim a proteção das pessoas no meio digitalizado.

A risco crescente à segurança da informação e a necessidade de ter um maior padrão de controle para proteção das informações pessoais depositadas em confiança nas instituições, passaram a exigir uma regulamentação que pudesse trazer algumas garantias mínimas para os titulares bem como alguns novos direitos que permitissem o seu empoderamento no tocante a um maior poder de decisão sobre o uso de suas informações pessoais.

Daí o surgimento do movimento contemporâneo em prol da proteção dos dados pessoais em todo o mundo e a a construção de um novo framework legal através de legislações específicas, com grande necessidade de harmonização para se adaptarem às normas já existentes bem como adequar os modelos de negócios do contexto digital da economia para que a proteção de dados pessoais seja possível de forma efetiva e eficaz e com respeito aos direitos fundamentais prevalentes no documento constitucional:

> [..] a compreensão das mais diversas legislações acerca da proteção dos dados pessoais dentro da nova realidade digital precisou evoluir e foi se modificando ao longo dos últimos 30 anos, resultando em reflexos diretos na seara jurídica – seja na resolução de conflitos ou na criação de mecanismo

> de suporte para as questões digitais, como: como realizar um contrato na esfera digital? Como proteger a privacidade dos cidadãos dentro do mundo virtual? Qual a responsabilidade das empresas frente ao manuseio e tratamento das informações fornecidas pelos clientes?[5]

A proteção de dados pessoais e a sua relação com os direitos fundamentais

O surgimento da LGDP no Brasil tem íntima relação com a necessidade de atualização do arcabouço regulatório nacional frente aos impactos socioeconômicos trazidos com a evolução tecnológica. De forma mais ampla, pode-se afirmar que o nascimento de regulações específicas para a proteção dos dados pessoais em países de todo o mundo é resultado da associação: evolução x expansão dos direitos humanos com a atualização e consequente adaptação de documentos internacionais de proteção aos direitos humanos[6].

Com isso em vista, afirma-se que os instrumentos de regulação dos dados pessoais surgem com o objetivo de proteger direitos fundamentais como: privacidade, intimidade, honra, direito de imagem e a dignidade humana. Acrescenta-se ainda que tais mecanismos têm ligação direta com a internacionalização dos direitos humanos vivenciada pelo mundo contemporâneo, conforme pontua Leandro Alvarenga Miranda, em sua obra *Proteção de dados pessoais e o paradigma da privacidade*: "A preocupação com a privacidade é histórica e remonta aos primórdios das culturas hebraica, grega e chinesa. [...] a evolução das normas e a criação da codificação vieram acompanhadas da consolidação dos direitos individuais do homem"[7].

Tal relação é tão clara que o GDPR aponta no art. (1) que toma por base o artigo 8º, n. 1 da Carta dos Direitos Fundamentais da União Europeia e o artigo 16º, n. 1 do Tratado sobre o funcionamento da União Europeia para a criação do novo regulamento de proteção de dados europeu.

E, embora o instrumento regulatório brasileiro não faça menção direta à documentos específicos que originam o seu teor, é notável a influência de alguns tratados internacionais de que o Brasil é signatário e que – de certa forma – trazem a questão dos dados pessoais em seu texto.

Entre esses documentos é possível citar: a Convenção de Berna de 1886 que já trazia a questão da base de dados em seu texto, ainda que de maneira indefinida e incipiente; o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual relacionados ao Comércio (TRIPS – aprovado no Brasil em 1994) pontua no artigo 10 (2) que as compilações de dados devem receber o mesmo tratamento da criação intelectual, embora não se aprofunde em relação à proteção pessoal dos dados compilados.

A proteção aos direitos fundamentais também é visualizada através o art. 2º da LGPD, no qual são mencionados princípios encontrados no texto constitucional brasileiro como cerne do desenvolvimento de todo e qualquer tratamento de dados pessoais. Dentre os artigos constitucionais que podem ser relacionados com os princípios apontados no art. 2º da LGPD destacam-se os art. 3º, I, II; art. 4º, II; art. 5º, X, XII; art. 7º, XXVII; art. 219[8].

Da mesma forma, o GDPR pontua que o regulamento toma por base os direitos

fundamentais e que visa proteger e garantir a privacidade, liberdade, segurança, justiça das pessoas, assim como promover o progresso econômico e social, além de garantir a segurança jurídica dos países, através do preâmbulo (1), (2), (13)[9] e art. 1º (2)[10].

Breve histórico da proteção de dados pessoais no Brasil

O Brasil já previa certa proteção aos dados pessoais em suas normas internas através dos seguintes: i) Código de Defesa do Consumidor – no art. 43[11]; ii) Decreto 7.962 de 2013 (LGL\2013\2685) (Comércio Eletrônico) – no art. 4º, VII[12]; iii) Marco Civil da Internet – no art. 7º, I, III, VII, VIII, IX, X, XI e art. 11[13] § 1º, § 2º[14].

Todavia, com o rápido desenvolvimento e expansão da tecnologia em todo o mundo, surgiu a necessidade de criação de leis específicas para a proteção desses dados. Isso porque na nova realidade da Era Digital, os dados são uma nova forma de riqueza, de modo que a atuação das empresas dentro do contexto digital passou a necessitar da criação de mecanismos de regulação e proteção dos dados pessoais dos usuários.

Em 2018, o Brasil passou a fazer parte do grupo dos países dotados de um Lei Geral de Proteção de Dados (LGPD) através da sanção da Lei 13.709, de 14 de agosto de 2018 (LGL\2018\7222). Nota-se que o principal objetivo da lei foi a atualização dos mecanismos regulatórios do país frente às necessidades surgidas com o desenvolvimento e expansão da tecnologia e aumento cada vez mais expressivo da coleta, processamento, transmissão e armazenamento de dados no ambiente virtual.

Também é necessário pontuar que a "corrida" aprovação da lei foi visivelmente influenciada pelo início da vigência do GDPR em 25 de maio de 2018, tendo em vista que a discussão em torno da regulamentação de dados pessoais teve início em 2010 no Brasil, por meio da abertura de uma consulta pública por parte do Ministério da Justiça. O resultado desta consulta foi a criação do Projeto de Lei 4.060, de 2012, que mais à frente recebeu em anexo o Projeto de Lei 5.276 de 2016.

Depois de muita conversa e questionamentos acerca das ideias propostas chegou-se ao Projeto de Lei da Câmara 53/18 que gerou a Lei 13.709. É notável que o texto da LGPD é amplamente inspirado pelo GDPR, embora o regulamento nacional seja mais enxuto e traga em seu conteúdo regras mais abertas do que o proposto pela União Europeia.

Ao sancionar a Lei 13. 709/2018 o Presidente Temer vetou alguns artigos que se mostravam incongruentes com a Constituição Nacional, como a criação de um órgão regulador, procedimento que só pode ser iniciado pelo executivo e estava com um erro em sua iniciativa ao ser proposto pela Câmara.

Com a atualização do corpo legislativo nacional em relação à proteção de dados pessoais, a LGPD passa a trazer completa proteção aos dados pessoais em qualquer mídia ou suporte, com a exigência do consentimento prévio e expresso para as hipóteses de tratamento (a não ser que recaia em alguma exceção) e não mais apenas aos capturados em plataforma digital (como podia haver o entendimento neste sentido no tocante a interpretação do Marco Civil da Internet), conforme deixa claro o art. 1º[15].

Determinações da nova lei de proteção

de dados

Na medida em que a economia digital gira em torno dos dados pessoais, é preciso delimitar alguns limites e melhores práticas, para proteção do consumidor e evitar inclusive concorrência desleal. As novas regras vêm com um escopo de permitir que a livre iniciativa possa inovar desde que siga uma cartilha de valores que estejam condizentes com o respeito aos direitos humanos fundamentais, mas acima de tudo, que aja com a máxima transparência possível no tocante ao uso (tratamento) dos dados pessoais.

Toda a redação da regulamentação de proteção de dados pessoais tem como principal linha condutora a transparência. Ou seja, mesmo nas hipóteses em que não é exigido o consentimento prévio e expresso há que ser transparente sempre.

Assim, a regulamentação traz novos direitos para os titulares e, por sua vez, obrigações às empresas, como: permitir que o usuário tenha a possibilidade de acesso ao dado que está sendo tratado, de retificação, portabilidade dos dados para outra empresa, apagamento até oposição ao tratamento realizado.

Além disso, exige aplicação de medidas técnicas e administrativas que garantam a proteção dos dados pessoais, mesmo sem detalhais quais sejam, procedimentos de governança, atualização de políticas e normas e camada de gestão, já que é preciso nomear uma pessoa que será responsável pela relação com as autoridades.

As organizações devem estar prontas para cumprir essas adequações, com um canal apropriado para receber e dar andamento às solicitações de modo que alcance todos os seus sistemas e empresas para as quais os dados foram compartilhados. Ou seja, precisam avaliar seu ambiente e verificar se está preparada para estar aderente à legislação.

Claramente que a LGPD também traz exceções: a lei não se aplica quando o tratamento dos dados é realizado por uma pessoa física, para fins exclusivamente particulares e não econômicos, para fins exclusivamente jornalísticos e artísticos, e para tratamentos realizados para fins de segurança pública e defesa nacional.

Um outro aspecto relevante a citar é o de que o dano anonimizado, conforme previsto pelo artigo 5º, não é considerado um dado pessoal, logo, deixa de estar passível de proteção conforme a lei.

Caso haja infrações, as sanções administrativas envolvem advertência, com indicação de prazo para adoção de medidas corretivas; multa simples, de até 2% do faturamento da empresa (limitada, no total, a R$ 50 milhões por infração); publicização da infração após devidamente apurada e confirmada a sua ocorrência; bloqueio dos dados pessoais a que se refere a infração até a regularização da atividade de tratamento pelo controlador; eliminação dos dados pessoais a que se refere a infração; suspensão parcial ou total do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, suspensão, proibição parcial ou total do exercício da atividade de tratamento dos dados pessoais.

Relevância da lei em um contexto globalizado

Como já foi destacado, um dos fatores que pressionou essa corrida legislativa em

vários países foi a entrada em vigor do General Data Protection Regulation (GDPR) na União Europeia, em maio deste ano. Isso porque o Estado que não possui lei de mesmo nível pode passar a sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com os países da região. Considerando o contexto econômico atual, este é um luxo que a maioria das nações, especialmente os da América Latina, não podem se dar.

Os efeitos da GDPR são principalmente econômicos, sociais e políticos. É apenas uma das muitas regulamentações que vão surgir nesta linha, onde se busca trazer mecanismos de controle para equilibrar as relações dentro de um cenário de negócios digitais sem fronteiras.

Portanto, não apenas virão regras sobre proteção de dados pessoais, mas também sobre demais usos de tecnologia com alto impacto na sociedade, tais como a Inteligência Artificial, a robotização, o Blockchain, entre outros. Há uma grande preocupação em um modelo de "dados abertos" (*Open Society*) com cibersegurança. Pois não dá mais para continuar com puxadinhos digitais, como quando vimos casos de vazamentos de dados que foram mantidos anos em segredo.

A importância da lei, resumidamente, é o estabelecimento de segurança jurídica para os envolvidos no processo de tratamento de dados, deixando mais claro quais os controles que devem ser aplicados e quais as obrigações e responsabilidades das partes, porque apesar de termos alguma legislação setorial (como as resoluções do Banco Central aplicáveis às Instituições Financeiras, por exemplo), era necessária uma lei que pudesse alcançar a todos, em todos os setores econômicos.

Considerando que o atual estágio tecnológico impõe a análise massiva de dados, a economia digital depende do tratamento de dados pessoais, em especial, serviços e produtos altamente especializados. Afinal, a grande questão não é proibir ou demonizar o uso de dados pessoais pelas empresas. O desafio é fazer isso de forma equilibrada, protegendo a privacidade dos cidadãos, mas sem inviabilizar a inovação e os negócios.

O cidadão deve ter o direito de ser proprietário da sua própria informação e poder negociar livremente a mesma. O governo e as empresas podem tratar dados, mas o indivíduo tem o direito de saber quais dados estão sendo coletados e com quem estão sendo compartilhados e para quais finalidades. Deve haver uma base de princípios e regras a serem seguidas, e respeitar a capacidade jurídica de se contratar e a liberdade para tanto. Por isso, novamente, o princípio norteador é o da transparência muito mais que qualquer outro.

Afinal, as relações negociais dependem diretamente dos dados se desenvolverem, para garantir a segurança jurídica das partes, evitar golpes, fraudes, inadimplência e oferecer melhores experiências na oferta de produtos e serviços, otimizando mão de obra e especializando negócios. Informação verdadeira e transparente, utilizada de forma legítima e proporcional, garante crescimento econômico e social.

Planejamento estratégico e aplicabilidade

Passada a primeira etapa de ter uma lei ou regra sobre o tratamento dos dados, agora é hora de educar o mercado. Esse tipo de legislação é evolutiva e leva um tempo de amadurecimento. Apesar do prazo que foi

conferido de adaptação, é sabido que levará mais tempo para promover toda a mudança necessária de modo a se atender as novas exigências.

Além disso, a conformidade à proteção de dados é o tipo de projeto contínuo, que exigirá uma revisitação da pauta periodicamete, visto que os negócios estão também em transformação, assim como a tecnologia, trazendo inovação e novas funcionalidades, logo o que é feito hoje sofrerá alterações em curto espaço de tempo e os procedimentos bem como a documentação sobre proteção de dados pessoais, precisará de atualização em intervalos não superiores a dois anos, especialmente no tocante às políticas de privacidade, termos de uso e contratos.

Logo, ter a lei é apenas o começo de uma longa jornada que teremos que atravessar tanto no âmbito público como privado. Atender aos requisitos da nova lei exige investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de processos e, acima de tudo, mudança de cultura.

Mostrar aos gestores, profissionais das áreas de compliance, jurídico, analytics, ciência de dados, tecnologia da informação, segurança da informação, negócios e marketing a importância de estarmos alinhados com o contexto de Transformação Digital, ao garantir a competitividade econômica com os países que já regulamentaram os ativos mais valiosos da Sociedade da Informação.

Mais que isso, é incorporar uma cultura empresarial que aplique e valorize as melhores práticas de gestão para atingir a compliance de dados. Enaltecer as razões e a necessidade de mecanismos de controle para equilibrar as relações dentro de um cenário de negócios digitais sem fronteiras. A linha mestra é a garantia da liberdade, mas a base é a transparência.

Os bens de conhecimento estão nas grandes bases de dados e para esse tratamento é necessário transparência, reter dados pessoais com a justificativa legal compatível e anomização. Vamos mostrar como construir uma cultura de proteção para manter a valorização dos ativos intangíveis e das ações. O investidor precisa de proteção e de blindagem legal do patrimônio e da reputação. Vivemos uma nova era de mais responsabilidade, onde tecnologia e informação resultam em poder.

Desdobramentos e consequências

A LGPD traz um grande impacto social e econômico, especialmente sobre sistema da pequena empresa e startups. Tanto por que traz exigências que aumentam os custos empresariais e passam a ter que entrar na prioridade dos gestores (*road map)* mas como também exigem alguns processos de governança corporativa (de TI, de Segurança de Informação, de Gestão de Dados) que não eram tão comuns neste ambiente e que podem até dificultar (burocratizar) suas atividades que estão mais acostumadas com leveza e velocidade.

Ademais, o cidadão, que é o titular precisará saber mais sobre o que é proteção de dados pessoais, o que vai exigir investimento em campanhas educativas e orientativas.

O conceito de *privacy by design* é um grande desafio para ser implementado e deve passar a ser ensinado nas Universidades, pois é a melhor forma de garantir a sustentabilidade do modelo trazido pelo novo Marco Legal.

Um fator de complexidade adicional na temática da proteção de dados pessoais é não

ser um Tratado Internacional. Ou seja, acaba exigindo que as instituições e as empresas precisem realizar todo um trabalho de análise comparada das legislações para poderem se adequar dependendo de como é o seu modelo operacional.

Apesar de vivermos uma sociedade globalizada, da internet ser um grande território internacional e de se querer permitir o livre fluxo de dados, em matéria de proteção de dados pessoais acabou-se utilizando os mecanismos das leis nacionais e dos regulamentos regionais, e esta é a maior crítica que se pode ter quanto ao desdobramento que se teve deste assunto. Vamos esperar que para o futuro, os temas de grande impacto como da Inteligência Artificial possam alcançar um tratamento mais internacional e evitar a solução país a país.

Bibliografia

AGÊNCIA CÂMARA NOTÍCIAS. Comissão discute marco regulatório para a proteção de dados pessoais. *Agência Câmara Notícias*, maio 2017. Disponível em: [www2.camara.leg.br/camaranoticias/noticias/ciencia-e-tecnologia/534978-comissao-discute-marco-regulatorio-para-a-protecao-de-dados-pessoais.html]. Acesso em: mar. 2018.

ALCANTARA, Larissa de. *Tecnologia e inovação*: big data e internet das coisas. São Paulo: Bok2, 2017.

ARTICLE 19. *Proteção de dados pessoais no Brasil*: análise dos projetos de lei em tramitação no Congresso Nacional. 2016. Disponível em: [http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf]. Acesso em: mar. 2018.

ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARES. *Brasil, país digital [site*]. Disponível em: [https://brasilpaisdigital.com.br/]. Acesso em: mar. 2018.

BAUMAN, Zygmunt. *O mal-estar da pós-modernidade.* Rio de Janeiro: Zahar, 1997.

BIONI, Bruno Ricardo. *Proteção de dados pessoais:* a função e os limites do consentimento. Rio de Janeiro: Forense, 2018.

CASTELLANO, Ana Carolina H.; FORNARA, Matheus Tormen. Startaups, Cibersegurança e Proteção de Dados. *Jota*, 25 maio 2017. Disponível em: [www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/startups-ciberseguranca-e-protecao-de-dados-25052017]. Acesso em: mar. 2018.

CASTTELLS, Manuel. *A sociedade em rede.* São Paulo: Paz e Terra, 2009.

COSTA, Larissa Carolina Lotufo da; COSTA, Vinicius Lotufo da. *Regulamentação da proteção de dados pessoais no Brasil:* breve histórico, impactos legais e realidade brasileira. In: Anais do I Congresso de Direito Propriedade Intelectual e Desenvolvimento Econômico-Social. Franca: Unesp, 2018.

COTS, Márcio; OLIVEIRA, Ricardo. *Lei Geral de Proteção de Dados Pessoais Comentada.* São Paulo: Ed. RT, 2018.

GREENWALD, Glenn. Why privacy matters? *Ted Talks*, 10.10.2014. Disponível em: [www.youtube.com/watch?v=pcSlowAhvUk]. Acesso em: mar. 2018.

LEMOALLE, Edouard; CARBONI, Guilherme. Lei Europeia de Proteção de Dados e seus efeitos no Brasil. *Jota*, 12.02.2018. Disponível em: [www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais-gdpr-e-seus-efeitos-no-brasil-12022018]. Acesso em: mar. 2018.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (Coord.). *Comentários ao GDPR*: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Ed. RT, 2018.

MIRANDA, Leandro Alvarenga. *A proteção de dados pessoais e o paradigma da privacidade*. São Paulo: All Print Ed., 2018.

PINHEIRO, Patrícia Peck. *Direito digital*. 6. ed. rev. atual e amp. São Paulo: Saraiva, 2016.

PINHEIRO, Patricia Peck. *Proteção de dados pessoais:* comentários à Lei n. 13. 709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

REUTERS. Privacy issues emerge as major business risk for Facebook. *New York Times*, 19.03.2018. Disponível em: [www.reuters.com/article/us-facebook-privacy-costs-analysis/privacy-issues-emerge-as-major-business-risk-for-facebook-idUSKBN1GW01F]. Acesso em: mar. 2018.

ROSATI, Florencia; PETRINELLI, Ludmilla. Tracking privacy trends in Latin America in the age of the GDPR. *Cecile Park Media*, fev. 2017. Disponível em: [www.ebv.com.ar/images/publicaciones/dplfebruary2017estudiobeccarvarela.pdf]. Acesso em: mar. 2018.

SAUAIA, Hugo Moreira Lima. *A proteção de dados pessoais no brasil.* Rio de Janeiro: Lumen Juris, 2018.

SOUZA, Carlos Affonso; LEMOS, Ronaldo; BOTTINO, Celina (Coord.). *Marco civil da internet:* jurisprudência comentada. São Paulo: Ed. RT, 2017.

1 CASTTELLS, Manuel. *A sociedade em rede*. São Paulo: Paz e Terra, 2009.

2 BIONI, Bruno Ricardo. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2018. p. 9.

3 SAUAIA, Hugo Moreira Lima. *A proteção de dados pessoais no Brasil*. Rio de Janeiro: Lumen Juris, 2018. p. 12.

4 BAUMAN, Zygmunt. *O mal-estar da pós-modernidade*. Rio de Janeiro: Zahar, 1997.

5 COSTA, Larissa Carolina Lotufo da; COSTA, Vinicius Lotufo da. Regulamentação da Proteção de Dados Pessoais no Brasil: breve histórico, impactos legais e realidade brasileira. *Anais do I Congresso de Direito Propriedade Intelectual e Desenvolvimento Econômico-Social*. Franca: Unesp, 2018.

6 PINHEIRO, Patricia Peck. *Proteção de dados pessoais*: comentários à Lei n. 13. 709/2018 (LGPD). São Paulo: Saraiva Educação, 2018.

7 MIRANDA, Leandro Alvarenga. *A proteção de dados pessoais e o paradigma da privacidade*. São Paulo: All Print Ed., 2018. p. 19-20.

8 Art. 3º Constituem objetivos fundamentais da República Federativa do Brasil: I – construir uma sociedade livre, justa e solidária; II – garantir o desenvolvimento nacional.Art. 4º A República Federativa do Brasil rege-se nas suas relações internacionais pelos seguintes princípios: [...] II – prevalência dos direitos humanos.
Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...] 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; [...] XII – 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; [...]
Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social: [...] XXVII – proteção em face da automação, na forma da lei.
Art. 219. O mercado interno integra o patrimônio nacional e será incentivado de modo a viabilizar o desenvolvimento cultural e socioeconômico, o bem-estar da população e a autonomia tecnológica do País, nos termos de lei federal. Parágrafo único. O Estado estimulará a formação e o fortalecimento da inovação nas empresas, bem como nos demais entes, públicos ou privados, a constituição e a manutenção de parques e polos tecnológicos e de demais ambientes promotores da inovação, a atuação dos inventores independentes e a criação, absorção, difusão e transferência de tecnologia.

9 (1) A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. [...](2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares.
(13) A fim de assegurar um nível coerente de proteção das pessoas singulares no conjunto da União e evitar que as divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno, é necessário um regulamento que garanta a segurança jurídica e a transparência aos operadores económicos, incluindo as micro, pequenas e médias empresas, que assegure às pessoas singulares de todos os Estados-Membros o mesmo nível de direitos suscetíveis de proteção judicial e imponha obrigações e responsabilidades iguais aos responsáveis pelo tratamento e aos seus subcontratantes, que assegure um controlo coerente do tratamento dos dados pessoais,

sanções equivalentes em todos os Estados-Membros, bem como uma cooperação efetiva entre as autoridades de controlo dos diferentes Estados-Membros. [...]

10 Artigo 1.º Objeto e objetivos [...] 2. O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

11 Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de 5 (cinco) dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores. § 6º Todas as informações de que trata o *caput* deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

12 Art. 4º Para garantir o atendimento facilitado ao consumidor no comércio eletrônico, o fornecedor deverá: [..] VII – utilizar mecanismos de segurança eficazes para pagamento e para tratamento de dados do consumidor.

13 Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; [...] III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...] VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre

as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; [...] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

14 PINHEIRO, Patrícia Peck. *Direito digital*. 6. ed. rev. atual e amp. São Paulo: Saraiva, 2016.

15 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", grifo nosso.

Publicado originalmente na Revista dos Tribunais, São Paulo, v.108, n.1000, p.309-323, fev.2019.